Oracle® Fusion Middleware

Administrator's Guide for Oracle WebCenter

11*g* Release 1 (11.1.1)

E12405-08

August 2010

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

E12405-08

Primary Author: Rosie Harvey

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

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

Contents

Part II Getting Started With Oracle WebCenter Administration

2 Getting WebCenter Spaces Up and Running

3 Maintaining WebCenter Spaces

4 Getting Custom WebCenter Applications Up and Running

5 Maintaining Custom WebCenter Applications

Part III Basic Systems Administration for Oracle WebCenter

6 Starting Enterprise Manager Fusion Middleware Control

7 Deploying WebCenter Applications

8 Starting and Stopping WebCenter Applications

9 Setting Application Properties

Part IV Managing Services, Portlet Producers, and External Applications

10 Managing Oracle WebCenter Services

11 Managing Content Repositories

12 Managing the Announcements and Discussions Services

13 Managing the Events Service

14 Managing the Instant Messaging and Presence Service

15 Managing the Mail Service

16 Managing the People Connections Service

17 Managing the RSS Service

18 Managing the Search Service

20 Managing the Worklist Service

21 Managing Portlet Producers

22 Managing External Applications

Part V Advanced Systems Administration for Oracle WebCenter

23 Managing Security

24 Configuring the Identity Store

25 Configuring the Policy and Credential Store

26 Configuring WebCenter Applications and Components to Use SSO

27 Securing WebCenter Applications and Components with SSL

28 Configuring WS-Security for WebCenter Applications and Components

29 Managing Security for Portlet Producers

30 Monitoring Oracle WebCenter Performance

31 Managing Export, Import, Backup, and Recovery of WebCenter

Part VI Application Administration for Oracle WebCenter Spaces

32 Accessing WebCenter Spaces Administration Pages

33 Customizing WebCenter Spaces

34 Managing Users and Roles for WebCenter Spaces

35 Managing Pages in WebCenter Spaces

36 Making Applications Available in WebCenter Spaces

37 Managing Group Spaces in WebCenter Spaces

38 Exporting and Importing Group Spaces

Part VII Appendix

A WebCenter Configuration

Glossary

Index

List of Examples

List of Figures

List of Tables

Preface

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

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

Audience

This document is intended for:

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

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

Documentation Accessibility

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/support/contact.html` or visit `http://www.oracle.com/accessibility/support.html` if you are hearing impaired.

Related Documents

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

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

Conventions

The following text conventions are used in this document:

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

Part I

Understanding Oracle WebCenter

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

Part I contains the following chapter:

- Chapter 1, "Introduction to Oracle WebCenter Administration"

1 Introduction to Oracle WebCenter Administration

Welcome to Oracle WebCenter!

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

1.1 Introducing Oracle WebCenter

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

Oracle WebCenter provides an open and extensible solution that allows users to interact directly with services like instant messaging, documents, content management, discussion forums, wikis and tagging directly from within the context of a portal or an application. These tools and services empower end users and IT to build and deploy next-generation collaborative applications and portals.

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

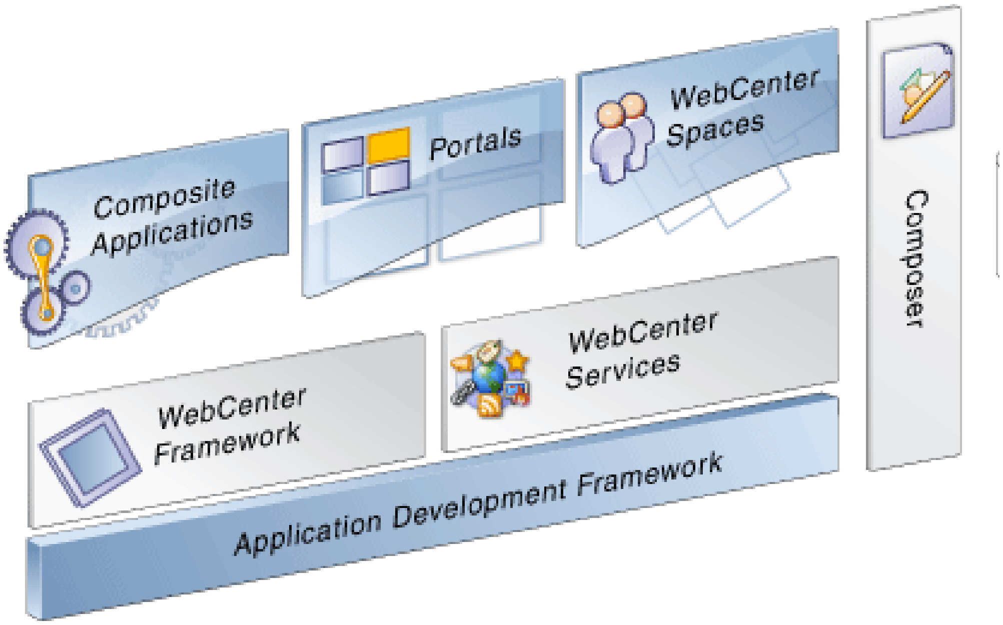
- Section 1.2, "Oracle WebCenter Architecture"
- Section 1.3, "Oracle WebCenter Topology"
- Section 1.4, "Oracle WebCenter Spaces"
- Section 1.5, "Custom WebCenter Applications"

1.2 Oracle WebCenter Architecture

Oracle WebCenter comprises the following components (shown in Figure 1–1):

- Oracle WebCenter Framework
- Oracle Application Development Framework
- Oracle Composer
- WebCenter Services
- WebCenter Spaces
- Portals
- Composite Applications

Figure 1–1 Oracle WebCenter Architecture



1.2.1 Oracle WebCenter Framework

Injects portal capabilities into ADF, including:

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

1.2.2 Oracle Application Development Framework

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 Oracle Composer

Oracle Composer provides:

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

1.2.4 WebCenter Services

Table 1–1 lists the services available to WebCenter application—both WebCenter Spaces and custom WebCenter applications.

Table 1–1 WebCenter Services

Services A Through M	Services N Through W
Announcements	Notes[1]
Blog	Page
Discussions	People Connections
Documents	RSS[2]
Events[1]	Recent Activities
Instant Messaging and Presence (IMP)	Search
Links	Tags

Table 1–1 (Cont.) WebCenter Services

Services A Through M	Services N Through W
Lists[1]	Wiki
Mail	Worklist

[1] WebCenter Spaces only.

[2] RSS news feeds are available from WebCenter Spaces only. The RSS Viewer task flow is available in both WebCenter Spaces and custom WebCenter applications.

WebCenter services include provides:

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

1.2.5 WebCenter Spaces

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

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

1.2.6 Portals

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

1.2.7 Composite Applications

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

1.3 Oracle WebCenter Topology

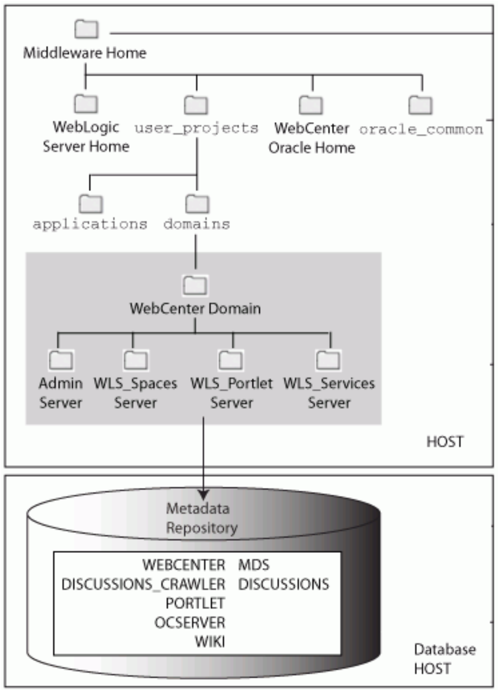
This section describes Oracle WebCenter topology and configuration in the following sections:

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

1.3.1 Oracle WebCenter Topology Out-of-the-Box

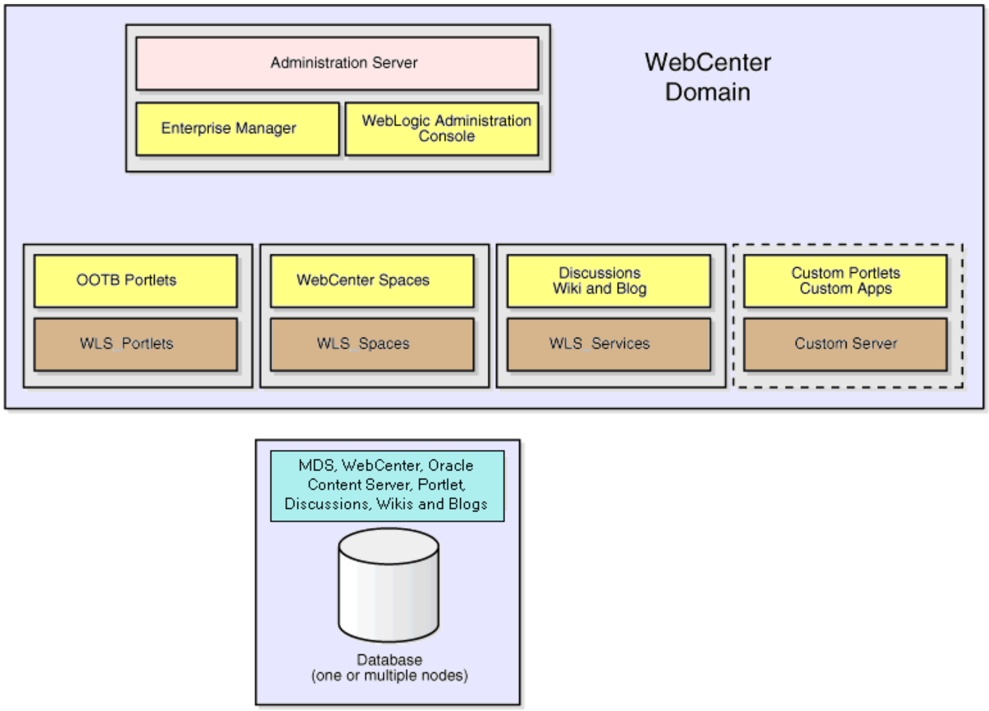
Oracle WebCenter installation creates a **WebCenter Oracle home** under the Oracle Middleware home directory and the **oracle_common** home directory, which contains WebCenter binaries and supporting files (Figure 1–2).

Figure 1–2 Directory Structure of an Oracle WebCenter Installation



The installation also creates a WebCenter domain (`wc_domain`), containing the administration server and several managed servers to host various WebCenter 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 Topology Out-of-the-Box


Administration Server
Enterprise Manager
WebLogic Administration Console
WebCenter Domain
OOTB Portlets
WLS_Portlets
WebCenter Spaces
WLS_Spaces
Discussions Wiki and Blog
WLS_Services
Custom Portlets Custom Apps
Custom Server
MDS, WebCenter, Oracle Content Server, Portlet, Discussions, Wikis and Blogs
Database (one or multiple nodes)

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

- WLS_Spaces - Hosts Oracle WebCenter Spaces
- WLS_Portlet - Hosts Oracle WebCenter Portlets
- WLS_Services - Hosts Oracle WebCenter Discussions and Oracle WebCenter Wiki and Blog Server, and any additional WebCenter services that you choose to integrate

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

1.3.2 Oracle WebCenter Managed Servers

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

Table 1–2 Oracle WebCenter Managed Servers and Applications

Managed Server	Application(s)
WLS_Spaces	webcenter webcenter-help
WLS_Portlets	portalTools wsrp-tools
WLS_Services	owc_discussions Oracle WebCenter Discussions Server owc_wiki Oracle WebCenter Wiki and Blog Server

1.3.3 Oracle WebCenter Startup Order

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

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

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

WebCenter application startup is not dependent on the availability of external services such as the Discussions server, or other back-end servers. For details, see Section 1.3.4, "Oracle WebCenter External Dependencies".

1.3.4 Oracle WebCenter External Dependencies

WebCenter applications have several external dependencies, as listed in Table 1–3. The Configuration column lists the type of information provided to Oracle WebCenter to configure or initialize the connection. The Access column lists the protocol used in run-time access of the service.

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

Table 1–3 External Resources - Access Types

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

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

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

1.3.5 Oracle WebCenter Configuration Considerations

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

Table 1–4 Oracle WebCenter Configuration Files

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

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

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

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

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

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

To find out more about WebCenter application configuration tools available, see Section 1.12, "Oracle WebCenter Administration Tools".

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

While WebCenter applications store post deployment configuration information in MDS, configuration information for portlet producers, Oracle WebCenter Discussions Server and Oracle WebCenter Wiki and Blog Server is stored in the file system or the database (see Table 1–5).

Table 1–5 Oracle WebCenter Configuration Location

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

The Oracle WebCenter Discussions Server stores configuration information in its database. Additionally, it stores startup configuration information in $DOMAIN_HOME/config/fmwconfig/servers/SERVER_NAME/owc_discussions_11.1.1.2.0. This directory contains the jive_startup.xml file, jive.license files, and a \logs directory containing log files for the discussions server instance.

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

1.3.6 Oracle WebCenter State and Configuration Persistence

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

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

1.3.7 Oracle WebCenter Log File Locations

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

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

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

You can also view and configure diagnostic logs through Fusion Middleware Control, see Section 30.3, "Viewing and Configuring Log Information".

1.4 Oracle WebCenter Spaces

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

To help you get started, see:

- Chapter 2, "Getting WebCenter Spaces Up and Running"

For information about administering WebCenter Spaces, see:

- Chapter 32, "Accessing WebCenter Spaces Administration Pages"
- Chapter 33, "Customizing WebCenter Spaces"
- Chapter 34, "Managing Users and Roles for WebCenter Spaces"
- Chapter 35, "Managing Pages in WebCenter Spaces"
- Chapter 36, "Making Applications Available in WebCenter Spaces"
- Chapter 37, "Managing Group Spaces in WebCenter Spaces"
- Chapter 38, "Exporting and Importing Group Spaces"

1.5 Custom WebCenter Applications

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

To help you get started, see:

- Chapter 4, "Getting Custom WebCenter Applications Up and Running"
- Chapter 5, "Maintaining Custom WebCenter Applications"
- Chapter 7, "Deploying WebCenter Applications"

1.6 Planning WebCenter Installations

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

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

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

1.7 Understanding the WebCenter 11g Installation

The out-of-the-box WebCenter topology is briefly described in Section 1.3, "Oracle WebCenter Topology." Specific areas of the WebCenter topology are described in the corresponding chapters, for example, security-related aspects of the WebCenter topology are described in Chapter 23, "Managing Security."

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

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

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

For postinstallation security configuration, see Section 23.2.5, "Post-deployment Security Configuration Tasks."

1.8 Understanding Administrative Operations, Roles, and Tools

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

Your ability to perform WebCenter administration tasks depends on which Oracle WebLogic Server role you are assigned—`Admin`, `Operator`, or `Monitor`. Table 1–6 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 1–6 WebCenter Operations and Oracle WebLogic Server Roles

Operation	Admin Role	Operator Role	Monitor Role
All WebCenter applications			
Start and stop	Yes	Yes	No
View performance metrics	Yes	Yes	Yes
View log information	Yes	Yes	Yes
Configure log files	Yes	Yes	Yes
View configuration	Yes	Yes	Yes
Configure new connections	Yes	Yes	No
Edit connections	Yes	Yes	No
Delete connections	Yes	Yes	No
Deploy applications	Yes	No	No
Configure security	Yes	No	No
View security (application roles/policies)	Yes	Yes	Yes
WebCenter Spaces only			
Export WebCenter Spaces	Yes	No	No
Import WebCenter Spaces	Yes	No	No

Table 1–7 summarizes which tools you can use to perform various administrative operations relating to WebCenter applications.

Table 1–7 WebCenter Operations and Administration Tools

Operation	Fusion Middleware Control	WLST Commands	WebLogic Server Admin Console	WebCenter Spaces Admin
All WebCenter 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
Deploy applications	Yes	Yes	Yes	No
Configure security	Yes	Yes	Yes	No
WebCenter Spaces only				

Table 1–7 (Cont.) WebCenter Operations and Administration Tools

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

1.9 Performance Monitoring and Diagnostics

Performance monitoring helps administrators identify issues and performance bottlenecks in their environment. Chapter 30, "Monitoring Oracle WebCenter Performance" describes the range of performance metrics available for WebCenter applications and how to monitor them using Fusion Middleware Control. It also describes how to troubleshoot issues by analyzing information that is recorded in WebCenter diagnostic log files.

1.10 WebCenter Application Deployment

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

Section 21.8, "Deploying Portlet Producer Applications" provides instructions for deploying WSRP and PDK-Java portlet producer applications.

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

1.11 Data Migration, Backup, and Recovery

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

Chapter 31, "Managing Export, Import, Backup, and Recovery of WebCenter" describes the backup, import, and export capabilities and tools available for these tasks.

1.12 Oracle WebCenter Administration Tools

Oracle offers the following tools for managing Oracle WebCenter:

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

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

- WebCenter Spaces Administration Pages

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

1.12.1 Oracle Enterprise Manager Fusion Middleware Control Console

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

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

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

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

1.12.1.1 Displaying Fusion Middleware Control Console

For information about starting Fusion Middleware Control, see Section 6.1, "Displaying Fusion Middleware Control Console".

1.12.2 Oracle WebLogic Server Administration Console

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

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

Use the Administration Console to:

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

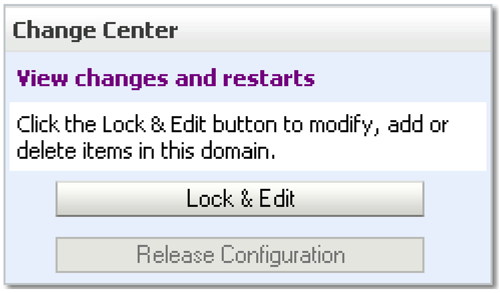
For more information about the Oracle WebLogic Server Administration Console, see "Displaying the Oracle WebLogic Server Administration Console" in the *Oracle Fusion Middleware Administrator's Guide*.

Locking Domain Configuration

In a production environment, you must lock configuration settings for a domain before making any configuration changes. Navigate to the Administration Console's Change Center (Figure 1–4), 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



Change Center

View changes and restarts

Click the Lock & Edit button to modify, add or delete items in this domain.

1.12.3 Oracle WebLogic Scripting Tool (WLST)

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

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

Oracle WebCenter offers WLST commands for managing WebCenter application connections (to content repositories, portlet producers, external applications, and other back-end services), and also for exporting and importing the WebCenter Spaces application. All Oracle WebCenter WLST commands are described in "Oracle WebCenter Custom WLST Commands" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference.*

1.12.3.1 Running Oracle WebLogic Scripting Tool (WLST) Commands

To run WLST from the command line:

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

   ```
   wlst.sh
   ```

   For example:

   ```
   WC_ORACLE_HOME/common/bin/wlst.sh
   ```

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

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

   where

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

   For example:

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

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

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

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

   or `setenv CONFIG_JVM_ARGS`

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

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

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

   For help on a particular command, type: `help('<WLST_command_name>')` at the WLST command prompt.

   See also, "Oracle WebCenter Custom WLST Commands" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference.*

1.12.4 System MBean Browser

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

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

To access application MBeans for WebCenter applications:

1. Log in to Fusion Middleware Control and navigate to the home page for WebCenter Spaces or the custom WebCenter application. For more information, see:
   - Section 6.2, "Navigating to the Home Page for WebCenter Spaces"
   - Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"
2. Do one of the following:
   - For WebCenter Spaces - From the **WebCenter** menu, choose **System MBean Browser**.
   - For WebCenter applications - From the **Application Deployment** menu, choose **System MBean Browser**.
3. Expand **Application Defined MBeans**, then **oracle.adf.share.config**, then **Server: name**, then **Application: name**, then **ADFConfig**, then **ADFConfig**, and **ADFConfig**.
4. 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.
5. Click **Apply** to update attribute values.
6. Navigate to the parent MBean (**ADFConfig**), select the **Operations** tab, and click **save** to save the changes.
7. Restart the managed server on which the WebCenter application is deployed. For more information, see Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."

1.12.5 WebCenter Spaces Administration Pages

WebCenter Spaces provides several administration pages of its own. WebCenter Spaces Administration appears only to users who have logged in to the application using an administrator user name and password. See also, Section 32.1, "Logging into WebCenter Spaces as an Administrator".

WebCenter Spaces administration pages allow you to:

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

For more details, see Section 32, "Accessing WebCenter Spaces Administration Pages".

Part II

Getting Started With Oracle WebCenter Administration

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

Part II contains the following chapters:

- Chapter 2, "Getting WebCenter Spaces Up and Running"
- Chapter 3, "Maintaining WebCenter Spaces"
- Chapter 4, "Getting Custom WebCenter Applications Up and Running"
- Chapter 5, "Maintaining Custom WebCenter Applications"

2 Getting WebCenter Spaces Up and Running

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

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

This chapter includes the following sections:

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

Audience

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

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

2.1 Role of the Fusion Middleware Administrator

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

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

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

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

  Oracle WebLogic Server provides two other roles, in addition to the `Admin` role, namely `Operator` and `Monitor`. To find out more about these role, see Table 1–6, " WebCenter Operations and Oracle WebLogic Server Roles"in Section 1.8, "Understanding Administrative Operations, Roles, and Tools".

- **WebCenter Spaces** - Assign one more users the `Administrator` role through WebCenter Spaces Administration. For details, see Section 34.2.4, "Giving a User Administrative Privileges".

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

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

2.2 Role of the WebCenter Spaces Administrator

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

Out-of-the-box, the default Fusion Middleware administrator (`weblogic`) is the only user assigned to the WebCenter Spaces `Administrator` role. The password is the one provided during installation. Use this administrator account to log in to WebCenter Spaces, and assign additional users the `Administrator` role. For details, see Section 34.2.4, "Giving a User Administrative Privileges".

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

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

2.3 Installing WebCenter Spaces

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

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

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

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

Step	Documentation	Role
Step 1 - Verify your Oracle WebCenter Spaces installation	Install WebCenter Spaces, start the managed server, log in to the application with default credentials, and assign administration privileges to one or more users: ■ Installing WebCenter Spaces ■ Starting Node Manager ■ Starting and Stopping Managed Servers for WebCenter Application Deployments ■ Logging into WebCenter Spaces as an Administrator ■ Giving a User Administrative Privileges Tip: WebCenter Spaces URL is `http://<host>:<port>/webcenter/spaces` If the default administrator was changed at install time, you must grant that user WebCenter Spaces administrative privileges before logging in to WebCenter Spaces. See Section 24.6, "Granting the WebCenter Spaces Administrator Role to a WebCenter Spaces User."	Fusion Middleware Admin
Step 2 - Launch Fusion Middleware Control	Launch Fusion Middleware Control Console, a Web-based management tool for WebCenter Spaces: ■ Displaying Fusion Middleware Control Console ■ Navigating to the Home Page for WebCenter Spaces Tip: Fusion Middleware Control Console URL is `http://<host>:<port>/em` Learn about the command-line administration tool WLST. See "Oracle WebLogic Scripting Tool (WLST)".	Fusion Middleware Admin
Step 3 - Configure WebCenter Spaces workflows	Connect the application to the BPEL server where WebCenter Spaces workflows are installed: ■ Back-End Requirements for WebCenter Spaces Workflows ■ Specifying the BPEL Server Hosting WebCenter Spaces Workflows	Fusion Middleware Admin
Step 4 - Connect back-end services	Configure back-end services for WebCenter Spaces through Fusion Middleware Control Console. See:	Fusion Middleware Admin
■ **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 ■ Managing the Wiki and Blog Services	
■ **Calendar Services**	■ Managing the Events Service	

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

Step	Documentation	Role
- **Secure Enterprise Search**	- Managing the Search Service	
- **Group Space Events, Links, Lists, Notes, People Connections, and Tags**	- No additional set up required. The WebCenter repository and MDS repository required for these services are configured out-of-the-box.	
Step 5 - Connect external applications and portlet producers	Configure external applications and portlet producers for WebCenter Spaces. See:	Fusion Middleware Admin
- **External Applications**	- Managing External Applications	
- **Portlet Producers**	- Registering WSRP Producers - Registering Oracle PDK-Java Producers	
Step 6 - Connect back-end severs to the same identity store as WebCenter Spaces	Ensure that back-end servers, supporting wikis and blogs, discussions and announcements, presence, and Oracle Content Server, share the same identity store as WebCenter Spaces: - Chapter 24, "Configuring the Identity Store" See also *Oracle Fusion Middleware Security Guide*.	Fusion Middleware Admin
Step 7 - Secure communication with WebCenter Spaces	Configure secure communication: - Chapter 27, "Securing WebCenter Applications and Components with SSL" - Chapter 28, "Configuring WS-Security for WebCenter Applications and Components" - Chapter 27, "Securing WebCenter Applications and Components with SSL" See also *Oracle Fusion Middleware Security Guide*.	Fusion Middleware Admin
Step 8 - Restart the managed server and WebCenter Spaces	Restart the managed server on which WebCenter Spaces is deployed to effect configuration changes, and then login to WebCenter Spaces with administrative privileges: - Starting and Stopping Managed Servers for WebCenter Application Deployments - Logging into WebCenter Spaces as an Administrator	Fusion Middleware Admin
Step 9 - Verify your WebCenter Spaces configuration	Verify WebCenter Spaces configuration: identity store, services, applications, and so on. - Logging into WebCenter Spaces as an Administrator Tip: WebCenter Spaces URL is `http://<host>:<port>/webcenter/spaces`	Fusion Middleware Admin
Step 10 - Customize WebCenter Spaces and grant application roles	The WebCenter Spaces administrator is responsible for WebCenter Spaces customizations and user role assignments: - Customizing WebCenter Spaces for the First Time (Roadmap)	WebCenter Spaces Admin

2.5 Customizing WebCenter Spaces for the First Time (Roadmap)

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

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

Step	Documentation	Role
Step 1 - Log in to WebCenter Spaces	Login to WebCenter Spaces with administrative privileges and access the administration pages: ▪ Logging into WebCenter Spaces as an Administrator Tip: WebCenter Spaces URL is `http://<host>:<port>/webcenter/spaces`	WebCenter Spaces Admin
Step 2 - Customize WebCenter Spaces	Customize WebCenter Spaces to suit your audience. Choose a name and logo for your application, apply a corporate brand, set language options, and more: ▪ Naming Your WebCenter ▪ Customizing the Online Help Link ▪ Choosing the Default Display Language ▪ Applying Look and Feel Using Skins ▪ Customizing Copyright and Privacy Statements ▪ ... for more options, see Chapter 33, "Customizing WebCenter Spaces".	WebCenter Spaces Admin
Step 3 - Determine self-registration policy	Establish your policy regarding new user registration. Allow users outside of the WebCenter Spaces community by to self -register on an invitation-only basis or extend self-registration to the public: ▪ Enabling Self-Registration By Invitation-Only ▪ Enabling Anyone to Self-Register	WebCenter Spaces Admin
Step 4 - Plan the public user experience	First impressions are extremely important. Determine the content displayed on your Welcome page and the appearance of WebCenter Spaces before users login: ▪ Customizing the Public Welcome Page ▪ Customizing the Login Page ▪ Customizing the Self-Registration Page ▪ Choosing the Default Display Language ▪ Granting Permissions to the Public-User	WebCenter Spaces Admin
Step 5 - Create roles and delegate responsibilities to other users	Create roles to characterize groups of WebCenter users and determine what they can see and do in WebCenter Spaces. Manage and assign roles for any user in the identity store: ▪ Understanding Users, Roles, and Permissions ▪ Assigning Users (and Groups) to Roles ▪ Defining Application Roles ▪ Giving a User Administrative Privileges ▪ Modifying Application Role Permissions	WebCenter Spaces Admin

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

Step	Documentation	Role
Step 6 - Customize personal spaces	Design a default personal space for your WebCenter users. Give them instant access to important information and applications relevant to their roles: ■ Setting Up a Default Look and Feel for Personal Pages ■ Creating a Business Role Page Encourage or enforce a consistent look and feel through default page schemes and default page templates: ■ Setting Up a Default Look and Feel for Personal Pages	WebCenter Spaces Admin
Step 7 - Set up discussion forums and announcements	Configure default options for discussion forums and announcements: ■ Setting Discussion Forum Options for WebCenter Spaces	WebCenter Spaces Admin
Step 8 - Set up people connection components	Configure defaults for activity streams, personal profiles, connections, messages boards, and feedback: ■ Configuring the People Connections Service for WebCenter Spaces	WebCenter Spaces Admin
Step 9 - Set up mail notifications	Configure default options for everyone's mail: ■ Setting Send Mail Notifications for WebCenter Spaces	WebCenter Spaces Admin
Step 10 - Provide group spaces and group space templates	In WebCenter, users can create and manage group spaces without centralized administration. Give them a head-start by creating templates for the types of group spaces they are likely to build: ■ Building Group Spaces ■ Creating Group Space Templates	WebCenter Spaces Admin
Step 11 - Customize the Sidebar	Give users quick access to frequently used applications and collaboration services such as mail, worklist assignments, and personal contacts. Display, hide, reorganize, and lock the content of everyone's Personal Sidebar: ■ Hiding and Showing Task Flows in the Sidebar ■ Locking Sidebar Content	WebCenter Spaces Admin
Step 12 - Organize the applications pane	Make WebCenter the single place a user needs to go. Allow users direct access to applications outside WebCenter Spaces that require an HTML form-based login. Expose key external applications in everyone's Personal Sidebar: ■ Making an Application Available to WebCenter Users ■ Arranging the Applications List ■ Locking Applications Displayed in the Applications Pane	WebCenter Spaces Admin

3 Maintaining WebCenter Spaces

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

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

This chapter includes the following sections:

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

Audience

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

> **Note:** Administrators maintaining custom WebCenter applications should refer to Chapter 5, "Maintaining Custom WebCenter Applications".

3.1 Role of the Fusion Middleware Administrator

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

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

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

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

3.2 Role of the WebCenter Spaces Administrator

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

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

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

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

3.3 System Administration for WebCenter Spaces (Roadmap)

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

Table 3–1 Roadmap - Administering and Monitoring WebCenter Spaces

Step	Documentation	Role
Step 1 - Stop and start the managed server	Restart the managed server on which WebCenter Spaces is deployed to effect configuration changes or for routine maintenance: ■ Starting and Stopping Managed Servers for WebCenter Application Deployments Tip: The managed server for WebCenter Spaces is named `WLS_Spaces`.	Fusion Middleware Admin
Step 2 - View and manage log files	Identify and diagnose problems through log files. WebCenter Spaces logs record all types of events, including startup and shutdown information, errors, warnings, and other information: ■ Viewing and Configuring Log Information	Fusion Middleware Admin

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

Step	Documentation	Role
Step 3 - Monitor performance	Analyze the performance of WebCenter Spaces and monitor its current status through Fusion Middleware Control Console: ■ Viewing Performance Information ■ Monitoring WebCenter Spaces Fusion Middleware administrators granted one of these roles can view metrics: `Admin`, `Operator`, `Monitor`. To find out more, see in "Understanding Administrative Operations, Roles, and Tools".	Fusion Middleware Admin
Step 4 - Tune application properties	Reconfigure performance related parameters for the WebCenter environment, WebCenter application, and WebCenter services: ■ Tuning Oracle WebCenter Performance	Fusion Middleware Admin
Step 3 - Stop and start WebCenter Spaces	Fusion Middleware administrators may shut down WebCenter Spaces for maintenance purposes and then restart the application: ■ Starting WebCenter Spaces Using Fusion Middleware Control ■ Stopping WebCenter Spaces Using Fusion Middleware Control	Fusion Middleware Admin
Step 4 - Modify back-end services	Add, modify, and delete connections through Fusion Middleware Control Console. See:	Fusion Middleware Admin
■ **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 ■ Managing the Wiki and Blog Services	
■ **Calendar Services**	■ Managing the Events Service	
■ **Secure Enterprise Search**	■ Managing the Search Service	
■ **Group Space Events, Links, Lists, Notes, Tags, and People Connections**	■ Setting Up the WebCenter Repository ■ Setting Up the MDS Repository	
Step 4 - Modify external applications and portlet producers	Add, modify, and delete connections through Fusion Middleware Control Console. See:	Fusion Middleware Admin
■ **External Applications**	■ Managing External Applications	
■ **Portlet Producers**	■ Registering WSRP Producers ■ Registering Oracle PDK-Java Producers	

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

Step	Documentation	Role
Step 5 - Configure SSL communication	Configure secure communication: - Chapter 27, "Securing WebCenter Applications and Components with SSL" - Chapter 28, "Configuring WS-Security for WebCenter Applications and Components" - Chapter 26, "Configuring WebCenter Applications and Components to Use SSO" See also *Oracle Fusion Middleware Security Guide*.	Fusion Middleware Admin
Step 6 - Reconfigure identity store or policy store	Reconfigure your identity or policy stores: - Chapter 24, "Configuring the Identity Store" - Chapter 25, "Configuring the Policy and Credential Store" See also *Oracle Fusion Middleware Security Guide*.	Fusion Middleware Admin
Step 7 - Reconfigure WebCenter repository	Reconfigure the WebCenter repository: - Setting Up the WebCenter Repository	Fusion Middleware Admin
Step 8 - Reconfigure MDS repository	Reconfigure the application's MDS repository: - Setting Up the MDS Repository See also *Oracle Fusion Middleware Administrator's Guide*: - 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
Step 9 - Reconfigure WebCenter Spaces workflows	Install WebCenter Spaces workflows on a different BPEL server and reconfigure the connection: - Installing WebCenter Spaces Workflows - Specifying the BPEL Server Hosting WebCenter Spaces Workflows	Fusion Middleware Admin
Step 10 - Export WebCenter Spaces	Use the export facility to move content to a remote instance or between stage and production environments: - Exporting an Entire WebCenter Spaces Application - Exporting Group Spaces - Exporting Group Space Templates	Fusion Middleware Admin
Step 11 - Import WebCenter Spaces	Use the import facility to restore WebCenter Spaces from a backup or to move content to a remote instance or between stage and production environments: - Importing an Entire WebCenter Spaces Application - Importing Group Spaces - Importing Group Space Templates	Fusion Middleware Admin
Step 12 - View and manage log files	Identify and diagnose problems through log files. WebCenter Spaces logs record all types of events, including startup and shutdown information, errors, warnings, and other information: - Viewing and Configuring Log Information	Fusion Middleware Admin

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

Step	Documentation	Role
Step 13 - Monitor performance	Analyze the performance of WebCenter Spaces and monitor its current status through Fusion Middleware Control Console: ▪ Viewing Performance Information ▪ Monitoring WebCenter Spaces	Fusion Middleware Admin

3.4 Application Administration for WebCenter Spaces (Roadmap)

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

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

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

Step	Documentation	Role
Step 1 - Modify Application Settings	Modify application-wide settings as required: ▪ Naming Your WebCenter ▪ Customizing the Online Help Link ▪ Choosing the Default Display Language ▪ Applying Look and Feel Using Skins ▪ Customizing Copyright and Privacy Statements ▪ ... for more options, see Chapter 33, "Customizing WebCenter Spaces".	WebCenter Spaces Admin
Step 2 - Manage Personal Spaces	Manage personal pages and business role pages. Push content to personal spaces: ▪ Managing Business Role Pages ▪ Managing Personal Pages	WebCenter Spaces Admin
Step 3 - Manage Group Spaces	Take any group space temporarily offline and close down any group spaces that is inactive. Manage anyone's group space: ▪ Viewing Group Space Information ▪ Changing the Status of a Group Space	WebCenter Spaces Admin
Step 4 - Manage Group Space Templates	Manage group space templates. Review and delete any template: ▪ Managing Group Space Templates	WebCenter Spaces Admin
Step 5 - Maintain Users and Roles	Maintain security. Modify user role permissions and assign new roles: ▪ Modifying Application Role Permissions ▪ Assigning a User to a Different Role	WebCenter Spaces Admin
Step 6 - Manage the Applications List	Maintain external application links. Add, modify, and delete entries: ▪ Making an Application Available to WebCenter Users ▪ Editing Links in the Applications Pane ▪ Removing Links from the Applications Pane	WebCenter Spaces Admin

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

Step	Documentation	Role
Step 7- Maintain the Sidebar	Hide Sidebar content when services temporarily unavailable. Expose new services when available: ■ Hiding and Showing Task Flows in the Sidebar	WebCenter Spaces Admin

4 Getting Custom WebCenter Applications Up and Running

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

The chapter includes the following sections:

- Section 4.1, "Installing Oracle WebCenter and Oracle WebCenter Framework Libraries"
- Section 4.2, "Deploying Custom WebCenter Applications for the First Time (Roadmap)"

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

Audience

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

4.1 Installing Oracle WebCenter and Oracle WebCenter Framework Libraries

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

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

Custom WebCenter applications can be deployed to any WebLogic Server instance that is provisioned with the Oracle WebCenter Framework shared library files. For details, see, Section 7.1.3.1, "Creating and Provisioning a WebLogic Managed Server Instance".

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

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

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

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

Step	Documentation	Role
Step 1 - Verify your Oracle WebCenter installation	Verify your Oracle WebCenter installation and settings. See: ■ Installing Oracle WebCenter and Oracle WebCenter Framework Libraries ■ Starting Node Manager Installation is described in the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter*.	Fusion Middleware Admin
Step 2 - Launch Fusion Middleware Control	Launch the Fusion Middleware Control Console, a Web-based management tool for WebCenter applications. See: ■ Displaying Fusion Middleware Control Console ■ Navigating to the Home Page for Custom WebCenter Applications Learn about the command-line administration tool WLST. See "Oracle WebLogic Scripting Tool (WLST)".	Fusion Middleware Admin
Step 3 - Deploy the custom WebCenter application	Create a suitable container in which to deploy the custom WebCenter application archive: ■ Creating and Provisioning a WebLogic Managed Server Instance ■ Creating and Registering the Metadata Service Repository ■ Deploying the Application to a WebLogic Managed Server Instance See also, "Deploying WebCenter Applications".	Fusion Middleware Admin
Step 4 - Connect back-end services	Configure back-end services for the custom WebCenter application through Fusion Middleware Control.	Fusion Middleware Admin
■ **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	

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

Step	Documentation	Role
■ **Secure Enterprise Search**	■ Managing the Search Service	
■ **Wiki and Blog Services**	■ Managing the Wiki and Blog Services	
■ **External Applications**	■ Managing External Applications	
■ **Portlet Producers**	■ Registering WSRP Producers ■ Registering Oracle PDK-Java Producers	
■ **Group Space Events, Links, Lists, Notes, and Tags**	■ Setting Up the WebCenter Repository ■ Setting Up the MDS Repository	
Step 5 - Connect to an identity store	Ensure that your identity store is installed, configured, and contains all the required user data. See: ■ Chapter 24, "Configuring the Identity Store" See also *Oracle Fusion Middleware Security Guide*.	Fusion Middleware Admin
Step 6 - Restart the managed server	Restart the managed server on which the application is deployed. See: ■ Starting and Stopping Managed Servers for WebCenter Application Deployments	Fusion Middleware Admin
Step 7 - Verify custom WebCenter application configuration	Login to the application to verify the configuration: identity store, services, applications, and so on.	Fusion Middleware Admin

5 Maintaining Custom WebCenter Applications

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

- Section 5.1, "System Administration for Custom WebCenter Applications (Roadmap)"

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

Audience

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

5.1 System Administration for Custom WebCenter Applications (Roadmap)

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

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

Table 5–1 Roadmap - Maintaining Custom WebCenter Applications

Step	Documentation	Role
Step 1 - Stop and start the managed server	Restart the managed server on which the custom WebCenter application is deployed to effect configuration changes or for routine maintenance: ■ Starting and Stopping Managed Servers for WebCenter Application Deployments	Fusion Middleware Admin
Step 2 - Stop and start the custom WebCenter application	Shut down the application for maintenance purposes and then restart the application: ■ Starting and Stopping Custom WebCenter Applications	Fusion Middleware Admin
Step 3 Maintain back-end services	Add, modify, and delete connections through the Fusion Middleware Control Console:	Fusion Middleware Admin

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

Step	Documentation	Role
■ **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	
■ **Secure Enterprise Search**	■ Managing the Search Service	
■ **Wiki and Blog Services**	■ Managing the Wiki and Blog Services	
Step 4 - Maintain external applications and portlet producers	Add, modify, and delete connections through Oracle Enterprise Manager Fusion Middleware Control Console. See:	Fusion Middleware Admin
■ **External Applications**	■ Managing External Applications	
■ **Portlet Producers**	■ Registering WSRP Producers ■ Registering Oracle PDK-Java Producers	
Step 5 - Reconfigure your identity store	■ Chapter 24, "Configuring the Identity Store" See also, *Oracle Fusion Middleware Security Guide*.	Fusion Middleware Admin
Step 6 - Reconfigure the MDS repository	■ Setting Up the MDS Repository	Fusion Middleware Admin
Step 7 - Reconfigure WebCenter repository	■ Setting Up the WebCenter Repository	
Step 8 - Export custom WebCenter application data	Migrate data to a remote instance or between stage and production environments: ■ Exporting WebCenter Services Metadata and Data (Custom WebCenter Applications) ■ Exporting Portlet Client Metadata (Custom WebCenter Applications) ■ Migrating Security for Custom WebCenter Applications ■ Migrating Data (Custom WebCenter Applications) See also, "Managing Export, Import, Backup, and Recovery of WebCenter".	Fusion Middleware Admin
Step 9 - Import custom WebCenter application data	Use the import facility to move content to a remote instance or between stage and production environments: ■ Importing WebCenter Services Metadata and Data (Custom WebCenter Applications) ■ Importing Portlet Client Metadata (Custom WebCenter Applications) ■ Migrating Security for Custom WebCenter Applications ■ Migrating Data (Custom WebCenter Applications)	Fusion Middleware Admin

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

Step	Documentation	Role
Step 10 - View and manage log files	Identify and diagnose problems through log files. Custom WebCenter application logs record all types of events, including startup and shutdown information, errors, warnings, and other information: ■ Viewing and Configuring Log Information	Fusion Middleware Admin
Step 11 - Monitor performance	Analyze the performance of the custom WebCenter application and monitor its current status through Fusion Middleware Control Console: ■ Viewing Performance Information ■ Monitoring Custom WebCenter Applications	Fusion Middleware Admin
Step 12 - Tune application properties	Reconfigure performance related parameters for the WebCenter environment, WebCenter application, and WebCenter services: ■ Tuning Oracle WebCenter Performance	Fusion Middleware Admin

Part III

Basic Systems Administration for Oracle WebCenter

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

Part III contains the following chapters:

6 Starting Enterprise Manager Fusion Middleware Control

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

This chapter includes the following sections:

- Section 6.1, "Displaying Fusion Middleware Control Console"
- Section 6.2, "Navigating to the Home Page for WebCenter Spaces"
- Section 6.3, "Navigating to the Home Page for Custom WebCenter 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 Oracle WebCenter pages. Your role determines what you can see and do after logging in. To find out more, see Table 1–6, " WebCenter Operations and Oracle WebLogic Server Roles".

To access the Fusion Middleware Control Console:

1. Start Fusion Middleware Control.

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

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

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

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

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

- On UNIX: `DOMAIN_HOME/config/config.xml`

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

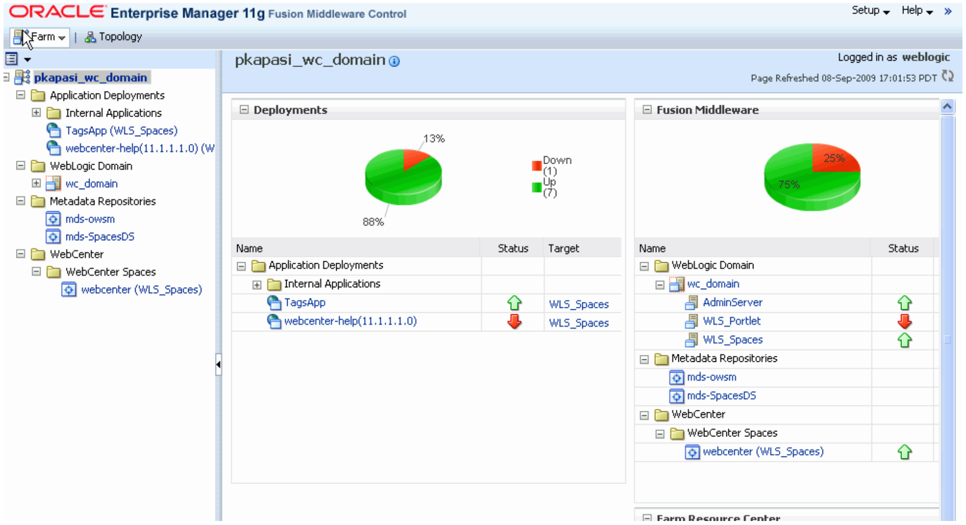
3. Enter a valid administrator **User Name** and **Password** details for the farm.

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

4. Click **Login**.

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

Figure 6–1 Farm Home Page



Name	Status	Target
Application Deployments		
Internal Applications		
TagsApp	↑	WLS_Spaces
webcenter-help(11.1.1.1.0)	↓	WLS_Spaces

Name	Status
WebLogic Domain	
wc_domain	
AdminServer	↑
WLS_Portlet	↓
WLS_Spaces	↑
Metadata Repositories	
mds-owsm	
mds-SpacesDS	
WebCenter	
WebCenter Spaces	
webcenter (WLS_Spaces)	↑

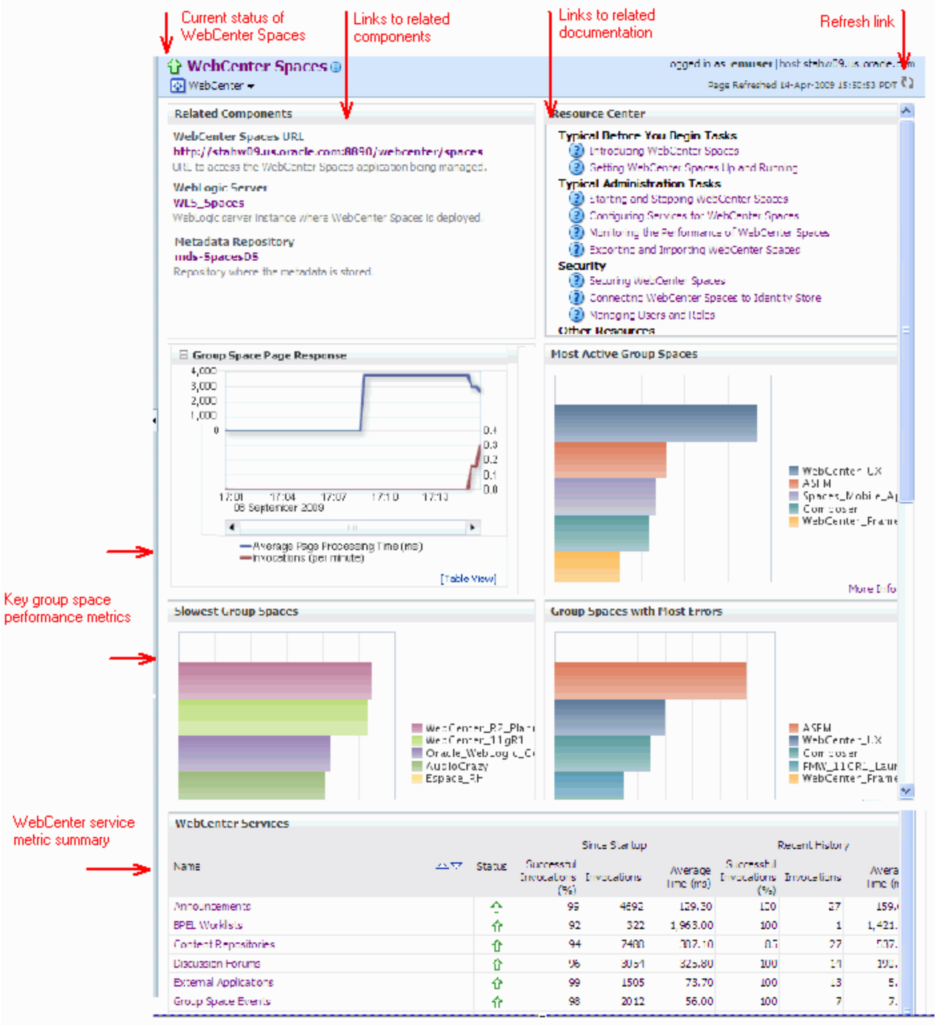
From the navigation pane, you can drill down to view and manage all components in your farm, including WebCenter Spaces and any custom WebCenter applications that you may have deployed. For detailed instructions, see

- Section 6.2, "Navigating to the Home Page for WebCenter Spaces".
- Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications".

6.2 Navigating to the Home Page for WebCenter Spaces

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

Figure 6–2 WebCenter Spaces Home Page



WebCenter Spaces

WebCenter

Logged in as emuser | host stahw09.us.oracle.com

Page Refreshed 14-Apr-2009 15:50:53 PDT

Related Components

WebCenter Spaces URL
http://stahw09.us.oracle.com:8890/webcenter/spaces
URL to access the WebCenter Spaces application being managed.

WebLogic Server
WLS_Spaces
WebLogic server instance where WebCenter Spaces is deployed.

Metadata Repository
mds-SpacesDS
Repository where the metadata is stored.

Resource Center

Typical Before You Begin Tasks
- Introducing WebCenter Spaces
- Getting WebCenter Spaces Up and Running

Typical Administration Tasks
- Starting and Stopping WebCenter Spaces
- Configuring Services for WebCenter Spaces
- Monitoring the Performance of WebCenter Spaces
- Exporting and Importing WebCenter Spaces

Security
- Securing WebCenter Spaces
- Connecting WebCenter Spaces to Identity Store
- Managing Users and Roles

Other Resources

WebCenter Services

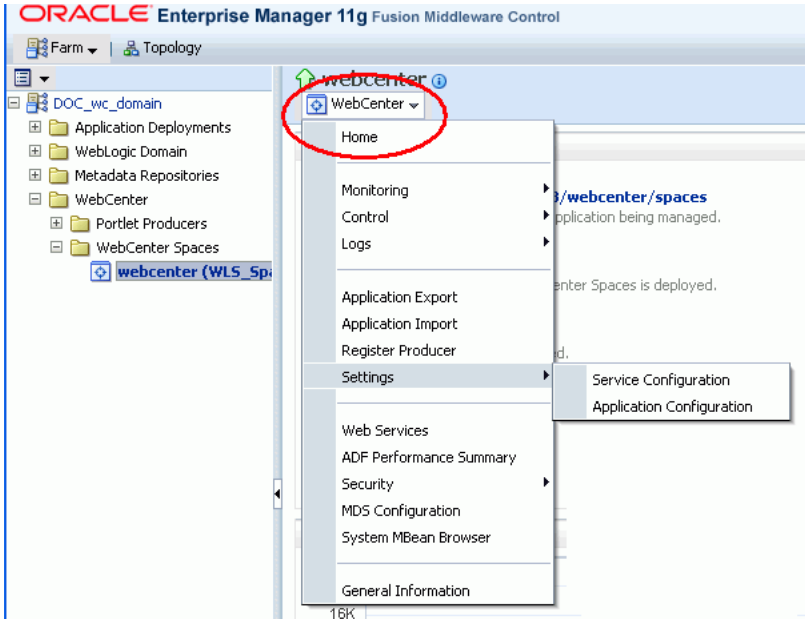
		Since Startup			Recent History		
Name	Status	Successful Invocations (%)	Invocations	Average Time (ms)	Successful Invocations (%)	Invocations	Average Time (m
Announcements	⇧	95	4692	129.30	100	27	159.
BPEL Worklists	⇧	92	322	1,963.00	100	1	1,421.
Content Repositories	⇧	94	7400	307.10	97	27	507.
Discussion Forums	⇧	96	3051	325.80	100	11	192.
External Applications	⇧	99	1505	73.70	100	13	5.
Group Space Events	⇧	98	2012	56.00	100	7	7.

From here you can:

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

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

Figure 6–3 WebCenter Menu for WebCenter Spaces



From the WebCenter menu, you can:

- Start and stop WebCenter Spaces
- Configure application settings
- Manage back-end services
- Manage external applications
- 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 WebCenter Spaces
- Configure security policies and roles.
- Configure ADF and MDS options.
- View Web Services-related information.

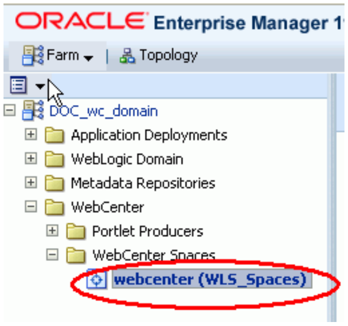
To navigate to the main home page for WebCenter Spaces:

1. Login to Fusion Middleware Control.

   See Section 6.1, "Displaying Fusion Middleware Control Console".

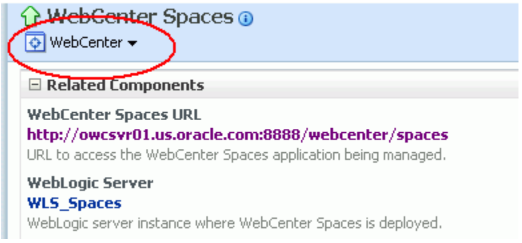
2. In the Navigator (Figure 6–4), expand **WebCenter**.
3. Expand **WebCenter Spaces**.
4. Select **webcenter** to navigate to the home page for your WebCenter Spaces installation.

Figure 6–4 Navigating to the WebCenter Spaces Home Page



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

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



WebCenter Spaces URL
http://owcsvr01.us.oracle.com:8888/webcenter/spaces
URL to access the WebCenter Spaces application being managed.

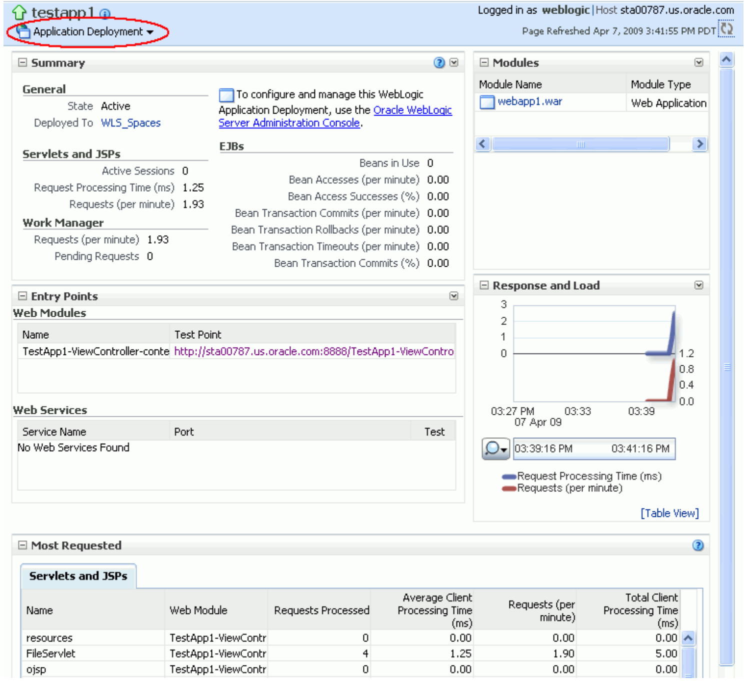
WebLogic Server
WLS_Spaces
WebLogic server instance where WebCenter Spaces is deployed.

6.3 Navigating to the Home Page for Custom WebCenter Applications

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

Note: WebCenter Spaces has a different home page, see Navigating to the Home Page for WebCenter Spaces.

Figure 6–6 Custom WebCenter Application Home Page



testapp1

Application Deployment ▾

Logged in as **weblogic** | Host sta00787.us.oracle.com

Page Refreshed Apr 7, 2009 3:41:55 PM PDT

Summary

General

State	Active
Deployed To	WLS_Spaces

To configure and manage this WebLogic Application Deployment, use the Oracle WebLogic Server Administration Console.

Servlets and JSPs

Active Sessions	0
Request Processing Time (ms)	1.25
Requests (per minute)	1.93

Work Manager

Requests (per minute)	1.93
Pending Requests	0

EJBs

Beans in Use	0
Bean Accesses (per minute)	0.00
Bean Access Successes (%)	0.00
Bean Transaction Commits (per minute)	0.00
Bean Transaction Rollbacks (per minute)	0.00
Bean Transaction Timeouts (per minute)	0.00
Bean Transaction Commits (%)	0.00

Modules

Module Name	Module Type
webapp1.war	Web Application

Entry Points

Web Modules

Name	Test Point
TestApp1-ViewController-conte	http://sta00787.us.oracle.com:8888/TestApp1-ViewContro

Web Services

Service Name	Port	Test
No Web Services Found		

Response and Load

Most Requested

Servlets and JSPs

Name	Web Module	Requests Processed	Average Client Processing Time (ms)	Requests (per minute)	Total Client Processing Time (ms)
resources	TestApp1-ViewContr	0	0.00	0.00	0.00
FileServlet	TestApp1-ViewContr	4	1.25	1.90	5.00
ojsp	TestApp1-ViewContr	0	0.00	0.00	0.00

From here you can:

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

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

- Manage external applications (see Chapter 22, "Managing External Applications").
- Manage back-end services (see Chapter 10, "Managing Oracle WebCenter Services").
- Manage portlet producers (see Chapter 21, "Managing Portlet Producers").

- Monitor detailed performance metrics for WebCenter services (see Chapter 30, "Monitoring Oracle WebCenter Performance").

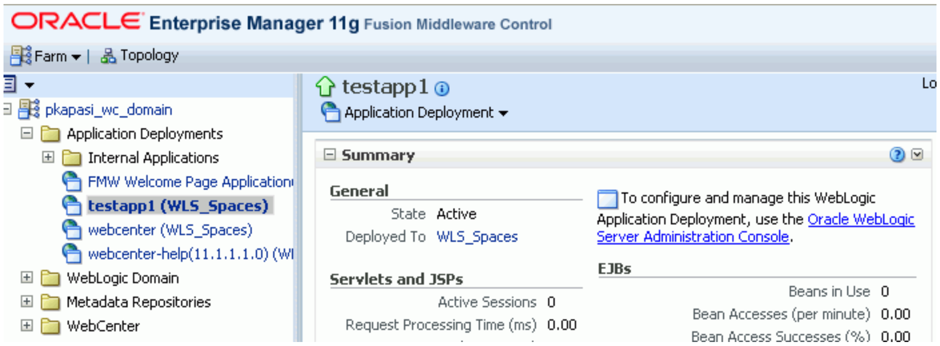
To navigate to the main home page for your custom WebCenter application:

1. Login to Fusion Middleware Control.

   See Section 6.1, "Displaying Fusion Middleware Control Console".

2. In the Navigator (Figure 6–7), expand **Application Deployments**.

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



General

State Active

Deployed To WLS_Spaces

To configure and manage this WebLogic Application Deployment, use the Oracle WebLogic Server Administration Console.

Servlets and JSPs

Active Sessions 0

Request Processing Time (ms) 0.00

EJBs

Beans in Use 0

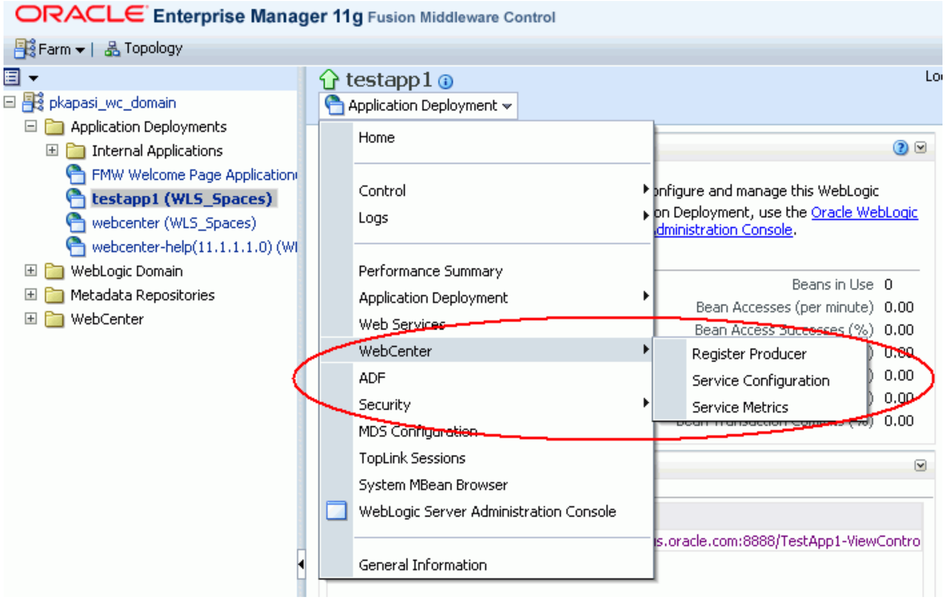
Bean Accesses (per minute) 0.00

Bean Access Successes (%) 0.00

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

   Notice WebCenter menu options display on the **Application Deployment** menu (Figure 6–8).

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



6.4 Navigating to Dependent Components

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

- **WebCenter Spaces** - From the home page, click links in "Related Components" to navigate to the WebCenter Spaces application itself, WebLogic Server installation pages, and MDS repository pages in Fusion Middleware Control. See also, Section 6.2, "Navigating to the Home Page for WebCenter Spaces".
- **Custom WebCenter 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 ADF, MDS repository, and security. See also, Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications".

7 Deploying WebCenter Applications

This chapter provides instructions for deploying, undeploying, and redeploying custom WebCenter applications from an Enterprise Archive, or EAR file, created with Oracle JDeveloper (for information on how to create an EAR file, see "How to Create Deployment Profiles in Oracle JDeveloper" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*). It does not contain instructions for deploying or installing Oracle WebCenter Spaces. For information about installing Oracle WebCenter Spaces and other WebCenter components, see "Installing Oracle WebCenter" in the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter*. For information about deploying WSRP and PDK-Java portlet producer applications, see Section 21.8, "Deploying Portlet Producer Applications."

This chapter includes the following sections:

- Section 7.1, "Deploying Custom WebCenter Applications"
- Section 7.2, "Undeploying Custom WebCenter Applications"
- Section 7.3, "Redeploying Custom WebCenter 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 Custom WebCenter Applications

This section describes the steps required to deploy a custom WebCenter application, which has been created in JDeveloper, to a production domain. The deployment steps in this section assume that you 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*. 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 Prerequisites"
- Section 7.1.2, "Preparing the Application EAR File"
- Section 7.1.3, "Preparing the Target Environment"

- Section 7.1.4, "Deploying the Application to a WebLogic Managed Server Instance"
- Section 7.1.5, "Transporting Customizations Between Environments"
- Section 7.1.6, "Configuring Applications to Run in a Distributed Environment"

7.1.1 Deployment Prerequisites

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

> **Note:** Oracle does not recommend deploying custom WebCenter applications to any of the three preconfigured Managed Servers created during the installation, or to the Administration Server. For WebCenter applications created in JDeveloper, follow the process described in Section 7.1.3.2, "Creating and Registering the Metadata Service Repository" and Section 7.1.3.1, "Creating and Provisioning a WebLogic Managed Server Instance" to create and provision a new WLS Managed Server before deploying.

Before deploying, you must:

- Prepare the application EAR file, as described in Section 7.1.2, "Preparing the Application EAR File."
- Prepare the target environment, as described in Section 7.1.3, "Preparing the Target Environment."

After preparing the EAR file and the target environment, continue by deploying the application as described in Section 7.1.4, "Deploying the Application to a WebLogic Managed Server Instance."

7.1.2 Preparing the Application EAR File

Before you deploy an application, you must first create a deployment profile. The deployment profile packages or archives the custom WebCenter 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 Custom WebCenter Application to a WebLogic Managed Server" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*.

7.1.2.1 EAR File Contents

The EAR file packages multiple information artifacts, which include:

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

an application with registered producers is packaged. This customization data is packaged with the rest of the metadata of a custom WebCenter application.

7.1.3 Preparing the Target Environment

Before deploying a custom WebCenter application, you must create a WebLogic Managed Server instance and provision it with a required set of shared libraries. You must also create and register a Metadata Service (MDS) repository to store application metadata such as page personalizations and customizations. Finally, you must prepare the target environment so that it can host the deployed application.

> **Note:** Oracle does not recommend deploying custom WebCenter applications to any of the three preconfigured Managed Servers created during the installation, or to the Administration Server. For custom WebCenter applications, follow the process described in Section 7.1.3.1, "Creating and Provisioning a WebLogic Managed Server Instance" to create and provision a new WLS Managed Server, and Section 7.1.3.2, "Creating and Registering the Metadata Service Repository" to create and register the MDS repository before configuring your target environment and deploying your application.

This section includes the following topics:

- Section 7.1.3.1, "Creating and Provisioning a WebLogic Managed Server Instance"
- Section 7.1.3.2, "Creating and Registering the Metadata Service Repository"
- Section 7.1.3.3, "Configuring the Target Environment"

7.1.3.1 Creating and Provisioning a WebLogic Managed Server Instance

You can create a WebLogic Managed Server instance using the WLS Administration Console, or using Fusion Middleware Control. You can also create a WebLogic Managed Server instance and provision it using WLST commands in a Jython script. A sample Jython script that you can modify to suit the needs of your local environment is available for download from the Oracle Technology Network (OTN). Using a script is a good approach in circumstances where new Managed Servers must be created on an on-going basis.

These three options are described in the following sections:

- Section 7.1.3.1.1, "Creating and Provisioning a WebLogic Managed Server Using a Jython Script"
- Section 7.1.3.1.2, "Creating and Provisioning a WebLogic Managed Server Using the WLS Administration Console"
- Section 7.1.3.1.3, "Creating a WebLogic Managed Server Using Fusion Middleware Control"

7.1.3.1.1 Creating and Provisioning a WebLogic Managed Server Using a Jython Script

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

```
http://www.oracle.com/technology/products/webcenter/release11_
demos.html
```

under Administration Samples. The example script creates a new WebLogic Managed Server instance, deploys the shared libraries required to run a WebCenter application, and checks that the new Managed Server is ready for deployment.

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

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

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

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

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

5. Run the script from your *`MW_HOME`*`/as11r1wc/common/bin` folder:

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

6. Start the newly created WebLogic Managed Server using the following command:

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

   Where:

- *custom_server_id* is the name of the new Managed Server you created (for example, CustomAppServer3).
- *server_ip_addr* is the IP address of the administration server.
- *server_port_num* is the port number of the administration server.
- *user_name* is the user name to access the server (for example, weblogic).
- *password* is the password to access the server (for example, weblogic).

7. Once the Managed Server is started, check that the schema is registered (the registered MDS schema should appear when you click your WLS domain in Fusion Middleware Control).

   You can now continue to deploy your custom WebCenter application as described in Section 7.1.4, "Deploying the Application to a WebLogic Managed Server Instance," or portlet producer application as described in Section 21.8, "Deploying Portlet Producer Applications."

7.1.3.1.2 Creating and Provisioning a WebLogic Managed Server Using the WLS Administration Console

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

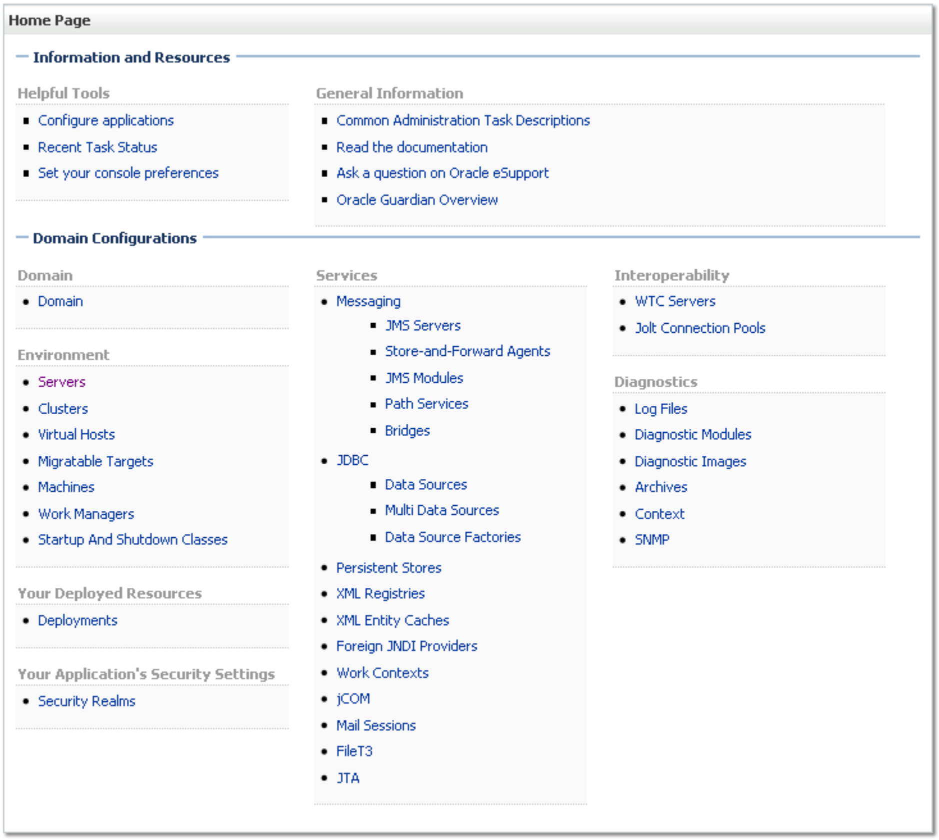
To create a WebLogic Managed Server using the WLS Administration Console:

1. Log in to the WLS Administration Console.

   For information on logging into the WLS Administration Console, see Section 1.12.2, "Oracle WebLogic Server Administration Console."

2. Navigate to the WLS Administration Console's Home page (see Figure 7–1).

Figure 7–1 WLS Administration Console Home Page



Home Page

Information and Resources

Helpful Tools

- Configure applications
- Recent Task Status
- Set your console preferences

General Information

- Common Administration Task Descriptions
- Read the documentation
- Ask a question on Oracle eSupport
- Oracle Guardian Overview

Domain Configurations

Domain

- Domain

Environment

- Servers
- Clusters
- Virtual Hosts
- Migratable Targets
- Machines
- Work Managers
- Startup And Shutdown Classes

Your Deployed Resources

- Deployments

Your Application's Security Settings

- Security Realms

Services

- Messaging
  - JMS Servers
  - Store-and-Forward Agents
  - JMS Modules
  - Path Services
  - Bridges
- JDBC
  - Data Sources
  - Multi Data Sources
  - Data Source Factories
- Persistent Stores
- XML Registries
- XML Entity Caches
- Foreign JNDI Providers
- Work Contexts
- jCOM
- Mail Sessions
- FileT3
- JTA

Interoperability

- WTC Servers
- Jolt Connection Pools

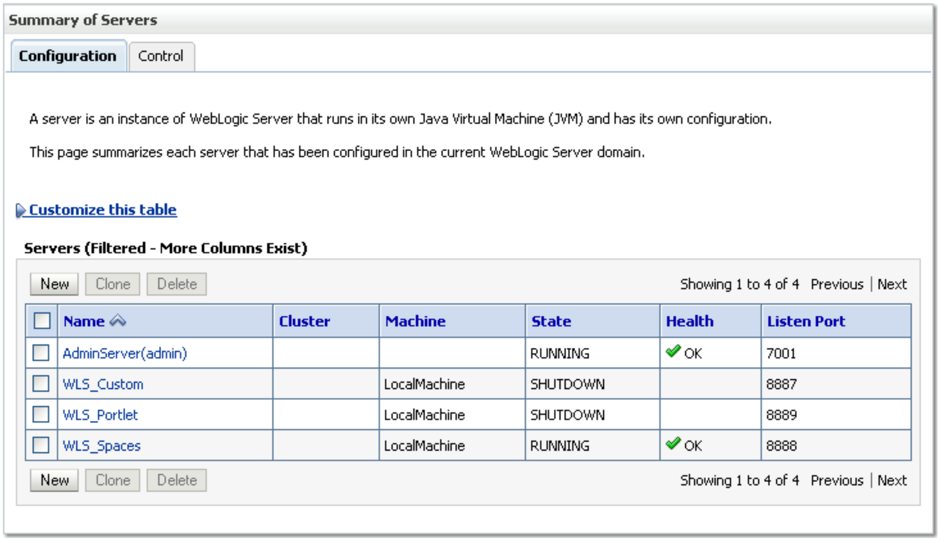
Diagnostics

- Log Files
- Diagnostic Modules
- Diagnostic Images
- Archives
- Context
- SNMP

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

   The Summary of Servers pane displays (see Figure 7–2).

Figure 7–2 Summary of Servers Pane



Summary of Servers

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.

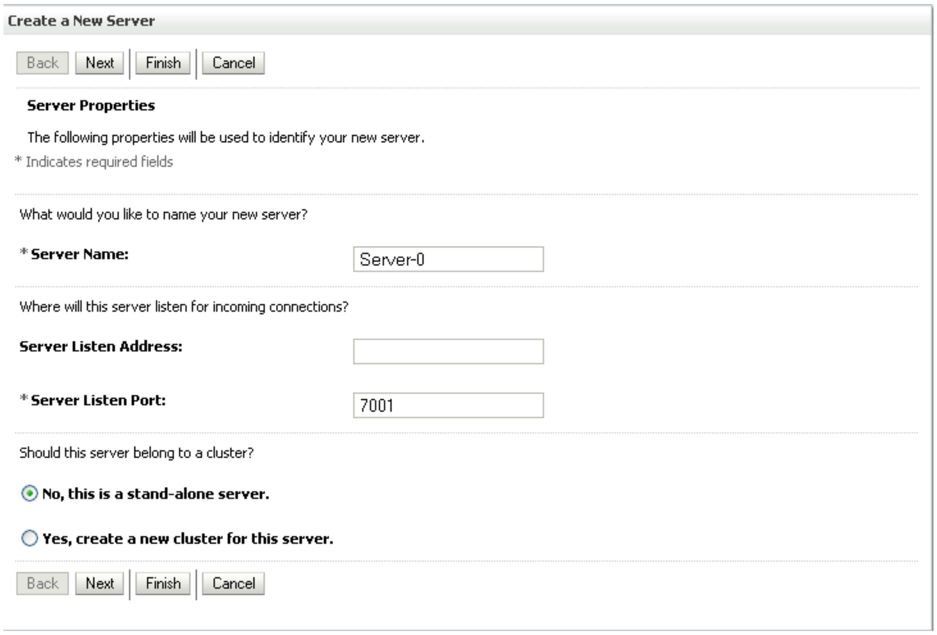
Servers (Filtered - More Columns Exist)

□	Name	Cluster	Machine	State	Health	Listen Port
□	AdminServer(admin)			RUNNING	✓ OK	7001
□	WLS_Custom		LocalMachine	SHUTDOWN		8887
□	WLS_Portlet		LocalMachine	SHUTDOWN		8889
□	WLS_Spaces		LocalMachine	RUNNING	✓ OK	8888

4. On the Summary of Servers pane, click **New** to create a WebLogic Managed Server instance.

   The Create a New Server pane displays (see Figure 7–3).

Figure 7–3 Create a New Server pane



Create a New Server

Server Properties

The following properties will be used to identify your new server.

* Indicates required fields

What would you like to name your new server?

* **Server Name:** Server-0

Where will this server listen for incoming connections?

Server Listen Address:

* **Server Listen Port:** 7001

Should this server belong to a cluster?

● **No, this is a stand-alone server.**

○ **Yes, create a new cluster for this server.**

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

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

6. Click **Finish**, then **Save** to generate the new Managed Server.

7. On the Domain Structure pane, click **Deployment**.

   In this step, we provision the new Managed Server with the shared libraries required to run a custom WebCenter application. Several shared libraries are deployed, but you must ensure that the required libraries are targeted to the newly created Managed Server.

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

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

For a custom WebCenter application that consumes portlets and services *only,* you must deploy the following libraries to the new Managed Server or cluster:

- content-management-cmis-rest-app-lib(10.3.2,10.3.2)
- content-management-cmis-rest-web-lib(10.3.2,10.3.2)
- content-management-faces-web-lib(10.3.2,10.3.2)
- content-management-web-lib(10.3.2,10.3.2)
- jaxrs-framework-web-lib(10.3.2,10.3.2)
- jersey-web-lib(1.0,1.0.2)
- oracle-ridc-client-app-lib(10.3.2,10.3.2)
- oracle-ucm-spi-app-lib(10.3.2,10.3.2)
- p13n-app-lib-base(10.3.2,10.3.2)
- p13n-core-web-lib(10.3.2,10.3.2)
- vcr-app-lib(10.3.2,10.3.2)
- adf.oracle.domain(1.0,11.1.1.0.0)
- adf.oracle.domain.webapp(1.0,11.1.1.1.0)
- jsf(1.2,1.2.9.0)
- jstl(1.2,1.2.0.1)
- ohw-rcf(5,5.0)
- ohw-uix(5,5.0)
- UIX(11,11.1.1.1.0)
- oracle.adf.dconfigbeans(1.0,11.1.1.0.0)
- oracle.adf.management(1.0,11.1.1.1.0)
- oracle.dconfig-infra
- oracle.jrf.system.filter
- oracle.jsp.next(11.1.1,11.1.1)
- oracle.sdp.client(11.1.1,11.1.1)
- oracle.soa.workflow.wc(11.1.1,11.1.1)
- oracle.webcenter.composer(11.1.1,11.1.1)
- oracle.webcenter.framework(11.1.1,11.1.1)
- oracle.webcenter.framework.view(11.1.1,11.1.1)
- oracle.webcenter.jive.dependency(11.1.1,11.1.1)
- oracle.webcenter.skin(11.1.1,11.1.1)
- oracle.wsm.seedpolicies(11.1.1,11.1.1)
- oracle.portlet-producer.jpdk(11.1.1,11.1.1)
- oracle.portlet-producer.wsrp(11.1.1,11.1.1)

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

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

- `adf.oracle.domain(1.0,11.1.1.0.0)`
- `adf.oracle.domain.webapp(1.0,11.1.1.1.0)`
- `jsf(1.2,1.2.9.1)`
- `jstl(1.2,1.2.0.1)`
- `ohw-rcf(5,5.0)`
- `ohw-uix(5,5.0)`
- `UIX(11,11.1.1.1.0)`
- `oracle.adf.dconfigbeans(1.0,11.1.1.0.0)`
- `oracle.dconfig-infra`
- `oracle.jrf.system.filter`
- `oracle.jsp.next(11.1.1,11.1.1)`
- `oracle.webcenter.skin(11.1.1,11.1.1)`
- `oracle.wsm.seedpolicies(11.1.1,11.1.1)`
- `oracle.portlet-producer.jpdk(11.1.1,11.1.1)`
- `oracle.portlet-producer.wsrp(11.1.1,11.1.1)`

8. In addition, for both WebCenter and portlet producer applications, you must deploy the following applications:

   - `DMS application`
   - `wsm-pm`

   For each shared library or application to add:

   - Click the library or application link.
   - Open the Target tab for the library or application.
   - Supply the target to the newly created Managed Server.

9. Select the checkbox of the new Managed Server and click **Save**.

10. On the Domain Structure pane, expand Environment and click **Startup and Shutdown classes**. The following classes should show as available:

    - `Audit Loader Startup Class`
    - `DMS-Startup`
    - `DMS-Shutdown`
    - `JMX Framework Startup Class`

- `JOC-Shutdown`
- `JOC-Startup`
- `JPS-Startup Class`
- `JRF Startup Class`
- `ODL-Startup`
- `OWSM Startup Class`

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

11. For each class in the list above:
    - Click the class name.
    - On the Target tab, check the newly created Managed Server.
    - Click **Save**.
12. When all the shared libraries and application assignments are complete, do one of the following:
    - Start the new Managed Server using Fusion Middleware Control as described in Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."
    - Start the new Managed Server by opening a terminal window and invoking the following command from your domain's `/bin` directory (under *`MW_HOME`*`/user_projects` unless the default location has been changed):

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

      Where:

      – `custom_server_id` is the name of the new Managed Server you created (for example, `CustomAppServer3`).

      – `server_ip_addr` is the IP address of the administration server.

      – `server_port_num` is the port number of the administration server.

      – `user_name` is the user name to access the server (for example, `weblogic`).

      – `password` is the password to access the server (for example, `weblogic`).

      Once the Managed Server is started, you can continue to deploy your WebCenter application as described in Section 7.1.4, "Deploying the Application to a WebLogic Managed Server Instance," or portlet producer application as described in Section 21.8, "Deploying Portlet Producer Applications."

7.1.3.1.3 Creating a WebLogic Managed Server Using Fusion Middleware Control

Use Fusion Middleware Control to create a WebLogic Managed Server instance for custom WebCenter application deployment.

> **Note:** Although you can create a WebLogic Managed Server using Fusion Middleware Control, you must use the WebLogic Administration Console to provision it as described in Section 7.1.3.1.2, "Creating and Provisioning a WebLogic Managed Server Using the WLS Administration Console," or modify the Jython script described in Section 7.1.3.1.1, "Creating and Provisioning a WebLogic Managed Server Using a Jython Script" to provision the shared libraries required to run a custom WebCenter application.

To create a WebLogic Managed Server using Fusion Middleware Control:

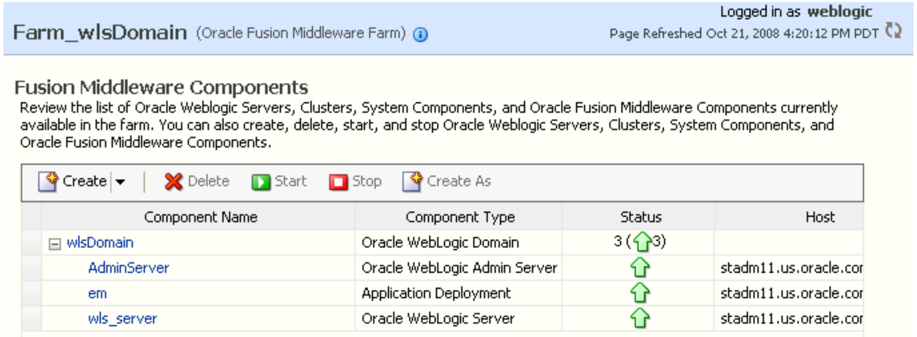
1. Log in to Fusion Middleware Control.

   See Section 6.1, "Displaying Fusion Middleware Control Console."

2. From the Farm menu, choose **Create/Delete Component**s.

   The Fusion Middleware Components page opens (Figure 7–4).

Figure 7–4 Fusion Middleware Components Page


Logged in as **weblogic**
Farm_wlsDomain (Oracle Fusion Middleware Farm)
Page Refreshed Oct 21, 2008 4:20:12 PM PDT
Create
Delete
Start
Stop
Create As

Fusion Middleware Components

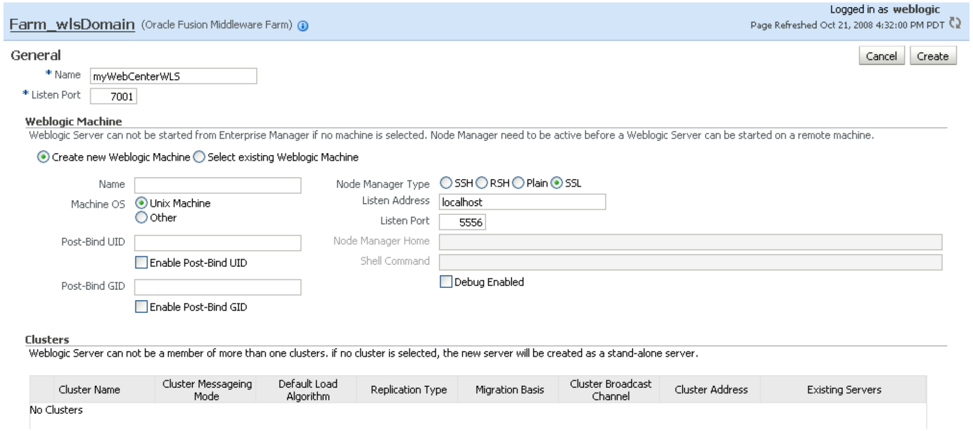
Review the list of Oracle Weblogic Servers, Clusters, System Components, and Oracle Fusion Middleware Components currently available in the farm. You can also create, delete, start, and stop Oracle Weblogic Servers, Clusters, System Components, and Oracle Fusion Middleware Components.

Component Name	Component Type	Status	Host
⊟ wlsDomain	Oracle WebLogic Domain	3 (⇧3)	
AdminServer	Oracle WebLogic Admin Server	⇧	stadm11.us.oracle.cor
em	Application Deployment	⇧	stadm11.us.oracle.cor
wls_server	Oracle WebLogic Server	⇧	stadm11.us.oracle.cor

3. From the Create menu, select **WebLogic Server**.

4. Enter a unique name for the WebLogic server (for example, `myWebCenterWLS`, as shown in Figure 7–5).

Figure 7–5 Create WebLogic Server Page


Logged in as **weblogic**
Farm_wlsDomain (Oracle Fusion Middleware Farm)
Page Refreshed Oct 21, 2008 4:32:00 PM PDT
Cancel
Create

General

* Name: myWebCenterWLS

* Listen Port: 7001

Weblogic Machine

Weblogic Server can not be started from Enterprise Manager if no machine is selected. Node Manager need to be active before a Weblogic Server can be started on a remote machine.

● Create new Weblogic Machine ○ Select existing Weblogic Machine

Name:

Machine OS: ● Unix Machine ○ Other

Post-Bind UID:

□ Enable Post-Bind UID

Post-Bind GID:

□ Enable Post-Bind GID

Node Manager Type: ○ SSH ○ RSH ○ Plain ● SSL

Listen Address: localhost

Listen Port: 5556

Node Manager Home:

Shell Command:

□ Debug Enabled

Clusters

Weblogic Server can not be a member of more than one clusters. if no cluster is selected, the new server will be created as a stand-alone server.

Cluster Name	Cluster Messageing Mode	Default Load Algorithm	Replication Type	Migration Basis	Cluster Broadcast Channel	Cluster Address	Existing Servers
No Clusters							

5. Under Weblogic Machine, create or select the application server instance where this WebLogic Managed Server instance should be created.
6. Click **Create**.
7. When the Confirmation page displays, click **Close**.
8. In the Fusion Middleware Components page, select the new WebLogic Managed Server instance, and click **Start**.
9. Continue by provisioning the shared libraries as described in Section 7.1.3.1.2, "Creating and Provisioning a WebLogic Managed Server Using the WLS Administration Console" omitting the steps (steps 4 to 7) for creating the Managed Server, or using a modified version of the Jython script described in Section 7.1.3.1.1, "Creating and Provisioning a WebLogic Managed Server Using a Jython Script."

7.1.3.2 Creating and Registering the Metadata Service Repository

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

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 7.1.4, "Deploying the Application to a WebLogic Managed Server Instance").

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

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

This section contains the following subsections:

- Creating an MDS Schema Using the Repository Creation Utility
- Registering an MDS Schema Using Fusion Middleware Control
- Registering an MDS Schema Using WLST

7.1.3.2.1 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.

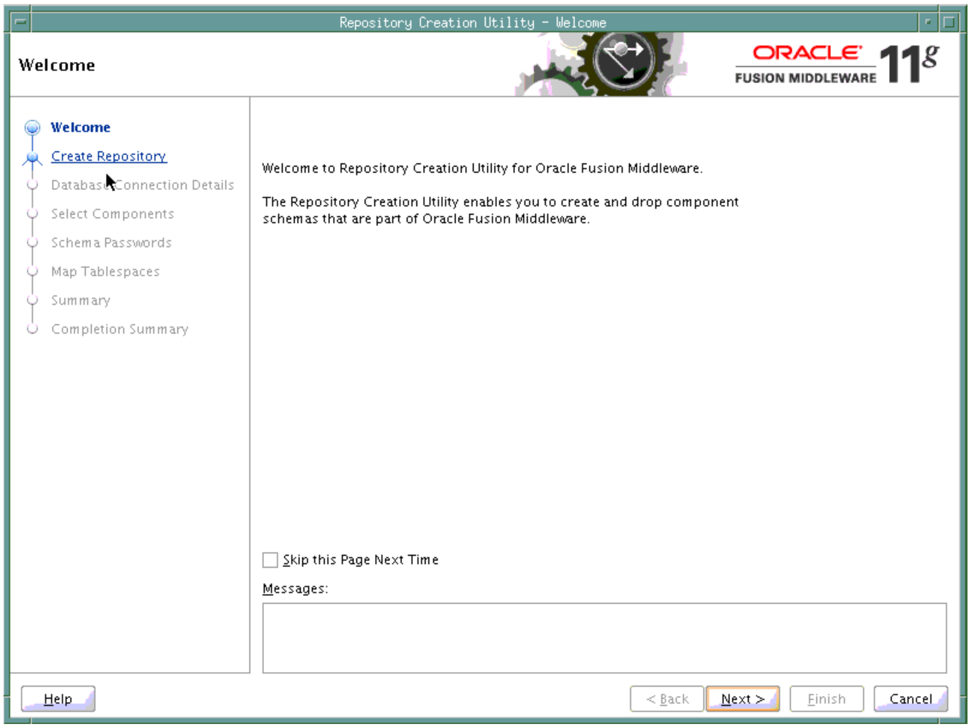
To create the MDS schema:

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

```
rcu
```

The RCU Welcome page displays (see Figure 7–6).

Figure 7–6 RCU Welcome Page



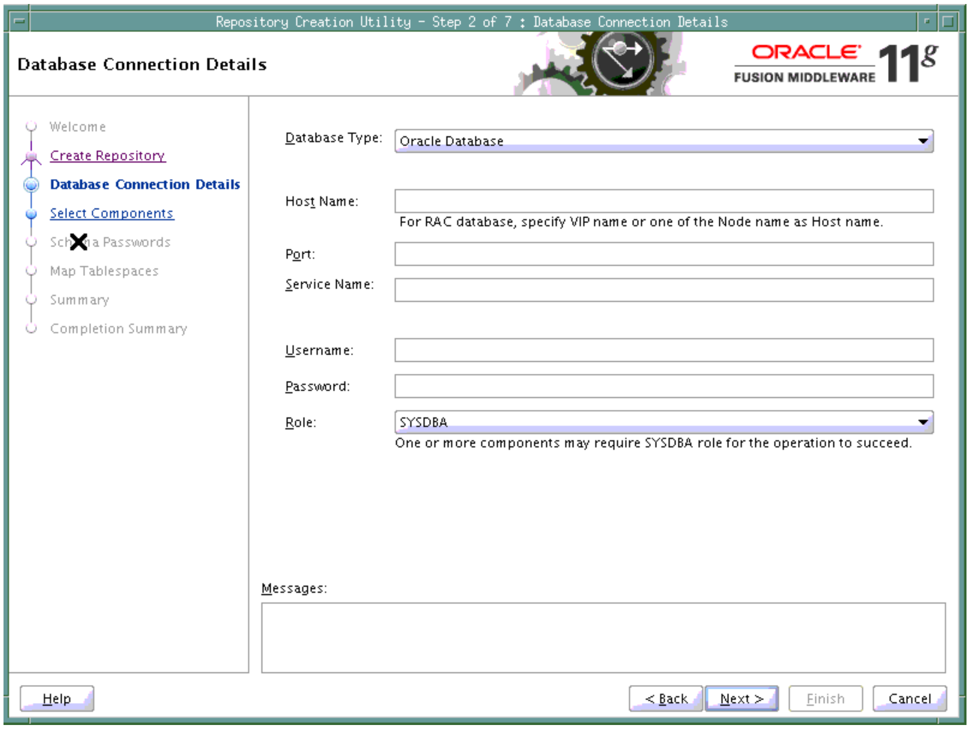
Welcome to Repository Creation Utility for Oracle Fusion Middleware.

The Repository Creation Utility enables you to create and drop component schemas that are part of Oracle Fusion Middleware.

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

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

Figure 7–7 Database Connection Details Page



Database Type: Oracle Database

Host Name:

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

Port:

Service Name:

Username:

Password:

Role: SYSDBA

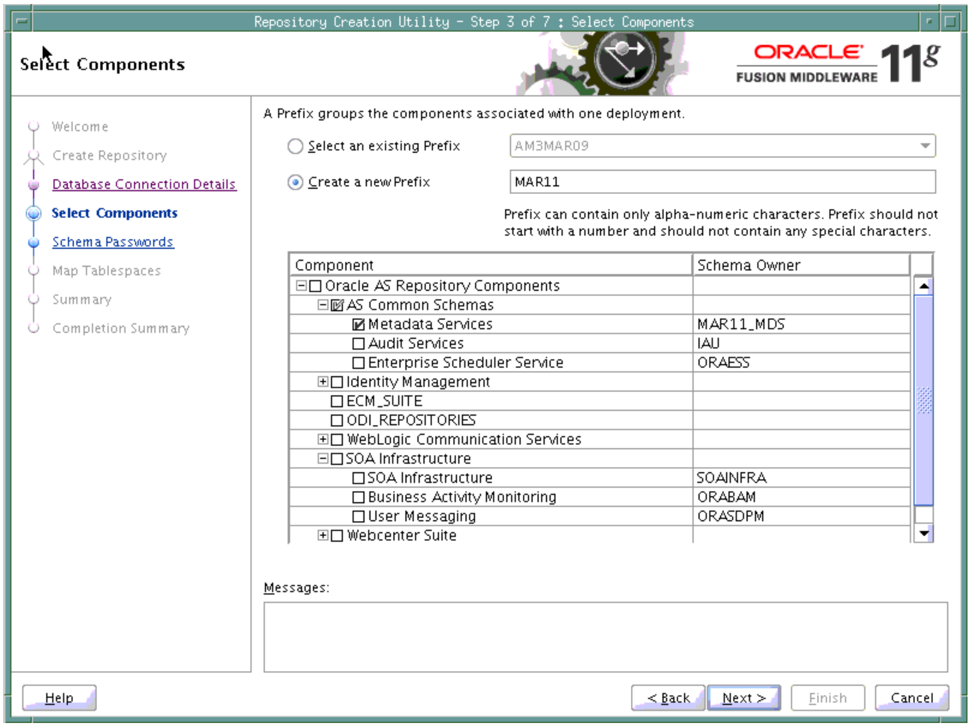
One or more components may require SYSDBA role for the operation to succeed.

Messages:

4. Provide the connection details for the database to which to add the schema by selecting the **Database Type**, entering the **Host Name**, **Port**, **Service Name**, **Username** and **Password** and clicking **Next**.
5. Click **OK** when prompted by the Prerequisites pop-up.

   The Select Components page displays (see Figure 7–8).

Figure 7–8 Select Components Page



A Prefix groups the components associated with one deployment.

○ Select an existing Prefix AM3MAR09

● Create a new Prefix MAR11

Prefix can contain only alpha-numeric characters. Prefix should not start with a number and should not contain any special characters.

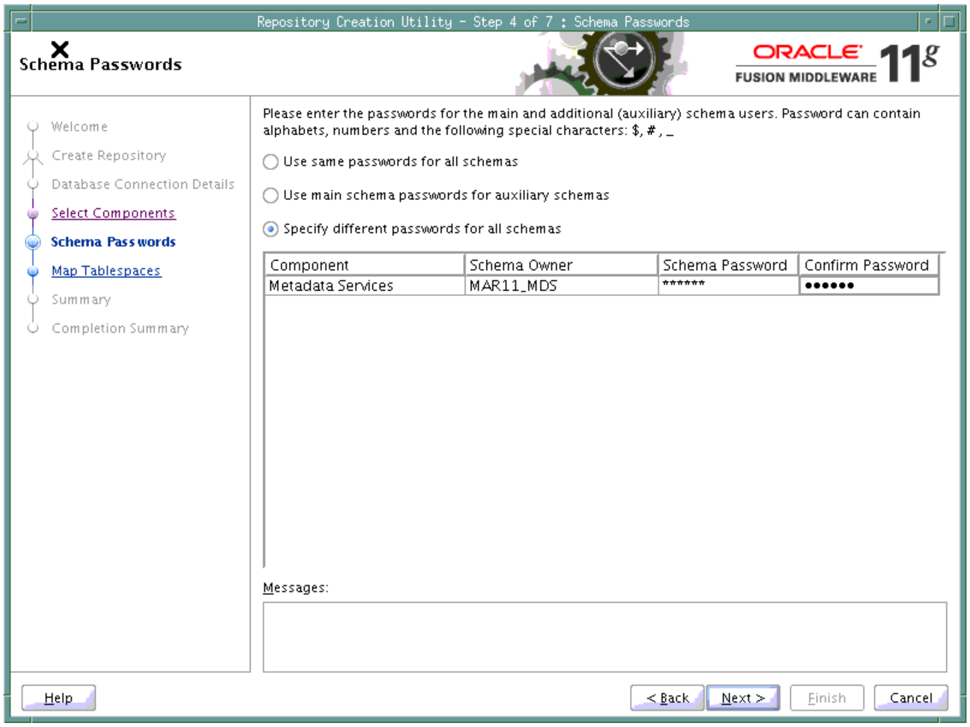
Component	Schema Owner
⊟☐ Oracle AS Repository Components	
⊟☒ AS Common Schemas	
☑ Metadata Services	MAR11_MDS
☐ Audit Services	IAU
☐ Enterprise Scheduler Service	ORAESS
⊞☐ Identity Management	
☐ ECM_SUITE	
☐ ODI_REPOSITORIES	
⊞☐ WebLogic Communication Services	
⊟☐ SOA Infrastructure	
☐ SOA Infrastructure	SOAINFRA
☐ Business Activity Monitoring	ORABAM
☐ User Messaging	ORASDPM
⊞☐ Webcenter Suite	

Messages:

6. Check **Create a New Prefix** and enter a prefix to be prepended to the schema name.
7. Check the **Metadata Services** component. All other components should be left unchecked.
8. Click **Next**, and click **OK** when prompted by the Prerequisites pop-up.

   The Schema Passwords page displays (see Figure 7–9).

Figure 7–9 Schema Passwords Page



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:

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**.

7.1.3.2.2 Registering an MDS Schema Using Fusion Middleware Control

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

To register an MDS repository using Fusion Middleware Control:

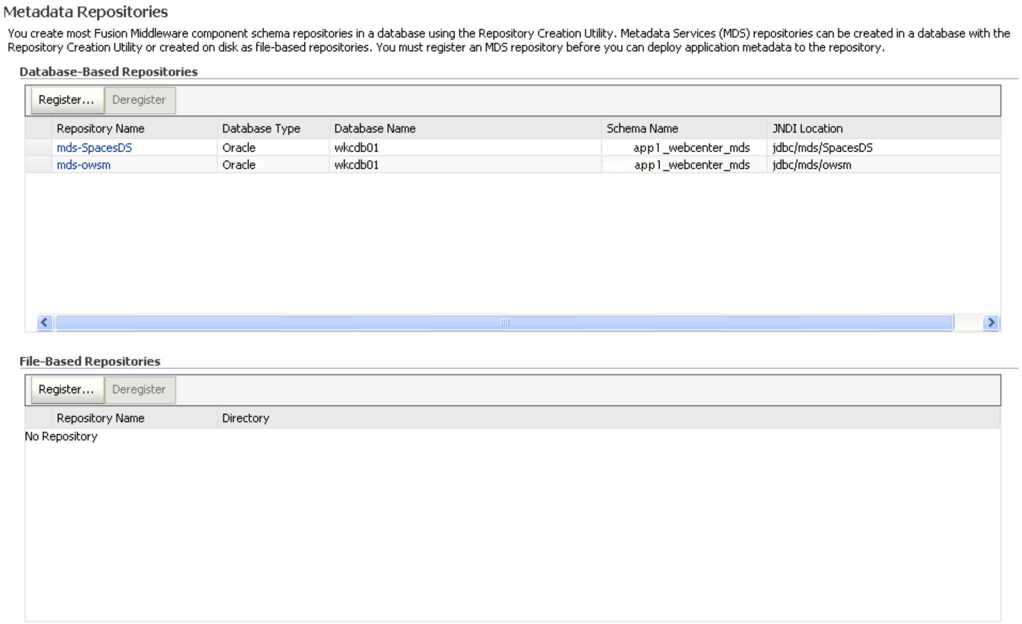
1. Open Fusion Middleware Control and log in to the target domain.

   For information on logging into Fusion Middleware Control, see Section 6, "Starting Enterprise Manager Fusion Middleware Control."

2. In the Navigation pane, expand the **farm**, then **WebLogic Domain**.
3. Select the domain to which you want to deploy.
4. From the WebLogic Domain menu, select **Metadata Repositories**.

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

Figure 7–10 Metadata Repositories Page



Metadata Repositories

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

Database-Based Repositories

Register... Deregister

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

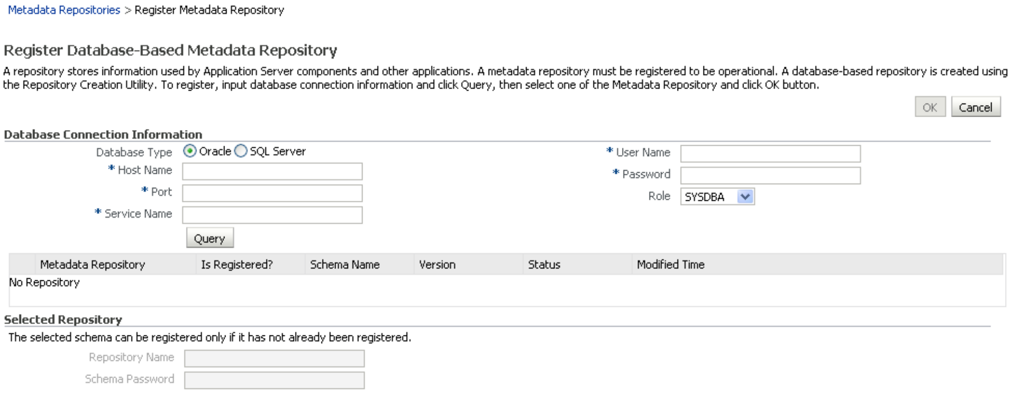
Register... Deregister

Repository Name	Directory
No Repository	

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

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

Figure 7–11 Register Database-based Metadata Repository Page



Metadata Repositories > Register Metadata Repository

Register Database-Based Metadata Repository

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

OK Cancel

Database Connection Information

Database Type	● Oracle ○ SQL Server	* User Name	
* Host Name		* Password	
* Port		Role	SYSDBA
* Service Name			

Query

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.

7.1.3.2.3 Registering an MDS Schema Using WLST

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

To register an MDS schema using WLST:

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

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

   Where:

   - *mds_name* is the name of the MDS schema to register.
   - *db_vendor* is the vendor of the database being used.
   - *host_name* is the host ID of the Database Server.
   - *port_number* is the port number of the Database Server.
   - *db_name* is the name of the database being used to store the MDS.
   - *username* is the database schema user name.
   - *password* is the database schema password.
   - *target_server* is the name of the target server. For multiple targets, separate the target server names with a comma. Be sure to include the WLS administration server in the list of targets so that the MDS database repository name appears in 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')
```

7.1.3.3 Configuring the Target Environment

After your target Managed Server has been created and provisioned, but *before* you deploy your custom WebCenter application, you must configure your JDBC database connections, and connections to the Identity Store and Policy and Credential Store.

This section contains the following subsection:

- Section 7.1.3.3.1, "Configuring the JDBC Data Source"

7.1.3.3.1 Configuring the JDBC Data Source

If your custom WebCenter application contains JDBC database connections, you must choose how JDeveloper migrates those database connections to the Oracle WebLogic Managed Server. Through JDeveloper, you can configure the JDBC data source as either an application-level data source with password indirection, or as a global data source. Be sure to choose Global data source, by unchecking the **Auto Generate and Synchronize weblogic-jdbc.xml Descriptors During Deployment** checkbox in the Application Properties dialog. For more information about configuring a custom WebCenter application's JDBC database connections, see "Packaging the Database Connections" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*.

7.1.4 Deploying the Application to a WebLogic Managed Server Instance

Before deploying a custom WebCenter application archive, it is important to ensure that all the required shared libraries are published in the target WebLogic Managed Server instance, and that the database connections have been configured.

> **Note:** Oracle does not recommend deploying custom WebCenter applications to any of the three preconfigured Managed Servers created during the installation, or to the Administration Server. For custom WebCenter applications created in JDeveloper, follow the process described in Section 7.1.3.2, "Creating and Registering the Metadata Service Repository" and Section 7.1.3.1, "Creating and Provisioning a WebLogic Managed Server Instance" 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 `WLS_Portlet` server.

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

- Section 7.1.4.1, "Deploying Applications Using Oracle JDeveloper"
- Section 7.1.4.2, "Deploying Applications Using Fusion Middleware Control"
- Section 7.1.4.3, "Deploying Applications Using WLST"
- Section 7.1.4.4, "Deploying Applications Using the WLS Administration Console"
- Section 7.1.4.5, "Saving and Reusing the Deployment Plan"

As explained in Section 7.1.2, "Preparing the Application EAR File," the packaged EAR file consists of several information artifacts, which includes the application bits, the application configuration, the application metadata, and the portlet customizations.

During the deployment, these information artifacts 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 7–1:

Table 7–1 Information Artifact Target Stores

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

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

Although the application deployment fails if the MDS location is incorrect or not supplied, the application will deploy if the target producer is incorrectly specified. 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 21.2.1, "Registering a WSRP Producer Using Fusion Middleware Control" and Section 21.4.1, "Registering an Oracle PDK-Java Producer Using Fusion Middleware Control") or WLST commands (see Section 21.2.2, "Registering a WSRP Producer Using WLST" or Section 21.4.2, "Registering an Oracle PDK-Java Producer Using WLST"), and redeploy the application.
- Export and import the portlet customization using WLST commands (see Section 31.2, "Exporting and Importing Custom WebCenter 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.

7.1.4.1 Deploying Applications Using Oracle JDeveloper

You can deploy custom WebCenter 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 Custom WebCenter Application to a Managed Server" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*.

7.1.4.2 Deploying Applications Using Fusion Middleware Control

When deploying a custom WebCenter application using Fusion Middleware Control you must know the location of the WebCenter application archive, and whether a deployment plan exists for the application. See Section 7.1.4.5, "Saving and Reusing the Deployment Plan" for more information about deployment plans.

To deploy a custom WebCenter application using Fusion Middleware Control:

1. Log in to Fusion Middleware Control.

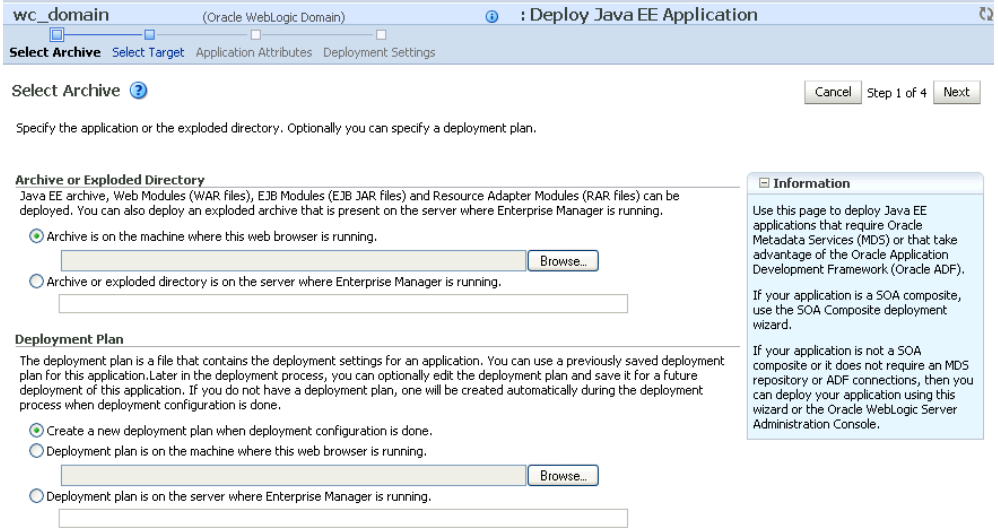
   See Section 6.1, "Displaying Fusion Middleware Control Console."

2. In the Navigation pane, expand **WebLogic Domain** and click the domain in which your target Managed Server was created.

3. From the WebLogic Domain menu, select **Application Deployment** > **Deploy**.

   The Select Archive page displays (see Figure 7–12).

Figure 7–12 Select Archive Page



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.

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.

4. In the Archive or Exploded Directory section, do one of the following:

   - Select **Archive is on the machine where this web browser is running** and enter the location of the archive or click **Browse** to find the archive file.
   - Select **Archive or exploded directory is on the server where Enterprise Manager is running** and enter the location of the archive or click **Browse** to find the archive file.

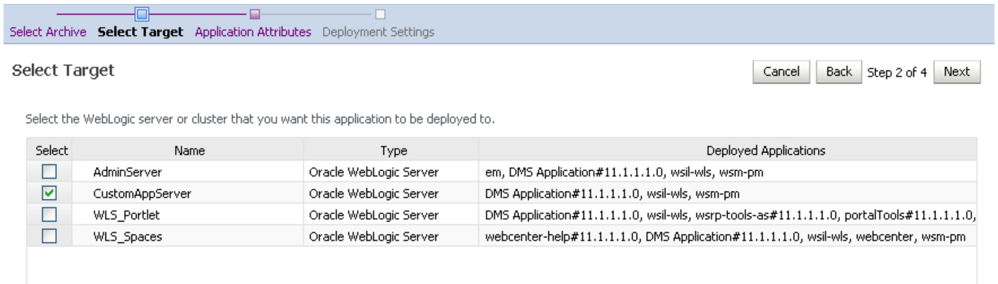
5. In the Deployment Plan section, do one of the following:

   - Select **Create a new deployment plan when deployment configuration is done** to automatically create a new deployment plan after the redeployment process.
   - Select **Deployment plan is on the machine where this web browser is running** and enter the path to the plan or click **Browse** to find the plan.
   - Select **Deployment plan is on the server where Enterprise Manager is running** and enter the path to the plan or click **Browse** to find the plan.

6. Click **Next**.

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

Figure 7–13 Select Target Page



Select Target

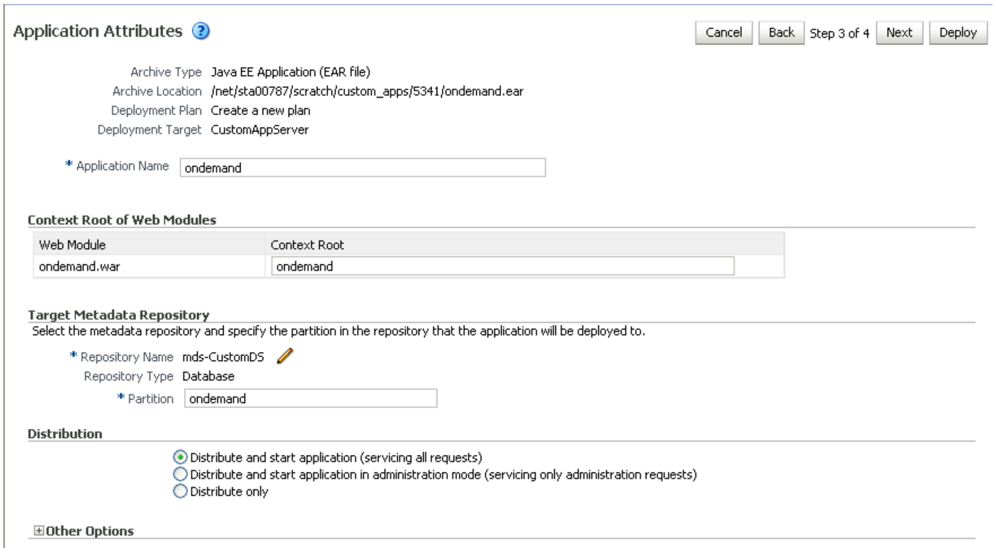
Select the WebLogic server or cluster that you want this application to be deployed to.

Select	Name	Type	Deployed Applications
□	AdminServer	Oracle WebLogic Server	em, DMS Application#11.1.1.1.0, wsil-wls, wsm-pm
☑	CustomAppServer	Oracle WebLogic Server	DMS Application#11.1.1.1.0, wsil-wls, wsm-pm
□	WLS_Portlet	Oracle WebLogic Server	DMS Application#11.1.1.1.0, wsil-wls, wsrp-tools-as#11.1.1.1.0, portalTools#11.1.1.1.0,
□	WLS_Spaces	Oracle WebLogic Server	webcenter-help#11.1.1.1.0, DMS Application#11.1.1.1.0, wsil-wls, webcenter, wsm-pm

7. Select the target server(s) to deploy the application to (see Section 7.1.4, "Deploying the Application to a WebLogic Managed Server Instance" for an overview of selecting the targets) and click **Next**.

   The Application Attributes page displays (see Figure 7–14).

Figure 7–14 Application Attributes Page



Application Attributes

Archive Type Java EE Application (EAR file)
Archive Location /net/sta00787/scratch/custom_apps/5341/ondemand.ear
Deployment Plan Create a new plan
Deployment Target CustomAppServer

* Application Name ondemand

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

Distribution

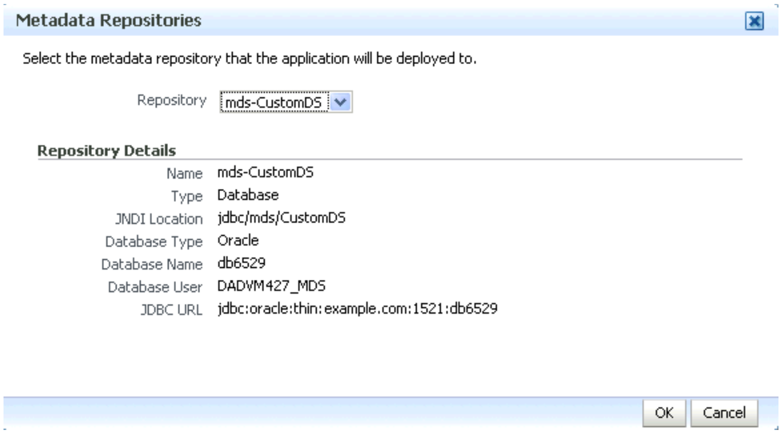
● Distribute and start application (servicing all requests)
○ Distribute and start application in administration mode (servicing only administration requests)
○ Distribute only

⊞Other Options

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 7–15. Use the Repository dropdown to select the required repository and then click **OK**.

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

Figure 7–15 Select Metadata Repository Window



Metadata Repositories

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

Repository: mds-CustomDS

Repository Details

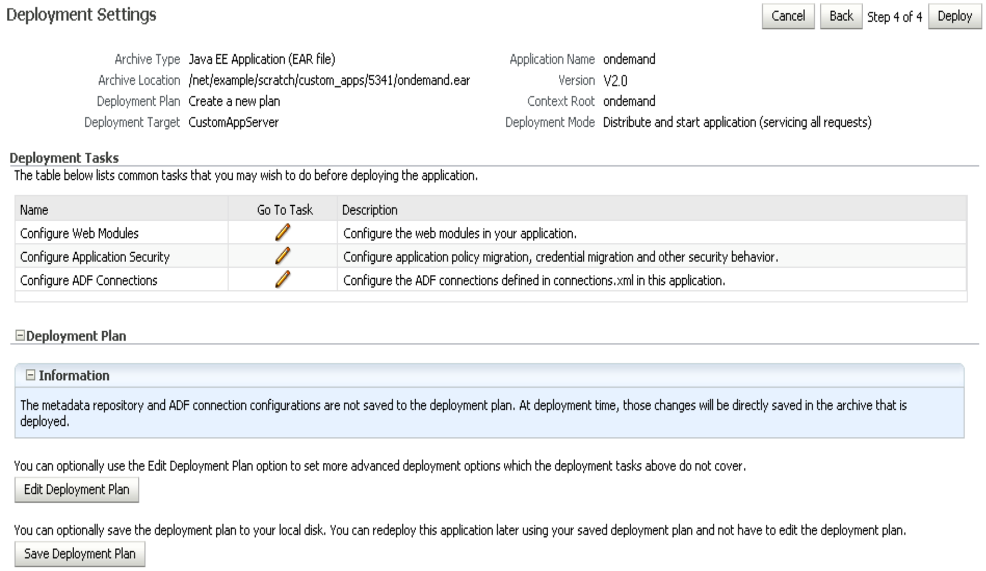
Name	mds-CustomDS
Type	Database
JNDI Location	jdbc/mds/CustomDS
Database Type	Oracle
Database Name	db6529
Database User	DADVM427_MDS
JDBC URL	jdbc:oracle:thin:example.com:1521:db6529

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 7–16).

Figure 7–16 Deployment Settings Page



Deployment Settings

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	CustomAppServer	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.

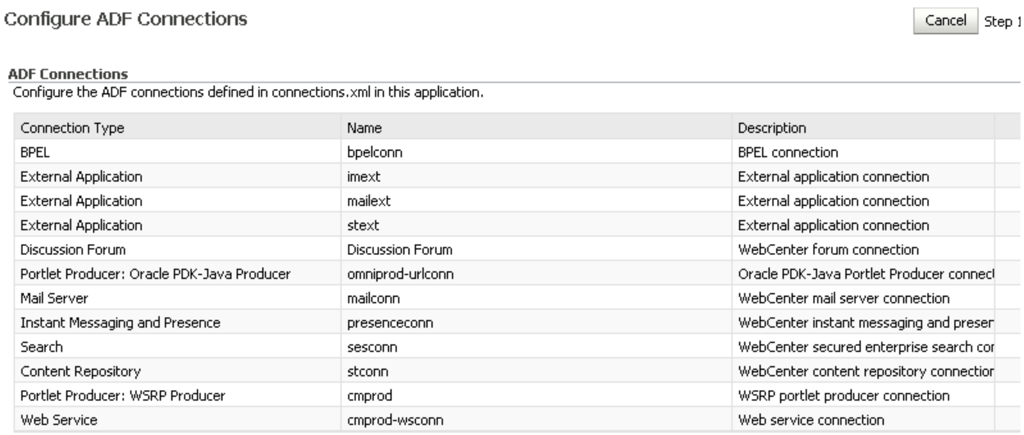
You can optionally save the deployment plan to your local disk. You can redeploy this application later using your saved deployment plan and not have to edit the deployment plan.

You have now provided the Target MDS location (described in Section 7.1.4, "Deploying the Application to a WebLogic Managed Server Instance").

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

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

Figure 7–17 Configure ADF Connections Page



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 connectior
Portlet Producer: WSRP Producer	cmprod	WSRP portlet producer connection
Web Service	cmprod-wsconn	Web service connection

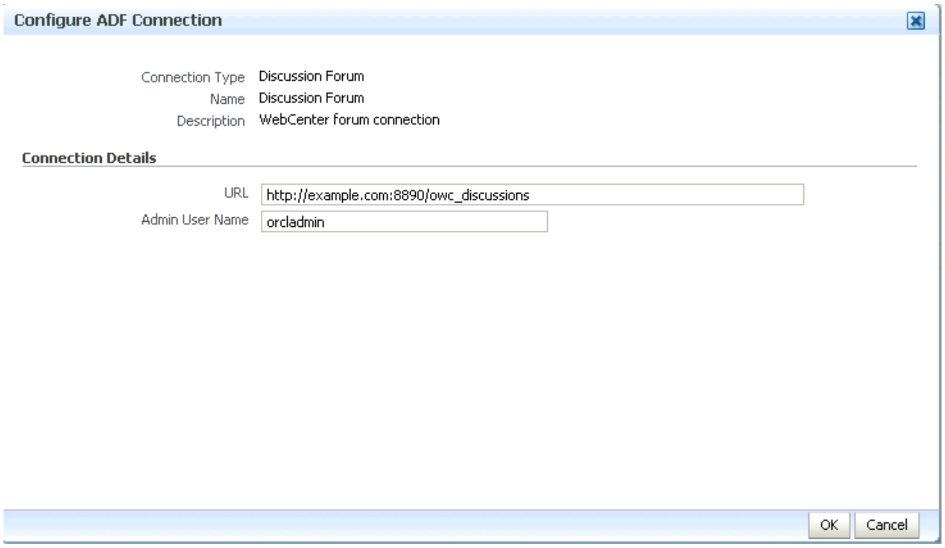
This screenshot shows the Configure ADF Connections page.

****

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

For a Discussion Forum connection (shown in Figure 7–18), for example, 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 7–18 Discussion Forum Connection Settings



Connection Type Discussion Forum
Name Discussion Forum
Description WebCenter forum connection

Connection Details

URL http://example.com:8890/owc_discussions
Admin User Name orcladmin

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 7.1.4, "Deploying the Application to a WebLogic Managed Server Instance".

> **Note:** If any target producers are not reachable as the application starts for the first time, the import 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 21.2.1, "Registering a WSRP Producer Using Fusion Middleware Control" and Section 21.4.1, "Registering an Oracle PDK-Java Producer Using Fusion Middleware Control") or WLST commands (see Section 21.2.2, "Registering a WSRP Producer Using WLST" or Section 21.4.2, "Registering an Oracle PDK-Java Producer Using WLST") to modify the producer URL endpoint, and then redeploy the application as described in Section 7.3.2, "Redeploying WebCenter Applications Using Fusion Middleware Control".

13. If required, specify additional deployment options such as the Web modules to include in your application or security migration settings.
14. 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 WebCenter 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:** When after deploying, you reconfigure connections for custom WebCenter applications, these post-deployment customizations are preserved in the MDS repository and do not need to be set again when you redeploy the application.

7.1.4.3 Deploying Applications Using WLST

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

To deploy a custom WebCenter application using WLST:

1. Start the WLST shell.

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

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

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

   Where:

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

     You should see the following message:

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

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

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

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

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

   ```
   archive.setAppMetadataRepository(repository='respository',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 custom WebCenter application using the WLST deploy command.

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

Where:

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

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

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

Note: Since WLST does not prompt you to modify connections during deployment, the connection information in the EAR file is used to identify the target producer location in the last start-up. If that location is unreachable, correct the location after deploying the application by bringing up the target producers and restarting the application. Migration of portlet customizations 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 21.2.1, "Registering a WSRP Producer Using Fusion Middleware Control" and Section 21.4.1, "Registering an Oracle PDK-Java Producer Using Fusion Middleware Control") or WLST commands (see Section 21.2.2, "Registering a WSRP Producer Using WLST" or Section 21.4.2, "Registering an Oracle PDK-Java Producer Using WLST") to modify the producer URL endpoint, and then redeploy the application as described in Section 7.3.2, "Redeploying WebCenter Applications Using Fusion Middleware Control."

7.1.4.4 Deploying Applications Using the WLS Administration Console

You can use the WLS Administration Console to deploy a custom WebCenter application or a portlet producer application. However, the Console does not offer a means to change ADF connections, including the essential MDS connection. To use the Console to deploy a WebCenter application, the MDS connection in the EAR file must be configured to the target deployment repository. Follow steps 1-5 in Section 7.1.4.3, "Deploying Applications Using WLST", then follow the steps below to deploy a custom WebCenter application or portlet producer application using the WLS Administration Console.

> **Note:** For custom WebCenter applications, follow the instructions for creating a new WebLogic Managed Server as described in Section 7.1.3.1, "Creating and Provisioning a WebLogic Managed Server Instance" before deploying. For portlet producer applications, you can optionally create a new WebLogic Managed Server or deploy to the `WLS_Portlet` server.

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

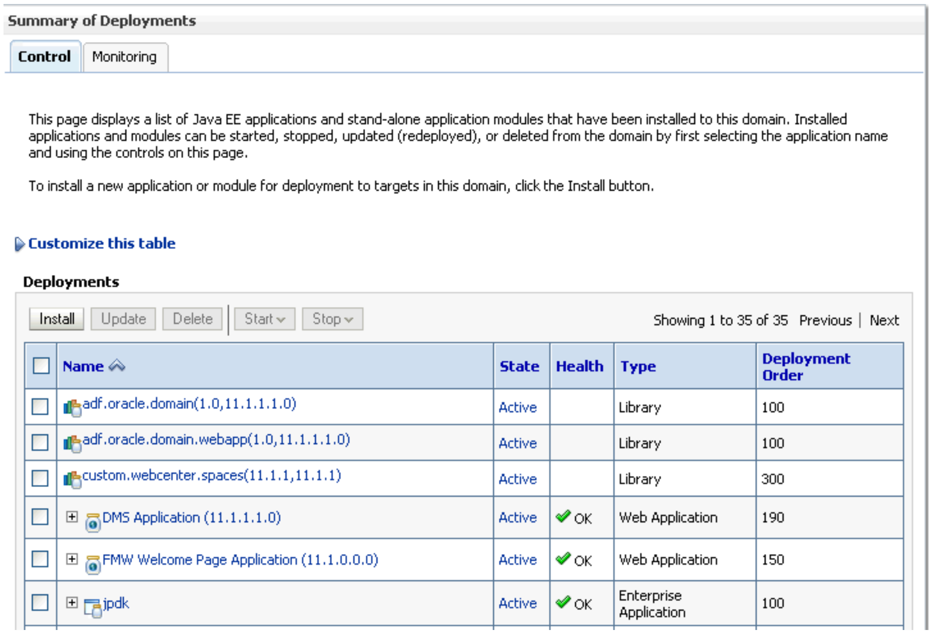
1. Log in to the WLS Administration Console.

   For information on logging into the WLS Administration Console, see Section 1.12.2, "Oracle WebLogic Server Administration Console."

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

   The Deployments Summary pane displays (see Figure 7–19).

Figure 7–19 Deployment Summary Pane



Summary of Deployments

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.

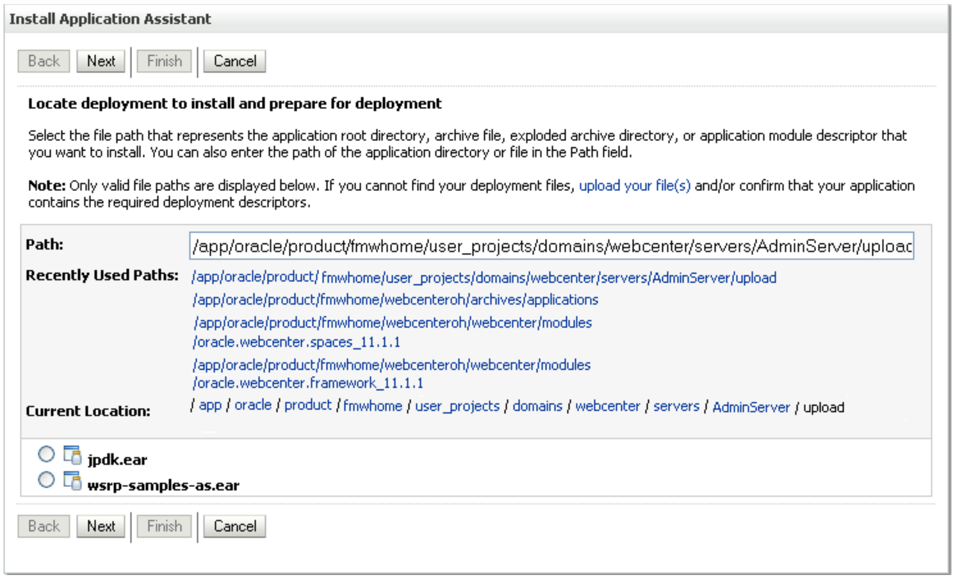
Deployments

□	Name	State	Health	Type	Deployment Order
□	adf.oracle.domain(1.0,11.1.1.1.0)	Active		Library	100
□	adf.oracle.domain.webapp(1.0,11.1.1.1.0)	Active		Library	100
□	custom.webcenter.spaces(11.1.1,11.1.1)	Active		Library	300
□	⊞ DMS Application (11.1.1.1.0)	Active	✓ OK	Web Application	190
□	⊞ FMW Welcome Page Application (11.1.0.0.0)	Active	✓ OK	Web Application	150
□	⊞ jpdk	Active	✓ OK	Enterprise Application	100

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

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

Figure 7–20 Install Application Assistant Page



Locate deployment to install and prepare for deployment

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

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

Path: /app/oracle/product/fmwhome/user_projects/domains/webcenter/servers/AdminServer/uploac

Recently Used Paths: /app/oracle/product/ fmwhome/user_projects/domains/webcenter/servers/AdminServer/upload
/app/oracle/product/fmwhome/webcenteroh/archives/applications
/app/oracle/product/fmwhome/webcenteroh/webcenter/modules
/oracle.webcenter.spaces_11.1.1
/app/oracle/product/fmwhome/webcenteroh/webcenter/modules
/oracle.webcenter.framework_11.1.1

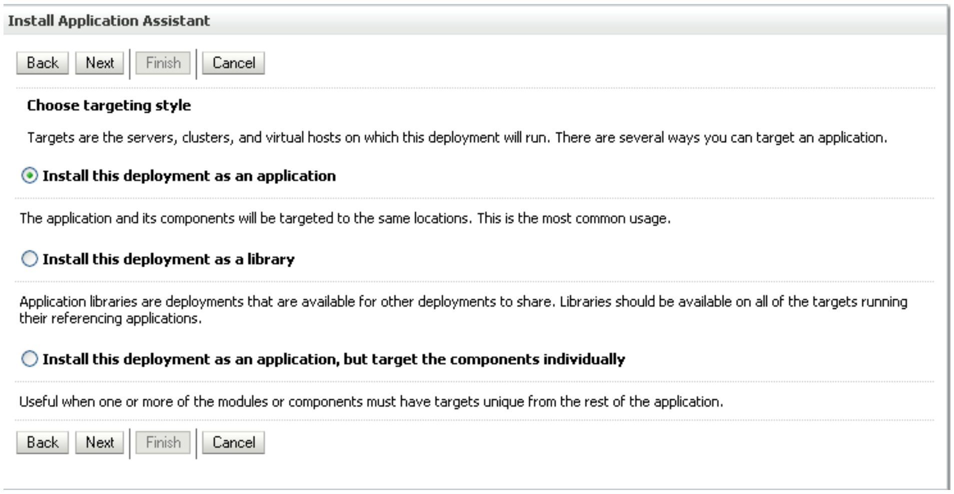
Current Location: / app / oracle / product / fmwhome / user_projects / domains / webcenter / servers / AdminServer / upload

○ **jpdk.ear**
○ **wsrp-samples-as.ear**

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

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

Figure 7–21 Install Application Assistant - Page 2



Choose targeting style

Targets are the servers, clusters, and virtual hosts on which this deployment will run. There are several ways you can target an application.

● **Install this deployment as an application**

The application and its components will be targeted to the same locations. This is the most common usage.

○ **Install this deployment as a library**

Application libraries are deployments that are available for other deployments to share. Libraries should be available on all of the targets running their referencing applications.

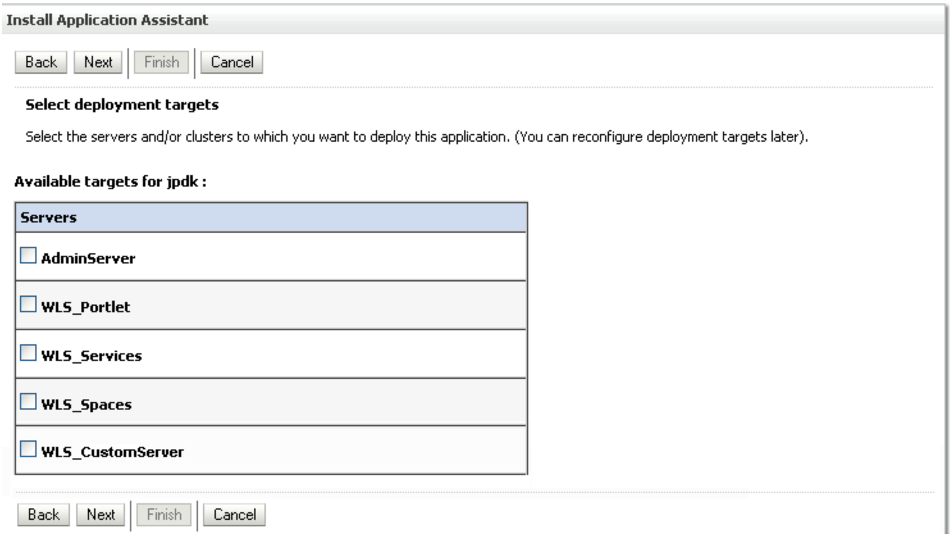
○ **Install this deployment as an application, but target the components individually**

Useful when one or more of the modules or components must have targets unique from the rest of the application.

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

   Page 3 of the Install Application Assistant displays (see Figure 7–22).

Figure 7–22 Install Application Assistant - Page 3



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
□ AdminServer
□ WLS_Portlet
□ WLS_Services
□ WLS_Spaces
□ WLS_CustomServer

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 21.2.1, "Registering a WSRP Producer Using Fusion Middleware Control" and Section 21.4.1, "Registering an Oracle PDK-Java Producer Using Fusion Middleware Control") or WLST commands (see Section 21.2.2, "Registering a WSRP Producer Using WLST" or Section 21.4.2, "Registering an Oracle PDK-Java Producer Using WLST") to modify the producer URL endpoint, and then redeploy the application as described in Section 7.3.2, "Redeploying WebCenter Applications Using Fusion Middleware Control."

7.1.4.5 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 7.1.4.2, "Deploying Applications Using Fusion Middleware Control." If there are deployment descriptors packaged within the EAR file, the deployment uses the data in these files.

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 WebCenter Applications Using Fusion Middleware Control," or using WLST as described in Section 7.3.3, "Redeploying WebCenter Applications Using WLST."

7.1.5 Transporting Customizations Between Environments

You can export and import customizations made to pages, WebCenter Services, and portlets (PDK-Java and WSRP version 2 producers) of a deployed application. For more information, see Chapter 31.2, "Exporting and Importing Custom WebCenter Applications for Data Migration."

7.1.6 Configuring Applications to Run in a Distributed Environment

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

7.2 Undeploying Custom WebCenter Applications

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

> **Note:** When a custom WebCenter application is undeployed, its application credentials and MDS customizations are kept in 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 WebCenter Applications Using Fusion Middleware Control"
- Section 7.2.2, "Undeploying WebCenter Applications Using WLST"
- Section 7.2.3, "Removing an Application's Credential Map"

7.2.1 Undeploying WebCenter Applications Using Fusion Middleware Control

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

To undeploy a custom WebCenter application using Fusion Middleware Control:

1. Log in to Fusion Middleware Control.

   See Section 6.1, "Displaying Fusion Middleware Control Console."
2. From the Navigation pane, expand **Application Deployments**, then click the application that you want to undeploy.
3. From the Application Deployment menu, select **Application Deployment > Undeploy**.
4. On the confirmation page, click **Undeploy**.
5. When the operation completes, click **Close**.

7.2.2 Undeploying WebCenter Applications Using WLST

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

To undeploy a custom WebCenter application using WLST:

1. Start the WLST shell.

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

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

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

   Where:

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

     You should see the following message:

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

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

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

   Where:

   - `app_name` is the deployment name for the deployed application.

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

7.2.3 Removing an Application's Credential Map

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

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

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

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

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

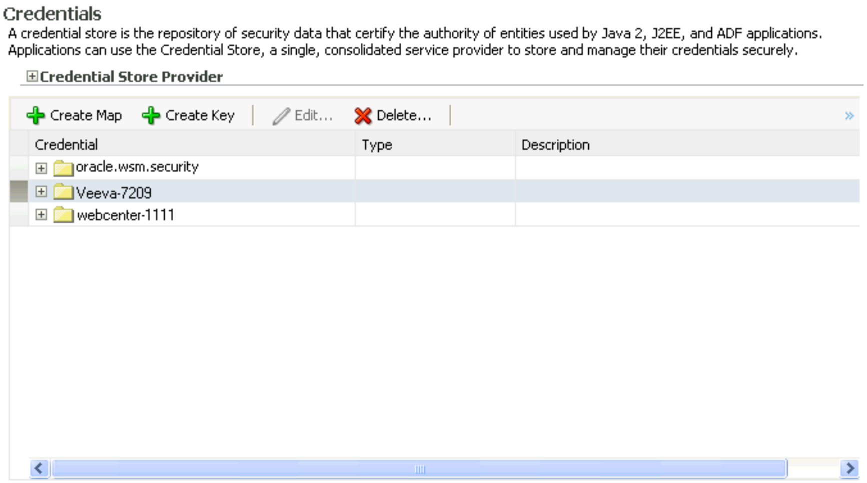
2. Log in to Fusion Middleware Control.

   For information on logging into Fusion Middleware Control, see Section 6, "Starting Enterprise Manager Fusion Middleware Control."

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

   The Credentials pane displays (see Figure 7–23).

Figure 7–23 Credentials Pane



Credentials

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

Credential	Type	Description
⊞ oracle.wsm.security		
⊞ Veeva-7209		
⊞ webcenter-1111		

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

7.3 Redeploying Custom WebCenter Applications

This section describes how to redeploy a custom WebCenter application using Fusion Middleware Control or from the command line using WLST. When you redeploy a new version of an application, you 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 Custom WebCenter Applications".

This section contains the following subsections:

- Section 7.3.1, "Redeployment Considerations"
- Section 7.3.2, "Redeploying WebCenter Applications Using Fusion Middleware Control"
- Section 7.3.3, "Redeploying WebCenter Applications Using WLST"

7.3.1 Redeployment Considerations

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

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 Application Metadata"
- Section 7.3.1.3, "Preserving Portlet Customizations and Personalizations"

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

7.3.1.1 Preserving Application Configuration

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

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

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

7.3.1.1.1 Preserving Configuration Across Deployment Using WLST

If you use the WLST to configure the custom WebCenter application, you can easily build a script to remove all the connections and 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 Application Metadata

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

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

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

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

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

7.3.1.3 Preserving Portlet Customizations and Personalizations

Portlet customizations are packaged with the metadata in the EAR file. Application startup after deployment kicks off the portlet customization migration to the target producers. The target producers are identified by resolving connection customizations. If you have modified your producer connections 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 WebCenter Applications Using Fusion Middleware Control

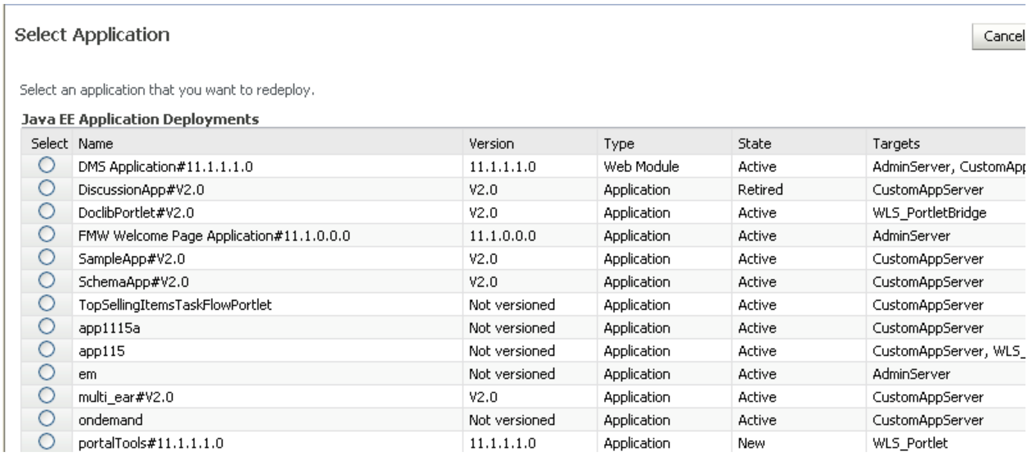
This section describes how to redeploy a custom WebCenter application using Fusion Middleware Control.

To redeploy a custom WebCenter application using Fusion Middleware Control:

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

The Select Application page displays (see Figure 7–24).

Figure 7–24 Select Application Page



Select Application

Cancel

Select an application that you want to redeploy.

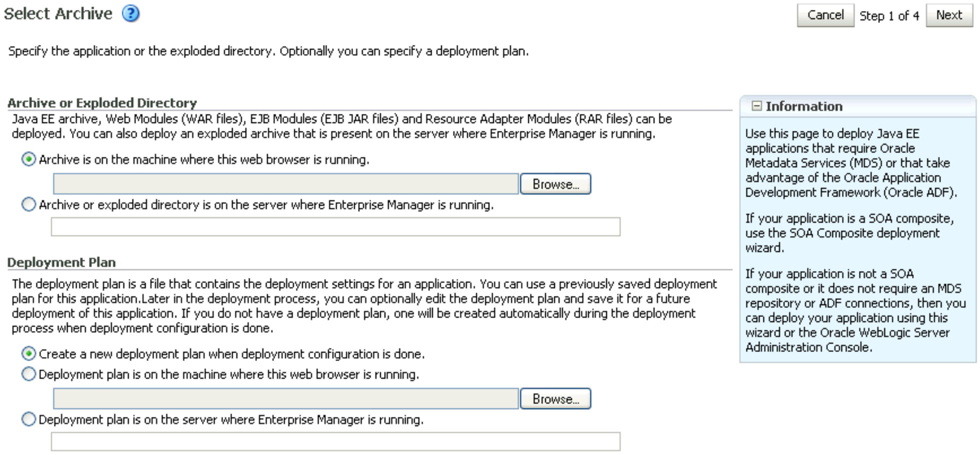
Java EE Application Deployments

Select	Name	Version	Type	State	Targets
○	DMS Application#11.1.1.1.0	11.1.1.1.0	Web Module	Active	AdminServer, CustomApp
○	DiscussionApp#V2.0	V2.0	Application	Retired	CustomAppServer
○	DoclibPortlet#V2.0	V2.0	Application	Active	WLS_PortletBridge
○	FMW Welcome Page Application#11.1.0.0.0	11.1.0.0.0	Application	Active	AdminServer
○	SampleApp#V2.0	V2.0	Application	Active	CustomAppServer
○	SchemaApp#V2.0	V2.0	Application	Active	CustomAppServer
○	TopSellingItemsTaskFlowPortlet	Not versioned	Application	Active	CustomAppServer
○	app1115a	Not versioned	Application	Active	CustomAppServer
○	app115	Not versioned	Application	Active	CustomAppServer, WLS_
○	em	Not versioned	Application	Active	AdminServer
○	multi_ear#V2.0	V2.0	Application	Active	CustomAppServer
○	ondemand	Not versioned	Application	Active	CustomAppServer
○	portalTools#11.1.1.1.0	11.1.1.1.0	Application	New	WLS_Portlet

4. Select the application that you want to redeploy.

5. Click **Next** to display the Select Archive page (see Figure 7–25).

Figure 7–25 Select Archive Page



Select Archive

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.

Browse...

○ 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.

Browse...

○ 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:

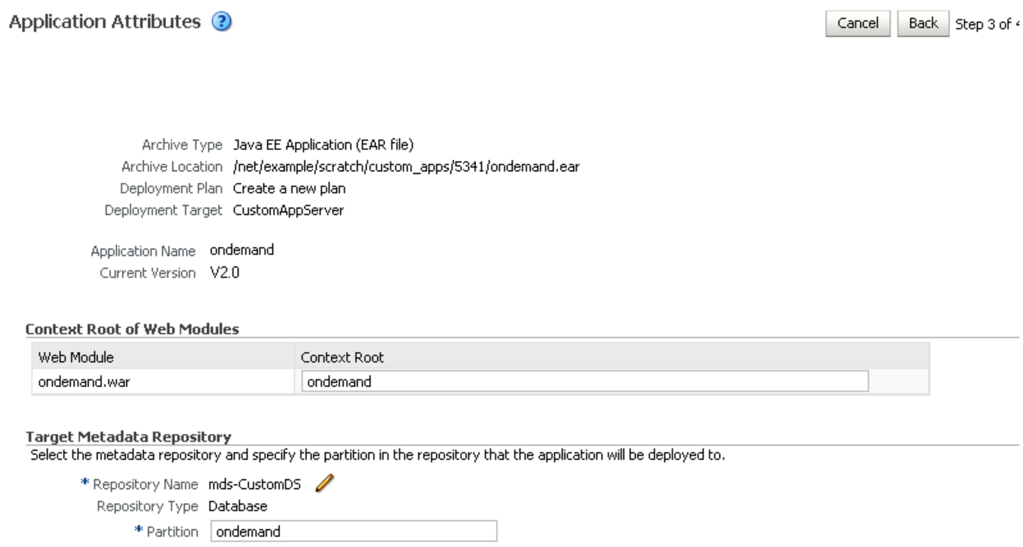
   - Select **Create a new deployment plan when deployment configuration is done** to automatically create a deployment plan after the redeployment process.
   - Select **Deployment plan is on the machine where this web browser is running** and enter the path to the plan or click **Browse** to find the 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 7–26).

Figure 7–26 Application Attributes Page



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.

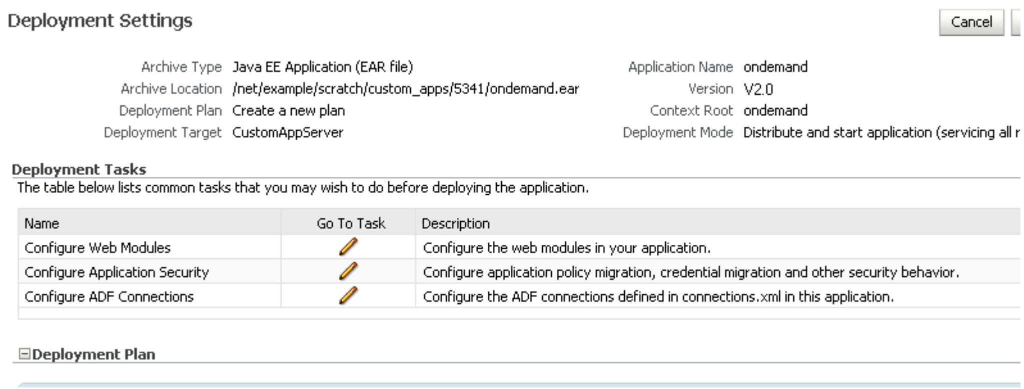
10. In the Target Metadata Repository section, select the MDS repository and enter the **Partition**.

    > **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 7–27).

Figure 7–27 Deployment Settings Page



Deployment Settings

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	CustomAppServer	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 connections.xml in this application.

⊟Deployment Plan

12. On this page, you can perform common tasks before deploying your application, such as configuring connections, or you can edit the deployment plan or save it to a disk. You can:

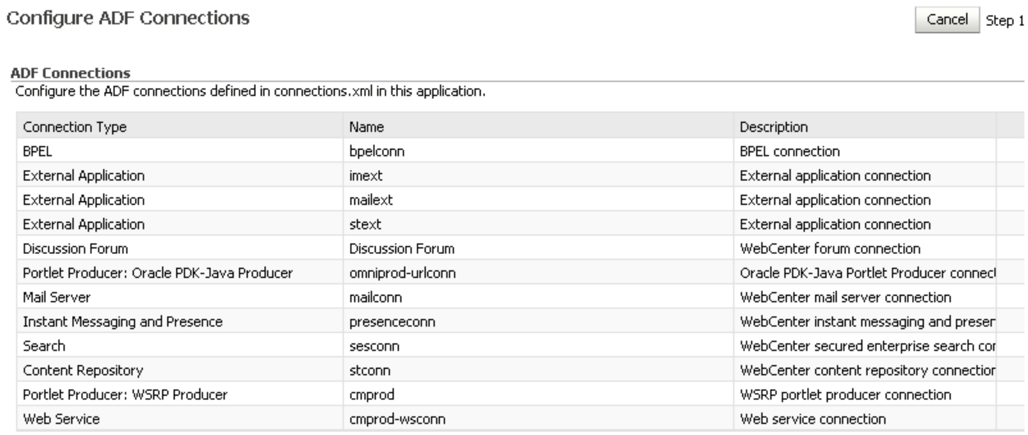
    - Configure web modules
    - Configure application security for application roles and policies
    - Configure ADF connection settings

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

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

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

Figure 7–28 Configure ADF Connections Page



Configure ADF Connections

ADF Connections

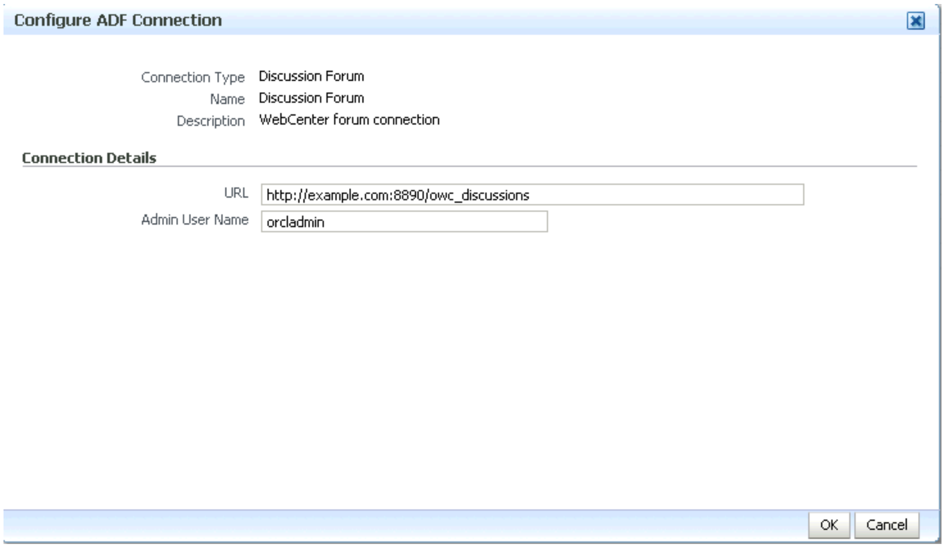
Configure the ADF connections defined in connections.xml in this application.

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 connectior
Portlet Producer: WSRP Producer	cmprod	WSRP portlet producer connection
Web Service	cmprod-wsconn	Web service connection

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

For a Discussion Forum connection (shown in Figure 7–18), for example, 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 7–29 Discussion Forum Connection Settings



Configure ADF Connection

Connection Type Discussion Forum
Name Discussion Forum
Description WebCenter forum connection

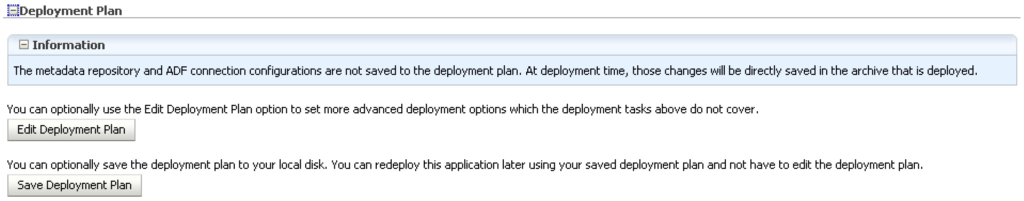
Connection Details

URL http://example.com:8890/owc_discussions
Admin User Name orcladmin

15. If required, specify additional deployment options such as the Web modules to include in your application or security migration settings.
16. Expand Deployment Plan.

    The Deployment Plan settings display (see Figure 7–30).

Figure 7–30 Deployment Settings Page - Deployment Plan Section



Deployment Plan

Information

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

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

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

You can edit and save the deployment plan to your local hard drive, if you choose, so that you can use those settings to redeploy the application again later. See Section 7.1.4.5, "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 WebCenter Applications Using WLST

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

To redeploy a custom WebCenter application using WLST:

1. Start the WLST shell.

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

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

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

   Where:

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

     You should see the following message:

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

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

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

   Where:

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

7.4 Post-Deployment Configuration

After your custom WebCenter 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, "Configuring Security"
- Section 7.4.2, "Configuring Connections"
- Section 7.4.3, "Configuring Data Sources"
- Section 7.4.4, "Tuning the Application"

7.4.1 Configuring Security

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 23.2.5, "Post-deployment Security Configuration Tasks."

7.4.2 Configuring Connections

After deploying your custom WebCenter 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
- External applications
- Discussions server
- Mail server
- Instant Messaging and Presence (IMP) server
- Search
- WSRP portlet producers
- PDK-Java portlet producers
- Web Services

7.4.3 Configuring Data Sources

After deploying your custom WebCenter application to a custom Managed Server, check that the datasources 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 custom WebCenter application, see "Configuring JDBC Data Sources" in *Oracle Fusion Middleware Configuring and Managing JDBC for Oracle WebLogic Server*.

7.4.4 Tuning the Application

After your custom WebCenter 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 Performance." Also see the chapter on "Oracle WebCenter Performance Tuning" in the Oracle Fusion Middleware Performance and Tuning Guide, and Section 30, "Monitoring Oracle WebCenter Performance" for information on how to diagnose performance problems.

8 Starting and Stopping WebCenter Applications

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

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

This chapter includes the following sections:

- Section 8.1, "Starting Node Manager"
- Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments"
- Section 8.3, "Starting and Stopping WebCenter Spaces"
- Section 8.4, "Starting and Stopping Custom WebCenter Applications"

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

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

Audience

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

8.1 Starting Node Manager

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

To start Node Manager:

1. (First time only). Run the following script to set `StartScriptEnabled=true` in the `nodemanager.properties` file:

   ```
   (UNIX)    ORACLE_COMMON_HOME/common/bin/setNMProps.sh
   (Windows) ORACLE_COMMON_HOME\common\bin\setNMProps.cmd
   ```

2. To start the Node Manager:

   a. Navigate to `WL_HOME/server/bin`.

   b. From the command line, enter:

   ```
   WL_HOME/server/bin>./startNodeManager.sh
   ```

When you start Node Manager, it reads the `nodemanager.properties` file with the `StartScriptEnabled=true` property, and uses the start scripts when it subsequently starts the managed servers. Note that you need to run the `setNMProps` script only once.

8.2 Starting and Stopping Managed Servers for WebCenter Application Deployments

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

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

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

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

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

1. Login to Fusion Middleware Control and navigate to the home page for WebCenter Spaces or your custom WebCenter application as follows:

   - Section 6.2, "Navigating to the Home Page for WebCenter Spaces"
   - Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"

2. Navigate to the home page for this application's managed server:

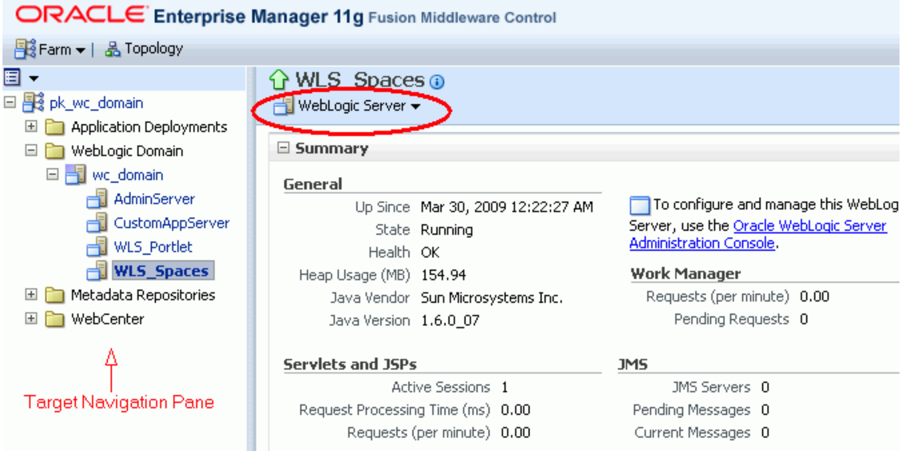
   - For WebCenter Spaces - Find **WebLogic Server** (Related Components section), and then click the name of the managed server. For WebCenter Spaces, this is always *WLS_Spaces*.

- For custom WebCenter applications - Find **Deployed On** (Summary section), and then click the name of the managed server.

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

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

Figure 8–1 Managed Server Home Page



General

Up Since Mar 30, 2009 12:22:27 AM
State Running
Health OK
Heap Usage (MB) 154.94
Java Vendor Sun Microsystems Inc.
Java Version 1.6.0_07

To configure and manage this WebLog Server, use the Oracle WebLogic Server Administration Console.

Work Manager

Requests (per minute) 0.00
Pending Requests 0

Servlets and JSPs

Active Sessions 1
Request Processing Time (ms) 0.00
Requests (per minute) 0.00

JMS

JMS Servers 0
Pending Messages 0
Current Messages 0

3. From the **WebLogic Server** menu:

   - To start the managed server, choose **Control** > **Start Up**.
   - To stop the managed server, choose **Control** > **Shut Down**.

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

8.3 Starting and Stopping WebCenter Spaces

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

- Starting WebCenter Spaces Using Fusion Middleware Control
- Stopping WebCenter Spaces Using Fusion Middleware Control

Alternatively, use WLST:

- Starting WebCenter Spaces Using WLST
- Stopping WebCenter Spaces Using WLST

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

8.3.1 Starting WebCenter Spaces Using Fusion Middleware Control

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

To start WebCenter Spaces through Fusion Middleware Control:

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

   See Section 6.2, "Navigating to the Home Page for WebCenter Spaces".

2. From the main WebCenter menu, choose **WebCenter** >**Control > Start Up**.

   Alternatively, right-click **WebCenter Spaces (WLS_Spaces)** in the Target Navigation Pane to access this menu option.

   A progress message displays.

3. Click **Close**.

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

8.3.2 Starting WebCenter Spaces Using WLST

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

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

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

8.3.3 Stopping WebCenter Spaces Using Fusion Middleware Control

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

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

To stop a WebCenter Spaces application through Fusion Middleware Control:

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

   See Section 6.2, "Navigating to the Home Page for WebCenter Spaces".

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

   Alternatively, right-click **WebCenter Spaces (WLS_Spaces)**in the Target Navigation Pane to access this menu option.

3. Click **OK** to continue.

   A progress message displays.

4. Click **Close**.

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

8.3.4 Stopping WebCenter Spaces Using WLST

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

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

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

8.4 Starting and Stopping Custom WebCenter Applications

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

- Starting Custom WebCenter Applications Using Fusion Middleware Control
- Stopping Custom WebCenter Applications Using Fusion Middleware Control

Alternatively, use WLST:

- Starting Custom WebCenter Applications Using WLST
- Stopping Custom WebCenter Applications Using WLST

8.4.1 Starting Custom WebCenter Applications Using Fusion Middleware Control

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

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

To start a custom WebCenter application through Fusion Middleware Control:

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

   See Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications".

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

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

   A progress message displays.

3. Click **Close**.

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

8.4.2 Starting Custom WebCenter Applications Using WLST

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

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

8.4.3 Stopping Custom WebCenter Applications Using Fusion Middleware Control

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

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

To stop a custom WebCenter application:

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

   See Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications".

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

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

3. Click **OK** to continue.

   A progress message displays.

4. Click **Close**.

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

8.4.4 Stopping Custom WebCenter Applications Using WLST

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

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

9 Setting Application Properties

This chapter includes the following sections:

- Section 9.1, "Setting Application Properties for WebCenter Spaces"
- Section 9.2, "Setting Additional Properties for Custom WebCenter Applications"

Audience

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

9.1 Setting Application Properties for WebCenter Spaces

The WebCenter Spaces home page (in Fusion Middleware Control) is your starting place for configuring WebCenter Spaces 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 WebCenter service connections, external applications, and portlet producers for WebCenter Spaces. To access this page, see Section 6.2, "Navigating to the Home Page for WebCenter Spaces".

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

- Section 9.1.1, "Specifying the BPEL Server Hosting WebCenter Spaces Workflows"
- Section 9.1.2, "Enabling Oracle SES Crawlers in WebCenter Spaces"
- Section 9.1.3, "Choosing the First Page Displayed in WebCenter Spaces"

9.1.1 Specifying the BPEL Server Hosting WebCenter Spaces Workflows

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

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

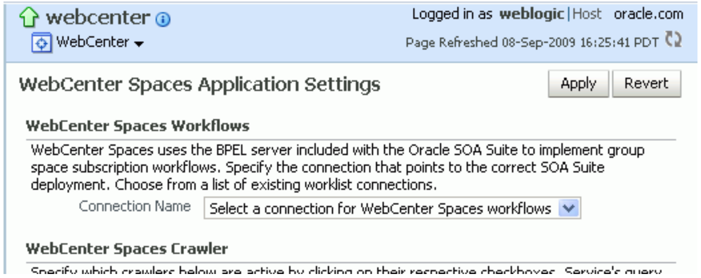
To configure a connection to the WebCenter Space workflows:

1. Login to Fusion Middleware Control, and navigate to the home page for WebCenter Spaces.

   See Section 6.2, "Navigating to the Home Page for WebCenter Spaces".

2. From the **WebCenter** menu, choose **Settings** > **Application Configuration**.

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


webcenter
WebCenter
Logged in as weblogic | Host oracle.com
Page Refreshed 08-Sep-2009 16:25:41 PDT
Apply
Revert
Connection Name
Select a connection for WebCenter Spaces workflows

WebCenter Spaces Application Settings

WebCenter Spaces Workflows

WebCenter Spaces uses the BPEL server included with the Oracle SOA Suite to implement group space subscription workflows. Specify the connection that points to the correct SOA Suite deployment. Choose from a list of existing worklist connections.

WebCenter Spaces Crawler

Specify which crawlers below are active by clicking on their respective checkboxes. Service's query

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 WebCenter Spaces.

   Ensure that you choose the connection that points to the SOA instance in which WebCenter Spaces workflows are deployed. If that connection is not listed you must create it. To define the connection, see Section 20.3, "Setting Up Worklist Connections".

4. Click **Apply**.

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

   See Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments".

9.1.2 Enabling Oracle SES Crawlers in WebCenter Spaces

Out-of-the-box, WebCenter Spaces uses its own WebCenter Search service for searching and returning WebCenter Spaces content. If preferred, you can use Oracle Secure Enterprise Search (SES) to search and return unified results for most WebCenter Spaces resources, including documents, discussions, announcements, group spaces, lists, pages, wikis and blogs. To set up Oracle SES searching, see Section 18.4, "Configuring Oracle SES to Search WebCenter Spaces".

If Oracle SES Search is configured to search WebCenter Spaces resources you can enable or disable the feature at any time through Fusion Middleware Control or using the WLST command `setSpacesCrawlProperties`. You can also configure a suitable full crawl frequency for WebCenter Spaces. For instructions, see step 3 in Section 18.4.2, "Setting Up WebCenter Spaces for Oracle SES Search".

9.1.3 Choosing the First Page Displayed in WebCenter Spaces

By default, when users log in to WebCenter Spaces the first page they see is the page that they accessed last. If you prefer the same landing page to display when users log in you can override this default behavior by setting the system property `oracle.webcenter.spaces.disableLastAccessPageBehavior` in the domain startup script `setDomainEnv`.

When this property is set, users see the following pages when they log in:

- **First page in their personal space.** If the administrator creates one or more role based pages for personal spaces, the first of these pages always displays.
- **First group space page**. When users login in with a direct group space URL the first page of that group space displays. The group space moderator determines which page displays first within a group space.

To set `oracle.webcenter.spaces.disableLastAccessPageBehavior`:

1. Shutdown `WLS_Spaces` (the managed server on which WebCenter Spaces is deployed).
2. Edit the domain startup script `setDomainEnv` located at:

   UNIX: `DOMAIN_HOME/bin/setDomainEnv.sh`

   Windows: `DOMAIN_HOME\bin\setDomainEnv.cmd`
3. Add the following JVM property: -D`oracle.webcenter.spaces.disableLastAccessPageBehavior=true`
4. Restart the managed server.
5. (Optional) Login as administrator, create a business role page, place it first in the page sequence, and provide the content you want users to see when they first login to their personal space.

9.2 Setting Additional Properties for Custom WebCenter Applications

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

See also, Appendix A.4, "Tuning Oracle WebCenter Performance".

Part IV

Managing Services, Portlet Producers, and External Applications

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

Part IV contains the following chapters:

- Chapter 10, "Managing Oracle WebCenter Services"
- Chapter 11, "Managing Content Repositories"
- Chapter 12, "Managing the Announcements and Discussions Services"
- Chapter 13, "Managing the Events Service"
- Chapter 14, "Managing the Instant Messaging and Presence Service"
- Chapter 15, "Managing the Mail Service"
- Chapter 16, "Managing the People Connections Service"
- Chapter 17, "Managing the RSS Service"
- Chapter 18, "Managing the Search Service"
- Chapter 19, "Managing the Wiki and Blog Services"
- Chapter 20, "Managing the Worklist Service"
- Chapter 21, "Managing Portlet Producers"
- Chapter 22, "Managing External Applications"

10

Managing Oracle WebCenter Services

This chapter provides an overview of managing Oracle WebCenter services in WebCenter applications. It also describes how to configure and manage the WebCenter and MDS repositories.

This chapter includes the following sections:

- Section 10.1, "Introduction to Managing Services"
- Section 10.2, "Setting Up the WebCenter Repository"
- Section 10.3, "Setting Up the MDS Repository"

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 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.

Services provide a variety of functionality in support of personal and team objectives. For example, the Documents service provides features for uploading and managing content. The Discussions service provides features for creating, managing, and participating in discussion forums.

Always use Fusion Middleware Control or the WLST command-line tool to review and configure back-end services for WebCenter applications. Any changes that you make to WebCenter applications, post deployment, are stored in the MDS metatdata store as customizations. For more information, see Section 1.3.5, "Oracle WebCenter Configuration Considerations."

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

10.2 Setting Up the WebCenter Repository

The Events, Links, Lists, People Connections, and Tags services store information in the WebCenter repository, which is a database with the WebCenter schema installed. The WebCenter schema is included with the product. To install the WebCenter schema, follow the steps described in the section, "Installing Oracle WebCenter" in the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter*.

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

Table 10–1 describes what information these services store in the WebCenter repository. For more information, see the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

For information on backing up and migrating this information, see Chapter 31, "Managing Export, Import, Backup, and Recovery of WebCenter."

Table 10–1 WebCenter Services Storing Content in WebCenter Repository

WebCenter Services	Description	Content Stored in WebCenter Repository	WebCenter Spaces	Custom WebCenter Application
Events	Scheduled appointments, meetings, presentations, or any other kind of gathering for a particular group space. Group space members can view such events on the group space's dedicated Events page or in any Events task flow that is located on a page in the group space.	Group space event details, such as, meetings, appointments, presentations, and so on. Note: Personal events are stored in Microsoft Exchange Server 2003 and 2007.	Yes	No
Links	Links connect different pieces of previously unlinked information, producing context between items. As users build webs of related information, this knowledge can be communicated to the wider group.	Link maps, that is, relationship information such as what object is linked to what other object.	Yes	Yes
Lists	Enables users to track issues, capture project milestones, publish project assignments, and so on.	List data, that is, column values in List rows.	Yes	No
Tags	Enables users to apply their own meaningful terms to items, making those items more easily discoverable in search results and the Tag Center - a dynamically generated page that displays all the tags users have added.	Resources, bookmarks created on resources, and tag words used in each bookmark.	Yes	Yes

For custom WebCenter applications, you must set up a database connection to the WebCenter repository. This database connection can be of type **JDBC Data Source** or **JDBC URL**. For information on different types of data sources, see the section, "What You May Need to Know About Database Connections and Application Security

Migration When Deploying WebCenter Applications" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*.

Depending on the connection type used in an application, do one of the following:

- Create a global data source, if the application does not include an application-level data source with password indirection. For information on creating global data sources, see the section, "Creating a JDBC Data Source" in *Oracle Fusion Middleware Configuring and Managing JDBC for Oracle WebLogic Server*.
- Map the connection credentials, if the application uses an application-level data source with password indirection. The password is set through the Oracle WebLogic Administration Console on the **Credential Mappings** tab under **Security**. If you change the password for an indirect data source on the **Connection Pool** tab under **Configuration**, then it 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 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 Security Guide*.

In a typical business scenario, applications are deployed to different managed servers, and multiple databases are used as repositories for the applications. The repository that you use in a development environment is different from that in a production environment, and therefore, when migrating custom WebCenter applications from development to production, you 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-name`*`DS`. For example, if the application has a connection name `connection1`, then the JNDI name is `jdbc/connection1DS`.

10.3 Setting Up the MDS Repository

Some WebCenter services, such as Notes, RSS News Feed, Recent Activities, Worklist, Lists, Events, Search, Page, and Mail store information in the MDS repository. To enable these services in WebCenter applications you must configure the MDS repository. For information, see Section 7.1.3.2, "Creating and Registering the Metadata Service Repository."

> **See Also:** "Managing the Oracle Metadata Repository" in the *Oracle Fusion Middleware Administrator's Guide*.

11 Managing Content Repositories

Oracle WebCenter enables content integration through:

- Content Repository data controls, which enable read-only access to a content repository, and maintain tight control over the way the content displays in a custom WebCenter 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, available through the Documents service, 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 custom WebCenter application, or can be added to editable pages at runtime through the Documents service.

This chapter describes how to configure and manage content repositories used by WebCenter applications. For more information about managing and including content in WebCenter applications, see:

- "Integrating Content" in *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter* to configure content repository connections that provide access to decentralized content, and learn how to create custom display templates to integrate and publish decentralized content in your WebCenter application using Content Presenter, as well as how 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* to integrate the Documents service in custom WebCenter 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* to work with the Documents service and task flows at runtime in WebCenter applications.

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

This chapter contains the following sections:

- Section 11.1, "What You Should Know About Content Repository Connections"
- Section 11.2, "Content Repository Prerequisites"
- Section 11.3, "Registering Content Repositories"
- Section 11.4, "Changing the Active (or Default) Content Repository Connection"
- Section 11.5, "Modifying Content Repository Connection Details"
- Section 11.6, "Deleting Content Repository Connections"
- Section 11.7, "Setting Connection Properties for the WebCenter Spaces Content Repository"
- Section 11.8, "Testing Content Repository Connections"
- Section 11.9, "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 Repository Connections

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

- **WebCenter Spaces** - In WebCenter Spaces, every group space and personal space has its own document folder, unique to its parent space. The back-end service providing this functionality is Oracle Content Server. When a content repository is made active (see Section 11.4, "Changing the Active (or Default) Content Repository Connection"), it becomes the default content repository and additional properties become available for configuration. WebCenter Spaces *requires* the default content repository to be Oracle Content Server. Additionally, administrators may connect WebCenter Spaces to other content repositories that WebCenter Spaces may use.
- **Other WebCenter applications** - When a content repository is made active (see Section 11.4, "Changing the Active (or Default) Content Repository Connection"), Documents service task flows use that content repository in instances where no specific connection details are provided. There is no particular requirement on the default content repository used.

When Oracle Content Server is the content repository (required for WebCenter Spaces), the Documents service and Oracle Content Server must be connected to the embedded LDAP identity store.

Just like other service connections, post-deployment content repository connections are registered and managed through Fusion Middleware Control or using the WLST command-line tool. Connection information is stored in configuration files and in the MDS repository. For more information, see Section 1.3.5, "Oracle WebCenter Configuration Considerations."

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

Once connection details are defined, WebCenter users can expose the content of the connected content repositories through several ADF Faces components, such as `<af:image>`, `<af:inlineFrame>`, and `<af:goLink>`, and built-in Documents service task flows (Content Presenter, Document Manager, Document List Viewer, and Recent Documents). For more information, see "Working with Page Content" and "Working with the Documents Service" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

11.1.1 What You Should Know About Microsoft SharePoint Repository Connections

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 the native Microsoft SharePoint Web services as the interface to Microsoft SharePoint content and services.

See also: Section 11.2.2.1, "Microsoft SharePoint - Installation."

11.2 Content Repository Prerequisites

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

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

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

- Section 11.2.1, "Oracle Content Server Prerequisites"
- Section 11.2.2, "Microsoft SharePoint Prerequisites"
- Section 11.2.3, "Oracle Portal Prerequisites"
- Section 11.2.4, "File System Prerequisites"

11.2.1 Oracle Content Server Prerequisites

This section discusses the prerequisites for an Oracle Content Server content repository in the following subsections:

- Section 11.2.1.1, "Oracle Content Server - Installation"

- Section 11.2.1.2, "Oracle Content Server - Configuration"
- Section 11.2.1.3, "Oracle Content Server - Security Considerations"
- Section 11.2.1.4, "Oracle Content Server - Limitations in WebCenter"

11.2.1.1 Oracle Content Server - Installation

Oracle Content Server 10.1.3.5.1 installation is integrated with the Oracle WebCenter installation as part of the Universal Content Management (UCM) media shipped with Oracle WebCenter. You can also choose to install Oracle Content Server separately from the UCM media and then integrate it with Oracle WebCenter, provided certain configuration requirements are satisfied. Before installing Oracle Content Server, ensure that Oracle HTTP Server is installed on the same system.

For information about installing Oracle Content Server, see the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter*.

11.2.1.2 Oracle Content Server - Configuration

After installing Oracle Content Server, you must configure the server to use the same LDAP-based identity store that Oracle WebCenter has been configured to use. You can optionally configure Oracle Content Server to use full-text search and indexing, and configure Secure Sockets Layer (SSL) for secure identity propagation. Table 11–1 lists the various configuration tasks and specifies whether these tasks are mandatory or optional.

> **See Also:** "Administering Content Server" in *Getting Started With Content Server* at:
> `http://download-west.oracle.com/docs/cd/E10316_01/cs/cs_doc_10/getting_started/index.htm`

Table 11–1 Oracle WebCenter-Specific Postinstallation Configuration Tasks for Oracle Content Server

Task	Mandatory/Optional
Configuring the Identity Store	Mandatory
Enabling Full-Text Searching and Indexing	Optional
Configuring Secure Sockets Layer (SSL)	Optional

> **Note:** If you intend to manage Oracle Content Server through a browser or add content on the server through WebDAV, then you must configure Oracle Content Server to work with Oracle HTTP Server.

11.2.1.2.1 Configuring the Identity Store

Both Oracle Content Server and Oracle WebCenter must be configured to use the same LDAP-based identity store, and this identity store must be supported by the User and Role API. To enable communication between Oracle Content Server and an LDAP-based identity store, you must add a JPS user provider configured for this identity store.

To add a JPS user provider to Oracle Content Server:

1. Stop Oracle Content Server and the domain Administration Server. For information, see the section "Oracle Content Server - Installation" in *Oracle Fusion Middleware Installation Guide for Oracle WebCenter*.

   > **See Also:** "Starting and Stopping a Content Server" in *Getting Started With Content Server* at: `http://download-west.oracle.com/docs/cd/E10316_01/cs/cs_doc_10/getting_started/index.htm`

2. Update the Oracle Content Server's JPS configuration file, `jps-config.xml`:

   a. Navigate to *`CONTENT_SERVER_HOME`*`/config`.

   b. Open `jps-config.xml` in an editor and add a `serviceInstanceEntry`.

   Example 11–1 shows the correct values for OID. Some specific properties like `idstore.type` will vary from Example 11–1, depending on the type of identity store being configured. For the permissible values for other LDAPs, including the embedded LDAP, see the appendix "OPSS System and Configuration Properties" in the *Oracle Fusion Middleware Security Guide*.

   > **Note:** ■
   >
   > - Ensure that all entries in the service instance match your LDAP server.
   > - The `security.principal.key` and `security.principal.alias` values (in **bold**) used in Example 11–1 must match the input you provide when running the script. See Step 3.

Example 11–1 serviceInstanceEntry in Oracle Content Server's jps-config.xml

```
<serviceInstance name="idstore.oid" provider="idstore.ldap.provider">
   <property name="subscriber.name" value="dc=example,dc=com"/>
   <property name="idstore.type" value="OID"/>
   <property name="security.principal.key" value="ldap.credential"/>
   <property name="security.principal.alias" value="JPS"/>
   <property name="ldap.url" value="ldap://ldaphost:389"/>
   <extendedProperty>
     <name>user.search.bases</name>
     <values>
      <value>cn=users,dc=example,dc=com</value>
     </values>
   </extendedProperty>
   <extendedProperty>
     <name>group.search.bases</name>
     <values>
       <value>cn=groups,dc=example,dc=com</value>
     </values>
   </extendedProperty>
   <property name="username.attr" value="cn"/>
   <property name="user.login.attr" value="cn"/>
   <property name="groupname.attr" value="cn"/>
</serviceInstance>
```

   c. Make sure that the `<jpsContext>` entry in the `jps-config.xml` file refers to this new `serviceInstance`. That is, the value for `serviceInstanceRef` should match the value of the `serviceInstance` name. For example, for OID it should be set to `idstore.oid`:

```
<jpsContext name="default">
  <serviceInstanceRef ref="idstore.oid"/>
```

3. Run the new script to set up the credentials for `idstore.oid` or other LDAP in the identity store:

   - Navigate to *`CONTENT_SERVER_HOME`*`/custom/FusionLibraries/tools`.

   Note: Ensure that the script is executable (for example, `chmod +x run_credtool.sh`).

   - For Windows, run the `run_credtool.cmd` script. For Linux, run the `./run_credtool.sh` script.

     When the script prompts for input, defaults are shown in `[]`.

   - Enter the input on the line following the prompt. The following extracts show you which defaults to take:

     For Windows:

     ```
     input] Alias: [JPS]
     [input] Key: [ldap.credential]
     [input] User Name:
     cn=user name
     [input] Password:password
     [input] JPS Config:
     [WC_ORACLE_HOME\ucm\custom\FusionLibraries\tools/../../../config/jps-config
     .xml]
     ```

     For Linux:

     ```
     [input] Alias: [JPS]
     [input] Key: [ldap.credential]
     [input] User Name:
     cn=user name
     [input] Password:password
     [input] JPS Config:
     [WC_ORACLE_HOME/ucm/custom/FusionLibraries/tools/../../../config/jps-config
     .xml]
     ```

   Note: The Alias and Key input must match the values used in the serviceInstance `security.principal.alias` and `security.principal.key` respectively.

   ---

4. Restart Oracle Content Server and the domain Administration Server. For more information, see the section "Oracle Content Server - Installation" in *Oracle Fusion Middleware Installation Guide for Oracle WebCenter*.

   See Also: "Starting and Stopping a Content Server" in *Getting Started With Content Server* at:
   `http://download-west.oracle.com/docs/cd/E10316_01/cs/cs_doc_10/getting_started/index.htm`

5. Check that the `JpsUserProvider` is available in Oracle Content Server:

   a. Start the Oracle Content Server console and log on as an administrator.

   b. From the **Administration** menu, select **Providers**.

   c. Ensure that the `jpsuser` provider is listed on the **Providers** page and its status is good in the **Connection State** column.

   d. If an `ldapuser` provider is enabled, disable it.

      To disable the `ldapuser` provider, on the **Providers** page, in the **Action** column, click the **info** link next to the provider. In the new page that opens, under the **JPS User Provider Information** section, click the **Disable** button.

11.2.1.2.2 Enabling Full-Text Searching and Indexing

By default, the database used by Oracle Content Server is set up to provide metadata-only searching and indexing capabilities. However, you can modify the default configuration of the database to additionally support full-text searching and indexing. You can use `OracleTextSearch` on DB2 or SQLServer, if Secure Enterprise Search 11g or additional Oracle Database is setup to support search indexing. Configuring full-text searching and indexing capabilities is optional, but advisable. For full-text search, it is recommended that you use the `OracleTextSearch` option.

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

`http://download.oracle.com/docs/cd/E10316_01/owc.htm`

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

Securing Oracle Content Server with SSL involves the following tasks:

- Configuring a Keystore and Key on the Client Side
- Configuring a Keystore and Key on the Server Side
- Verifying Signatures of Trusted Clients
- Securing Identity Propagation

You can also refer to "SSL Properties" in *Content Integration Suite Administration Guide* available at `http://download.oracle.com/docs/cd/E10316_01/ouc.htm`. 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`.

For more information about configuration for SSL, see Chapter 27, "Securing WebCenter Applications and Components with SSL."

Configuring a Keystore and Key on the Client Side

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

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

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

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

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

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

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

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

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

Configuring a Keystore and Key on the Server Side

To configure a keystore on the Oracle Content Server side:

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

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

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

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

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

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

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

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

Verifying Signatures of Trusted Clients

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

1. In your development environment, go to *JDEV_HOME*/`jdk/bin` and open the command prompt.

2. To verify the signature of trusted clients, import the client's public key in to the server keystore by running the following keytool command:

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

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

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

   When the tool prompts you if the key is self-certified, you must enter `Yes`. Example 11–2 shows a sample output that is generated after this procedure is completed successfully.

Example 11–2 Sample Output Generated by the Keytool

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

Securing Identity Propagation

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

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

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

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

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

7. In **Connection Class**, enter the class of the connection, for example, `idc.provider.KeepaliveSocketIncomingConnection`.

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

    The new incoming provider is now added.
16. Go to the new provider directory that was created in step 4.
17. To specify truststore and keystore, create a file named `sslconfig.hda`.
18. Copy the server keystore to the server.
19. Configure the `sslconfig.hda` file. Example 11–3 shows how the `.hda` file should look after you include the truststore and keystore information.

Example 11–3   Sample sslconfig.hda File

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

11.2.1.3 Oracle Content Server - Security Considerations

To secure identity propagation, you must configure SSL on Oracle Content Server. This is required when Oracle Content Server and your WebCenter application are not on the same system or the same trusted private network. For information, see Section 11.2.1.2.3, "Configuring Secure Sockets Layer (SSL)."

11.2.1.4 Oracle Content Server - Limitations in WebCenter

None.

11.2.2 Microsoft SharePoint Prerequisites

This section discusses the prerequisites for a connection to Oracle WebCenter adapter for Microsoft SharePoint in the following subsections:

- Section 11.2.2.1, "Microsoft SharePoint - Installation"
- Section 11.2.2.2, "Microsoft SharePoint - Configuration"
- Section 11.2.2.3, "Microsoft SharePoint - Security Considerations"
- Section 11.2.2.4, "Microsoft SharePoint - Limitations in WebCenter"

11.2.2.1 Microsoft SharePoint - Installation

Oracle WebCenter 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.

The only supported Microsoft SharePoint 2007 Document Library version settings are:

- Require Check Out : No
- Content Approval : No
- Document Version History : No versioning

If any other version settings are configured, the adapter does not function correctly. For example, if `RequireCheck Out` is set to `yes`, upload operations fails. Similarly, if document version history or content approval are enabled, new versions or documents have restricted visibility.

Before You Begin:

You must first create a managed server suitable for deployment of custom WebCenter applications as described in Section 7.1.3.1, "Creating and Provisioning a WebLogic Managed Server Instance" and Section 7.1.3.2, "Creating and Registering the Metadata Service Repository."

Installing the Microsoft SharePoint Adapter Using WLS Administration Console

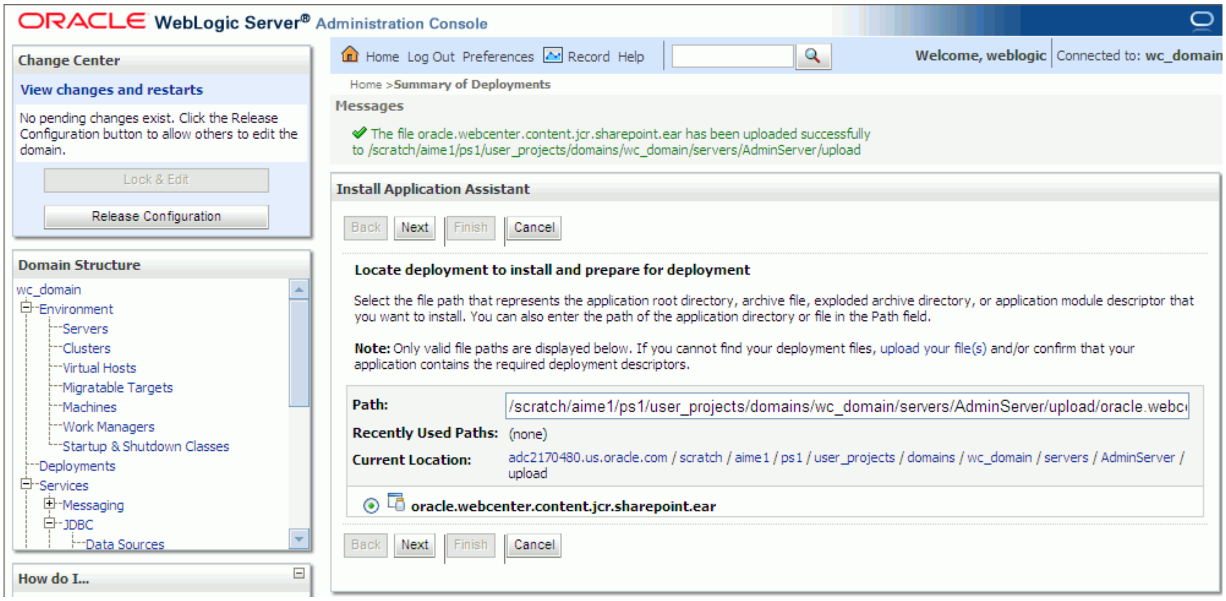
To install the adapter:

1. Log in to the WLS Administration Console.

   For information on logging into the WLS Administration Console, see Section 1.12.2, "Oracle WebLogic Server Administration Console."

2. Navigate to the WLS Administration Console's Home page.
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 the **Deployment Archive**, select the `oracle.webcenter.content.jcr.sharepoint.ear` file from the `/Disk1/WebCenter/services/content/adapters` directory in the **Oracle Fusion Middleware 11g Companion DVD**, and then click **Next**.
7. After you see the message that the EAR file has been uploaded successfully, as shown in Figure 11–1, click **Next**.

Figure 11–1 Install Application Assistant



No pending changes exist. Click the Release Configuration button to allow others to edit the domain.

Messages

✓ The file oracle.webcenter.content.jcr.sharepoint.ear has been uploaded successfully to /scratch/aime1/ps1/user_projects/domains/wc_domain/servers/AdminServer/upload

Install Application Assistant

Locate deployment to install and prepare for deployment

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

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

Path: /scratch/aime1/ps1/user_projects/domains/wc_domain/servers/AdminServer/upload/oracle.webc

Recently Used Paths: (none)

Current Location: adc2170480.us.oracle.com / scratch / aime1 / ps1 / user_projects / domains / wc_domain / servers / AdminServer / upload

● **oracle.webcenter.content.jcr.sharepoint.ear**

8. Select **Install this deployment as a library**, if not already selected, and click **Next**.
9. In **Select deployment targets**, select the managed server to which the custom WebCenter application will be deployed. This must not be an out-of-the-box managed servers. Click **Next**.
10. In **Optional Settings**, accept the defaults and click **Finish**.

Installing the WLST Scripts for Microsoft SharePoint

1. In the Oracle Fusion Middleware 11g Companion DVD, open the `/Disk1/WebCenter/services/content/adapters` directory.
2. Copy the following commands and paste them in the *`ORACLE_HOME`*`/common/wlst` directory:
   - `DocLibSharePointWLST.py`
   - `DocLibGenericWLST.py`
3. To run WLST commands, see Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool (WLST) Commands."

For information about managing connections using WLST, see Section 11.10, "Managing Microsoft SharePoint Connections Using WLST."

11.2.2.2 Microsoft SharePoint - Configuration

For information, see Section 11.3.3, "Registering Content Repositories Using WLST" and Section 11.5.2, "Modifying Content Repository Connection Details Using WLST."

11.2.2.3 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.

11.2.2.4 Microsoft SharePoint - Limitations in WebCenter

WebCenter Spaces does not support Microsoft Sharepoint as the primary document store, and therefore, you must use Oracle Universal Content Management (UCM) instead. However, to show additional documents that are stored in a SharePoint repository, you can configure a SharePoint connection to be used by the Documents service task flows.

11.2.3 Oracle Portal Prerequisites

This section discusses the prerequisites for an Oracle Portal content repository in the following subsections:

- Section 11.2.3.1, "Oracle Portal - Installation"
- Section 11.2.3.2, "Oracle Portal - Configuration"
- Section 11.2.3.3, "Oracle Portal - Security Considerations"
- Section 11.2.3.4, "Oracle Portal - Limitations in WebCenter"

11.2.3.1 Oracle Portal - Installation

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

11.2.3.2 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*.

11.2.3.3 Oracle Portal - Security Considerations

None.

11.2.3.4 Oracle Portal - Limitations in WebCenter

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

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

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

  - Portlet.
  - Portlet instance.
  - URL items.
  - Mobile items.
  - Page links.
  - Item links.
- Items defined as:
  - Expired.
  - Hidden.

11.2.4 File System Prerequisites

This section discusses the prerequisites for a file system content repository in the following subsections:

- Section 11.2.4.1, "File System - Security Considerations"
- Section 11.2.4.2, "File System - Limitations in WebCenter"

11.2.4.1 File System - Security Considerations

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

11.2.4.2 File System - Limitations in WebCenter

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

11.3 Registering Content Repositories

This section contains the following subsections:

- Section 11.3.1, "What You Should Know About Registering Content Repositories for WebCenter Spaces"

  Section 11.3.2, "Registering Content Repositories Using Fusion Middleware Control"

- Section 11.3.3, "Registering Content Repositories Using WLST"

11.3.1 What You Should Know About Registering Content Repositories for WebCenter Spaces

Consider the following when registering Oracle Content Server repositories for WebCenter Spaces:

- At the start up, WebCenter Spaces applications create seed data, if it does not already exist.
- For active connections in WebCenter Spaces, the Spaces Root and Application Name values are used to create the seed data in the WebCenter Spaces repository, to enable storage of the group space data.

- The Spaces Root value is used as the name for the root folder within the content repository under which all group spaces content is stored.
- The Application Name value is used when creating the following security settings:
  - The name of the security group
  - The prefix for the role (the name format is `applicationNameUser`)
  - The prefix for all folder and content item accounts
  - To stripe users permissions on accounts for the particular WebCenter Spaces application
  - To stripe default attributes for the particular WebCenter 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`.
- Oracle does not recommend changing the `Spaces Root` and `Application Name` values. However, if you change the `Spaces Root` value after configuring and running a WebCenter Spaces application, then you must also change the `Application Name` value, and vice versa. That is, you must change both values (`Spaces Root` and `Application Name`) if the WebCenter Spaces application already contains the seed data.

  When you change these values, the existing seed data is not renamed in the Oracle Content Server repository. Instead, new seed data is created using the new values, when you start the application. Once the application is started, new group space data is created under the new `Spaces Root` and existing group space data under the old `Spaces Root` is no longer available. This means that any group space that had the Documents service provisioned prior to changing the `Spaces Root` will no longer have it provisioned.

> **Note:** Although the `Spaces Root` and `Application Name` values change, the old root content repository folder still appears in search results, like any other root folder in Oracle Content Server.

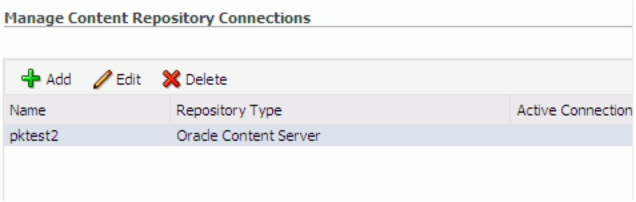
11.3.2 Registering Content Repositories Using Fusion Middleware Control

To register a content repository:

1. Log in to Fusion Middleware Control and navigate to the home page for WebCenter Spaces or the custom WebCenter application:
   - Section 6.2, "Navigating to the Home Page for WebCenter Spaces"
   - Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"
2. Do one of the following:
   - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings** > **Service Configuration**.
   - For custom WebCenter applications - From the **Application Deployment** menu, choose **WebCenter** > **Service Configuration**.
3. From the list of services on the WebCenter Service Configuration page, select **Content Repository**.

4. To connect to a new content repository, click **Add** (Figure 11–2).

Figure 11–2 Configuring Content Repository Connections



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 11–2.

Table 11–2 Manage Content Repository Connections

Field	**Description**
Connection Name	Enter a unique name for this content repository connection. The name must be unique (across all connection types) within the WebCenter application.
Repository Type	Choose the type of repository you want to connect to. Select one of the following: ■ **Oracle Content Server** - an Oracle Universal Content Management repository. See Section 11.2.1, "Oracle Content Server Prerequisites". ■ **Oracle Portal** - an Oracle Portal content repository. See Section 11.2.3, "Oracle Portal Prerequisites". ■ **File System** - a computer file system. See Section 11.2.4, "File System Prerequisites". **Caution:** File system connections *must not* be used in production or enterprise application deployments. This feature is provided for development purposes only. (WebCenter Spaces) If you are setting up the backend content repository for WebCenter Spaces, that is, the repository used by WebCenter Spaces to store group space and personal space documents, you must select **Oracle Content Server**.

Table 11–2 (Cont.) Manage Content Repository Connections

Field	**Description**
Active Connection	Select to make this the *default* content repository for your WebCenter application. You can connect your WebCenter application to multiple content repositories; all connections are used. One connection must be designated the *default* (or active) connection. Do one of the following: ■ For WebCenter Spaces: Select to make this the *active connection*, that is, the back-end repository that WebCenter Spaces uses to store group space and personal space documents. The active connection must be to an Oracle Content Server. If this is the *active connection* for WebCenter Spaces, some additional configuration is required -- see Table 11–3, " Content Repository Connection - WebCenter Spaces Repository Details". ■ For custom WebCenter applications: Select to make this the *active connection*; that is, the default connection for Documents service task flows (Content Presenter, Document Manager, Document List Viewer, and Recent Documents). When no specific connection details are provided for these task flows, this default (active) connection is used. Deselecting this option does not disable the content repository connection. If a content repository is no longer required, you must delete the connection.

6. (For the active connection in WebCenter Spaces only.) Enter additional details for the WebCenter Spaces repository (see Table 11–3).

> **See Also:** Section 11.3.1, "What You Should Know About Registering Content Repositories for WebCenter Spaces"

Table 11–3 Content Repository Connection - WebCenter Spaces Repository Details

Field	**Description**
Administrator User Name	Enter the user name of the content repository administrator. For example: `sysadmin` Administrative privileges are required for this connection so that operations can be performed on behalf of WebCenter users.
Spaces Root	Enter the root folder under which all group spaces content is stored. Specify a content repository folder that does not yet exist and use the format: `/foldername`. For example: `/MyWebCenterSpaces` The `spacesRoot` cannot be `/`, the root itself, and it must be unique across applications. The folder specified is created for you when the WebCenter application starts up. Invalid entries include: `/`, `/foldername/`, `/foldername/subfolder`

Table 11–3 (Cont.) Content Repository Connection - WebCenter Spaces Repository

Field	Description
Application Name	Enter a unique name for this WebCenter Spaces application within this content repository. For example: `MyWCS` The name must begin with an alphabetical character, followed by any combination of alphanumeric characters or the underscore character. The string must be less than or equal to 30 characters. This name is used to separate data when multiple WebCenter Spaces applications share the same content repository and should be unique across applications.

7. Enter connection details for the content repository. For detailed parameter information, see:

   - Table 11–4, " Oracle Content Server Connection Parameters"
   - Table 11–5, " Connection Details - Oracle Content Server - Cache Details"
   - Table 11–6, " Oracle Portal Connection Parameters"
   - Table 11–7, " File System Connection Parameters"

Table 11–4 Oracle Content Server Connection Parameters

Field	Description
RIDC Socket Type	Specify whether Oracle Content Server connects on the content server listener port or the Web server filter, and whether the listener port is SSL enabled. Choose from: ■ **Socket** - Uses an `intradoc` socket connection to connect to the Oracle Content Server. The client IP address must be added to the list of authorized addresses in the Oracle Content Server. In this case, the client is the machine on which Oracle WebCenter is running. ■ **Socket SSL** - Uses an `intradoc` socket connection to connect to the Oracle Content Server that is secured using the SSL protocol. The client's certificates must be imported in the server's trust store for the connection to be allowed. This is the most secure option, and the recommended option whenever identity propagation is required (for example, in WebCenter Spaces). ■ **Web** - Uses an HTTP(S) connection to connect to the Oracle Content Server. For WebCenter Spaces, the **Web** option is not suitable for a back-end Oracle Content Server repository that is being used to store group space and personal space documents, because it does not allow identity propagation. For more information on the configuration parameters required for each RIDC socket type, see the table "Oracle Content Server Connection Parameters for Each RIDC Socket Type" in *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*.
Server Host	Enter the host name of the machine where the Oracle Content Server is running. For example: `mycontentserver.mycompany.com` Server Host is required when the RIDC Socket Type is set to **Socket** or **Socket SSL**.

Table 11–4 (Cont.) Oracle Content Server Connection Parameters

Field	Description
Server Port	Enter the port on which the Oracle Content Server listens: - Socket - Port specified for the `incoming` provider in the server. - Socket SSL - Port specified for the `sslincoming` provider in the server. For example: `4444` Server Port is required when the RIDC Type is set to **Socket** or **Socket SSL**.
Connection Timeout (ms)	Specify the length of time allowed to log in to Oracle Content Server (in milliseconds) before issuing a connection timeout message. If no timeout is set, there is no time limit for the login operation.
Authentication Method	Choose from: - **Identity Propagation** - Oracle Content Server and the WebCenter application use the same identity store to authenticate users. (WebCenter Spaces) Identity propagation is required on the active connection for WebCenter Spaces, that is, for the content repository being used to store group space and personal space documents. - **External Application** - An external application authenticates users against the Oracle Content Server. Select this option if you want to use public, shared, or mapped credentials. 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.
Web URL	Enter the Web server URL for the Oracle Content Server. Use the format: `http://<hostname>:<port>/<web_root>/<plugin_root>` For example: `http://mycontentserver/cms/idcplg` Web URL is applicable when the RIDC Type is set to **Web**.
Associated External Application	Select the external application used to authenticate users against the Oracle Content Server. Associated External Application is applicable when CIS Type is set to **Web**.
Key Store Location	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. For example: `D:\keys\keystore.xyz` Key Store Location is required when the RIDC Type is set to **Socket SSL**.
Key Store Password	Enter the password required to access the keystore. For example: `T0PS3CR3T` Key Store Password is required when the RIDC Type is set to **Socket SSL**.

Table 11–4 (Cont.) Oracle Content Server Connection Parameters

Field	Description
Private Key Alias	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. Ensure that the alias does not contain special characters or white space. For example: `enigma` Private Key Alias is required when the RIDC Type is set to **Socket SSL**.
Private Key Password	Enter the password to be used with the private key alias in the key store. For example: `c0d3bR3ak3R` Private Key Password is required when the RIDC Socket Type is set to **Socket SSL**.

Table 11–5 Connection Details - Oracle Content Server - Cache Details

Element	Description
Cache Invalidation Interval (minutes)	Specify the polling interval (in minutes) used by the Oracle Content Server service provider interface (SPI) to check for cache invalidations. The default is 0 which means that cache invalidation is disabled. The minimum interval is 2 minutes.
Maximum Cached Document Size (bytes)	Enter the maximum size (in bytes) for documents that are cached in the virtual content repository (VCR) binary cache. The default is 1024 bytes (1K). Tune this value based on your machine's memory configuration and the types of binary documents that you expect to cache.
Administrator User Name	Enter a user name with administrative rights for this Oracle Content Server instance.
Administrator Password	Enter the password for the Oracle Content Server administrator.

Table 11–6 Oracle Portal Connection Parameters

Field	Description
Data Source Name	Enter the JNDI DataSource location used to connect to the portal. For example: `jdbc/MyPortalDS` The datasource must be on the server where the WebCenter application is deployed.
Connection Timeout (ms)	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.

Table 11–6 (Cont.) Oracle Portal Connection Parameters

Field	Description
Authentication Method	Specify how to authenticate users against Oracle Portal. Choose from: ■ **Identity Propagation** - Select this option when the WebCenter 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. If an external application is used for authentication, use the **Associated External Application** dropdown list to identify the application.
Associated External Application	Associate Oracle Portal with an external application. External application credential information is used to authenticate Oracle Portal users. You can select an existing external application from the dropdown list, or click **Create New** to configure a new external application now.

Table 11–7 File System Connection Parameters

Field	Description
Base Path	Enter the full path to a folder on a local file system in which your content is placed. For example: `C:\MyContent` **Caution:** File system content *must not* be used in production or enterprise application deployments. This feature is provided for development purposes only.

8. Click **OK** to save this connection.
9. To start using the new (active) connection you must restart the managed server on which the WebCenter application is deployed.

The registered connections are now available to Documents service task flows, which you can add to pages in WebCenter Spaces or custom WebCenter applications. See also, "Working with the Documents Service" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

11.3.3 Registering Content Repositories Using WLST

Use the following WLST commands to register new content repository connections:

- **Oracle Content Server** - `createJCRContentServerConnection`
- **File System** - `createJCRFileSystemConnection`
- **Oracle Portal** - `createJCRPortalConnection`
- **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='true'`. See Section 11.4, "Changing the Active (or Default) Content Repository Connection".

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

> **Note:** To start using the new (active) connection you must restart the managed server on which the WebCenter application is deployed. See "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

11.4 Changing the Active (or Default) Content Repository Connection

WebCenter applications support multiple content repository connections but only one content repository connection can be designated the active (or default) connection.

In WebCenter Spaces, the *active connection* becomes the default back-end repository for group space and personal space documents and the repository must be an Oracle Content Server.

For other WebCenter applications, the *active connection* becomes the default connection for Documents service task flows (Content Presenter, Document Manager, Document List Viewer, and Recent Documents). When no specific connection details are provided for these task flows, the default (active) connection is used.

This section contains the following subsections:

- Section 11.4.1, "Changing the Active (or Default) Content Repository Connection Using Fusion Middleware Control"
- Section 11.4.2, "Changing the Active (or Default) Content Repository Connection Using WLST"

11.4.1 Changing the Active (or Default) Content Repository Connection Using Fusion Middleware Control

To change the active (or default) content repository connection:

1. Log in to Fusion Middleware Control and navigate to the home page for WebCenter Spaces or the custom WebCenter application:
   - Section 6.2, "Navigating to the Home Page for WebCenter Spaces"
   - Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"
2. Do one of the following:
   - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings** > **Service Configuration**.
   - For custom WebCenter applications - From the **Application Deployment** menu, choose **WebCenter** > **Service Configuration**.
3. From the list of services on the WebCenter Services Configuration page, select **Content Repository**.

   The Manage Content Repository Connections table indicates the current active connection (if any).
4. Select the connection you want to become the active (or default) connection, and then click **Edit**.
5. Select the **Active Connection** checkbox.

6. Click **OK** to update the connection.
7. To start using the updated active connection you must restart the managed server on which the WebCenter application is deployed.

11.4.2 Changing the Active (or Default) Content Repository Connection Using WLST

Use the following WLST commands with `Primary='true'` to designate an existing content repository connection as the default connection:

- **Oracle Content Server** - `setJCRContentServerConnection`
- **File System** - `setJCRFileSystemConnection`
- **Oracle Portal** - `setJCRPortalConnection`
- **Microsoft SharePoint** - `setJCRSharePointConnection`

For command syntax and examples, see the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

To subsequently disable a default content repository connection, run the same WLST command with `isPrimary='false'`. Connection details are retained but the connection is no longer named as the primary connection in `adf-config.xml`.

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

> **Note:** To start using the new (active) connection you must restart the managed server on which the WebCenter application is deployed. See, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

11.5 Modifying Content Repository Connection Details

This section contains the following subsections:

- Section 11.5.1, "Modifying Content Repository Connection Details Using Fusion Middleware Control"
- Section 11.5.2, "Modifying Content Repository Connection Details Using WLST"

11.5.1 Modifying Content Repository Connection Details Using Fusion Middleware Control

To update content repository connection details:

1. Log in to Fusion Middleware Control and navigate to the home page for WebCenter Spaces or the custom WebCenter application:
   - Section 6.2, "Navigating to the Home Page for WebCenter Spaces"
   - Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"
2. Do one of the following:
   - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings** > **Service Configuration**.
   - For custom WebCenter applications - From the **Application Deployment** menu, choose **WebCenter** > **Service Configuration**.

3. From the list of services on the WebCenter Services Configuration page, choose **Content Repository**.
4. Select the connection name, and click **Edit**.
5. Edit connection details, as required. For detailed parameter information, see:
   - Table 11–4, " Oracle Content Server Connection Parameters"
   - Table 11–6, " Oracle Portal Connection Parameters"
   - Table 11–7, " File System Connection Parameters"
6. Click **OK** to save your changes.
7. To start using the updated (active) connection details, you must restart the managed server on which the WebCenter application is deployed.

11.5.2 Modifying Content Repository Connection Details Using WLST

Use the following WLST commands to edit content repository connections:

- **Oracle Content Server** - `setJCRContentServerConnection`
- **File System** - `setJCRFileSystemConnection`
- **Oracle Portal** - `setJCRPortalConnection`
- **Microsoft SharePoint** - `setJCRSharePointConnection`

For command syntax and examples, see the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

To configure a particular connection as the active (or default) connection, set `isPrimary='true'`. See Section 11.4, "Changing the Active (or Default) Content Repository Connection".

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

> **Note:** To start using the updated (active) connection details, you must restart the managed server on which the WebCenter application is deployed. See "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

11.5.3 Modifying Cache Settings of Virtual Content Repository (VCR)

For each content connection, caches are created automatically at runtime. However, you can configure or modify Universal Content Management (UCM) repository caches in two ways: in the EAR project file `META-INF/p13n-cache-config.xml` or in the Portal Administration Console (under **Configuration & Monitoring** > **Service Administration**). Cache settings configured in the Portal Administration Console take precedence over the file-based settings. You can also flush the caches from the Portal Administration Console.

> **Note:** If you already have a `p13n-cache-config.xml` file configured for another repository, you can add the UCM repository cache settings to this file.

Table 11–8 and Table 11–9 describe the default cache settings in the p13n-cache-config.xml file. Table 11–8 describes the VCR caches, which are caches used by the VCR component. These caches are repository-specific and can exist for any repository. Table 11–9 describes the SPI caches, which are specific to the UCM SPI adapter component.

The pattern for the cache entry names is <elementName>.<repositoryName>, where <repositoryName> is the name of the UCM repository as specified in the META-INF/content-config.xml file. For example, nodeCache.StellentRepository.

Note that some <time-to-live> values are specified in milliseconds.

Table 11–8 VCR-Level Cache Entry Descriptions

Cache Entry Name	Description
nodeCache.<repositoryName>	Caches node Id of repository's node instance. Defaults: enabled = true; time-to-live = 60000, max-entries = 50.
nodePathCache.<repositoryName>	Caches node path to repository's node Id. Default values: enabled = true; time-to-live = 2 minutes (2*60*1000), max-entries = 200.
typeCache.<repositoryName>	Caches type Id of repository's type instance. Default values: enabled = true; time-to-live = 300000, max-entries = 200.
typeNameCache.<repositoryName>	Caches type name for repository's type Id. Default values: enabled = true; time-to-live = 10 minutes (10*60*1000), max-entries = 200.
binaryCache.<repositoryName>	Default values: enabled = true; time-to-live = 5 minutes (5*60*1000), max-entries = 50. The maximum binary entry size is specified as the repository property binaryCacheMaxEntrySize which has a default value of 102400 bytes (100 kb).
searchCache.<repositoryName>	Caches search results for a repository. Default values: enabled = true; time-to-live = 300000, max-entries = 500.
nativeAuthCache.<repositoryName>	Authorization cache for a repository when using native security. Default values: enabled = true; time-to-live = 5000, max-entries = 5000.

Table 11–9 SPI-Level Cache Entry Descriptions

Cache Entry Name	Description
repo.ucm.typeNameCache.<repositoryName>	Caches UCM server type metadata by type name. Default values: enabled = true; time-to-live = 1800000 (30 minutes), max-entries = 5000
repo.ucm.nodePathToUidCache.<repositoryName>	Caches UCM server node Ids by node path. Default values: enabled = true; time-to-live = 1800000 (30 minutes), max-entries = 5000
repo.ucm.nodeUidCache.<repositoryName>	Caches UCM server node metadata by node Id. Default values: enabled = true; time-to-live = 1800000 (30 minutes), max-entries = 5000
repo.ucm.securityInfoCache.<repositoryName>	Caches UCM server node security information. Default values: enabled = true; time-to-live = 1800000 (30 minutes), max-entries = 5000

Table 11–9 (Cont.) SPI-Level Cache Entry Descriptions

Cache Entry Name	Description
`repo.ucm.securityUserCache.<repositoryName>`	Caches the relationship between the UCM user names and UCM server user Ids (user security information.) Default value: 10 minutes (`10*60*1000`), time-to-live =user authentication decision is valid, max-entries=`5000`
`repo.ucm.typeNamesCache.<repositoryName>`	Caches the list of UCM type names. Default values: enabled=`true`, time-to-live=`1800000` (30 minutes), max-entries=`5000`
`repo.ucm.indexedFieldsCache.<repositoryName>`	Caches information about which UCM fields are indexed. Default values: enabled=`true`, time-to-live=`1800000` (30 minutes), max-entries=`5000`

11.6 Deleting Content Repository Connections

This section contains the following subsections:

- Section 11.6.1, "Deleting Content Repository Connections Using Fusion Middleware Control"
- Section 11.6.2, "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.

11.6.1 Deleting Content Repository Connections Using Fusion Middleware Control

To delete a content repository connection:

1. Log in to Fusion Middleware Control and navigate to the home page for WebCenter Spaces or the custom WebCenter application:
   - Section 6.2, "Navigating to the Home Page for WebCenter Spaces"
   - Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"
2. Do one of the following:
   - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings** > **Service Configuration**.
   - For custom WebCenter applications - From the **Application Deployment** menu, choose **WebCenter** > **Service Configuration**.
3. From the list of services on the WebCenter Services Configuration page, choose **Content Repository**.
4. Select the connection name, and click **Delete**.
5. To effect this change you must restart the managed server on which the WebCenter application is deployed.

11.6.2 Deleting Content Repository Connections Using WLST

Use the WLST command `deleteConnection` to remove a content repository connection. For command syntax and examples, see "deleteConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

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

> **Note:** To effect this change you must restart the managed server on which the WebCenter application is deployed. See, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

11.7 Setting Connection Properties for the WebCenter Spaces Content Repository

You can view, modify, and delete connection properties for the back-end Oracle Content Server repository that is being used by WebCenter Spaces to store group space and personal space documents. Specifically, you can define the root folder under which group space content is stored, the name of the content repository administrator, and a unique application identifier for separating application data on the Oracle Content Server.

This section contains the following subsections:

- Section 11.7.1, "Setting Connection Properties for the WebCenter Spaces Content Repository Using Fusion Middleware Control"
- Section 11.7.2, "Setting Connection Properties for the WebCenter Spaces Content Repository Using WLST"

11.7.1 Setting Connection Properties for the WebCenter Spaces Content Repository Using Fusion Middleware Control

To set content repository connection properties:

1. Log in to Fusion Middleware Control and navigate to the home page for WebCenter Spaces or the custom WebCenter application. See Section 6.2, "Navigating to the Home Page for WebCenter Spaces".
2. From the **WebCenter** menu, choose **Settings** > **Service Configuration**.
3. From the list of services on the WebCenter Services Configuration page, choose **Content Repository**.
4. Select the connection name, and click **Edit**.
5. (For the active connection in WebCenter Spaces only.) Set connection properties for the WebCenter Spaces repository (see Table 11–10).

Table 11–10 Content Repository Connection - WebCenter Spaces Repository Details

Field	Description
Administrator User Name	Enter the user name of the content repository administrator. For example: `sysadmin` Administrative privileges are required for this connection so that operations can be performed on behalf of WebCenter users.

Table 11–10 (Cont.) Content Repository Connection - WebCenter Spaces Repository

Field	Description
Spaces Root	Enter the root folder under which group space content is stored. Specify a folder that does not yet exist and is unique across applications. Use the format: `/foldername`. This name cannot be the same as the Application Name. For example: `/MyWebCenterSpaces` If it does not already exist, the folder specified is automatically created when the WebCenter application starts. Invalid entries include: `/`, `/foldername/`, `/foldername/subfolder`
Application Name	Enter a unique name for this WebCenter Spaces application within this content repository. For example: `MyWCS` The name must begin with an alphabetical character, followed by any combination of alphanumeric characters or the underscore character. The string must be less than or equal to 30 characters.

6. Click **OK** to save your changes.
7. To start using the updated (active) connection properties, you must restart the managed server on which the WebCenter application is deployed.

11.7.2 Setting Connection Properties for the WebCenter Spaces Content Repository Using WLST

The following commands are valid only for the WebCenter Spaces application to view, set, and delete properties for the Oracle Content Server repository that is being used by WebCenter Spaces to store group space and personal space documents:

- `listDocumentsSpacesProperties`
- `setDocumentsSpacesProperties`
- `deleteDocumentsSpacesProperties`

For command syntax and detailed examples, see the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

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

11.8 Testing Content Repository Connections

After setting up content repository connections, you can test them to make sure that you can access the content repository, as described in the following sections:

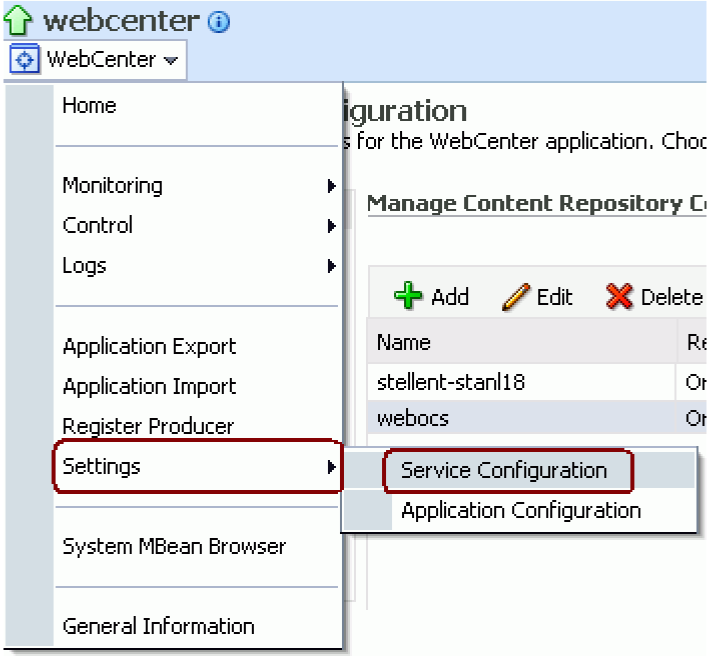
- Section 11.8.1, "Testing Oracle Content Server Connections"
- Section 11.8.2, "Testing Oracle Portal Connections"

11.8.1 Testing Oracle Content Server Connections

To verify a connection of the socket type `web`, log in to the Web interface of Oracle Content Server as `administrator`. You can obtain the URL of a socket type connection through Fusion Middleware Control as follows:

1. In Fusion Middleware Control, from the **WebCenter** menu, choose **Settings** and select **Service Configuration** (Figure 11–3).

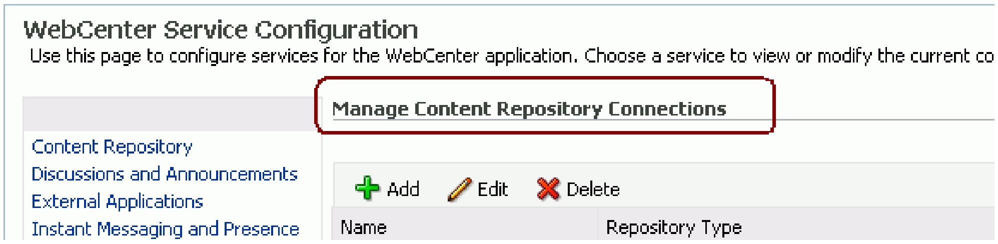
Figure 11–3 Fusion Middleware Control WebCenter Menu



s for the WebCenter application. Choo

2. On the **Manage Content Repository Connections** page, select the connection and click **Edit** (Figure 11–4).

Figure 11–4 Manage Content Repository Connections Page


WebCenter Service Configuration
Manage Content Repository Connections
Content Repository
Discussions and Announcements
External Applications
Instant Messaging and Presence
Add
Edit
Delete
Name
Repository Type

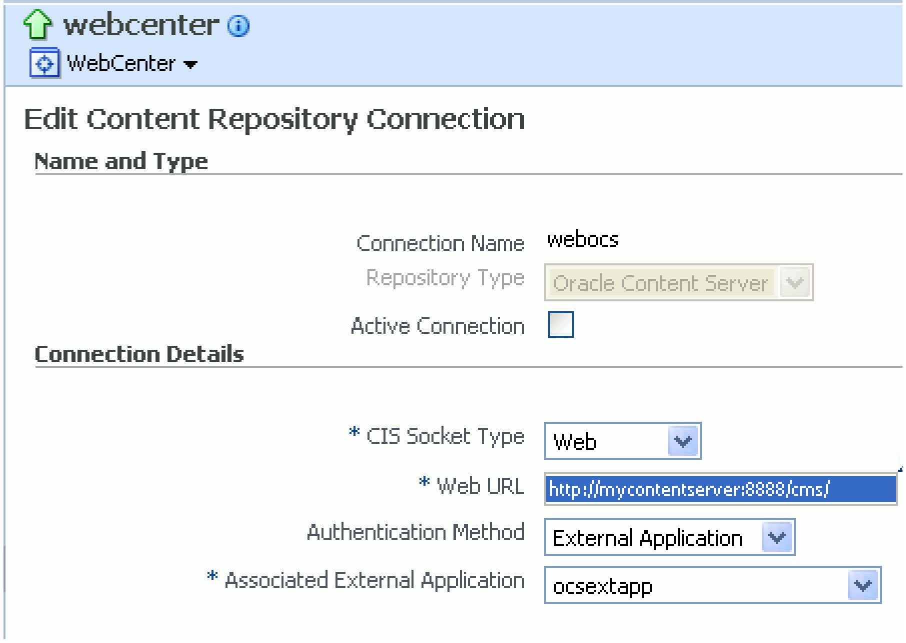
Use this page to configure services for the WebCenter application. Choose a service to view or modify the current co

3. On the **Edit Content Repository Connection** page, copy the Web URL (Figure 11–5).

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 11–5 Edit Content Repository Connection Page



webcenter

WebCenter

Edit Content Repository Connection

Name and Type

Connection Name webocs

Repository Type Oracle Content Server

Active Connection □

Connection Details

* CIS Socket Type Web

* Web URL http://mycontentserver:8888/cms/

Authentication Method External Application

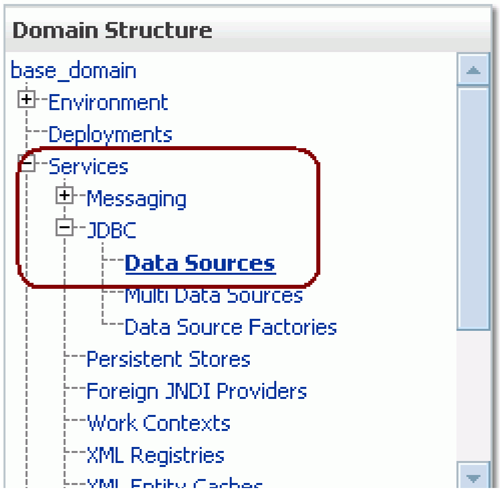
* Associated External Application ocsextapp

11.8.2 Testing Oracle Portal Connections

To verify the full state of an Oracle Portal connection:

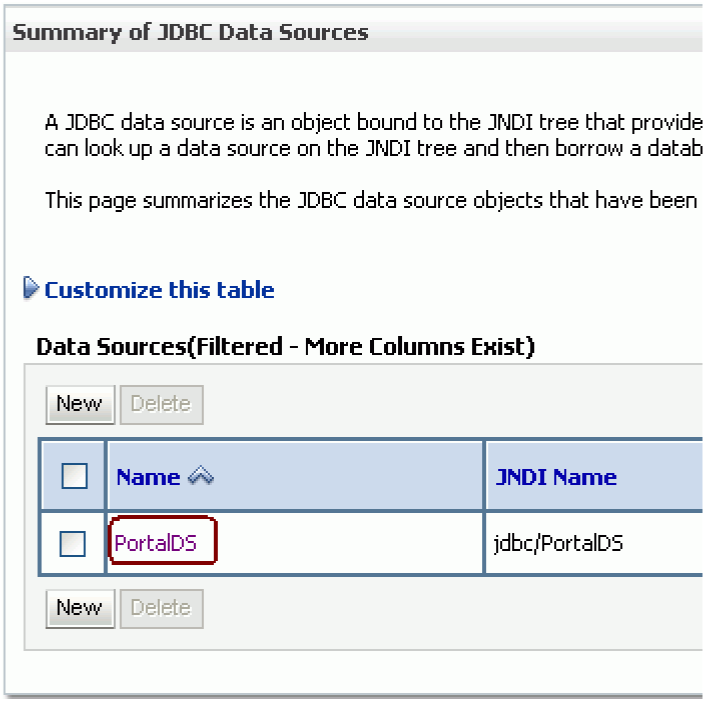
1. In the Oracle WebLogic Administration Console, under **Domain Structure**, expand **Services** > **JDBC**, then double-click **Data Sources** (Figure 11–6).

Figure 11–6 Oracle WebLogic Administration Console



2. On the **Summary of JDBC Data Sources** page, select the data source you intend to test (Figure 11–7).

Figure 11–7 Summary of JDBC Data Sources Page



Summary of JDBC Data Sources

A JDBC data source is an object bound to the JNDI tree that provide
can look up a data source on the JNDI tree and then borrow a datab

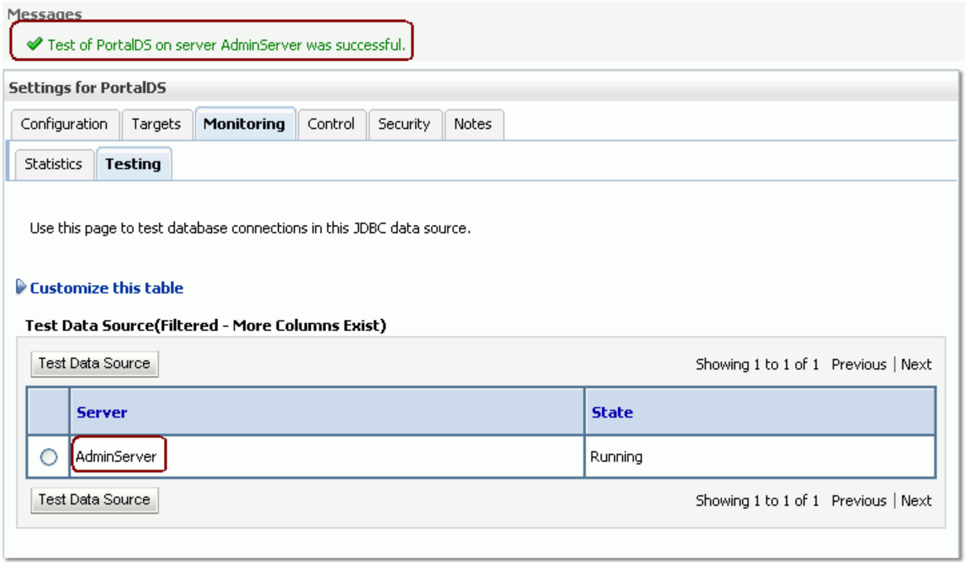
This page summarizes the JDBC data source objects that have been

Data Sources(Filtered - More Columns Exist)

□	Name	JNDI Name
□	PortalDS	jdbc/PortalDS

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 11–8).

Figure 11–8 Data Source Settings Section



Messages

✓ Test of PortalDS on server AdminServer was successful.

Settings for PortalDS

Use this page to test database connections in this JDBC data source.

Test Data Source(Filtered - More Columns Exist)

	Server	State
○	AdminServer	Running

11.9 Changing the Maximum File Upload Size

By default, the maximum upload size for files is:

- 2 MB for custom WebCenter applications. This default is imposed by Apache MyFaces Trinidad, which handles uploading files from a browser to the application server.
- 2 GB for WebCenter Spaces applications.

The WebCenter application developer can customize the default file upload size at design time by setting the `UPLOAD_MAX_MEMORY`, `UPLOAD_MAX_DISK_SPACE`, and `UPLOAD_TEMP_DIR` parameters in the `web.xml` file. For information about manually editing `web.xml`, see Section A.1.2, "web.xml".

For more information, see "Setting Parameters to Upload Files to Content Repositories" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*.

11.10 Managing Microsoft SharePoint Connections Using WLST

Use the commands listed in Table 11–11 to manage connections to SharePoint content repositories.

Configuration changes made using these WebCenter WLST commands are only effective after your restart the Managed Server on which the WebCenter application is deployed. For details, see *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter*.

Table 11–11 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 application.	Online

For information about how to install WLST scripts for Microsoft SharePoint, see Installing the WLST Scripts for Microsoft SharePoint.

11.10.1 createJCRSharePointConnection

Module: Oracle WebCenter

Use with WLST: Online

11.10.1.1 Description

Creates a connection to a Microsoft SharePoint 2007 repository.

11.10.1.2 Syntax

```
createJCRSharePointConnection(appName, name, url, [extAppId, timeout, isPrimary,
server, applicationVersion])
```

Argument	Definition
appName	Name of the WebCenter application in which to perform this operation.

Argument	Definition
name	Connection name. The name must be unique (across all connection types) within the WebCenter application.
url	Web address of the SharePoint site to which you want to connect. For example, if the SharePoint site address is `http://mysharepoint.mycompany.com`, enter this value for the `url` argument.
extAppId	Optional. External application used to authenticate WebCenter users against the SharePoint repository. This value should match the name of an existing external application connection. See also `listExtAppConnections`. If `extAppId` is not set, the SharePoint repository connection will not work. `extAppId` can be set or changed at any time using the setJCRSharePointConnection command.
timeout	Optional. Length of time allowed to log in to the SharePoint repository (in ms) before issuing a connection timeout message. If no timeout is set, there is no time limit for the login operation.
isPrimary	Optional. Valid values are `true` and `false`. `true` specifies that this connection is the primary connection used by the Documents service. The argument defaults to `false`. If this parameter is omitted, the primary connection used by the Documents service does not change. In WebCenter Spaces, the primary connection *must* be an Oracle Content Server connection.
server	Optional. Name of the managed server where the WebCenter application is deployed. For example, `WC_Spaces`. Required when applications with the same name are deployed to different servers and also when you have a cluster.
applicationVersion	Optional. Version number of the deployed application. Required if more than one version of the WebCenter application is deployed.

11.10.1.3 Example

The following example creates a connection to a Microsoft SharePoint site.

```
wls:/weblogic/serverConfig> createJCRSharePointConnection(appName='webcenter',
name='MySPConnection', url='http://mysharepoint.mycompany.com',
extAppId='myExtApp')
```

11.10.2 setJCRSharePointConnection

Module: Oracle WebCenter

Use with WLST: Online

11.10.2.1

Edits an existing Microsoft SharePoint 2007 repository connection. This command requires that you specify values for `appName` and `name`, plus at least one additional argument.

11.10.2.2 Syntax

```
setJCRSharePointConnection(appName, name, [url, extAppId, timeout, isPrimary,
server, applicationVersion])
```

Argument	Definition
appName	Name of the WebCenter application in which to perform this operation.
name	Name of an existing SharePoint connection.
url	Optional. Web address of the SharePoint site to which you want to connect. For example, if the SharePoint site address is `http://mysharepoint.mycompany.com`, enter this value for the `url` argument.
extAppId	Optional. External application used to authenticate WebCenter users against the SharePoint repository. This value should match the name of an existing external application connection. See also `listExtAppConnections`. If `extAppId` is not set, no change is made to the current external application ID. If no external application is set, the SharePoint connection will not work.
timeout	Optional. Length of time allowed to log in to the SharePoint repository (in ms) before issuing a connection timeout message. If no timeout is set, there is no time limit for the login operation.
isPrimary	Optional. Valid values are `true` and `false`. `true` specifies that this connection is the primary connection used by the Documents service. When set to `false`, and the specified connection is the primary connection used by the Documents service, the primary connection is reset. If this parameter is not set, the primary connection used by the Documents service does not change. This argument has no default. In WebCenter Spaces, the primary connection *must* be an Oracle Content Server connection.
server	Optional. Name of the managed server where the WebCenter application is deployed. For example, `WC_Spaces`. Required when applications with the same name are deployed to different servers and also when you have a cluster.
applicationVersion	Optional. Version number of the deployed application. Required if more than one version of the WebCenter application is deployed.

11.10.2.3

The following example edits SharePoint repository connection details.

```
wls:/weblogic/serverConfig> setJCRSharePointConnection(appName='webcenter',
name='MySPConnection', url='http://mysharepoint.mycompany.com',
extAppId='myExtApp')
```

11.10.3 listJCRSharePointConnections

Module: Oracle WebCenter

Use with WLST: Online

11.10.3.1

Without any arguments, this command lists all of the SharePoint connections that are configured for a named WebCenter application.

11.10.3.2 Syntax

```
listJCRSharePointConnections(appName, [verbose, name, server, applicationVersion])
```

Argument	Definition
appName	Name of the WebCenter application in which to perform this operation.
verbose	Optional. Displays SharePoint connection details in verbose mode. Valid options are `true` and `false`. When set to `true`, `listJCRSharePointConnections` lists all SharePoint connections that are configured for a WebCenter application, along with their details. When set to `false`, only connection names are listed. This argument defaults to `false`.
name	Optional. Name of an existing SharePoint connection. When specified you can view connection details for a specific SharePoint connection. If you supply a value for `name`, you must supply a value for `verbose`.
server	Optional. Name of the managed server where the WebCenter application is deployed. For example, `WC_Spaces`. Required when applications with the same name are deployed to different servers and also when you have a cluster.
applicationVersion	Optional. Version number of the deployed application. Required if more than one version of the WebCenter application is deployed.

11.10.3.3

The following example lists the names of all the SharePoint connections that are configured for an application named `webcenter`.

```
wls:/weblogic/serverConfig> listJCRSharePointConnections(appName='webcenter')
```

The following example lists connection details for all of the SharePoint connections that are configured.

```
wls:/weblogic/serverConfig> listJCRSharePointConnections(appName='webcenter',
verbose=true)
```

12 Managing the Announcements and Discussions Services

This chapter describes how to configure and manage the Announcements and Discussions services for WebCenter Spaces and custom WebCenter applications. These two services are grouped together because they both use the same connection to a back-end Oracle WebCenter Discussions server.

Always use Fusion Middleware Control or WLST command-line tool to review and configure back-end services for WebCenter applications. Any changes that you make to WebCenter applications, post deployment, are stored in MDS metatdata store as customizations. See Section 1.3.5, "Oracle WebCenter Configuration Considerations."

> **Note:** Changes that you make to WebCenter services configuration, through Fusion Middleware Control or using WLST, are not dynamic so you must restart the managed server on which the WebCenter application is deployed for your changes to take effect. See Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."

This chapter includes the following sections:

Audience

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

12.1 What You Should Know About Discussions Server Connections

The Discussions service enables users to start, publish, and store discussions in WebCenter applications. The Announcements service lets you create and expose announcements on your application pages.

The Discussions service and the Announcements service require a connection to the WebCenter Discussions server. Both services use the same connection. The Oracle WebCenter Discussions software is installed automatically with Oracle Fusion Middleware.

You can register connections for your WebCenter application through the Fusion Middleware Control Console or using WLST:

- Section 12.3.1, "Registering Discussions Servers Using Fusion Middleware Control"
- Section 12.3.2, "Registering Discussions Servers Using WLST"

WebCenter Spaces

Some additional configuration is required to use Discussions and Announcements services in WebCenter Spaces. This includes choosing the category (on the discussions server) under which all WebCenter Spaces discussions and announcements are stored, and more. This configuration takes place inside WebCenter Spaces. For more information, see Section 12.10, "Setting Discussion Forum Options for WebCenter Spaces."

In WebCenter Spaces, the `group.mapping` parameter determines whether a subcategory or a single forum is created on the discussions server for new group spaces. For more information, see Table 12–4.

You can register additional WebCenter Discussion connections through the Fusion Middleware Control Console, but only one connection is active at a time.

12.2 Discussions Server Prerequisites

This section includes the following subsections:

- Section 12.2.1, "Discussions Server - Installation"
- Section 12.2.2, "Discussions Server - Security Considerations"
- Section 12.2.3, "Discussions Server - Limitations"

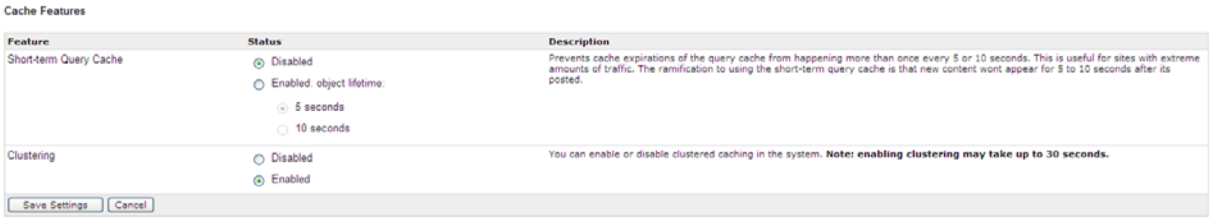
12.2.1 Discussions Server - Installation

The Oracle WebCenter Discussions software is installed automatically with Oracle Fusion Middleware.

12.2.1.1 Discussions Server - High Availability Installation

To set up Oracle WebCenter Discussions for high availability, install the WLS_Services domain in a clustered environment. Then log on to the Oracle WebCenter Discussions admin console, go to the Cache Features page, and select to enable clustering (Figure 12–1).

Figure 12–1 Cache Features - Clustering



Cache Features

Feature	Status	Description
Short-term Query Cache	● Disabled ○ Enabled: object lifetime: ● 5 seconds ○ 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 wont appear for 5 to 10 seconds after its posted.
Clustering	○ Disabled ● Enabled	You can enable or disable clustered caching in the system. **Note: enabling clustering may take up to 30 seconds.**

12.2.2 Discussions Server - Security Considerations

- By default, all Web service calls are secured and require Web Services Security (WS-Security) trusted authentication. WS-Security establishes a trust relationship between your WebCenter application and Oracle WebCenter Discussions so that your WebCenter application can pass the user identity information to the server without knowing the user's credentials.

  To enable the WS-Security trusted authentication for Oracle WebCenter Discussions, you must do the following:

  1. Ensure that the WebCenter domain (`wc_domain`) has been configured.

     For more information about the WebCenter domain, see Chapter 1, "Introduction to Oracle WebCenter Administration."

  2. In WebCenter, generate a Java keystore certificate and export the certificate containing the WebCenter domain public key.

     Go to *`JDK_HOME`*`/jdk/bin` and open a command prompt. Run the following commands:

     ```
     keytool -genkeypair -keyalg RSA -dname "consumer_dname" -alias orakey
     -keypass key_password -keystore keystore -storepass keystore_password
     -validity days_valid

     keytool -exportcert -v -alias orakey -keystore keystore -storepass
     keystore_password -rfc -file orakey.cer
     ```

     For example:

     ```
     keytool -genkeypair -keyalg RSA -dname "cn=spaces,dc=example,dc=com" -alias
     orakey -keypass welcome1 -keystore webcenter.jks -storepass welcome1
     -validity 1064

     keytool -exportcert -v -alias orakey -keystore webcenter.jks -storepass
     welcome1 -rfc -file orakey.cer
     ```

     The output keystore file from the second command (`webcenter.jks`) is the certificate to use in the WebCenter connection to Oracle WebCenter Discussions.

     For more information, see Section 28.1.1, "Setting Up the WebCenter Domain Keystore."

  3. Configure WS-Security for WebCenter Discussions, depending on your topology, following either Section 28.1.2, "Configuring the Discussions Server for a Simple Topology," Section 28.2.2, "Configuring the Discussions Server for

a Typical Topology," or Section 28.3.2, "Configuring the Discussions Server for a Complex Topology."

For example, with a simple topology, using keytool, import the certificate containing the public key of the WebCenter domain:

```
keytool -importcert -alias df_orakey_public -file orakey.cer -keystore
owc_discussions.jks -storepass keystore_password
```

Then create the keystore certificate properties file named `keystore.properties`. The following example shows properties for a sample certificate:

```
org.apache.ws.security.crypto.provider=org.apache.ws.security.components.cr
ypto.Merlin
org.apache.ws.security.crypto.merlin.keystore.type=jks
org.apache.ws.security.crypto.merlin.keystore.password=welcome1
org.apache.ws.security.crypto.merlin.keystore.alias=df_orakey_public
org.apache.ws.security.crypto.merlin.file=/<replace dir path where you run
keytool>/owc_discussions.jks
```

Note: You can confirm that the keystore has been configured on the domain in Fusion Middleware Control domain configuration.

4. Copy the `keystore.properties` file in the *`domain`*`/lib` directory and jar it in `jive_crypto.jar` with the following command:

```
jar cvf jive_crypto.jar keystore.properties
```

5. Log on to the Oracle WebCenter Discussions admin console, go to the Systems Properties page, and change the following property value:

```
webservices.soap.custom.crypto.fileName=keystore.properties
```

6. Restart the managed server on which the discussions server is deployed.
7. In WebCenter, create a connection to Oracle WebCenter Discussions. Select one of the following three ways to create and configure this connection:
   - WLST (see Section 12.3.2, "Registering Discussions Servers Using WLST")
   - Fusion Middleware Control (see Section 12.3.1, "Registering Discussions Servers Using Fusion Middleware Control")
   - JDeveloper (see "Integrating the Discussions Service" in *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*)

Note: Connection parameters must be specified properly for WS-Security. The `keystore.location` should be `webcenter.jks`. For example, see Table 12–4, " Additional Discussion Connection Properties".

- Oracle WebCenter Discussions-specific Web Services messages sent by WebCenter applications to Oracle WebCenter 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 27, "Securing WebCenter Applications and Components with SSL."

- By default, Oracle WebCenter Discussions 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 Oracle WebCenter Discussions.

  For your production environment, you must reassociate the identity store with an external LDAP server, as described in Section 24.1, "Reassociating the Identity Store with an External LDAP." In addition, you must either move the Fusion Middleware administrator account to the external LDAP (as described in Section 24.5, "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 24.5.1, "Migrating the WebCenter Discussions Server to Use an External LDAP."

- You can configure Oracle WebCenter Discussions to leverage single sign-on security using Oracle Access Manager, Oracle Single Sign-On, or SAML-based single sign-on. For information, see Chapter 26, "Configuring WebCenter Applications and Components to Use SSO." For additional Discussions-specific configuration instructions for Oracle Access Manager (OAM), see also Chapter 26.1.7.2, "Configuring the Discussions Server for SSO."

  Note: If you set up SAML single sign-on (SSO), with WebCenter Spaces as the source application and Oracle WebCenter Discussions as the destination application, then you can access Oracle WebCenter Discussions administration pages from WebCenter Spaces as follows:

  - Group Space > Settings > Services page
  - Administration > WebCenter Administration > Services page

  However, because the administration pages of Oracle WebCenter Discussions do not participate in SSO, if you access the administration pages directly, you are required to log in to Oracle WebCenter Discussions again.

- If WebCenter 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 Discussions 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`

12.2.3 Discussions Server - Limitations

The Oracle WebCenter Discussions URL supports only English and Spanish languages for displaying labels; however, data can be entered in UTF-8 format. Oracle recommends using the WebCenter application (with all WebCenter-supported languages) for user operations in the discussions server. All WebCenter-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 Oracle WebCenter 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 Oracle WebCenter is deployed must have the environment variable `LC_ALL` set to `utf-8`.

WebCenter 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 WebCenter Spaces. For more information, see Section 34.1.4, "Understanding Discussions Server Role and Permission Mapping."

12.3 Registering Discussions Servers

You can register multiple discussion server connections for a WebCenter 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 WebCenter application is deployed.

This section includes the following subsections:

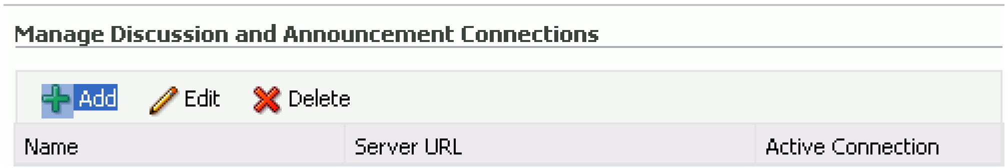
- Section 12.3.1, "Registering Discussions Servers Using Fusion Middleware Control"
- Section 12.3.2, "Registering Discussions Servers Using WLST"

12.3.1 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 WebCenter Spaces or the custom WebCenter application. For more information, see:
   - Section 6.2, "Navigating to the Home Page for WebCenter Spaces"
   - Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"
2. Do one of the following:
   - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings** > **Service Configuration**.
   - For custom WebCenter applications - From the **Application Deployment** menu, choose **WebCenter** > **Service Configuration**.
3. From the list of services on the WebCenter Service Configuration page, select **Discussions and Announcements**.
4. To connect to a new discussions server, click **Add** (Figure 12–1).

Figure 12–2 Configuring Discussion and Announcement Connections



Manage Discussion and Announcement Connections

Name	Server URL	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 12–1).

Table 12–1 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 WebCenter application.
Active Connection	Select to use this connection for the Discussions and Announcements services in the WebCenter application. While you can register multiple discussions server connections for a WebCenter application, only one connection is used for discussion and announcement services—the default (or active) connection.

6. Enter connection details for the discussions server. For details, see Table 12–2.

Table 12–2 Discussion and Announcement Connection - Connection Details

Field	Description
Server URL	Enter the URL of the discussions server hosting discussion forums and announcements. For example: `http://discuss-server.com:8890/owc_discussions`
Administrator User Name	Enter the user name of the discussions server administrator. This account is used by the Discussions and Announcements services to perform administrative operations on behalf of WebCenter users. In WebCenter Spaces, this account mostly is used for managing group space discussions and announcements. It is not necessary for this user to be a `super admin`. However, the user must have administrative privileges on the application root category configured for the WebCenter Spaces, that is, the category (on the discussions server) under which all group space discussions and announcements are stored.
Connection Secured	Select to indicate that a secured (WS-Security) discussions server connection should be established. Additional WS-Security configuration is also required. Use the **Additional Properties** section to specify the keystore information (Table 12–4). Do not deselect this option: WS-Security is mandatory for discussions server connections.

7. Configure advanced options for the discussion and announcement connection (Table 12–3).

Table 12–3 Discussion and Announcement 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 application waits for a response from the discussions 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.

8. Sometimes, additional parameters are required to connect to the discussions server, for example, those listed in Table 12–4.

Table 12–4 Additional Discussion Connection Properties

Additional Connection Property	Description
keystore.location	Enter the certificate file path in your local directory. For example, `/fmwconfig/webcenter.jks`. Keystore information is required to communicate with the discussions server over WS-Security. For more information, see Section 12.2.2, "Discussions Server - Security Considerations."
keystore.type	Enter the keystore type associated with the certificate. Valid values are `jks` (Java keystore) and `pks`.
keystore.password	Enter the keystore password. To encrypt this password, check **Is Property Secured**.
encryption.key.alias	Enter the key alias to be used for encryption. This is the sign and encryption key alias specified during the WebCenter domain keystore configuration. For more information about the values for different topologies, see Chapter 28, "Configuring WS-Security for WebCenter Applications and Components."
encryption.key.password	Enter the password for accessing the encryption key. To encrypt this password, check **Is Property Secured**.
group.mapping	(WebCenter Spaces only) Determines whether a subcategory or a single forum is created on the discussions server for new group spaces. When set to `forum` (the default), a single forum is created under the application root category per group space. When set to `category`, a subcategory is created under the application root category per group space. When a subcategory that supports multiple forums is more suitable, set `group.mapping` to `category`. If a group space template has been configured with a forum-based taxonomy, then the template takes precedence over this connection entry. If a group space template does not define the mapping (the Blank template, for example), then this `group.mapping` property is used. If there is no value in the template or the connection, then the default setting is used (`forum`).

If additional parameters are required to connect to the discussions server, expand **Additional Properties** and enter details as required (Table 12–5).

Table 12–5 Discussion and Announcement Connection - Additional Properties

Field	Description
Add	Click **Add** to specify an additional connection parameter: ▪ **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. For example, select this option to secure the `admin.password` property where the value is the actual password.
Delete	Click **Delete** to remove a selected property. Select the correct row before clicking **Delete**. **Note:** Deleted rows appear disabled until you click **OK**.

9. Click **OK** to save this connection.
10. To start using the new (active) connection you must restart the managed server on which the WebCenter application is deployed. For more information, see Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."

For WebCenter Spaces, some additional configuration is recommended for the Discussions service. For details, see Section 12.10, "Setting Discussion Forum Options for WebCenter Spaces."

12.3.2 Registering Discussions Servers Using WLST

Use the WLST command `createDiscussionForumConnection` to create a discussion server connection. For command syntax and examples, see the section, "createDiscussionForumConnection" in the *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 12.5.2, "Modifying Discussions Server Connection Details Using WLST."

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

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

12.4 Choosing the Active Connection for Discussions and Announcements

You can register multiple discussion server connections for a WebCenter application, but only one connection is active at a time.

For WebCenter Spaces and any custom WebCenter applications, the *active connection* becomes the back-end 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 12.4.1, "Choosing the Active Connection for Discussions and Announcements Using Fusion Middleware Control"
- Section 12.4.2, "Choosing the Active Discussion for Discussions and Announcements Using WLST"

12.4.1 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 WebCenter Spaces or the custom WebCenter application. For more information, see:
   - Section 6.2, "Navigating to the Home Page for WebCenter Spaces"
   - Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"
2. Do one of the following:
   - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings** > **Service Configuration**.
   - For custom WebCenter applications - From the **Application Deployment** menu, choose **WebCenter** > **Service Configuration**.
3. From the list of services on the WebCenter Services Configuration page, choose **Discussions and Announcements**.

   The Manage Discussion and Announcement Connections table indicates the current active connection (if any).
4. Select the connection you want to make the active (or default) connection, and then click **Edit**.
5. Select the **Active Connection** check box.
6. Click **OK** to update the connection.
7. To start using the new (active) connection you must restart the managed server on which the WebCenter application is deployed. See Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."

12.4.2 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 the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

To disable a Discussions and Announcements connection, either delete it, make another connection the 'active connection', or use the `removeDiscussionForumServiceProperty` command:

```
removeDiscussionForumServiceProperty('appName='webcenter',
property='selected.connection')
```

Using this command, connection details are retained but the connection is no longer named as an active connection. For more information, see the section, "removeDiscussionForumServiceProperty" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

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

> **Note:** To start using the new (active) connection you must restart the managed server on which the WebCenter application is deployed. For more information see, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

12.5 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 WebCenter application is deployed.

This section includes the following subsections:

- Section 12.5.1, "Modifying Discussions Server Connection Details Using Fusion Middleware Control"
- Section 12.5.2, "Modifying Discussions Server Connection Details Using WLST"

12.5.1 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 WebCenter Spaces or the custom WebCenter application. For more information, see:
   - Section 6.2, "Navigating to the Home Page for WebCenter Spaces"
   - Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"
2. Do one of the following:
   - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings** > **Service Configuration**.
   - For custom WebCenter applications - From the **Application Deployment** menu, choose **WebCenter** > **Service Configuration**.
3. From the list of services on the WebCenter Service Configuration page, choose **Discussions and Announcements**.
4. Select the connection name, and click **Edit**.

5. Edit connection details, as required. For detailed parameter information, see Table 12–2 and Table 12–4.
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 application is deployed. See Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."

12.5.2 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 the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

To set additional parameters, such as WS-Security parameters, to connect to your discussions server, use the `setDiscussionForumConnectionProperty` command. For more information, see the section, "setDiscussionForumConnectionProperty" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

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

> **Note:** To start using the updated (active) connection you must restart the managed server on which the WebCenter application is deployed. For more information, see the section, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

12.6 Deleting Discussions Server Connections

You can delete discussion server connections at any time but take care when deleting the active connection. If you delete the active connection, none of the Discussions or Announcements task flows work, as they all require a back-end discussions server.

This section includes the following subsections:

- Section 12.6.1, "Deleting a Discussions Server Connection Using Fusion Middleware Control"
- Section 12.6.2, "Deleting a Discussions Server Connection Using WLST"

12.6.1 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 WebCenter Spaces or the custom WebCenter application. For more information, see:
   - Section 6.2, "Navigating to the Home Page for WebCenter Spaces"
   - Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"
2. Do one of the following:

- For WebCenter Spaces - From the **WebCenter** menu, choose **Settings** > **Service Configuration**.
- For custom WebCenter applications - From the **Application Deployment** menu, choose **WebCenter** > **Service Configuration**.

3. From the list of services on the WebCenter Services Configuration page, select **Discussions and Announcements**.
4. Select the connection name, and click **Delete**.
5. To effect this change you must restart the managed server on which the WebCenter application is deployed. For more information, see Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."

> **Note:** Before restarting the managed server, mark another connection as active; otherwise, the service is disabled.

12.6.2 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 the *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 1.12.3.1, "Running Oracle WebLogic Scripting Tool (WLST) Commands."

> **Note:** To effect this change you must restart the managed server on which the WebCenter application is deployed. For more information, see the section, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

12.7 Setting Up Discussions Service Defaults

Use the WLST command `setDiscussionForumServiceProperty` to set defaults for the Discussions service in your WebCenter 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 inside category 3.

- `ForumGatewayManager.AUTO_START`: Mail communication through group space mail distribution lists of a mail server can be published as discussion forum posts on a Discussions server, as described in Section 12.10.3, "Enabling Discussion Forums to Publish Group Space Mail." This parameter starts or stops the gateway for this communication.

  For WebCenter Spaces, the default value is `true`, which means that as soon as you configure mail server settings through WebCenter Spaces administration, the gateway starts. Set this to `false`, and restart the managed server, to stop the gateway and disable this feature.

  For custom WebCenter applications, the default value is `false`. Set this to `true`, and restart the managed server, to start the gateway and enable this feature.

For command syntax and examples, see the section, "setDiscussionForumServiceProperty" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

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

12.8 Setting Up Announcements Service Defaults

Use the WLST command `setAnnouncementServiceProperty` to set defaults for the Announcements service:

- `miniview.page_size`: Maximum number of announcements displayed in the Announcements sidebar view.
- `mainview.page_size`: Maximum number of announcements displayed in the Announcements main view.
- `linksview.page_size`: Maximum number of announcements displayed in the Announcements links view.
- `announcements.expiration.days`: Number of days that announcements display and remain editable.

For command syntax and examples, see the section, "setAnnouncementServiceProperty" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

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

12.9 Testing Discussions Server Connections

Try accessing the discussions server with the following URL:

```
http://host:port/owc_discussions
```

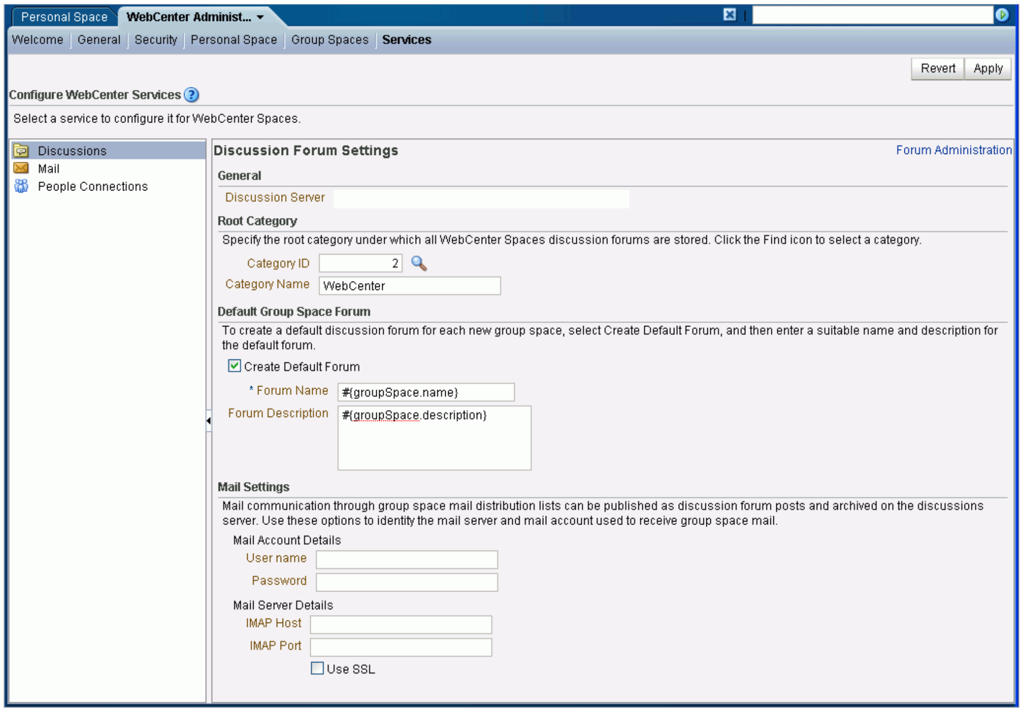
You should see a page listing all public information.

12.10 Setting Discussion Forum Options for WebCenter Spaces

In WebCenter Spaces, discussion forums allow group space members to capture, share, and preserve content that is relevant to their project or community goals.

As WebCenter Spaces administrator, you are responsible for setting discussion forum options through WebCenter Spaces Administration (Figure 12–3).

Figure 12–3 Setting Discussion Forum Options



Configure WebCenter Services

Select a service to configure it for WebCenter Spaces.

Discussion Forum Settings

General

Discussion Server

Root Category

Specify the root category under which all WebCenter Spaces discussion forums are stored. Click the Find icon to select a category.

Category ID 2

Category Name WebCenter

Default Group Space Forum

To create a default discussion forum for each new group space, select Create Default Forum, and then enter a suitable name and description for the default forum.

☑ Create Default Forum

* Forum Name #{groupSpace.name}

Forum Description #{groupSpace.description}

Mail Settings

Mail communication through group space mail distribution lists can be published as discussion forum posts and archived on the discussions server. Use these options to identity the mail server and mail account used to receive group space mail.

Mail Account Details

User name

Password

Mail Server Details

IMAP Host

IMAP Port

☐ Use SSL

From here, you can configure the following:

- Section 12.10.1, "Specifying Where Discussions and Announcements are Stored on the Discussions Server"
- Section 12.10.2, "Setting Up a Default Group Space Discussion Forum"
- Section 12.10.3, "Enabling Discussion Forums to Publish Group Space Mail"

> **Note:** The Fusion Middleware administrator maintains the connection between WebCenter Spaces and the discussions server. If you are experiencing issues with this connection, report the problem to the Fusion Middleware Administrator. See also, Section 12.3, "Registering Discussions Servers."

12.10.1 Specifying Where Discussions and Announcements are Stored on the Discussions Server

Administrators can change the root category (on the discussions server) under which all WebCenter Spaces discussions and announcements are stored.

If the root category is not defined within the connection, then the default system root category is selected. You can choose a different location. This might be useful when WebCenter Spaces is connected to a discussions server that is hosting discussion forums for multiple applications.

Oracle recommendations:

- Choose a category that is dedicated to this WebCenter Spaces application. There may be conflicts when multiple WebCenter Spaces applications share the same root category.

- Do not switch the root category after WebCenter Spaces is up and running. If you change the root category, then all the discussion forums under the old root continue to work, but you cannot use the Links service to create links to discussions or announcements stored in the old category.

Group spaces either own a category (supporting multiple forums) or a single forum under the root category that you specify. It is the group space's template that determines whether it can support multiple forums. For example:

- **Communities of Interest** - A subcategory is created under the root category for each new group space based on the Community of Interest template.
- **Group Projects** - As single forum is created under the root category for each new group space based on the Group Project template.
- **Group Spaces Based on Blank Templates** - By default, a single forum is created under the root category for each new group space based on the Blank template. Your systems administrator might override this if they feel that a subcategory, that supports multiple forums, is more suitable. See also, Section 12.3, "Registering Discussions Servers."

To specify where WebCenter Spaces discussion forums are stored:

1. Log on to WebCenter Spaces with administrative privileges.

   See Section 32.1, "Logging into WebCenter Spaces as an Administrator."
2. Click the **Administration** link at the top of the application.
3. Click the **Services** tab, and then select **Discussions**.
4. Specify an appropriate **Root Category** for storing WebCenter Spaces discussions.

   Click the **Find** icon to view the categories available and then select the most appropriate location.

   To create a new category especially for this WebCenter Spaces application, click **Create Category**. You must have system administrator permissions on the Discussions server to create new categories.
5. Click **Apply** to save the settings.

12.10.2 Setting Up a Default Group Space Discussion Forum

A default discussion forum is created for any group space based on the Community of Interest or Group Project template. This default forum is named after the group space.

Group spaces based on the Community of Interest template support multiple forums. You can choose your own name and description for the default forum in these group spaces or you can disable the default forums feature.

> **Note:** Default forum properties do not apply to group spaces based on the Group Project template. Project-based group spaces offer a single discussion forum that is always available and named after the group space.
>
> For example, even if the **Create Default Forum** option is deselected, then a default forum still is created for group spaces based on the Group Project template.

To set up or disable the default discussion forum for any group space based on the Community of Interest template:

1. Log on to WebCenter Spaces with administrative privileges.

   See Section 32.1, "Logging into WebCenter Spaces as an Administrator."

2. Click the **Administration** link at the top of the application.
3. Click the **Services** tab, and then select **Discussions**.
4. Select **Create Default Forum** to provide a default forum in group spaces.

   Deselect this option to disable this feature. Group space moderators and members with the `Discussions-Manage` permission can create a discussion forum when one is needed.

5. For default forums, enter a name and description:

   a. Use **Forum Name** to specify a name for the default discussion forum.

      To include the name of the parent group space in the forum name, use the syntax `#{groupSpace.name}`.

      For example: `General - #{groupSpace.Photography}`

   b. Use **Forum Description** to create a description based on the group space's name, with the syntax `#{groupSpace.description}`.

      For example: `#{groupSpace.This is a general discussion forum for the Photography group space.}`

      A group space named 'Photography', has a default discussion forum with the following description: This is a general discussion forum for the Photography group space.

6. Click **Apply** to save the settings.

12.10.3 Enabling Discussion Forums to Publish Group Space Mail

Mail communication through group space distribution lists can be published as discussion forum posts. When a mail is new, a new topic is created for it. When an mail is a reply to an existing mail, a topic reply is created for it. Emails sent to a group space distribution list get archived on the discussions server in the group space's default forum.

To enable this feature in WebCenter Spaces, you must specify the mail server and mail account used to receive group space mail. WebCenter Spaces monitors mail sent to this account and publishes mail content on the appropriate group space discussion forum.

> **Note:** Special formatting might done by mail servers that is not handled well in Oracle WebCenter Discussions. As a result, you may see special tags (like `<!DOCTYPE`), or other tags might not appear.

To ensure mail is not missed, the user account that you specify must be a member of every group space mail distribution list; that is, the user must be listed as a *default user* on the LDAP directory server. Default users are configured using a mail server connection property called **LDAP Default User**; this property takes multiple user names. See, Section 15.3, "Registering Mail Servers."

After you set up the mail server and account to receive group space mail for all of WebCenter Spaces, the moderator of each group space determines which mail distribution list is monitored and which discussion forum is used to publish the group space mail. While it is possible for multiple group spaces to use the same distribution list, it is archived only once.

See also "Publishing Group Space Mail in a Discussion Forum" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

To configure the mail server to receive and store group space mail:

1. Log on to WebCenter Spaces with administrative privileges.

   See Section 32.1, "Logging into WebCenter Spaces as an Administrator."

2. Click the **Administration** link at the top of the application.
3. Click the **Services** tab, and then select **Discussions**.
4. Configure **Mail Settings**:

   a. Enter the **User Name** and **Password** for the mail account used to receive group space mail. The user name and password are encrypted and stored in a secure store.

      The specified user must be listed as a default user on the LDAP directory server. See Section 15.3, "Registering Mail Servers."

   b. Enter the **Host** name and **Port** of the IMAP mail server used to receive group space mail.

      Specify the mail server that is managing all group space distribution lists.

   c. Enable or disable secure (encrypted) communication between WebCenter Spaces and the mail server.

      If you enable this option, then the mail server must support SSL.

5. Click **Apply** to save the settings.

12.11 Granting Administrator Role for Oracle WebCenter Discussions Server

The default domain administrator created for Oracle WebCenter is also the administrator for Oracle WebCenter Discussions. You can make a nondefault user the administrator for Oracle WebCenter Discussions.

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 for WebCenter Spaces and Oracle WebCenter Discussions server. For information on how to grant administrator privileges to a nondefault user for WebCenter Spaces, see Section 24.6, "Granting the WebCenter Spaces Administrator Role to a WebCenter Spaces User."

For Oracle WebCenter Discussions, the default user is the super administrator. This section describes how to grant administrator privileges to a nondefault user.

12.11.1 Granting the Administrator Role

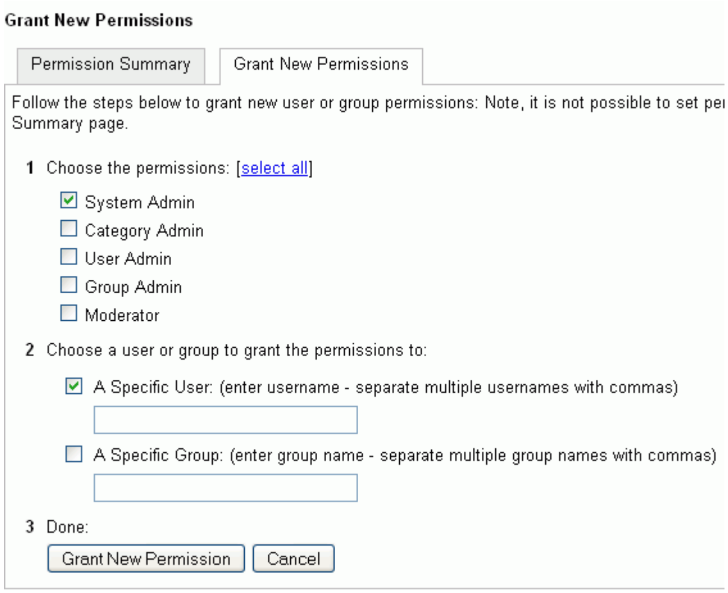
To grant the administrator role for Oracle WebCenter Discussions to a nondefault user:

1. Log on to the Jive Forum 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** check box.
6. Select the **A Specific User** check box and specify the user to whom you want to grant administrative privilege for Oracle WebCenter Discussions.
7. Click **Grant New Permission**.

   You can now log on to Oracle WebCenter Discussions as the user whom you have assigned the administrative privilege.

Figure 12–4 Granting the Administrator Role on Oracle WebCenter Discussions



Grant New Permissions

Follow the steps below to grant new user or group permissions: Note, it is not possible to set pe
Summary page.

1 Choose the permissions: [select all]

☑ System Admin
☐ Category Admin
☐ User Admin
☐ Group Admin
☐ Moderator

2 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)

3 Done:

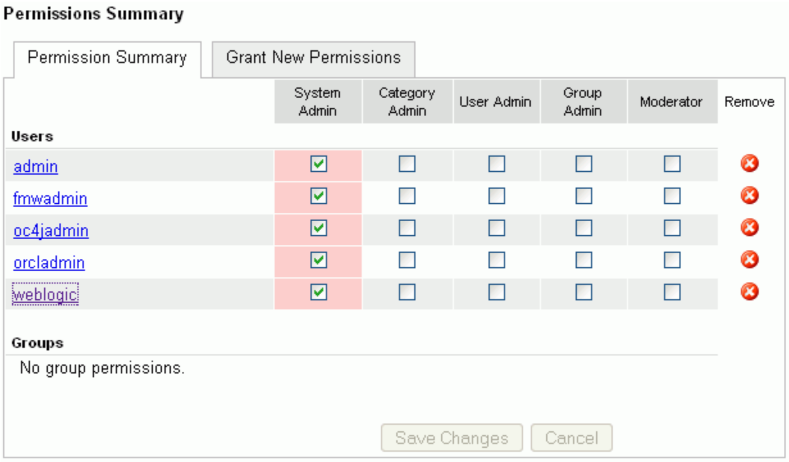
12.11.2 Revoking the Administrator Role

After assigning the administrator role to the required nondefault user, you may want to revoke the administrator role from the default user.

To revoke the administrator role:

1. Log on to Jive Forum Admin Console as the nondefault user whom you have assigned the administrator role.
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, under the **Permission Summary** tab, uncheck the **System Admin** check box for the required user, for example, **weblogic**. (Figure 12–5)

Figure 12–5 Revoking the Administrator Role



Permissions Summary

Permission Summary | Grant New Permissions

	System Admin	Category Admin	User Admin	Group Admin	Moderator	Remove
Users						
admin	☑	□	□	□	□	☒
fmwadmin	☑	□	□	□	□	☒
oc4jadmin	☑	□	□	□	□	☒
orcladmin	☑	□	□	□	□	☒
weblogic	☑	□	□	□	□	☒

Groups

No group permissions.

Save Changes | Cancel

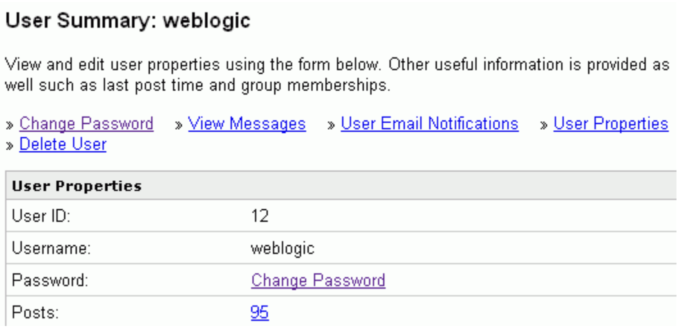
5. Click **Save Changes**.

   The administrative privileges for managing Oracle WebCenter Discussions are now revoked from the default user.

You may want to change the default password of the default user. To change the password:

1. Log on to the Jive Forum Admin Console as an administrator.
2. On the Admins & Moderators page, under the **Permission Summary** tab, click the link for the user, for example, **weblogic**.
3. On the User Profile page, click the **edit user settings** link.
4. Click the **Change Password** link. (Figure 12–6)

Figure 12–6 Changing Password



User Summary: weblogic

View and edit user properties using the form below. Other useful information is provided as well such as last post time and group memberships.

» Change Password » View Messages » User Email Notifications » User Properties
» Delete User

User Properties	
User ID:	12
Username:	weblogic
Password:	Change Password
Posts:	95

5. Enter the new password in the **New Password** and **Confirm Password** fields.
6. Click **Change Password**.

12.12 Troubleshooting Issues with Announcements and Discussions

This troubleshooting section includes the following subsections:

- Section 12.12.1, "Authentication Failed"
- Section 12.12.2, "Discussions Cannot Be Enabled in Group Spaces"

- Section 12.12.3, "Login Does Not Function Properly After Configuring Oracle Access Manager"
- Section 12.12.4, "Category Not Found Exceptions"

12.12.1 Authentication Failed

Problem

WS-Security does not appear to be set properly for the connection between WebCenter and Oracle WebCenter Discussions. 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:

- On Windows, keystore property paths should be separated by "\\".
- Remove extra whitespace in the properties file.
- For the WebCenter Discussions service, review `WLS_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 Oracle WebCenter Discussions server, review `WLS_Services-diagnostics.log` and `jive.error.log` inside your domain's `config/fmwconfig/servers/WLS_Services/owc_discussions_11.1.1/logs` directory. If the logs do not provide enough information to correct errors, then turn on debugging for Oracle WebCenter Discussions. To turn on debug logs, log on to the Oracle WebCenter Discussions admin console, go to page logs, the Debug tab, and enable. Restart the WLS_Services domain to change the logging setting.

12.12.2 Discussions Cannot Be Enabled in Group Spaces

Problem

Discussions cannot be enabled in any group space, even new group spaces.

Solution

This error may be caused due to various reasons. Check the following:

- Oracle WebCenter Discussions server is up and running and accessible. See Section 12.9, "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 the WebCenter Spaces). See Section 12.3, "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 the WebCenter Spaces, that is, the category (on the discussions server) under which all group space discussions and announcement are stored.

- Application root category, where all group space discussions and announcements are stored, exists on the back-end server.

  You can check the application root category ID configured for the WebCenter Spaces application by navigating WebCenter Administration, selecting **Services**, and then **Discussions**. See Section 12.10.1, "Specifying Where Discussions and Announcements are Stored on the Discussions Server."

12.12.3 Login Does Not Function Properly After Configuring Oracle Access Manager

Problem

When you log in to the Oracle WebCenter Discussions server after configuring Oracle Access Manager single sign-on, a `500 - Internal Server Error` occurs.

Solution

This error occurs if the LDAP back-end is configured for the discussions server and you add a new `SSOAuthFactory` property to configure single sign-on instead of editing the existing property.

Go to the Administration page and remove LDAP `AuthFactory` and single sign-on `AuthFactory` properties. If needed, run the following SQL to restore the correct value:

```
insert into jiveproperty
values('AuthFactory.className','oracle.jive.security.JpsAuthFactory');
```

Consider the following when configuring Oracle Access Manager single sign-on:

- If the discussions server *is not* configured with the LDAP `AuthFactory` property, then you must add a new property to configure single sign-on:

  ```
  AuthFactory.className=oracle.jive.security.JpsAuthFactory
  ```

- If the discussions server *is* configured with an LDAP `AuthFactory`, then you must edit the `AuthFactory.className` property while configuring single sign-on and set it to:

  ```
  oracle.jive.security.JpsAuthFactory
  ```

- Property values are case-sensitive.

12.12.4 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 administrator-services-discussions, then you could see exceptions like, "Category Not Found."

Solution

Restart the managed server on which the WebCenter application is deployed.

13 Managing the Events Service

This chapter describes how to configure and manage the Events service for WebCenter Spaces.

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

Any changes that you make to WebCenter applications, post deployment, are stored in MDS metatdata store as customizations. See Section 1.3.5, "Oracle WebCenter Configuration Considerations."

> **Note:** Changes that you make to WebCenter services configuration, through Fusion Middleware Control or using WLST, are not dynamic so you must restart the managed server on which the WebCenter application is deployed for your changes to take effect. See Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."

This chapter includes the following sections:

- Section 13.1, "What You Should Know About Events Connections"
- Section 13.2, "Events Service Prerequisites"
- Section 13.3, "Registering Events Servers"
- Section 13.4, "Choosing the Active Events Server Connection"
- Section 13.5, "Modifying Events Server Connection Details"
- Section 13.6, "Deleting Event Server Connections"
- Section 13.7, "Testing Event Server Connections"
- Section 13.8, "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."

13.1 What You Should Know About Events Connections

The Events service provides group calendars that you can use to schedule meetings, appointments, and any other type of team or group occasion. The Events service also provides you with a personal calendar where you can schedule events that are not related to a particular group space.

Note: The Events service is available only in WebCenter Spaces, not in custom WebCenter applications.

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 Spaces, the user must have an account on the Microsoft Exchange Server.

13.2 Events Service Prerequisites

This section includes the following subsections:

- Section 13.2.1, "Microsoft Exchange Server 2007 Prerequisites"
- Section 13.2.2, "Microsoft Exchange Server 2003 Prerequisites"

13.2.1 Microsoft Exchange Server 2007 Prerequisites

This section describes the Microsoft Exchange Server 2007 prerequisites when used as the server for the Events service.

This section includes the following subsections:

- Section 13.2.1.1, "Microsoft Exchange Server 2007 - Installation"
- Section 13.2.1.2, "Microsoft Exchange Server 2007 - Configuration"
- Section 13.2.1.3, "Microsoft Exchange Server 2007 - Security Considerations"
- Section 13.2.1.4, "Microsoft Exchange Server 2007 - Limitations"

13.2.1.1 Microsoft Exchange Server 2007 - Installation

Refer to the Microsoft Exchange Server 2007 documentation for installation information.

13.2.1.2 Microsoft Exchange Server 2007 - Configuration

To use Microsoft Exchange Server 2007 as the server for the Events service, 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://machine.example.com/EWS/Exchange.asmx"/>
    </wsdl:port>
  </wsdl:service>
</wsdl:definitions>
```

13.2.1.3 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** ***machine_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.mspx?mfr=true`

13.2.1.4 Microsoft Exchange Server 2007 - Limitations

There are currently no known limitations.

13.2.2 Microsoft Exchange Server 2003 Prerequisites

This section describes the Microsoft Exchange Server 2003 prerequisites when used as the server for the Events service.

This section includes the following subsections:

- Section 13.2.2.1, "Microsoft Exchange Server 2003 - Installation"
- Section 13.2.2.2, "Microsoft Exchange Server 2003 - Configuration"
- Section 13.2.2.3, "Microsoft Exchange Server 2003 - Security Considerations"
- Section 13.2.2.4, "Microsoft Exchange Server 2003 - Limitations"

13.2.2.1 Microsoft Exchange Server 2003 - Installation

Refer to the Microsoft Exchange Server 2003 documentation for installation information.

13.2.2.2 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 the WebCenter Personal Events Web Service Plug-in on the IIS machine. The plug-in is available on the Companion CD.

To install the WebCenter Personal Events Web Service Plug-in:

1. Extract the contents of the `ExchangeWebService.zip` file to a folder on the machine where Microsoft Exchange Server is installed. You can find the ZIP file in the following directory on the Oracle Fusion Middleware companion CD:

   ```
   /Disk1/WebCenter/services/cal/NT/ExchangeWebService.zip
   ```

2. Open Internet Information Services (IIS) Manager.
3. Under **Node *machine_name*** > **Web Sites** > **Default Web Site**, create a new virtual directory called `ExchangeWS`.
4. Point the new virtual directory to the folder to which you extracted the ZIP file.
5. Make sure the folder has **Read** privileges.
6. Right-click the virtual directory and choose **Properties**.
7. On the **Virtual Directory** tab, under Application settings, click **Create**.
8. Set the **Execute permissions** to **Scripts and Executables**.
9. On the **ASP.NET** tab, ensure that the **ASP.NET version** is **2.0.XXXXX**.
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
    ```

    Change the port, if necessary, to reflect the IIS port number.
12. Apply the changes and close the dialog.
13. Create a folder called `C:\WSErrorLogs`.
14. Test the web service by launching a web browser and going to the following URL:

    ```
    http://localhost/ExchangeWS/PersonalEventsWebService.asmx
    ```

13.2.2.3 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.mspx?mfr=true`

13.2.2.4 Microsoft Exchange Server 2003 - Limitations

There are currently no known limitations.

13.3 Registering Events Servers

You can register multiple events servers for a WebCenter 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 WebCenter application is deployed.

This section includes the following subsections:

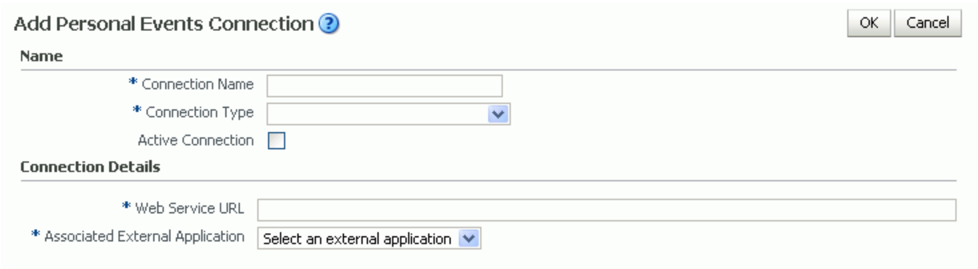
- Section 13.3.1, "Registering Events Servers Using Fusion Middleware Control"
- Section 13.3.2, "Registering Event Servers Using WLST"

13.3.1 Registering Events Servers Using Fusion Middleware Control

To register an events server with WebCenter applications:

1. Log in to Fusion Middleware Control and navigate to the home page for WebCenter Spaces. For more information, see Section 6.2, "Navigating to the Home Page for WebCenter Spaces."
2. From the **WebCenter** menu, choose **Settings** > **Service Configuration**.
3. From the list of services on the WebCenter Service Configuration page, select **Personal Events**.
4. To connect to a new events server instance, click **Add** (Figure 13–1).

Figure 13–1 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 13–1).

Table 13–1 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 application.
Connection Type	Choose the version of the Microsoft Exchange Server to connect to. Select one of the following: ■ **Microsoft Exchange Server 2003** ■ **Microsoft Exchange Server 2007**
Active Connection	Select to use this connection in the WebCenter application for the Events service. 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 13–2).

Table 13–2 Personal Events - Connection Details

Field	Description

Web Service URL	Enter the URL of the Web service exposing the event application.
	Use the format:
	`protocol://host:port/appWebServiceInterface/WSName`
	For example
	`http://myexchange.com:80/ExchangeWS/PersonalEventsWebService.asmx`
	`http://myexchange.com:80/EWS/Services.wsdl`

Associated External Application	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.

7. Click **OK** to save this connection.

8. To start using the new (active) connection you must restart the managed server on which the WebCenter application is deployed. For more information, see Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."

13.3.2 Registering Event Servers Using WLST

Use the WLST command `createPersonalEventConnection` to create an events service 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 1.12.3.1, "Running Oracle WebLogic Scripting Tool (WLST) Commands."

Note: To start using the new (active) connection you must restart the managed server on which the WebCenter application is deployed. See, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

13.4 Choosing the Active Events Server Connection

You can register multiple events server connections with WebCenter Spaces but only one connection is active at a time.

This section includes the following subsections:

- Section 13.4.1, "Choosing the Active Events Server Using Fusion Middleware Control"
- Section 13.4.2, "Choosing the Active Events Server Connection Using WLST"

13.4.1 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 WebCenter Spaces. For more information, see Section 6.2, "Navigating to the Home Page for WebCenter Spaces."
2. From the **WebCenter** menu, choose **Settings** > **Service Configuration**.
3. From the list of services on the WebCenter Services Configuration page, 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 application is deployed. For more information, see Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."

13.4.2 Choosing the Active Events Server Connection Using WLST

Use the WLST command `setPersonalEventConnection` with `default=true` to activate an existing events 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 1.12.3.1, "Running Oracle WebLogic Scripting Tool (WLST) Commands."

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

13.5 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 application is deployed.

This section includes the following subsections:

- Section 13.5.1, "Modifying Events Server Connection Details Using Fusion Middleware Control"
- Section 13.5.2, "Modifying Events Server Connection Details Using WLST"

13.5.1 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 WebCenter Spaces. For more information, see Section 6.2, "Navigating to the Home Page for WebCenter Spaces."
2. From the **WebCenter** menu, choose **Settings** > **Service Configuration**.
3. From the list of services on the WebCenter 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 13–2.
6. Click **OK** to save your changes.
7. To start using the updated (active) connection you must restart the managed server on which the WebCenter application is deployed. For more information, see Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."

13.5.2 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 1.12.3.1, "Running Oracle WebLogic Scripting Tool (WLST) Commands."

Note: To start using the updated (active) connection you must restart the managed server on which the WebCenter application is deployed. For more information, see the section, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

13.6 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 13.6.1, "Deleting Event Server Connections Using Fusion Middleware Control"
- Section 13.6.2, "Deleting Event Server Connections Using WLST"

13.6.1 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 WebCenter Spaces. For more information, see Section 6.2, "Navigating to the Home Page for WebCenter Spaces."
2. From the **WebCenter** menu, choose **Settings** > **Service Configuration**.
3. From list of services on the WebCenter 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 application is deployed. For more information, see Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."

13.6.2 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 1.12.3.1, "Running Oracle WebLogic Scripting Tool (WLST) Commands."

13.7 Testing Event Server Connections

To confirm the connection to the event servers:

1. In WebCenter Spaces, create a page in your personal space.
2. Add the Events task flow to the page.
3. Log in to your Microsoft Exchange Server account.
4. Your personal events from Microsoft Exchange Server should display in the task flow.

13.8 Troubleshooting Issues with Events

If users cannot see their personal events, verify the following:

- Is the Microsoft Exchange Server/IIS server is accessible from the managed server on which the WebCenter application is deployed? Can they ping each other?
- Is the configuration correct on the Microsoft Exchange Server? For more information, see Section 13.2.1.2, "Microsoft Exchange Server 2007 - Configuration" or Section 13.2.2.2, "Microsoft Exchange Server 2003 - Configuration."
- Is the events server connection correct in the managed server? For more information, see Section 13.3, "Registering Events Servers."
- Did the user enter the correct user name and password for the account on the Microsoft Exchange Server?

14 Managing the Instant Messaging and Presence Service

This chapter describes how to configure and manage the Instant Messaging and Presence (IMP) service for WebCenter Spaces and custom WebCenter applications.

Always use Fusion Middleware Control or WLST command-line tool to review and configure back-end services for WebCenter applications. Any changes that you make to WebCenter applications, post deployment, are stored in MDS metatdata store as customizations. See Section 1.3.5, "Oracle WebCenter Configuration Considerations."

Note: Changes that you make to WebCenter services configuration, through Fusion Middleware Control or using WLST, are not dynamic so you must restart the managed server on which the WebCenter application is deployed for your changes to take effect. See Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."

This chapter includes the following sections:

- Section 14.1, "What You Should Know About Instant Messaging and Presence Connections"
- Section 14.2, "Instant Messaging and Presence Server Prerequisites"
- Section 14.3, "Registering Instant Messaging and Presence Servers"
- Section 14.4, "Choosing the Active Connection for Instant Messaging and Presence"
- Section 14.5, "Modifying Instant Messaging and Presence Connection Details"
- Section 14.6, "Deleting Instant Messaging and Presence Connections"
- Section 14.7, "Setting Up Instant Messaging and Presence Service Defaults"
- Section 14.8, "Testing Instant Messaging and Presence Connections"
- Section 14.9, "Troubleshooting Issues with Instance Messaging and Presence"

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 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 is certified with Microsoft Office Communications Server (OCS) 2007 and Microsoft Office Live Communications Server (LCS) 2005, and it can integrate with other presence servers. Oracle WebLogic Communications Services (OWLCS) 11*g* is available for download on Oracle Technology Network (OTN) at `http://www.oracle.com/technology/index.html`. For information on OWLCS installation, see *Oracle Fusion Middleware Installation Guide for Oracle WebCenter*.

> **Note:** To add or remove buddies to your account, you must use the OCS, LCS, or OWLCS client. In WebCenter applications you can see buddies, but you cannot add or remove buddies. For more information, see the *Oracle WebLogic Communication Services Administrator's Guide*.

You can register the presence server connection for your WebCenter 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.

14.2 Instant Messaging and Presence Server Prerequisites

This section includes the following subsections:

- Section 14.2.1, "Microsoft Office Communications Server (OCS) Prerequisites"
- Section 14.2.2, "Microsoft Live Communications Server (LCS) Prerequisites"
- Section 14.2.3, "Oracle WebLogic Communications Server (OWLCS) Prerequisites"

14.2.1 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 14.2.1.1, "OCS - Installation"
- Section 14.2.1.2, "OCS - Configuration"
- Section 14.2.1.3, "OCS - Security Considerations"
- Section 14.2.1.4, "OCS - Limitations"

14.2.1.1 OCS - Installation

Refer to the Microsoft Office Communications Server 2007 documentation for installation information.

14.2.1.2 OCS - Configuration

To use Microsoft OCS 2007 as the presence server for the IMP service, you must install the Microsoft Unified Communications Managed API (UCMA) 2.0 SDK, and you must install the Oracle RTC Web service for Microsoft OCS 2007.

1. To install Microsoft UCMA 2.0, navigate to one of the following locations:

   - 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. The file extracts the setup files at `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. The file extracts setup files at `C:\Microsoft Unified Communications Managed API 2.0 SDK Installer package\amd64`.

   Go to the directory and run `vcredist_x86.exe`. This installs the Visual C++ 2008 redistributable. Then navigate to the `Setup` directory and run `UcmaRedist.msi`. This installs the UCMA 2.0 assemblies in the GAC.

2. To install the Oracle Web service for Microsoft OCS, extract the `owc_ocs2007.zip` from the Oracle Fusion Middleware companion CD. This creates a directory named `OCSWebServices`.

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 14–1. The Virtual Directory Creation Wizard displays.

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_ocs2007.zip` file; for example, `C:\OCSWebServices`. 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.

11. Click **Next**.

12. Click **Finish**. The newly created virtual directory appears under Default Web Site in the IIS Manager window.

13. Right-click the newly created virtual directory for the Oracle RTC Web service, and 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

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. 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 that you created for the Oracle RTC Web service. For example:

    ```
    http://localhost/RTC/OCSWebService.asmx
    ```

14.2.1.3 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 buddies and 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 14.3.1, "Registering Instant Messaging and Presence Servers Using Fusion Middleware Control."

14.2.1.4 OCS - Limitations

WebCenter applications do not support phone conferencing.

14.2.2 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 14.2.2.1, "LCS - Installation"
- Section 14.2.2.2, "LCS - Configuration"
- Section 14.2.2.3, "LCS - Security Considerations"
- Section 14.2.2.4, "LCS - Limitations"

14.2.2.1 LCS - Installation

Refer to the Microsoft Live Communications Server 2005 documentation for installation information.

14.2.2.2 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`

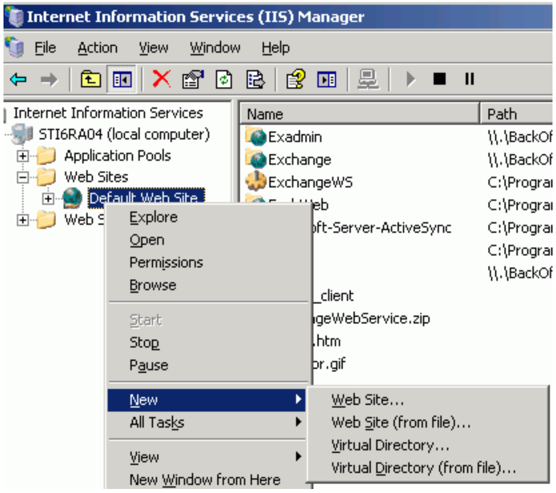
   `RTCService.asmx`

   `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 14–1. The Virtual Directory Creation Wizard displays.

Figure 14–1 Creating a Virtual Directory



6. Click **Next**.

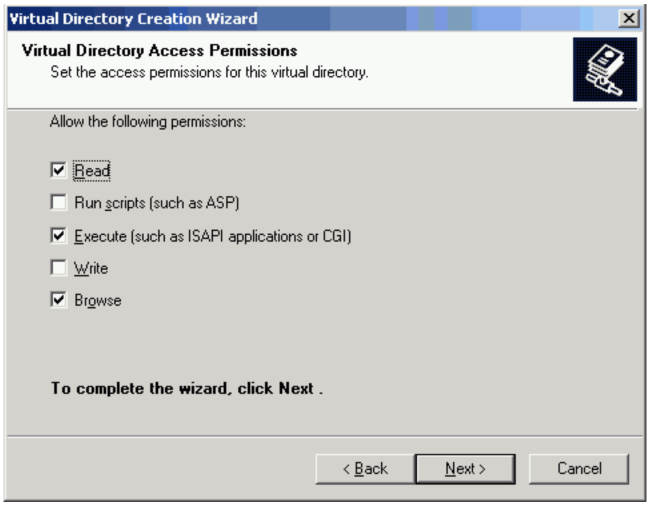
7. Enter an alias for the virtual directory in the **Alias** field, for example **RTC**.

8. Enter the path to the directory where you extracted the `owc_lcs.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 14–2)

Figure 14–2 Virtual Directory Properties



Virtual Directory Creation Wizard

Virtual Directory Access Permissions

Set the access permissions for this virtual directory.

Allow the following permissions:

☑ Read

☐ Run scripts (such as ASP)

☑ Execute (such as ISAPI applications or CGI)

☐ Write

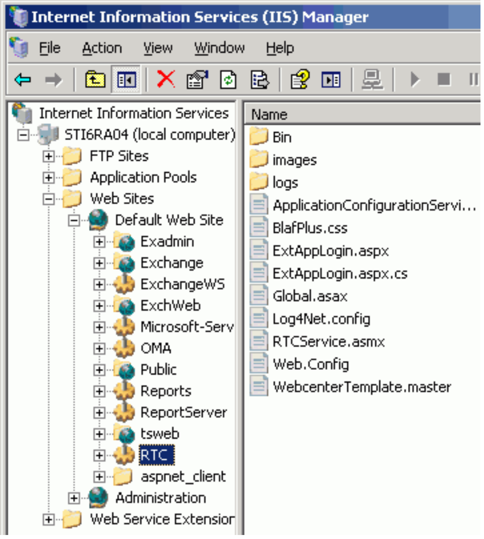
☑ Browse

To complete the wizard, click Next .

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 14–3).

Figure 14–3 Adding a Virtual Directory



Internet Information Services (IIS) Manager

Internet Information Services
STI6RA04 (local computer)
FTP Sites
Application Pools
Web Sites
Default Web Site
Exadmin
Exchange
ExchangeWS
ExchWeb
Microsoft-Serv
OMA
Public
Reports
ReportServer
tsweb
RTC
aspnet_client
Administration
Web Service Extensior

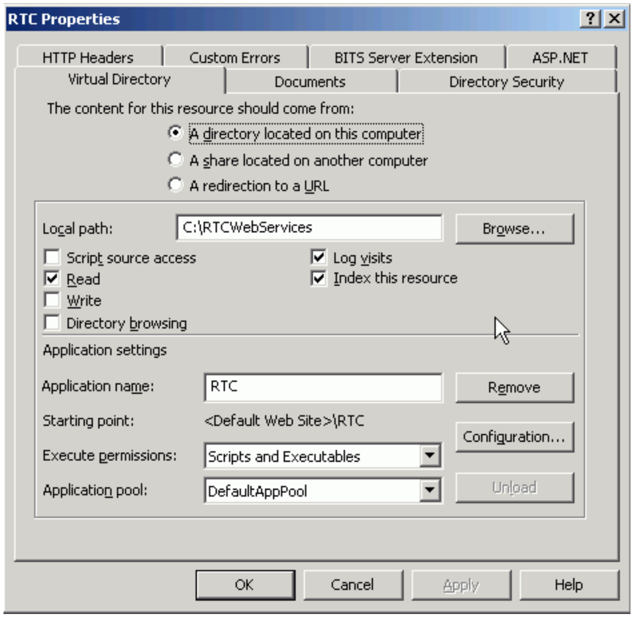
Name
Bin
images
logs
ApplicationConfigurationServi...
BlafPlus.css
ExtAppLogin.aspx
ExtAppLogin.aspx.cs
Global.asax
Log4Net.config
RTCService.asmx
Web.Config
WebcenterTemplate.master

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 14–4).

Figure 14–4 Virtual Directory Properties



The content for this resource should come from:

● A directory located on this computer
○ A share located on another computer
○ A redirection to a URL

Local path: C:\RTCWebServices

☐ Script source access
☑ Read
☐ Write
☐ Directory browsing
☑ Log visits
☑ Index this resource

Application settings

Application name: RTC

Starting point: <Default Web Site>\RTC

Execute permissions: Scripts and Executables

Application pool: DefaultAppPool

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
```

14.2.2.3 LCS - Security Considerations

You must configure an external application for Microsoft Live Communications Server connections so that users can supply credentials to authenticate themselves on the LCS server.

With a secured application, users get buddies and presence status. With LCS, if security is required, then LCS should be on a private trusted network.

LCS provides an option for changing external credentials, which works as an alternative to using an external application. A logged-in user can click any Presence tag and select **Change Credentials** from the menu.

For more information, see Section 14.3.1, "Registering Instant Messaging and Presence Servers Using Fusion Middleware Control."

14.2.2.4 LCS - Limitations

WebCenter applications do not support phone conferencing.

14.2.3 Oracle WebLogic Communications Server (OWLCS) Prerequisites

This section describes Oracle WebLogic Communications Server (OWLCS) prerequisites as the presence server for the Instant Messaging and Presence service.

This section includes the following subsections:

- Section 14.2.3.1, "OWLCS - Installation"
- Section 14.2.3.2, "OWLCS - Configuration"
- Section 14.2.3.3, "OWLCS - Security Considerations"
- Section 14.2.3.4, "OWLCS - Limitations"

14.2.3.1 OWLCS - Installation

For detailed OWLCS installation instructions, see the *Oracle WebLogic Communication Services Installation Guide*.

14.2.3.2 OWLCS - Configuration

OWLCS supports both identity propagation and external application-based connections. Oracle recommends using identity propagation for OWLCS connections, since additional security can be set with WS-Security.

OWLCS and the WebCenter application should point to the same LDAP-based identity store. If the OWLCS server and the WebCenter application use different LDAP-based identity stores, then you must configure an external application for the connection so that users can supply credentials to authenticate themselves on the OWLCS server.

For information on reassociating the WebCenter applications identity store, see Section 24.1, "Reassociating the Identity Store with an External LDAP."

If necessary, reconfigure OWLCS to use the same identity store. For more information, see the *Oracle WebLogic Communication Services Administrator's Guide*.

14.2.3.3 OWLCS - Security Considerations

If the OWLCS server is running with WS-Security enabled, then the administrator must set the `policyURI` parameter in the presence server connection.

If WS-Security is not required, then the administrator should disable WS-Security on the OWLCS server.

For more information, see Section 28.4, "Securing Oracle WebLogic Communication Services (OWLCS) with WS-Security" and Section 27.12, "Securing the WebCenter Spaces Connection to OWLCS with SSL."

14.2.3.4 OWLCS - Limitations

With OWLCS, user creation and deletion is manual. Any time a new user is added to (or removed from) the application's identity store, the same user must be created in (or removed from) the OWLCS user store.

Each OWLCS user has a watcher list, which is a list of the other users allowed to see his presence. This watcher list must be under 125 KB (approximately 400 users). In WebCenter, the presence of all users must be visible, even if they are not buddies of the logged-in user. To get their presence, WebCenter creates a new account on OWLCS with the group space GUID and adds this new user as a watcher of the visible users. In other words, each member of a group space has an entry of that group space GUID in his watcher list. A problem can arise when a user is part of many group spaces. Because the watcher list contains entries for each group space, its size can grow greater than 125KB. When that happens, updates to the watcher list are rejected, giving the user a "Subscription Request" popup with that scope GUID. If this happens, then the user should just cancel the subscription request.

14.3 Registering Instant Messaging and Presence Servers

You can register multiple presence server connections with a WebCenter application but only one of them is active at a time.

To start using the new (active) presence server you must restart the managed server on which the WebCenter application is deployed.

This section includes the following subsections:

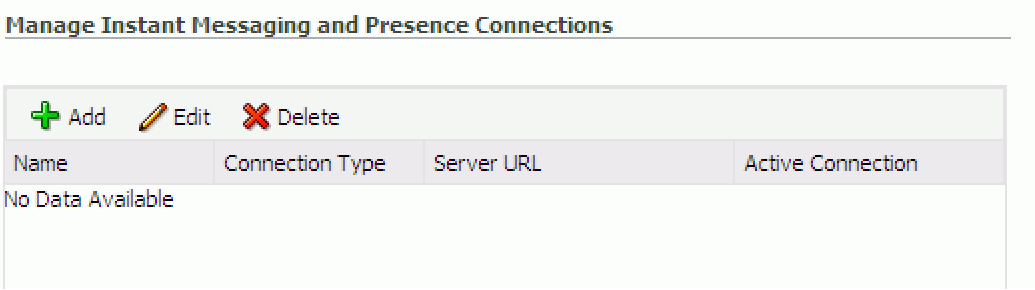
- Section 14.3.1, "Registering Instant Messaging and Presence Servers Using Fusion Middleware Control"
- Section 14.3.2, "Registering Instant Messaging and Presence Servers Using WLST"

14.3.1 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 WebCenter Spaces or the custom WebCenter application. For more information, see:
   - Section 6.2, "Navigating to the Home Page for WebCenter Spaces"
   - Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"
2. Do one of the following:
   - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings** > **Service Configuration**.
   - For WebCenter applications - From the **Application Deployment** menu, choose **WebCenter** > **Service Configuration**.
3. From the list of services on the WebCenter Service Configuration page, choose **Instant Messaging and Presence**.
4. To connect to a new presence server, click **Add** (Figure 14–5).

Figure 14–5 Configuring Instant Messaging and Presence Services



Manage Instant Messaging and Presence Connections

Name	Connection Type	Server URL	Active Connection
No Data Available			

5. Enter a unique name for this connection, specify the presence server type, and indicate whether this connection is the active (or default) connection for the application (Table 14–1).

Table 14–1 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 application.
Connection Type	Specify the type of presence server: ▪ **LCS** - Microsoft Live Communications Server ▪ **OCS** - Microsoft Office Communications Server ▪ **OWLCS** - Oracle WebLogic Communications Server Out-of-the-box, three presence connection types are available—LCS, OCS, and OWLCS.
Active Connection	Select to use this connection in the WebCenter application for instant messaging and presence services. While you can register multiple presence server connections for a WebCenter 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 14–2).

Table 14–2 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: `http://myocshost.com:8888`

Table 14–2 (Cont.) Instant Messaging and Presence Connection - Connection Details

Field	Description
Domain	Enter the domain associated with this connection. The domain specified is used to construct each user's IM ID. For example, if the domain is `oracle.com` and presence is requested for user with name `john`, then the IM address resolved is `john@oracle.com`. If the user IM address must be resolved from the Oracle Internet Directory/LDAP server, then specify the user profile attribute that provides the IM address here as `profile:<attribute>` where `profile` is a keyword and `attribute` is the user profile attribute name where the IM address is stored. For example, `profile:primarySipAddress`. WebCenter and the presence server should share the same Oracle Internet Directory/LDAP. The IM ID is the SIP ID; that is, `sip:john@oracle.com`. SIP is short for Session Initiation Protocol - an Internet protocol for live communication between people.
Connection Timeout (in seconds)	Specify a suitable timeout for the connection. This is the length of time (in seconds) the WebCenter application waits for a response from the presence server before issuing a connection timeout message. The default is -1 which means that the service default is used. The service default is 10 seconds.
Associated External Application	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. An external application is mandatory for Microsoft LCS and OCS connections. You can select an existing external application from the list, or click **Create New** to configure a new external application. The external application you configure for the Instant Messaging and Presence service must use the `POST` authentication method, and specify an additional field named `Account` (Name property) that is configured to `Display to User` (checked). For more information, see Chapter 22, "Managing External Applications."
Authentication Method	(OWLCS Only) Specify how to authenticate users against the instant messaging and presence server. Select from: ■ **Identity Propagation** - Select this option if you want the application and OWLCS to use the same user identity. ■ **External Application** - Use an external application to authenticate users against the instant messaging and presence server. Select this option to use public, shared, or mapped credentials. If an external application is used for authentication, use the **Associated External Application** list to identify the application. If the application you want is not listed, select **Create New...** to define the external application.
Policy URI	(OWLCS Only) Specify the URI to the WS-Security policy that is required for authentication on the Oracle WebLogic Communication Server. Specify `oracle/wss11_saml_token_with_message_protection_client_policy` when OWLCS is WS-Security enabled.

Table 14–2 (Cont.) Instant Messaging and Presence Connection - Connection Details

Field	Description
User Domain	(OCS Only) Enter the Active Directory domain on Microsoft Office Communications Server. The user domain is mandatory for OCS connections.
OCS Server	(OCS Only) Enter the name of the Microsoft Office Communications Server pool used for this connection. The pool name is mandatory for OCS connections. See the Microsoft Office Communications Server 2007 documentation for more information.
LCS Pool Name	(LCS Only) Enter the name of the Microsoft Live Communications Server pool used for this connection. The pool name is mandatory for LCS connections. See the Microsoft Live Communications Server documentation for details on the pool name.

7. Sometimes, additional parameters are required to connect to the presence server.

   If WS-Security is enabled on this connection, add a property named `recipient.alias` and enter the alias used to import the OWLCS certificate. Ensure that this value is unique and is not used by some other service. If no alias name is supplied, then the default value is used (`webcenter_owlcs`).

   Table 14–3 lists additional parameters.

Table 14–3 Additional IMP Connection Properties

Additional Connection Property	Description
presence.url	(OWLCS only) URL to the OWLCS Presence service. Required if the OWLCS Presence service is deployed on a separate node. When no value is specified, the `Server URL` property is used.
contacts.url	(OWLCS only) URL to the OWLCS Contact Management service. Required if the OWLCS Contact Management service is deployed on a separate node. When no value is specified, the `Server URL` property is used.
call.url	(OWLCS only) URL to the OWLCS Third Party Call service. Required if the OWLCS Third Party Call service is deployed on a separate node. When no value is specified, the `Server URL` property is used.
call.method	(OWLCS only) Third party call method. Valid values are: `sip` and `pstn`. The default value is `sip`. When set to `sip`, the IMP service forwards the user's SIP address to the third-party call service. The third-party call service must decide on the routing of the call. If it is set to `pstn`, then the user's phone number is based on the user's profile attribute (`BUSINESS_PHONE`). This default profile attribute (`BUSINESS_PHONE`) can be changed to any other attribute with the connection property `call.number.attribute`.
call.domain	(OWLCS only) Domain name of the PSTN gateway. Required when the `call.method` is `pstn`.

Table 14–3 (Cont.) Additional IMP Connection Properties

Additional Connection Property	Description
contact.number.attribute	(OWLCS only) User profile attribute used to store users' phone numbers. The default attribute is `BUSINESS_PHONE`. Required when the `call.method` is `pstn`.
primary.domain	(OWLCS and LCS) User domain. This property is required when WebCenter user names are qualified with a domain. For example, when user names are `xyz@example.com`, the `primary.domain` is `example.com`. This property is used by `IMPAddressResolver` to resolve user names to sip-address, and vice-versa. If this property is not supplied, then there could be inconsistencies in the resolver functions, which can affect IMP service performance.

If additional parameters are required to connect to the presence server, expand **Additional Properties** and enter details as required (Table 14–4).

Table 14–4 Instant Messaging and Presence Connection - Additional Properties

Field	Description
Add	Click **Add** to specify an additional connection parameter: ▪ **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. For example, select this option to secure the `admin.password` property where the value is the actual password.
Delete	Click **Delete** to remove a selected property. Select the correct row before clicking **Delete**. **Note:** Deleted rows appear disabled until you click **OK**.

8. Click **OK** to save this connection.
9. To start using the new (active) connection you must restart the managed server on which the WebCenter application is deployed. For more information, see Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."

14.3.2 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 the *Oracle Fusion Middleware WebLogic Scripting Tool Command Referenc*e.

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

To configure the Instant Messaging and Presence service to actively use a new IMP connection, set `default=true`. For more information, see Section 14.4.2, "Choosing the Active Connection for Instant Messaging and Presence Using WLST."

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

14.4 Choosing the Active Connection for Instant Messaging and Presence

You can register multiple instant messaging and presence server connections with a WebCenter application but only one connection is active at a time.

For WebCenter Spaces and any custom WebCenter application, the *active connection* becomes the back-end presence server for the Buddies task flow.

This section includes the following subsections:

- Section 14.4.1, "Choosing the Active Connection for Instant Messaging and Presence Using Fusion Middleware Control"
- Section 14.4.2, "Choosing the Active Connection for Instant Messaging and Presence Using WLST"

14.4.1 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 WebCenter Spaces or the custom WebCenter application. For more information, see:
   - Section 6.2, "Navigating to the Home Page for WebCenter Spaces"
   - Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"
2. Do one of the following:
   - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings** > **Service Configuration**.
   - For WebCenter applications - From the **Application Deployment** menu, choose **WebCenter** > **Service Configuration**.
3. From the list of services on the WebCenter Services Configuration page, 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** check box.
6. Click **OK** to update the connection.
7. To start using the new (active) connection you must restart the managed server on which the WebCenter application is deployed. See Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."

14.4.2 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 the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

To disable a presence server connection, either delete it, make another connection the 'active connection' or use the `removeIMPServiceProperty` command:

```
removeIMPServiceProperty('appName='webcenter', property='selected.connection')
```

Using this command, connection details are retained but the connection is no longer named as an active connection. For more information, see the section, "removeIMPServiceProperty" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

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

> **Note:** To start using this active connection you must restart the managed server on which the WebCenter 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*.

14.5 Modifying Instant Messaging and Presence Connection Details

You can modify instant messaging and presence server connection details at any time.

To start using an updated (active) connection you must restart the managed server on which the WebCenter application is deployed.

This section includes the following subsections:

- Section 14.5.1, "Modifying Instant Messaging and Presence Connections Details Using Fusion Middleware Control"
- Section 14.5.2, "Modifying Instant Messaging and Presence Connections Details Using WLST"

14.5.1 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 WebCenter Spaces or the custom WebCenter application. For more information, see:
   - Section 6.2, "Navigating to the Home Page for WebCenter Spaces"
   - Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"
2. Do one of the following:
   - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings** > **Service Configuration**.

- For WebCenter applications - From the **Application Deployment** menu, choose **WebCenter** > **Service Configuration**.

3. From the list of services on the WebCenter Service Configuration page, 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 14–2, " 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 application is deployed. For more information, see Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."

14.5.2 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 the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

If additional parameters are required to connect to your presence server, then use the `setIMPConnectionProperty` command. For more information, see the section, "setIMPConnectionProperty" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

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

> **Note:** To start using the updated (active) connection you must restart the managed server on which the WebCenter application is deployed. For more information, see the section, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

14.6 Deleting Instant Messaging and Presence Connections

You can delete instant messaging and presence connections at any time but take care when deleting the active connection. If you delete the active connection, Buddies task flows does not work and 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 22.5, "Deleting External Application Connections."

This section includes the following subsections:

- Section 14.6.1, "Deleting Instant Messaging and Presence Connections Using Fusion Middleware Control"
- Section 14.6.2, "Deleting Instant Messaging and Presence Connections Using WLST"

14.6.1 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 WebCenter Spaces or the custom WebCenter application. For more information, see:
   - Section 6.2, "Navigating to the Home Page for WebCenter Spaces"
   - Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"
2. Do one of the following:
   - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings** > **Service Configuration**.
   - For WebCenter applications - From the **Application Deployment** menu, choose **WebCenter** > **Service Configuration**.
3. From the list of services on the WebCenter Service Configuration page, 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 application is deployed. For more information, see Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."

> **Note:** Before restarting the managed server, mark another connection as active; otherwise, the service is disabled.

14.6.2 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 the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

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

14.7 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`: Whether the display name of the user should be resolved by making an LDAP lookup. Valid values are `true` and `false`. If enabled (`true`), then the IMP service makes an LDAP lookup to find each user's display name. This should be enabled only when the same LDAP store is used for both WebCenter and the presence server. If different LDAP servers are used, then irrelevant information may display. This property can impact performance.

For command syntax and detailed examples, see the section, "setIMPServiceProperty" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

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

14.8 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 Microsoft OCS or LCS connection, try accessing the endpoint for the WebCenter 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`

To verify an OWLCS connection, try accessing the endpoint for the following Web services. For example:

- `*protocol*://*host*:*port*/PresenceConsumerService/services/PresenceConsumer`
- `*protocol*://*host*:*port*/PresenceSupplierService/services/PresenceSupplier`
- `*protocol*://*host*:*port*/ThirdPartyCallService/services/ThirdPartyCall`
- `*protocol*://*host*:*port*/services`

14.9 Troubleshooting Issues with Instance Messaging and Presence

This section contains troubleshooting tips for the IMP service.

Problem

Buddies are not visible in a custom WebCenter application. Further, the presence status of users is not available.

Solution

Ensure the following:

- IMP connection is configured properly and the base URL and domain values are correct. See Section 14.3, "Registering Instant Messaging and Presence Servers."
- Web Services for the presence server is installed properly and is up and running. For Web Services installation for Microsoft Live Communications Server, see Section 10.2.2.2, "Microsoft Live Communications Server (LCS) Prerequisites." For Web Services installation for Oracle WebLogic Communications Server, see the *Oracle WebLogic Communication Services Administrator's Guide*.
- Back-end presence server (Microsoft Live Communications Server 2005, Microsoft Office Communications Server 2007, or Oracle WebLogic Communications Server) is up and running. A quick way to verify this is to ensure that the user can connect to the communications server by using a supported SIP client (Oracle Communicator or Microsoft Communicator).

- User is logged in with valid user credentials and the user exists on the communications server. For Microsoft OCS or LCS, verify that user has provided correct credentials in the external application.

15 Managing the Mail Service

This chapter describes how to configure and manage the Mail service for WebCenter Spaces and custom WebCenter 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 the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

Always use Fusion Middleware Control or WLST command-line tool to review and configure back-end services for WebCenter applications. Any changes that you make to WebCenter applications, post deployment, are stored in MDS metatdata store as customizations. See Section 1.3.5, "Oracle WebCenter Configuration Considerations."

> **Note:** Changes that you make to WebCenter services configuration, through Fusion Middleware Control or using WLST, are not dynamic so you must restart the managed server on which the WebCenter application is deployed for your changes to take effect. See Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."

This chapter includes the following sections:

- Section 15.1, "What You Should Know About Mail Server Connections"
- Section 15.2, "Mail Server Prerequisites"
- Section 15.3, "Registering Mail Servers"
- Section 15.4, "Choosing the Active (or Default) Mail Server Connection"
- Section 15.5, "Modifying Mail Server Connection Details"
- Section 15.6, "Deleting Mail Server Connections"
- Section 15.7, "Setting Up Mail Service Defaults"
- Section 15.8, "Testing Mail Server Connections"
- Section 15.9, "Setting Send Mail Notifications for WebCenter Spaces"
- Section 15.10, "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."

15.1 What You Should Know About Mail Server Connections

WebCenter supports the Microsoft Exchange Server or any mail server that supports IMAP4 and SMTP. To enable WebCenter users to access mail within a WebCenter application and perform basic operations such as read, reply, and forward, you must first register the appropriate mail server with the WebCenter application. The Mail service is not configured out-of-the-box.

You can register multiple mail server connections:

- **WebCenter Spaces** supports multiple mail connections. The mail connection marked *active* is the default connection for mail services in WebCenter Spaces. All additional connections are offered as alternatives; WebCenter Spaces users can choose which one they want to use through user preferences.
- **Custom WebCenter applications** only use one mail connection—the connection marked *active*. Any additional connections are ignored.

15.2 Mail Server Prerequisites

This section includes the following subsections:

- Section 15.2.1, "Mail Server - Installation"
- Section 15.2.2, "Mail Server - Configuration"
- Section 15.2.3, "Mail Server - Security Considerations"
- Section 15.2.4, "Mail Server - Limitations"

15.2.1 Mail Server - Installation

See your mail server documentation for installation information.

15.2.2 Mail Server - Configuration

You can allow WebCenter to create and manage group space distribution lists in WebCenter Spaces (or in custom WebCenter applications leveraging WebCenter Spaces group space management). This feature is supported only with Microsoft Exchange. The group space distribution list is created automatically whenever a group space is created. Users added or removed from the group space are implicitly added or removed from the corresponding group space distribution list, provided users created on Microsoft Exchange Active Directory correspond with users created in the identity store used by the WebCenter 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 15.3.1, "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 application's identity store, see Section 24.3, "Adding Users to the Embedded LDAP Identity Store."

Microsoft Exchange 2007 is the only mail server 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.

15.2.2.1 Configuring Microsoft Exchange Server 2007 for WebCenter

The Microsoft Exchange Server 2007 certificate must be added to the WebCenter keystore. This requires the following steps.

1. Section 15.2.2.1.1, "Obtain the Certificate from the Microsoft Exchange Server 2007."
2. Section 15.2.2.1.2, "Add the Certificate to the WebCenter Keystore."
3. Restart the server after the certificate is imported.

15.2.2.1.1 Obtain the Certificate from the Microsoft Exchange Server 2007

Obtain the certificate from your mail server installation administrator. This section describes one way to get the certificate from the Microsoft Exchange Server 2007.

Follow these steps to obtain the certificate from a Microsoft Exchange 2007 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 2007.

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 the *Oracle Fusion Middleware Command Reference for Oracle WebLogic Server*.

15.2.2.1.2 Add the Certificate to the WebCenter 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 26.3.2.1.2, "Generating and Registering Certificates," for information about adding the certificate to the keystore.

2. Restart the server.

15.2.2.1.3 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 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.

15.2.3 Mail Server - Security Considerations

For more information, see Section 27.9, "Securing the WebCenter Spaces Connection to IMAP and SMTP with SSL."

Note: If LDAP is configured to run in secure mode, then add the `LDAP Secured` property (set to `true/false`) to use LDAP while creating distribution lists. For more information, see Table 15–3.

15.2.4 Mail Server - Limitations

In WebCenter Spaces, the Mail service requires a Microsoft Exchange mail server connection to enable automatic group space distribution lists.

15.3 Registering Mail Servers

You can register multiple mail server connections. To start using the new mail connections you must restart the managed server on which the WebCenter application is deployed.

This section includes the following subsections:

- Section 15.3.1, "Registering Mail Servers Using Fusion Middleware Control"

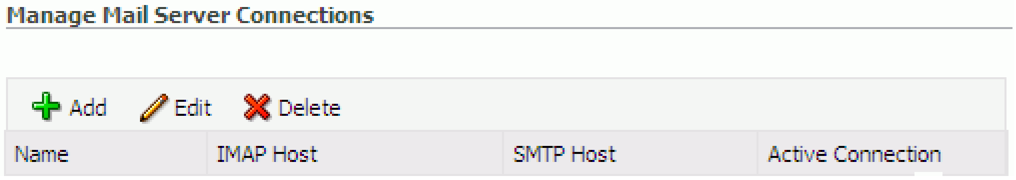
- Section 15.3.2, "Registering Mail Servers Using WLST"

15.3.1 Registering Mail Servers Using Fusion Middleware Control

To register a mail server with WebCenter applications:

1. Log in to Fusion Middleware Control and navigate to the home page for WebCenter Spaces or the custom WebCenter application. For more information, see:
   - Section 6.2, "Navigating to the Home Page for WebCenter Spaces"
   - Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"
2. Do one of the following:
   - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings** > **Service Configuration**.
   - For WebCenter applications - From the **Application Deployment** menu, choose **WebCenter** > **Service Configuration**.
3. From the list of services on the WebCenter Service Configuration page, select **Mail Server**.
4. To connect to a new mail server, click **Add** (Figure 15–1).

Figure 15–1 Configuring Mail Servers



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 15–1).

Table 15–1 Mail Server Connection - Name

Field	Description
Name	Enter a unique name for the connection. The name must be unique (across all connection types) within the WebCenter application.

Table 15–1 (Cont.) Mail Server Connection - Name

Field	Description
Active Connection	Select to indicate whether this connection is the default (or active) connection for the Mail service. You can register multiple mail server connections: ■ **WebCenter Spaces** supports multiple mail connections. The mail connection marked *active* is the default connection for mail services in WebCenter Spaces. All additional connections are offered as alternatives; WebCenter Spaces users can choose which one they want to use through user preferences. ■ **Custom WebCenter applications** only use one mail connection—the connection marked *active*. Any additional connections are ignored.

6. Enter connection details for the mail server (Table 15–2).

Table 15–2 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.
Associated External Application	(Mandatory) Associate the mail server with an external application. External application credential information is used to authenticate users against the IMAP and SMTP servers. The Mail service uses the same credentials to authenticate the user on both IMAP and SMTP. You can select an existing external application from the list, or click **Create New** to configure a new external application. The external application you configure for the Mail service must use the `POST` authentication method, and specify an additional field named `Email Address` (Name property) that is configured to `Display to User` (checked). For more information, see Chapter 22, "Managing External Applications." If your WebCenter 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. WebCenter Spaces offers this feature on its self-registration page.

7. Specify LDAP connection details for the Active Directory server managing group space distribution lists (Table 15–3).

   This section applies to WebCenter Spaces (or custom WebCenter applications leveraging the WebCenter Spaces group space management feature). WebCenter applications support Microsoft Exchange where distribution lists are managed on an Active Directory server.

> **Note:** Active Directory server details must be provided as part of the mail connection for *group space distribution lists* to work.

Table 15–3 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, `CN=Users,DC=oracle,DC=com`.
LDAP Domain	Enter the domain to be appended to distribution list names. In WebCenter Spaces, for example, if the domain value is set to `example.com`, then the Finance Project group space maintains a distribution list named `FinanceProject@example.com`.
LDAP Administrator User Name	Enter the user name of the LDAP directory server administrator. A valid user with privileges to make entries into the LDAP schema.
LDAP Administrator 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 group space distribution list that is created. The users specified must exist in the base LDAP schema (specified in the `LDAP Base DN` field).
LDAP Secured	Indicate whether a secured connection (SSL) is required between the WebCenter application and the LDAP directory server.

8. Configure advanced options for the mail server connection (Table 15–4).

Table 15–4 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 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 add can more parameters to the mail server connection (Table 15–5).

Table 15–5 Additional Mail Connection Properties

Additional Connection Property	Description
Various IMAP properties	Any valid IMAP connection property. For example, `mail.imap.connectionpoolsize`. For a list of valid protocol properties, see your mail server documentation. For a list of standard IMAP properties, see the Java Mail APIs: `http://java.sun.com/products/javamail/javadocs/com/sun/mail/imap/package-summary.html`
Various SMTP properties	Any valid SMTP connection property. For example, `mail.smtp.timeout`. For a list of valid protocol properties, see your mail server documentation. For a list of standard SMTP properties, see the Java Mail APIs: `http://java.sun.com/products/javamail/javadocs/com/sun/mail/smtp/package-summary.html`

If additional parameters are required to connect to the mail server, expand **Additional Properties** and enter details as required (see Table 15–6, " Mail Connection - Additional Properties").

Table 15–6 Mail Connection - Additional Properties

Field	Description
Add	Click **Add** to specify an additional connection parameter: ■ **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. For example, select this option to secure the `admin.password` property where the value is the actual password.
Delete	Click **Delete** to remove a selected property. Select the correct row before clicking **Delete**. **Note:** Deleted rows appear disabled until you click **OK**.

10. Click **OK** to save this connection.
11. To start using the new (active) connection you must restart the managed server on which the WebCenter application is deployed. For more information, see Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."

15.3.2 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 the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

To configure the Mail service to use the new mail server connection as its default connection, set `default=true`. For more information, see Section 15.4.2, "Choosing the Active (or Default) Mail Server Connection Using WLST."

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

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

15.4 Choosing the Active (or Default) Mail Server Connection

You can register multiple mail server connections with a WebCenter application but only one connection can be designated as the default connection.

For WebCenter Spaces and custom WebCenter applications, the *default connection* becomes the back-end mail server for:

- Mail task flows
- Group space distribution lists
- Anywhere there is a **Send Mail** icon

This section includes the following subsections:

- Section 15.4.1, "Choosing the Active (or Default) Mail Server Connection Using Fusion Middleware Control"
- Section 15.4.2, "Choosing the Active (or Default) Mail Server Connection Using WLST"

15.4.1 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 WebCenter Spaces or the custom WebCenter application. For more information, see:
   - Section 6.2, "Navigating to the Home Page for WebCenter Spaces"
   - Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"
2. Do one of the following:
   - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings** > **Service Configuration**.
   - For WebCenter applications - From the **Application Deployment** menu, choose **WebCenter** > **Service Configuration**.
3. From the list of services on the WebCenter Services Configuration page, 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 application is deployed. For more information, see Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."

15.4.2 Choosing the Active (or Default) Mail Server Connection Using WLST

Use the WLST command `setMailConnection` with `default=true` to make an existing mail server connection the default connection for the Mail service. For command syntax and examples, see the section, "setMailConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

A connection does not cease to be the default connection for the Mail service if you change the default argument from `true` to `false`.

To disable a mail connection, either delete it, make another connection the 'active connection', or use the `removeMailServiceProperty` command:

```
removeMailServiceProperty(appName='webcenter', property='selected.connection')
```

Using this command, connection details are retained but the connection is no longer named as an active connection. For more information, see the section, "removeMailServiceProperty" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

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

> **Note:** To start using the active connection you must restart the managed server on which the WebCenter 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*.

15.5 Modifying Mail Server Connection Details

You can modify mail server connection details at any time.

To start using updated mail connections you must restart the managed server on which the WebCenter application is deployed.

This section includes the following subsections:

- Section 15.5.1, "Modifying Mail Server Connection Details Using Fusion Middleware Control"
- Section 15.5.2, "Modifying Mail Server Connection Details Using WLST"

15.5.1 Modifying Mail Server Connection Details Using Fusion Middleware Control

To update mail server connection details:

1. Log in to Fusion Middleware Control and navigate to the home page for WebCenter Spaces or the custom WebCenter application. For more information, see:
   - Section 6.2, "Navigating to the Home Page for WebCenter Spaces"
   - Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"
2. Do one of the following:
   - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings** > **Service Configuration**.
   - For WebCenter applications - From the **Application Deployment** menu, choose **WebCenter** > **Service Configuration**.
3. From the list of services on the WebCenter Service Configuration page, select **Mail Server**
4. Select the connection name, and click **Edit**.
5. Edit connection details, as required. For detailed parameter information, see Table 15–2, " Mail Server Connection Parameters".
6. Click **OK** to save your changes.
7. To start using updated connection details you must restart the managed server on which the WebCenter application is deployed. For more information, see Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."

15.5.2 Modifying Mail Server Connection Details Using WLST

Use the WLST command `setMailConnection` to edit existing mail server connection details. For command syntax and examples, see the section, "setMailConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

If additional parameters are required to connect to your mail server, use the `setMailConnectionProperty` command. For more information, see the section, "setMailConnectionProperty" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

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

> **Note:** To start using the updated connections you must restart the managed server on which the WebCenter 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 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 22.5, "Deleting External Application Connections."

This section includes the following subsections:

- Section 15.6.1, "Deleting a Mail Connection Using Fusion Middleware Control"
- Section 15.6.2, "Deleting a Mail Connection Using WLST"

15.6.1 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 WebCenter Spaces or the custom WebCenter application. For more information, see:
   - Section 6.2, "Navigating to the Home Page for WebCenter Spaces"
   - Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"
2. Do one of the following:
   - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings** > **Service Configuration**.
   - For WebCenter applications - From the **Application Deployment** menu, choose **WebCenter** > **Service Configuration**.
3. From the list of services on the WebCenter Services Configuration page, 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 application is deployed. For more information, see Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."

   Note: Before restarting the managed server, mark another connection as active; otherwise, the service is disabled.

15.6.2 Deleting a Mail Connection Using WLST

Use the WLST command `deleteConnection` to remove a mail server connection. For command syntax and examples, see the section, "deleteConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

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

15.7 Setting Up Mail Service Defaults

Use the WLST command `setMailServiceProperty` to set defaults for the Mail service:

- `mail.messages.fetch.size`: Maximum number of messages displayed in mail inboxes
- `resolve.email.address.to.name`

For command syntax and examples, see the section, "setMailServiceProperty" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

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

15.8 Testing Mail Server Connections

Confirm that the mail server is up by connecting to the server using any client, such as Thunderbird or Outlook.

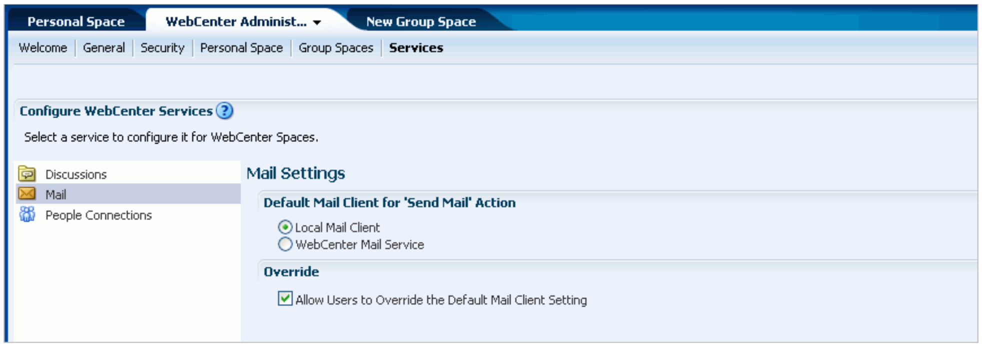
For Microsoft Exchange, go to **Administrative Tools** - **Services** to confirm that the following services are running (Status: Started):

- Microsoft Exchange IMAP4
- Simple Mail Transfer Protocol (SMTP)

15.9 Setting Send Mail Notifications for WebCenter Spaces

WebCenter Spaces administrators are responsible for setting mail options through WebCenter Spaces Administration (Figure 15–2).

Figure 15–2 Setting Mail Options



Configure WebCenter Services

Select a service to configure it for WebCenter Spaces.

Mail Settings

Default Mail Client for 'Send Mail' Action

● Local Mail Client
○ WebCenter Mail Service

Override

☑ Allow Users to Override the Default Mail Client Setting

From this page, you can assign the mail client for the "Send Mail" feature. This feature allows application resources to send mail directly from them, with the **Send Mail** icon (Figure 15–3).

Figure 15–3 Send Mail Icon

For example, from an announcement, users can click the **Send Mail** icon to open a mail window prepopulated with information including the announcement text, author, date created, and location. They can edit and add to the mail, as necessary. The way the mail window is prepopulated depends on the resource sending it. For example, from your Buddies list, users can click the **Send Mail** icon to open a mail window prepopulated only with the address of that person.

With group spaces, the mail can be addressed to the individual members of the group space, and, if the group space is configured with a distribution list, then it can be addressed to the distribution list. Group space moderators select the default for Send Mail actions (whether mails should be addressed to a distribution list, or individual member mail addresses, or both, or none) on the **Settings - Services - Mail** page.

> **Note:** When the **Send Mail** icon is clicked from a group space with a large number of members, length restrictions may prevent the local mail client from prepopulating the addresses of all group space members. The user gets an error and must enter the addresses manually. To avoid this error, configure a distribution list for the group space.

For all Send Mail notifications throughout WebCenter, you can choose to use either a local mail client or the WebCenter Mail service. The local mail client is the default. The Send Mail feature does not require the Mail service. That is, even if the Mail service has not been configured in your application, you can use the Send Mail feature with your local mail client.

The local mail (mailto) client allows plain text editing of the mail, but it does not allow attachments. Due to the limitations with the mailto URL (used for launching the local mail client), the text could be truncated.

The WebCenter Mail service launches the Mail Compose window. Although users cannot edit the prepopulated HTML (shown as the `content.html` attachment), they can view the prepopulated attachment, add other attachments, and add plain text to the compose window. If the WebCenter Mail service has not been configured in your application, then this option does not appear on the page.

You can select the checkbox to enable users to override the default mail client setting.

> **Note:** The Fusion Middleware administrator maintains the connection between WebCenter Spaces and the mail server. If you are experiencing issues with this connection, report the problem to the Fusion Middleware Administrator. See also, Section 15.3, "Registering Mail Servers."

15.10 Troubleshooting Issues with Mail

This section includes the following subsections:

- Section 15.10.1, "Mail Service is Not Accessible in Secure Mode"
- Section 15.10.2, "Mail Service is Not Accessible in Non-Secure Mode"
- Section 15.10.3, "Unable to Create Distribution Lists in the Non-Secure Mode"
- Section 15.10.4, "Unable to Create Distribution Lists in the Secure Mode"
- Section 15.10.5, "Unable to Configure the Number of Mails Downloaded"
- Section 15.10.6, "Unable to Publish and Archive Group Space Mail"
- Section 15.10.7, "Changing Passwords on Microsoft Exchange"
- Section 15.10.8, "Mail Content Sent as Attachments"

15.10.1 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 15.3, "Registering Mail Servers."
- Properties are set to `true` in your mail server.
  - `mail.imap.secured = true`
  - `mail.smtp.secured = true`

15.10.2 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 15.3, "Registering Mail Servers."
- Properties are set to `false` in your mail server.
  - `mail.imap.secured = false`
  - `mail.smtp.secured = false`

15.10.3 Unable to Create Distribution Lists in the Non-Secure Mode

Problem

You are unable to create group space distribution lists in non-secure mode (SSL not configured).

Solution

Check if the mail server has been reinstalled or the user has been deleted. Also ensure that the following parameters are configured accurately in non-secure mode, in the LDAP server:

- `ldapHost`
- `defaultUser`
- `ldapAdminPassword`
- `ldapBaseDN`
- `ldapPort`

See Section 15.3, "Registering Mail Servers."

15.10.4 Unable to Create Distribution Lists in the Secure Mode

Problem

You are unable to create group space distribution list in secure mode, that is, SSL is configured on the LDAP server.

Solution

Check if the mail server has been reinstalled or the user has been deleted. Also ensure that the following parameters are configured accurately in secure mode, in the LDAP server:

- `ldapHost`
- `defaultUser`
- `ldapAdminPassword`
- `ldapBaseDN`
- `ldapPort`
- `ldap.connection.secure, 'true'`

See Section 15.3, "Registering Mail Servers."

15.10.5 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 the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

15.10.6 Unable to Publish and Archive Group Space Mail

Problem

You are unable to archive group space mail.

Solution

If the archiving fails, check the following:

- In WebCenter Spaces, open WebCenter Administration pages, navigate to the Services tab, and then choose Discussions. Check whether the required configuration is accurate. See also, Section 12.10.3, "Enabling Discussion Forums to Publish Group Space Mail."
- Check whether the user account configured here is a member of the distribution list.
- For a particular group space, check whether the forum configured is available in the discussions server. See "Publishing Group Space Mail in a Discussion Forum" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.
- Check whether the user who sends mails to the distribution list is available in the discussions server and his mail address is the same.

15.10.7 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 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.

15.10.8 Mail Content Sent as Attachments

Problem

When users receive mail in WebCenter 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`.

16

Managing the People Connections Service

This chapter describes how to set application defaults for the People Connections service in WebCenter Spaces. You must log in to WebCenter Spaces with administrative privileges to set any of the application-wide properties described here.

This chapter includes the following sections:

- Section 16.1, "What You Should Know About Administering the People Connections Service"
- Section 16.2, "People Connections Prerequisites"
- Section 16.3, "Configuring the People Connections Service for WebCenter Spaces"
- Section 16.4, "Troubleshooting Issues with the People Connections Service"

Audience

The contents of this chapter is intended for WebCenter Spaces application administrators. Application administrators are users who are granted the WebCenter Spaces `Administrator` role or a custom role that grants the `Application-Manage` permission. Users with `Application-Configure and Manage People Connections` permission can also administer people connections.

> **Note:** The application skin determines the look and feel of your application. The application skin used for the screenshots in this chapter may not be the same as the application skin selected for your application; therefore, the look and feel of your application is likely to differ from that depicted in the screenshots in this chapter. However, the features depicted in the screenshots are the same.

16.1 What You Should Know About Administering the People Connections Service

People Connections administrative settings are useful for controlling all users' initial views of People Connections features, including:

- Activity Stream—A summary view of user activity
- Connections—Users who have agreed to be a given user's connections
- Profile—A summary of user information
- Message Board—A place for posting and receiving messages
- Feedback—A place for posting and receiving feedback

Use the People Connections administrative settings to enforce the values you specify or to enable users to override these values with their own People Connections Preferences (for more information, see the "Setting People Connections Preferences" section in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*).

Setting default values on the **WebCenter Administration** page affects all users' views of People Connections features. There are a few other levels at which these values can be set, and these setting levels are subject to an order of precedence:

- Administrative settings affect all users' views of People Connections features.
- Preferences settings affect the view of the user who set them, and they override administrative settings.
- Settings on a particular task flow affect just that task flow instance, and they override Preference settings:
  - Values set in edit mode (customization) affect all users' views of the task flow instance.
  - Values set in view mode (personalization) affect only that user's view of the task flow instance, and they override task flow customizations.

16.2 People Connections Prerequisites

No special set up is required to enable users to access the People Connections service. For the most part, the People Connections service stores information in the WebCenter Repository, which is a database with the WebCenter schema installed. The WebCenter schema is included with the product. To install the WebCenter schema, follow the steps described in the section, "Installing Oracle WebCenter" in the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter*.

For Profile information, all but three attributes are stored and read from the LDAP identity store that is configured against WebCenter Spaces. The three exceptions include: the profile photo, status message, and expertise. These are stored with other WebCenter data in the WebCenter Repository.

> **See Also:** For information about WebCenter Spaces and the LDAP identity store, see Chapter 24, "Configuring the Identity Store."

16.3 Configuring the People Connections Service for WebCenter Spaces

This section steps you through the process of setting application-wide values for People Connections features. It includes the following subsections:

- Section 16.3.1, "Accessing People Connections Administrative Settings"
- Section 16.3.2, "Configuring Activity Stream"
- Section 16.3.3, "Configuring Connections"
- Section 16.3.4, "Configuring Profile"
- Section 16.3.5, "Configuring Message Board"
- Section 16.3.6, "Configuring Feedback"

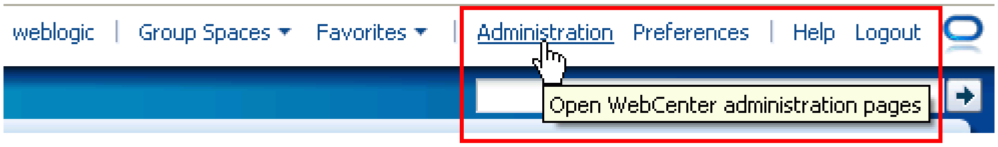
16.3.1 Accessing People Connections Administrative Settings

To access People Connections administrative settings:

1. Log in to WebCenter Spaces using your administrative user name and password.

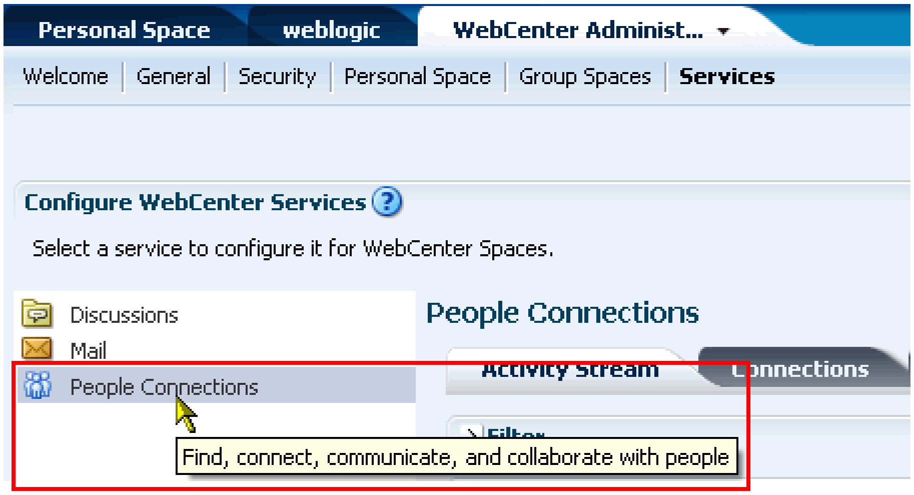
2. Click the **Administration** link at the top of the application (Figure 16–1) to open the **WebCenter Administrator Center** page.

Figure 16–1 Administration Link at the Top of the Application



3. Click the **Services** tab to bring it forward.
4. Select **People Connections** (Figure 16–2).

Figure 16–2 People Connections Option on the Services Tab



Tabs with the names of People Connections features appear to the right.

16.3.2 Configuring Activity Stream

Activity Stream provides a means of publishing your own application activity and tracking the activity of other users. The types of activity that are tracked depend on Activity Stream configuration. Table 16–1 lists the types of activities that may be tracked by Activity Stream.

Table 16–1 Activities Tracked by Activity Stream

Service	Tracked Activities	Scope	Activities Shared or Private
Announcements	■ Create announcement ■ Edit announcement ■ Delete announcement	Group space	Shared with other group space members
Discussions	■ Create forum ■ Delete forum ■ Create topic ■ Delete topic ■ Reply to topic ■ Delete reply	Group space	Shared with other group space members
Documents	■ Create document ■ Edit document ■ Delete document ■ Add tag ■ Remove tag	■ Group space ■ Personal space	■ Activities on group space documents are shared with other group space members. ■ Activities on personal space documents are private to user. ■ Activities on public page documents are shared with all users.
Events	■ Create an event ■ Edit an Event ■ Delete an event	Group space	Shared with other group space members
Group Space	■ Create group space ■ Join group space ■ Delete group space	Group space	Shared with other group space members
Lists	■ Create a list ■ Add a row to a list ■ Edit a list row ■ Delete a list	Group space	Shared with other group space members

Table 16–1 (Cont.) Activities Tracked by Activity Stream

Service	Tracked Activities	Scope	Activities Shared or Private
Page	■ Create page ■ Edit page ■ Delete page ■ Add tag ■ Remove tag	■ Group space ■ Personal space	■ Activities on group space pages are shared with other group space members. ■ Activities on personal space pages are private to user. ■ Activities on public pages are shared with all users.
People Connections	■ People are connected ■ Message Board post ■ Feedback post ■ Photo updated ■ Profile updated ■ Personal status note updated ■ Add tag to People Connections pages ■ Remove tag from People Connections pages	Personal space	Shared with whomever is permitted to view such activities (for more information, see this section and the section "Setting People Connections Preferences" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*).
Wiki and Blog	■ Create wiki ■ Edit wiki ■ Add wiki comment ■ Delete wiki ■ Create blog entry ■ Edit blog entry ■ Add blog entry comment ■ Delete blog entry **Note:** An Oracle WebCenter Wiki and Blog Server scheduled job (`ActivityPublishJob`) must be run in order for wiki and blog activities to be published to the Activity Stream. For more information, see Section 19.2.2.1.2, "About Administration Mode."	■ Group space ■ Personal space	■ Activities in a group space are shared with all group space members. ■ Activities in a personal space are shared with whomever is permitted to view such activities (for more information, see this section and the section "Setting People Connections Preferences" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*).

Activity Stream configuration falls under three categories:

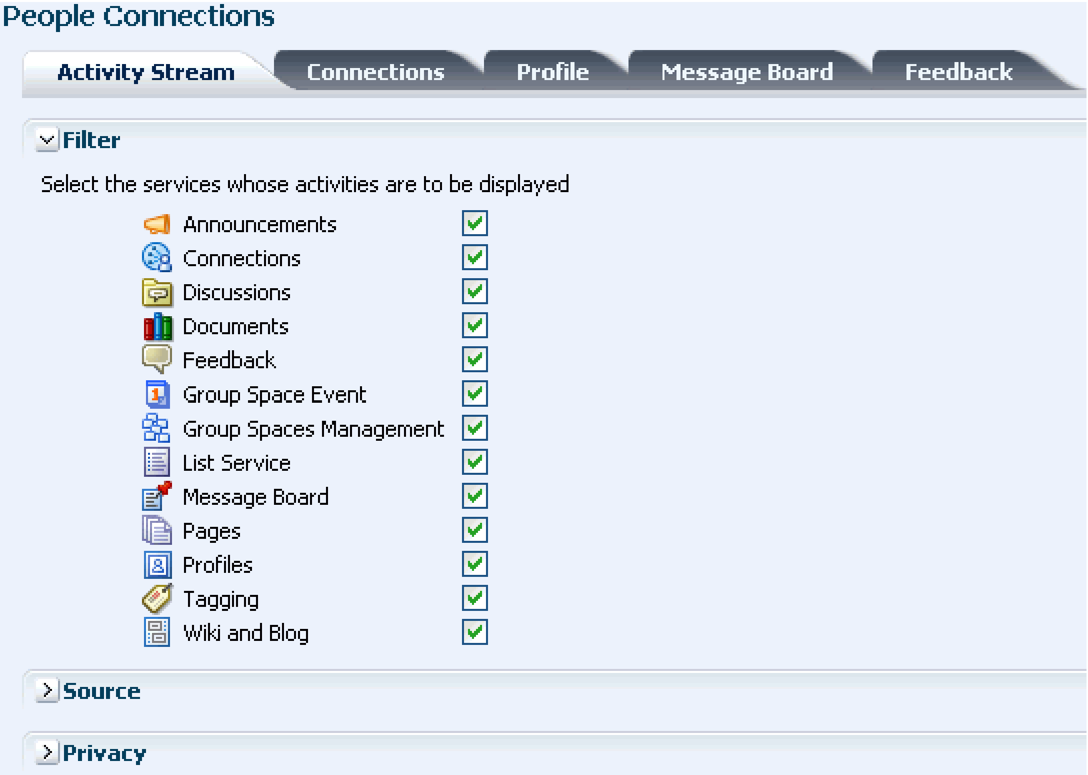
- **Filter**—Use Filter options to select the default services from which to show activities.
- **Source**—Use Source options to specify whether personal and group space activities are shown in Activity Stream.
- **Privacy**—Use Privacy options to set default user access to other users' Activity Stream information.

To configure Activity Stream:

1. Access People Connections administrative settings as described in Section 16.3.1.

2. Click the **Activity Stream** tab to bring it forward.
3. Expand the **Filter** node (Figure 16–3).

Figure 16–3 Activity Stream Filter Node



People Connections

Activity Stream | Connections | Profile | Message Board | Feedback

Filter

Select the services whose activities are to be displayed

- Announcements ☑
- Connections ☑
- Discussions ☑
- Documents ☑
- Feedback ☑
- Group Space Event ☑
- Group Spaces Management ☑
- List Service ☑
- Message Board ☑
- Pages ☑
- Profiles ☑
- Tagging ☑
- Wiki and Blog ☑

Source

Privacy

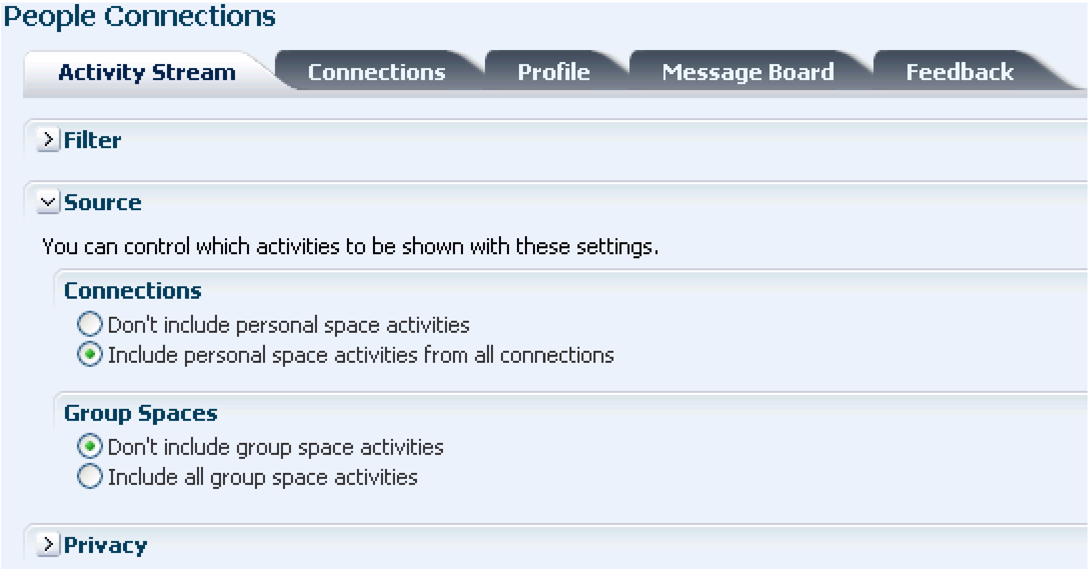
4. Select the default services from which to publish activity.

Note: The activities of services that are not selected are still tracked, but they do not appear in the Activity Stream. If you select to show the service activities at some later point, all of the activities that occurred when the service was not selected now appear in the Activity Stream.

See Also: For information about which service activities are tracked, see Table 16–1, " Activities Tracked by Activity Stream".

5. Expand the **Source** node (Figure 16–4).

Figure 16–4 Activity Stream Source Node



You can control which activities to be shown with these settings.

Connections

○ Don't include personal space activities
● Include personal space activities from all connections

Group Spaces

● Don't include group space activities
○ Include all group space activities

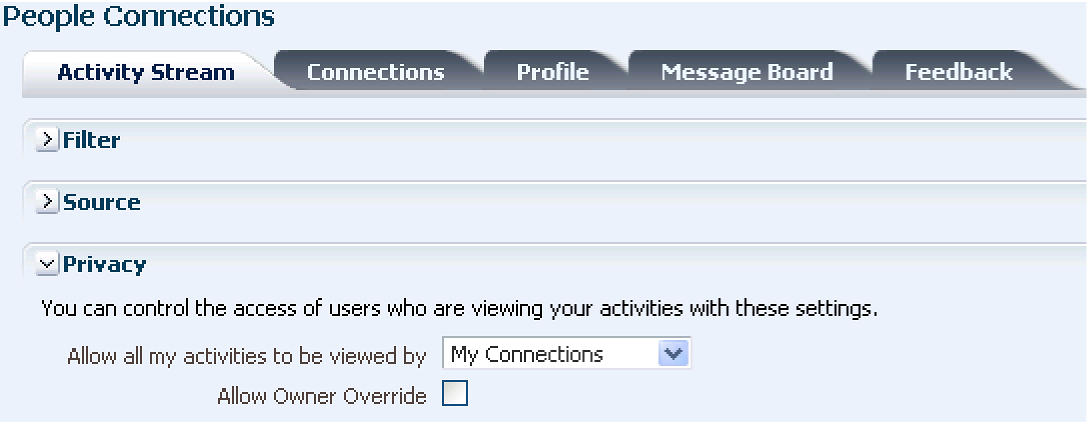
Table 16–2 lists and describes each option.

Table 16–2 Activity Stream Source Options

Option	Description
Connections	Select whether to track personal space activity from a user's connections Choose from: - **Don't include personal space activities**—Select to omit all personal space activity from Activity Stream. - **Include personal space activities from all connections**—Select to track all personal space activity from the current user and the current user's connections in Activity Stream.
Group Spaces	Select whether to track group space activity Choose from: - **Don't include group space activities**—Select to omit all group space activity from Activity Stream. - **Include all group space activities**—Select to track all group space activity from the group spaces to which the current user has access in Activity Stream.

6. Expand the **Privacy** node (Figure 16–5).

Figure 16–5 Activity Stream Privacy Node



You can control the access of users who are viewing your activities with these settings.

Allow all my activities to be viewed by: My Connections

Allow Owner Override □

Table 16–3 lists and describes each option.

Table 16–3 Activity Stream Privacy Options

Option	Description
Allow all of my activities to be viewed by	Specify who can view another user's activities Choose from: ■ **Everyone**—Any user, whether logged in or not, can view other users' activities. ■ **Authenticated Users**—Users who have logged in can view other users' activities. ■ **My Connections**—User A can view user B's activities if user B has accepted user A as a connection. User A can also view user A's activities. ■ **Myself**—A user can view only his own activities.
Allow Owner Override	Enable users to override the application default settings using their own People Connections Preferences (for more information, see the "Setting People Connections Preferences" section in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*).

7. Click **Apply** to save your configuration settings.

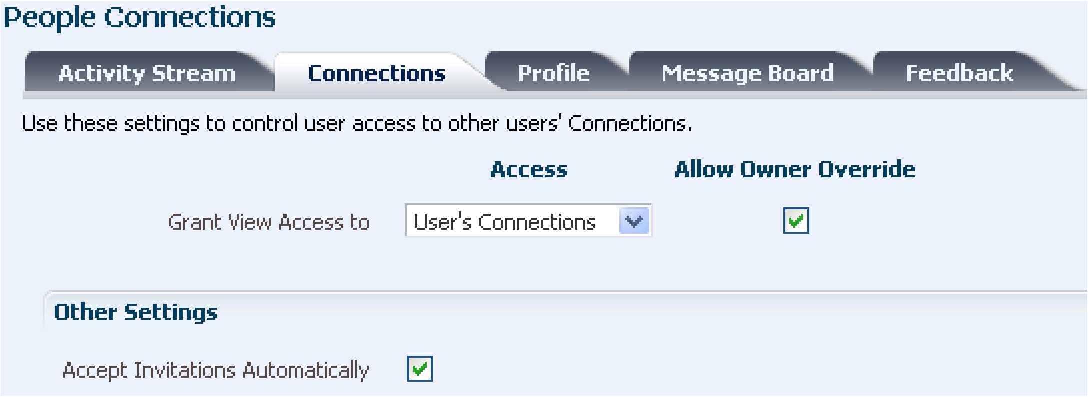
16.3.3 Configuring Connections

Connections configuration involves specifying who can view another user's connections and whether users accept invitations to connect automatically.

To configure Connections:

1. Access People Connections administrative settings as described in Section 16.3.1.
2. Click the **Connections** tab to bring it forward (Figure 16–6).

Figure 16–6 Connections Configuration Settings



People Connections

Use these settings to control user access to other users' Connections.

	Access	Allow Owner Override
Grant View Access to	User's Connections	☑

Other Settings

Accept Invitations Automatically ☑

Table 16–4 lists and describes each option.

Table 16–4 Connections Configuration Options

Option	Description
Grant View Access to	Classes of users to whom to grant automatic view access to a user's connections The users you select can view and interact with another user's connections. Choose from: ▪ **Everyone**—All users, including users who are not logged in, can see other users' connections. ▪ **Authenticated users**—Only users who are logged in can see other users' connections. ▪ **User's Connections**—Only the user himself and the users to whom he is connected can see his connections. ▪ **User Only**—Only a user can see his own connections.
Allow Owner Override	Option to allow or prohibit users from overriding the administrator View access setting: ▪ Select to allow users to override the administrative View access setting specified here using their personal Preferences (for more information, see the "Setting People Connections Preferences" section in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*). ▪ Clear to prohibit users from overriding the administrative View access setting.
Accept Invitations Automatically	▪ Select to specify that, by default, all invitations to connect are accepted automatically. ▪ Clear to specify that, by default, a user must explicitly accept or reject invitations to connect.

3. Click **Apply** to save your configuration settings.

16.3.4 Configuring Profile

Every WebCenter user has a profile that displays personal information, such as the user's email address, phone number, office location, department, manager, direct reports, and so on. All but three attributes are stored and read from the LDAP identity store that is configured against WebCenter Spaces. The three exceptions include the profile photo, status message, and expertise.

Personal profiles are presented in four sections: **Summary**, **Employee**, **Business Contact**, **Personal Information**. Each section provides information related to the section heading. For example, **Summary** includes a collection of basic details, such as the user's name, email address, and office location.

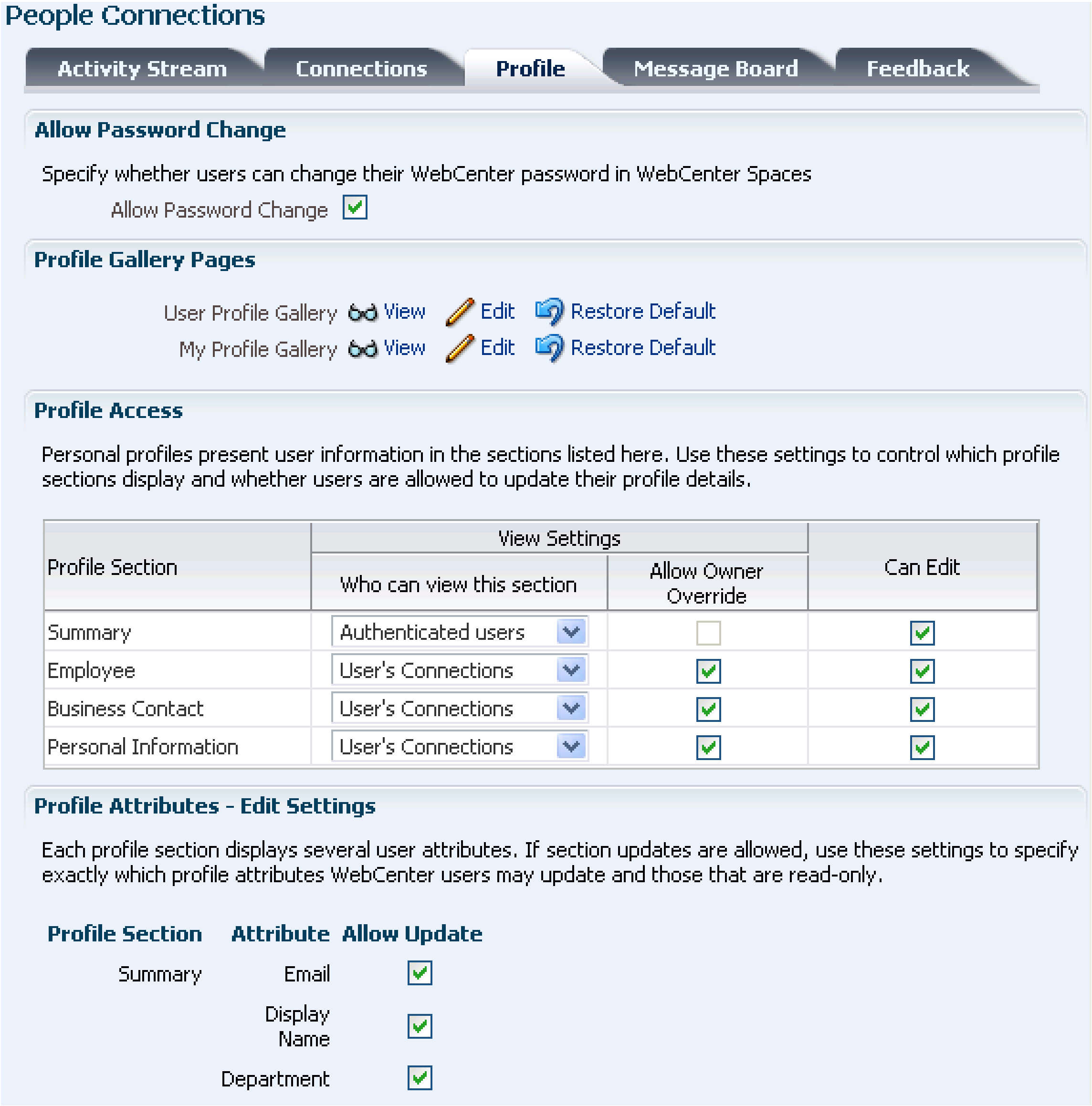
It is the administrator's job to specify the information to show in each section and whether users are allowed to edit their profile data and their application password within WebCenter Spaces.

> **Note:** In WebCenter Spaces, profile settings set on the **WebCenter Administration** > **Services** > **Profile** screen are *not* retained when you upgrade from Oracle WebCenter 11.1.1.1.0 to Oracle WebCenter 11.1.1.2.0. After the upgrade, a WebCenter administrator must reapply the required profile settings on the **WebCenter Administration** > **Services** > **People Connections** > **Profiles** screen.

To configure Profile:

1. Access People Connections administrative settings as described in Section 16.3.1.
2. Click the **Profile** tab to bring it forward (Figure 16–7).

Figure 16–7 Profile Configuration Settings



Allow Password Change

Specify whether users can change their WebCenter password in WebCenter Spaces

Allow Password Change ☑

Profile Gallery Pages

User Profile Gallery View Edit Restore Default

My Profile Gallery View Edit Restore Default

Profile Access

Personal profiles present user information in the sections listed here. Use these settings to control which profile sections display and whether users are allowed to update their profile details.

Profile Section	View Settings		Can Edit
	Who can view this section	Allow Owner Override	
Summary	Authenticated users	☐	☑
Employee	User's Connections	☑	☑
Business Contact	User's Connections	☑	☑
Personal Information	User's Connections	☑	☑

Profile Attributes - Edit Settings

Each profile section displays several user attributes. If section updates are allowed, use these settings to specify exactly which profile attributes WebCenter users may update and those that are read-only.

Profile Section	Attribute	Allow Update
Summary	Email	☑
	Display Name	☑
	Department	☑

Table 16–5 lists and describes each option.

Table 16–5 Profile Configuration Options

Option	Description
Allow Password Change	Specify whether users are allowed to change their application password ■ Select to enable users to change their application password. ■ Clear to prevent users from changing their application password. The option is useful when your organization provides a single, separate application for managing user credentials and, consequently, prefers not to offer password management through each application.
Profile Gallery Pages	Access and edit default **Gallery** pages **User Profile Gallery Page**—The page users see when they view another user's profile gallery. Choose either: ■ **View**—Click to view the other users' **Gallery** page. ■ **Edit**—Click to edit the other users' **Gallery** page in Oracle Composer. For more information, see the "Editing Pages" section in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*. **My Profile Gallery Page**—The page users see when they view their own profile gallery (by clicking their user name at the top of the application). Choose either: ■ **View**—Click to view the user's own **Gallery** page. ■ **Edit**—Click to edit the user's own **Gallery** page in Oracle Composer. For more information, see the "Editing Pages" section in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.
Profile Access	Specify which Profile sections to show and whether users are allowed to update their profile details Set application defaults in the following table columns: **Profile Section**—Identifies the groups of information shown in a user profile. **View Settings**—Specify which users can view a particular profile section, and indicate whether users can change these defaults in their personal Preferences (for more information, see the "Setting People Connections Preferences" section in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*). View Settings for the Summary section control not only who can view summary details but also for whom the user appears in people search results. Set values for: ■ **Who can view this section**—Specify which class of users can view the associated profile section by default. Choose from: **Everyone**—All users, including users who are not logged in, can see the associated profile section in other users' profiles. **Authenticated Users**—Only users who are logged in can see the associated profile section in other user's profiles. **User Only**—Only a user can see his own details in the associated profile section. **None**—The section is hidden from all users. ■ **Allow Owner Override**—Enable or disable users' from overriding the default application settings you specify here. Select to enable; clear to disable. **Can Edit**—Select to enable users to edit the associated profile section of their own personal profiles; clear to prohibit users from editing the associated profile section.
Profile Attributes	Indicate the section attributes that users are allowed to edit by default Under **Allow Update**: ■ Select an attribute to enable users to edit its value in their own profiles. ■ Clear an attribute to prohibit users from editing it in their own profiles.

3. Click **Apply** to save your configuration settings.

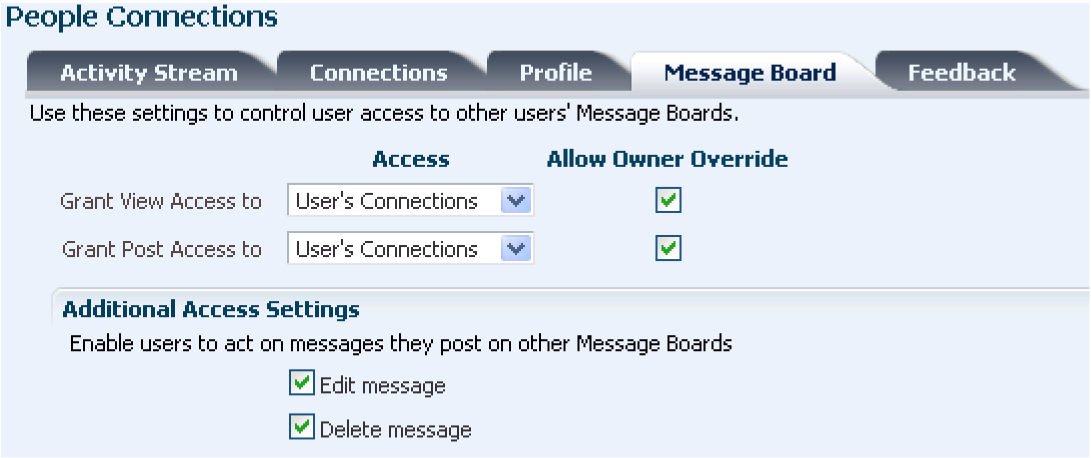
16.3.5 Configuring Message Board

Message Boards provide users with a means of viewing and posting messages to their connections. Message Board configuration settings control who can view and post to another user's Message Board and whether users can edit and delete messages they have posted.

To configure Message Board:

1. Access People Connections administrative settings as described in Section 16.3.1.
2. Click the **Message Board** tab to bring it forward (Figure 16–8).

Figure 16–8 Message Board Configuration Settings



Use these settings to control user access to other users' Message Boards.

	Access	Allow Owner Override
Grant View Access to	User's Connections	☑
Grant Post Access to	User's Connections	☑

Additional Access Settings

Enable users to act on messages they post on other Message Boards

☑ Edit message

☑ Delete message

Table 16–6 lists and describes each option.

Table 16–6 Message Board Configuration Options

Option	Description
Grant View Access to	Specify who can view Message Board messages - **Everyone**—All users, whether logged in or not, can see users' Message Board messages. - **Authenticated Users**—Only logged in users can see users' Message Board messages. - **User's Connections**—Only the user himself and the users to whom he is connected can view his Message Board. - **User Only**—Only a Message Board owner can see his Message Board messages.
Grant Post Access to	Specify who can post Message Board Messages - **Everyone**—All users, whether logged in or not, can post Message Board messages. - **Authenticated Users**—Only logged in users can post messages to Message Boards. - **User's Connections**—Only the user himself and the users to whom he is connected can post messages to his Message Board. - **User Only**—Only a Message Board owner can post messages to his Message Board.
Allow Owner Override	Specify whether users can override these administrative defaults - Select to enable users to edit the default settings through user Preferences (for more information, see the "Setting People Connections Preferences" section in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*). - Clear to enforce the administrator default application settings.
Additional Access Settings	Specify whether users who are allowed to post messages to Message Boards are also allowed to edit and delete their posts Choose from: - **Edit message**—Select to enable users to edit their own Message Board posts. - **Delete message**—Select to enable users to delete their own Message Board posts.

3. Click **Apply** to save your configuration settings.

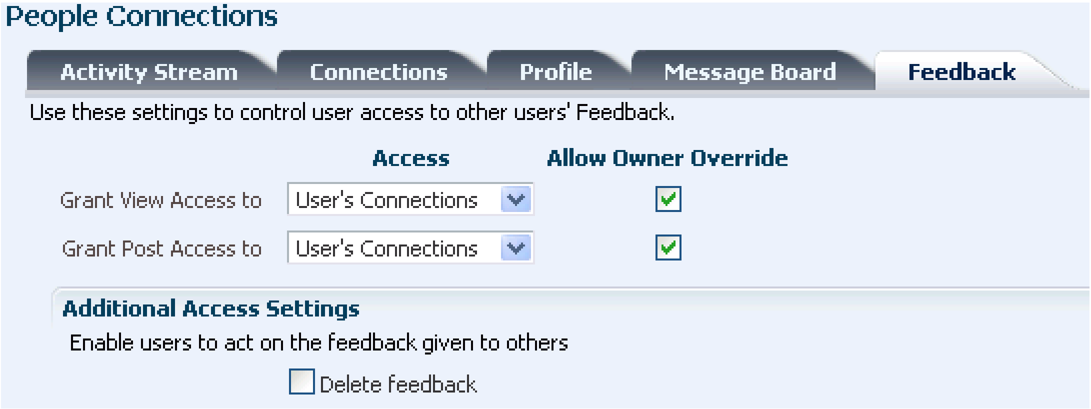
16.3.6 Configuring Feedback

Feedback provides a means of viewing and posting user feedback for other application users. Feedback configuration settings offer controls for identifying who can view, post, and delete feedback.

To configure Feedback:

1. Access People Connections administrative settings as described in Section 16.3.1.
2. Click the **Feedback** tab to bring it forward (Figure 16–9).

Figure 16–9 Feedback Configuration Settings



People Connections

Use these settings to control user access to other users' Feedback.

	Access	Allow Owner Override
Grant View Access to	User's Connections	☑
Grant Post Access to	User's Connections	☑

Additional Access Settings

Enable users to act on the feedback given to others

□ Delete feedback

Table 16–7 lists and describes each option.

Table 16–7 Feedback Configuration Options

Option	Description
Grant View Access to	Specify who can view user Feedback Choose from: ■ **Everyone**—All users, whether logged in or not, can see other users' Feedback. ■ **Authenticated Users**—Only logged in users can see other users' Feedback. ■ **User's Connections**—Only the user himself and the users to whom he is connected can view his Feedback. ■ **User Only**—Users are the only ones who can view the Feedback left for them.
Grant Post Access to	Specify who can post Feedback Choose from: ■ **Everyone**—All users, whether logged in or not, can post Feedback. ■ **Authenticated Users**—Only logged in users can post Feedback. ■ **User's Connections**—Only the user himself and the users to whom he is connected can post Feedback for him. ■ **User Only**—Disables other users from posting Feedback messages.
Allow Owner Override	Specify whether users can override these administrative defaults ■ Select to enable users to revise application default settings through user Preferences (for more information, see the "Setting People Connections Preferences" section in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*). ■ Clear to enforce the administrator default application settings.
Additional Access Settings	Indicate whether users can delete the Feedback they post **Delete feedback** ■ Select to enable users to delete the Feedback they post. ■ Clear to prohibit users from deleting the Feedback they post.

3. Click **Apply** to save your configuration settings.

16.4 Troubleshooting Issues with the People Connections Service

This section identifies the types of problems that may occur with each People Connections feature and provides suggestions for how to respond to them. It includes the following subsections:

- Section 16.4.1, "Troubleshooting Activity Stream"
- Section 16.4.2, "Troubleshooting Connections"
- Section 16.4.3, "Troubleshooting Profile"
- Section 16.4.4, "Troubleshooting Message Board"
- Section 16.4.5, "Troubleshooting Feedback"

16.4.1 Troubleshooting Activity Stream

Table 16–8 lists problems and responses for troubleshooting Activity Stream in WebCenter Spaces.

Table 16–8 Activity Stream Errors and Responses

Problem	Response
Unexpected error or exception	Contact Oracle Support Services.
Connections exception is thrown	Check the exception's detail for an explanation of the exception.
Service Framework exception is thrown	Check the exception's detail for an explanation of the exception.
Settings exception is thrown	Check the exception's detail for an explanation of the exception.
Property value entered is not reflected in task flow	An invalid value may have been entered for the task flow property. In such cases, the default value is used. Ensure that task flow properties have valid values. For more information, see the section, "Setting People Connections Task Flow Properties" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.
Database exception in Toplink module	Contact Oracle Support Services.
Query exception in Toplink module	Contact Oracle Support Services.
Unable to publish analytics event	Contact Oracle Support Services.
Operation not supported	Contact Oracle Support Services.
Cannot retrieve user Profile information	Contact Oracle Support Services.
Check for valid repository failed	Either the database is down or the WebCenter repository is not installed. Check the exception's detail for an explanation of the exception, and respond accordingly.
Activity exception during bulk publish	Check the individual activity exception's detail for an explanation of the exception.

16.4.2 Troubleshooting Connections

Table 16–9 lists problems and responses for troubleshooting Connections in WebCenter Spaces.

Table 16–9 Connections Errors and Responses

Problem	Response
Unexpected errors or exceptions	Contact Oracle Support Services.
User name null or blank	Supply a valid user name.
Could not find user name	Supply a valid user name.
Connection list name not specified	An invalid value may have been entered for the task flow property. Ensure that task flow properties have valid values. For more information, see the section, "Setting People Connections Task Flow Properties" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.
Insufficient privileges	Contact the application administrator, and request the required permission. For more information, see the section, "Contacting Your Application Administrator" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.
Cannot invite oneself as a connection	Supply a user name other than your own.
Cannot invite a user who has been invited	Wait for the invited user to act on your invitation.
Cannot invite a user who has invited you	Accept the invitation you have received from the user.
Cannot invite a user to whom you are connected	Supply a user name other than that of your existing connection.

16.4.3 Troubleshooting Profile

Table 16–10 lists problems and responses for troubleshooting Profile in WebCenter Spaces.

Table 16–10 Profile Errors and Responses

Problem	Response
Unexpected errors or exceptions	Contact Oracle Support Services.
Personal status message cannot be changed	Only you can change your personal status message.
User cannot view Profile.	Contact the application administrator, and request the required permission. For more information, see the section, "Contacting Your Application Administrator" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.
User cannot edit Profile.	Contact the application administrator, and request the required permission. For more information, see the section, "Contacting Your Application Administrator" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.
User was not specified	The supplied user name was null or blank. Enter a valid user name.
Modifying property is not allowed	The task flow property may be read-only. In this case, you cannot supply a value.
Error getting an Instant Message address	Contact the application administrator. For more information, see the section, "Contacting Your Application Administrator" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.
Error getting tag data	Contact the application administrator. For more information, see the section, "Contacting Your Application Administrator" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

Table 16–10 (Cont.) Profile Errors and Responses

Problem	Response
Tried to upload an invalid image	Try again with a valid image type. The file must have the mime-type *image*, and cannot have the extension `*.ico`.
Error instantiating object	Contact the application administrator. For more information, see the section, "Contacting Your Application Administrator" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.
Error instantiating Profile	Contact Oracle Support Services.

16.4.4 Troubleshooting Message Board

Table 16–11 lists problems and responses for troubleshooting Message Board in WebCenter Spaces.

Table 16–11 Message Board Errors and Responses

Problem	Response
Unexpected errors or exceptions	Contact Oracle Support Services.
Failed to create an instance of Message Board	Make sure the user is logged in.
Failed to persist Message Board message	Contact Oracle Support Services.
Failed to publish Message Board activity	Verify the reason for the failure in the Activity Stream subsystem.
Message Board message cannot be deleted	The application administrator must explicitly allow users to delete the messages they send. Contact the application administrator, and request the required permission. For more information, see Section 16.3.5, "Configuring Message Board." Also see the section, "Contacting Your Application Administrator" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.
Message Board message cannot be updated	Contact the application administrator, and request the required permission. For more information, see the section, "Contacting Your Application Administrator" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.
Message Board message cannot be added	Message content is empty. Enter message content, and try again. Otherwise, contact Oracle Support Services.
Message Board message cannot be hidden	User does not have permission to hide the message. You can hide only those messages you receive, and not the ones you send.
Failed to query preferences for Message Board	Contact Oracle Support Services.

16.4.5 Troubleshooting Feedback

Table 16–12 lists problems and responses for troubleshooting Feedback in WebCenter Spaces.

Table 16–12 Feedback Errors and Responses

Problem	Response
Unexpected errors or exceptions	Contact Oracle Support Services.
Failed to create an instance of Feedback	Make sure the user is logged in.
Failed to persist Feedback message	Contact Oracle Support Services.
Failed to publish Feedback activity	Verify the reason for the failure in the Activity Stream subsystem.

Table 16–12 (Cont.) Feedback Errors and Responses

Problem	Response
Feedback cannot be deleted	The application administrator must explicitly allow users to delete the Feedback they post. Contact the application administrator, and request the required permission. For more information, see Section 16.3.6, "Configuring Feedback." Also see the section, "Contacting Your Application Administrator" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*. Otherwise, contact Oracle Support Services.
Feedback cannot be updated	Contact the application administrator, and request the required permission. For more information, see the section, "Contacting Your Application Administrator" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.
Feedback cannot be added	Feedback content is empty. Enter Feedback content, and try again. Otherwise, contact Oracle Support Services.
Feedback cannot be hidden	User does not have permission to hide the Feedback. You can hide only the Feedback you receive; you cannot hide the Feedback you give.
Failed to query preferences for Feedback	Contact Oracle Support Services.

17

Managing the RSS Service

This chapter describes how to configure and manage the RSS service for WebCenter Spaces and custom WebCenter applications deployed to Oracle WebLogic Server.

This chapter includes the following sections:

- Section 17.1, "What You Should Know About the RSS Service"
- Section 17.2, "RSS Prerequisites"
- Section 17.3, "Specifying the RSS Feed Proxy"
- Section 17.4, "Testing RSS News Feed Connections"
- Section 17.5, "Supporting WebCenter Blog RSS Feeds"

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 the RSS Service

The RSS service provides the ability to expose information from WebCenter Services and external sources, as news feeds in WebCenter applications. The RSS service delivers content update information from the following WebCenter Services: Recent Activities, Discussions, Lists, and Announcements.

17.2 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. Depending on your network configuration, you may need to set up a proxy server for your application to display content from external RSS news feeds.

17.3 Specifying the RSS Feed Proxy

To specify the proxy host and port used by the RSS service, use the WLST command `setRssProxyConfig`. For command syntax and examples, see the section, "setRssProxyConfig" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information about how to run WLST commands, see Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool (WLST) Commands."

Note: To start using new proxy details, you must restart the managed server to which the WebCenter 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*.

Note: Proxy servers for the RSS service cannot be set by using Fusion Middleware Control.

17.4 Testing RSS News Feed Connections

To ensure that the proxy information is accurately configured for the RSS service:

1. In WebCenter Spaces, drag the RSS Viewer task flow to a page.
2. Edit the RSS Viewer task flow and set the URL to an external RSS feed. For example:

   `http://rss.cnn.com/rss/cnn_topstories.rss`

   If this feed renders correctly, it confirms that the proxy configuration is set up properly.

17.5 Supporting WebCenter Blog RSS Feeds

In WebCenter Spaces, when a user creates a blog by using the Blog service, an RSS feed is created for the blog so that users can get blog updates in their RSS reader of choice. This section describes the tasks that you must perform to support WebCenter blog RSS feeds.

To support WebCenter blog RSS feeds:

1. Set up Oracle WebCenter Wiki and Blog Server to use Basic Authentication.

   a. Open the `web.xml` from the `WEB-INF` directory of your deployed Oracle WebCenter Wiki and Blog Server.

   b. Replace the following entries:

```
<login-config>
            <auth-method>CLIENT-CERT,FORM</auth-method>
                <form-login-config>
                <form-login-page>
                  /login.jsp
                </form-login-page>
                <form-error-page>
                  /login.jsp
                </form-error-page>
             </form-login-config>
        </login-config>
```

   With

```
<login-config>
            <auth-method>BASIC</auth-method>
        </login-config>
```

   c. Save `web.xml`.

2. Create an external application and configure it to store a user's login credentials for reading a secure RSS feed. For information about creating external applications, see Chapter 22, "Managing External Applications", and the chapter "Securing Your WebCenter Application" in *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*.

   You must share the external application ID with WebCenter Spaces users creating blog RSS feeds.

WebCenter Spaces users can then specify the external application ID while creating an RSS Viewer task flow. Users also need to specify their credentials for the external application.

18 Managing the Search Service

This chapter describes how to configure and manage the Search service for WebCenter Spaces and custom WebCenter applications.

WebCenter Search allows users to search WebCenter objects. WebCenter services provide *search adapters* for objects that they manage, and you can integrate with the Oracle Secure Enterprise Search (SES) adapter to include non-WebCenter objects.

Additionally, with WebCenter Spaces, you can override the default WebCenter search adapters and make the Oracle SES adapter index and search all WebCenter objects. Oracle SES search provides unified ranking results. The results are listed together, instead of being grouped into separate sections for Documents, Discussions, and so on, with the most relevant items appearing first.

This chapter describes both of these modes of searching; that is, using the default WebCenter adapters and using the Oracle SES adapter.

Always use Fusion Middleware Control or the WLST command-line tool to review and configure back-end services for WebCenter applications. Any changes that you make to WebCenter applications, post deployment, are stored in MDS metatdata store as customizations. See Section 1.3.5, "Oracle WebCenter Configuration Considerations."

> **Note:** Changes that you make to WebCenter services configuration, through Fusion Middleware Control or using WLST, are not dynamic so you must restart the managed server on which the WebCenter application is deployed for your changes to take effect. See Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."

This chapter includes the following sections:

- Section 18.1, "What You Should Know About WebCenter Search with Oracle SES"
- Section 18.2, "WebCenter Search Prerequisites for using Oracle SES"
- Section 18.3, "Setting Up Oracle SES Connections"
- Section 18.4, "Configuring Oracle SES to Search WebCenter Spaces"
- Section 18.5, "Troubleshooting Issues with 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."

18.1 What You Should Know About WebCenter Search with Oracle SES

You can extend WebCenter searches to external content repositories by connecting the WebCenter application to an Oracle SES instance. Providing that the Oracle SES instance is set up to search external repositories, results from these search sources can appear alongside WebCenter application search results. Supported versions include Oracle SES 10.1.8.4.x. You can register multiple Oracle SES connections but only one of them is active at a time.

Additionally, with WebCenter Spaces, you can override the default search adapters and use Oracle SES to get unified ranking results. This provides a faster, more unified search experience across WebCenter objects. For more information, see Section 18.4, "Configuring Oracle SES to Search WebCenter Spaces."

18.2 WebCenter Search Prerequisites for using Oracle SES

This section includes the following subsections:

- Section 18.2.1, "Oracle SES - Installation"
- Section 18.2.2, "Oracle SES - Configuration"
- Section 18.2.3, "Oracle SES - Security"
- Section 18.2.4, "Oracle SES - Limitations"

18.2.1 Oracle SES - Installation

For installation directions, see the section, "Back-End Requirements for the Search Service" in *Oracle Fusion Middleware Installation Guide for Oracle WebCenter.*

> **See Also:** Check the Release Notes for the latest information on required patches from Oracle SES.

18.2.2 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 uses identity propagation when communicating with Oracle SES, WebCenter's user base must match that in Oracle SES. One way this can happen is by configuring WebCenter and Oracle SES to the same identity management system, such as Oracle Internet Directory.

   > **Note:** Oracle SES includes numerous identity plug-ins for identity management systems including Oracle Internet Directory, Oracle Content Server, and Microsoft Active Directory.

   Only one identity plug-in can be set up for each Oracle SES instance. If you are using Oracle SES to search WebCenter Spaces and you are using multiple crawler types (WebCenter Spaces crawler, Documents crawler, and Discussions crawler) on your Oracle SES instance, then each of those repositories (WebCenter Spaces, Oracle Content Server, and Oracle WebCenter Discussions) must share the same user base as Oracle SES.

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 username; for example, `cn=orcladmin`

   Password: Admin user password

c. Click **Submit**.

2. Each Oracle SES instance must have a trusted entity for allowing WebCenter end users to be securely propagated at query time. (A trusted entity allows the WebCenter 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.

   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 uses to authenticate itself to Oracle SES at query 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** check box.

      - 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 and password.

      - Do *not* select the **Use Identity Plug-in for authentication** check box.

   For more information, see the online help for that page in Oracle SES.

18.2.3 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 27.11, "Securing the WebCenter Spaces Connection to Oracle SES with SSL."

18.2.4 Oracle SES - Limitations

There are currently no known limitations.

18.3 Setting Up Oracle SES Connections

This section includes the following subsections:

- Section 18.3.1, "Registering Oracle SES Services"
- Section 18.3.2, "Choosing the Active Oracle SES Connection"
- Section 18.3.3, "Modifying Oracle SES Connection Details"
- Section 18.3.4, "Deleting Oracle SES Connections"
- Section 18.3.5, "Testing Oracle SES Connections"

18.3.1 Registering Oracle SES Services

You can register multiple Oracle SES connections with a WebCenter application but only one of them is active at a time.

To start using a new (active) Oracle SES connection you must restart the managed server on which the WebCenter application is deployed.

You can register Oracle SES connections using *either* Fusion Middleware Control *or* WLST. This section includes the following subsections:

- Section 18.3.1.1, "Registering Oracle SES Search Services Using Fusion Middleware Control"
- Section 18.3.1.2, "Registering and Modifying Oracle SES Services Using WLST"

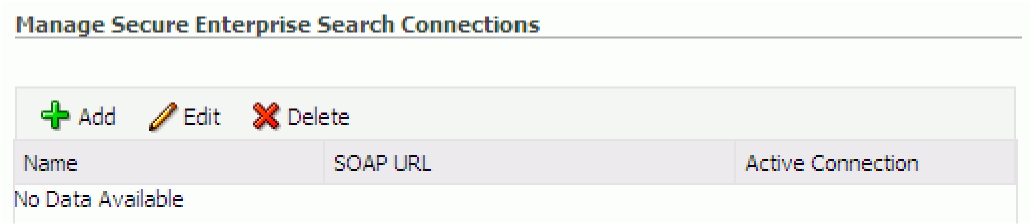
18.3.1.1 Registering Oracle SES Search Services Using Fusion Middleware Control

To register an Oracle SES instance with WebCenter applications:

1. Log in to Fusion Middleware Control and navigate to the home page for WebCenter Spaces or the custom WebCenter application. For more information, see:
   - Section 6.2, "Navigating to the Home Page for WebCenter Spaces"
   - Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"
2. Do one of the following:
   - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings** > **Service Configuration**.
   - For custom WebCenter applications - From the **Application Deployment** menu, choose **WebCenter** > **Service Configuration**.
3. From the list of services on the WebCenter Service Configuration page, select **Search**.

4. To connect to a new Oracle SES instance, click **Add** (Figure 18–1).

Figure 18–1 Configuring Oracle Secure Search Services



Manage Secure Enterprise Search Connections

Name	SOAP URL	Active Connection
No Data Available		

5. Enter a unique name for this connection, and indicate whether this connection is the active (or default) connection for the application (Table 18–1).

Table 18–1 Search Connection - Name

Field	Description
Name	Enter a unique name for the connection. The name must be unique (across all connection types) within the WebCenter application.
Active Connection	Select to use the Oracle SES instance defined on this connection to search repositories outside the WebCenter application and include Oracle SES search results in your result set. While you can register multiple search connections for a WebCenter 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 18–2).

Table 18–2 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:
	`http://host:port/search/query/OracleSearch`
	For example:
	`http://myHost:7777/search/query/OracleSearch`

Federation Trusted Entity Name	Enter the user name of the Oracle SES federation trusted entity created in Section 18.2.2, "Oracle SES - Configuration." **Tip:** This user is configured in the Oracle SES administration tool, on the Global Settings - Federation Trusted Entities page. The user must be present in both the identity management server configured for your WebCenter application and the identity management server configured for Oracle SES. The WebCenter application must authenticate itself as a trusted application to Oracle SES to perform searches on behalf of WebCenter users. Examples in this chapter use `wpadmin` for this value.
Federation Trusted Entity Password	Enter the password for the federation trusted entity. This is not required if you selected the **Use Identity Plug-in for authentication** check box when setting up the federation trusted entity.

7. On Advanced Configuration, enter the Oracle SES data group (also known as a source group) in which to search. This parameter is specific to the Oracle SES search adapter. If a value is not provided, then everything in the Oracle SES instance is searched.

8. Optionally, configure additional options for the Oracle SES connection (Table 18–3). With the exception of the Oracle Secure Enterprise Data Group parameter, these parameters apply to all search adapters.

> **Note:** These Oracle SES advanced configuration parameters can be left blank if you are setting up Oracle SES for the first time. You can return here to tune these parameters later.

Table 18–3 Oracle Secure Enterprise Search - Advanced Configuration

Field	Description
Oracle Secure Enterprise Search Data Group	Specify the Oracle SES data group in which to search. If a value is not provided, then everything in the Oracle SES instance 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** to see all the results.
Results per Service - Search Toolbar	Enter the number of search results displayed, per service, for searches submitted from the global search toolbar.
Number of Saved Searches in Search Page	Enter the number of saved searches displayed in the Saved Search dropdown list (on the main search page).

9. Click **OK** to save this connection.

10. To start using the new (active) connection you must restart the managed server on which the WebCenter application is deployed. For more information, see Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."

18.3.1.2 Registering and Modifying Oracle SES Services Using WLST

Use the WLST command `createSESConnection` to create an Oracle SES connection. Use `setSESConnection` to alter an existing Oracle SES connection. For command syntax and examples, see the sections, "createSESConnection" and "setSESConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

To configure the WebCenter Search service to actively use a new Oracle SES connection, set `default=true`. For more information, see Section 18.3.2.2, "Choosing the Active Oracle SES Connection Using WLST."

Use the WLST command `setSearchConfig` to edit properties relating to the Search service, such as the number of search results displayed. For command syntax and examples, see the section, "setSearchConfig" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

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

> **Note:** To start using the new (active) connection or settings, you must restart the managed server on which the WebCenter application is deployed. See, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

18.3.2 Choosing the Active Oracle SES Connection

You can register multiple Oracle SES connections with a WebCenter application but only one connection is active at a time.

For WebCenter Spaces and any custom WebCenter application, the *active connection* becomes the back-end search engine.

> **Note:** These steps in this section are not necessary if you selected the active connection in Section 18.3.1, "Registering Oracle SES Services."

This section includes the following subsections:

- Section 18.3.2.1, "Choosing the Active Oracle SES Connection Using Fusion Middleware Control"
- Section 18.3.2.2, "Choosing the Active Oracle SES Connection Using WLST"

18.3.2.1 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 WebCenter Spaces or the custom WebCenter application. For more information, see:
   - Section 6.2, "Navigating to the Home Page for WebCenter Spaces"
   - Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"
2. Do one of the following:
   - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings** > **Service Configuration**.
   - For custom WebCenter applications - From the **Application Deployment** menu, choose **WebCenter** > **Service Configuration**.
3. From the list of services on the WebCenter Services Configuration page, select **Search**.

   The Manage Secure Enterprise Search Connections table indicates the current active connection (if any).
4. Select the connection you want to make the active (or default) connection, and then click **Edit**.

5. Select the **Active Connection** check box.
6. Click **OK** to update the connection.
7. To start using the new (active) connection you must restart the managed server on which the WebCenter application is deployed. For more information, see Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."

18.3.2.2 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 the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

To subsequently disable an Oracle SES connection, run the same WLST command with `default=false`. Connection details are retained but the connection is no longer named as an active connection.

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

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

18.3.3 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 application is deployed.

> **Note:** The steps in this section are required only if you want to modify the details configured in Section 18.3.1, "Registering Oracle SES Services."

This section includes the following subsections:

- Section 18.3.3.1, "Modifying Oracle SES Connection Details Using Fusion Middleware Control"
- Section 18.3.3.2, "Modifying Oracle SES Connection Details Using WLST"

18.3.3.1 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 WebCenter Spaces or the custom WebCenter application. For more information, see:
   - Section 6.2, "Navigating to the Home Page for WebCenter Spaces"

- Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"

2. Do one of the following:

   - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings** > **Service Configuration**.
   - For custom WebCenter applications - From the **Application Deployment** menu, choose **WebCenter** > **Service Configuration**.

3. From the list of services on the WebCenter Service Configuration page, select **Search**.
4. Select the connection name, and click **Edit**.
5. Edit connection details, as required. For detailed parameter information, see Table 18–2.
6. Click **OK** to save your changes.
7. To start using the updated (active) connection you must restart the managed server on which the WebCenter application is deployed. For more information, see Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."

18.3.3.2 Modifying Oracle SES Connection Details Using WLST

Use the WLST command `setSESConnection` to edit an existing Oracle SES search connection. For command syntax and examples, see the section, "setSESConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

Use the command `setSearchSESConfig` to set additional Oracle SES connection properties, such as the Oracle SES data group in which to search. For syntax details and examples, see the section, "setSearchSESConfig" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

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

> **Note:** To start using the updated (active) connection you must restart the managed server on which the WebCenter application is deployed. For more information, see the section, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

18.3.4 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 18.3.4.1, "Deleting Search Connections Using Fusion Middleware Control"
- Section 18.3.4.2, "Deleting Search Connections Using WLST"

18.3.4.1 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 WebCenter Spaces or the custom WebCenter application. For more information, see:
   - Section 6.2, "Navigating to the Home Page for WebCenter Spaces"
   - Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"
2. Do one of the following:
   - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings** > **Service Configuration**.
   - For custom WebCenter applications - From the **Application Deployment** menu, choose **WebCenter** > **Service Configuration**.
3. From the Service Connection drop-down, select **Search**.
4. Select the connection name, and click **Delete**.
5. To effect this change you must restart the managed server on which the WebCenter application is deployed. For more information, see Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."

18.3.4.2 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 the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

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

Restart the managed server on which the WebCenter application is deployed. For more information, see Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."

18.3.5 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/OracleSearch
```

If the URL address *does not* render in the browser, then either the host or port for the Oracle SES server is incorrect, or Oracle SES has not been started.

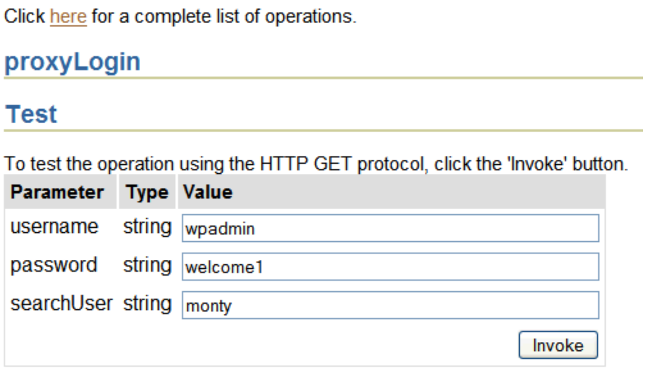
If the URL address *does* render in the browser, then click the **proxyLogin** operation to log in Oracle SES using proxy authentication.

Enter the following parameters:

- **username**: User name that WebCenter uses to authenticate itself to Oracle SES, created in Section 18.2.2, "Oracle SES - Configuration." This user must be a valid trusted entity registered in the federation trusted entities on Oracle SES.
- **password**: Password of this user created in Section 18.2.2, "Oracle SES - Configuration."
- **searchUser**: User name of an end user present in the identity management system used by Oracle SES

When a request is sent for **proxyLogin**, Oracle SES calls the identity plug-in (which returns the call) to authenticate the entity. Click **Invoke** to run the operation (Figure 18–2).

Figure 18–2 Web Services API proxyLogin



Click here for a complete list of operations.

proxyLogin

Test

To test the operation using the HTTP GET protocol, click the 'Invoke' button.

Parameter	Type	Value
username	string	wpadmin
password	string	welcome1
searchUser	string	monty

If the connection is good, then you should see a response similar to the following:

```
<?xml version='1.0' encoding='UTF-8'?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<SOAP-ENV:Body>
<ns1:proxyLoginResponse
xmlns:ns1="http://oracle.search.query.webservice/OracleSearchService.wsdl"
SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<return xmlns:ns2="http://oes.oracle.com/OracleSearch" xsi:type="ns2:Status">
<message xsi:type="xsd:string" xsi:nil="true"/>
<status xsi:type="xsd:string">successful</status>
</return>
</ns1:proxyLoginResponse>

</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

18.4 Configuring Oracle SES to Search WebCenter Spaces

With WebCenter Spaces, you can override the default search adapters and use Oracle SES to get unified ranking results for the following resources:

- Documents
- Group Spaces
- Group Space Announcements
- Group Space Discussions
- Lists
- Pages
- People
- Wikis and blogs

The results are listed together, instead of being grouped into separate sections for Documents, Discussions, and so on. The most relevant items appear 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.

You can create the following crawlers on Oracle SES to crawl WebCenter Spaces resources:

- **Oracle WebCenter Documents Crawler**: This uses the Oracle Content Server source type to crawl documents. The Oracle Content Server source type is provided out-of-the-box in Oracle SES.
- **Oracle WebCenter Discussions Crawler**: This uses the Database source type to crawl discussions and announcements. The Database source type is provided out-of-the-box in Oracle SES.
- **Oracle WebCenter Spaces Crawler**: This uses a Secure RSS source type to crawl the WebCenter Spaces application and certain objects, such as lists, pages, group spaces, wikis and blogs, and people connections profiles. You must create this source type in Oracle SES (one time for each Oracle SES instance).

> **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.

All crawlers (Documents, and Discussions, and WebCenter Spaces), must be configured on the same Oracle SES instance.

Even after Oracle SES is configured to search these specific WebCenter Spaces resources, all other non-crawled resources (for example, tags, notes, and events) continue to be returned in search results, in their own grouping.

This section describes the steps necessary to set up Oracle SES to search WebCenter Spaces:

- Section 18.4.1, "Setting Up Oracle SES for WebCenter Spaces"
- Section 18.4.2, "Setting Up WebCenter Spaces for Oracle SES Search"
- Section 18.4.3, "Setting Up Oracle Content Server for Oracle SES Search"
- Section 18.4.4, "Setting Up Oracle WebCenter Discussions for Oracle SES Search"
- Section 18.4.5, "Setting Up Oracle SES to Search WebCenter Spaces"

18.4.1 Setting Up Oracle SES for WebCenter Spaces

Run the following steps to set up WebCenter Spaces for Oracle SES search.

1. Verify that you have the latest information on required patches from Oracle SES. These are noted in the section "Back-End Requirements for the Search Service" in *Oracle Fusion Middleware Installation Guide for Oracle WebCenter* and in the Release Notes.
2. Verify that a federation trusted identity exists on Oracle SES for WebCenter, as described in Section 18.2.2, "Oracle SES - Configuration" and Section 18.3.5, "Testing Oracle SES Connections."

3. Get `webcenter_search_ses_plugins.zip` from the `$WC_ORACLE_HOME/ses` directory, and put it in the `OracleSES_Home` directory on the Oracle SES instance.

   > **Note:** `OracleSES_Home` represents the software location that you specified at the time of installing Oracle SES.
   >
   > The WebCenter instance and the Oracle SES instance might be on different computers.

4. Change to the Oracle SES home directory. For example:

   ```
   cd $OracleSES_Home
   ```

5. Run the following command to install necessary WebCenter plug-ins:

   ```
   unzip webcenter_search_ses_plugins.zip
   ```

   This adds the following WebCenter jar files to an SES installation:

   - `OracleSES_Home/search/lib/plugins/webcenter/search-auth-share.jar`
   - `OracleSES_Home/search/lib/plugins/webcenter/search-auth-plugin.jar`
   - `OracleSES_Home/search/lib/plugins/doc/search-crawl-ucm.jar`

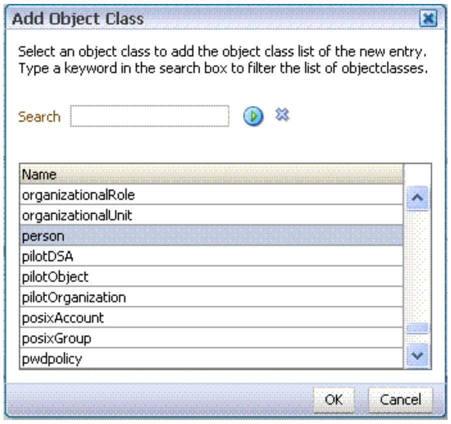
6. To use Oracle SES to search group spaces, lists, pages, or wikis, you must first create a *crawl admin user* in WebCenter Spaces and in your back-end identity management server (for example, `mycrawladmin`). You only need to create a crawl admin user once.

   > **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 18–3).

Figure 18–3 Oracle Directory Services Manager - Add Object Class

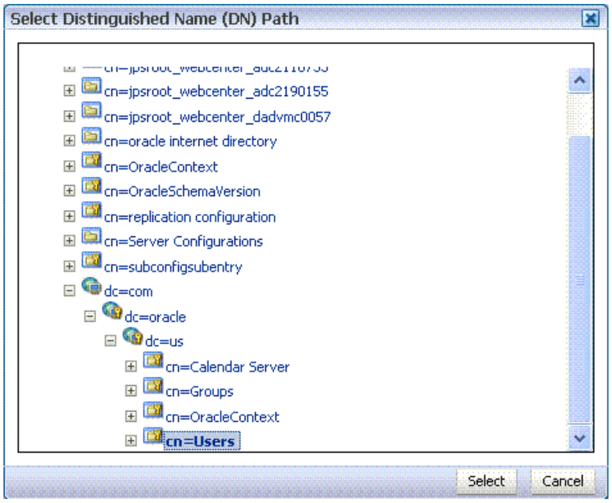


Select an object class to add the object class list of the new entry.
Type a keyword in the search box to filter the list of objectclasses.

Name
organizationalRole
organizationalUnit
person
pilotDSA
pilotObject
pilotOrganization
posixAccount
posixGroup
pwdpolicy

b. Find the distinguished name (DN) path, and click **Select** (Figure 18–4). This example selects "dc=com,dc=oracle,dc=us,cn=Users".

Figure 18–4 Oracle Directory Services Manager - Select DN Path



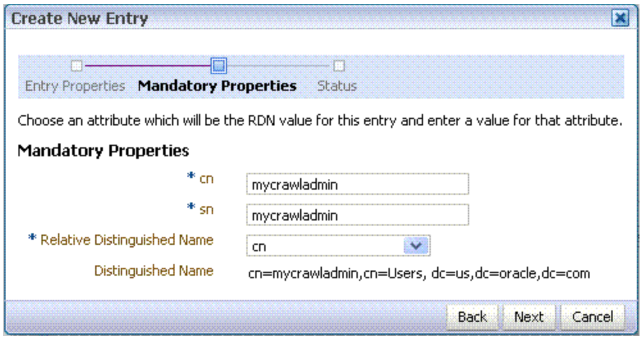
```
⊞ cn=jpsroot_webcenter_adc2190155
⊞ cn=jpsroot_webcenter_dadvmc0057
⊞ cn=oracle internet directory
⊞ cn=OracleContext
⊞ cn=OracleSchemaVersion
⊞ cn=replication configuration
⊞ cn=Server Configurations
⊞ cn=subconfigsubentry
⊟ dc=com
    ⊟ dc=oracle
        ⊟ dc=us
            ⊞ cn=Calendar Server
            ⊞ cn=Groups
            ⊞ cn=OracleContext
            ⊞ cn=Users
```

This screen shot shows the Oracle Directory Services Manager Select Distinguished Name (DN) Path page for adding a new user.

****

c. In the Create New Entry dialog, enter properties, and click **Next** (Figure 18–5).

Figure 18–5 Oracle Directory Services Manager - Create New Entry



Create New Entry

Entry Properties Mandatory Properties Status

Choose an attribute which will be the RDN value for this entry and enter a value for that attribute.

Mandatory Properties

* cn: mycrawladmin

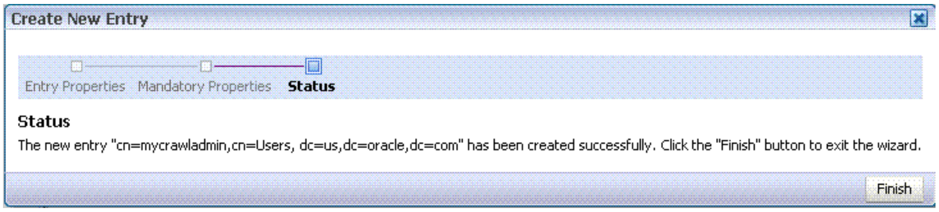
* sn: mycrawladmin

* Relative Distinguished Name: cn

Distinguished Name: cn=mycrawladmin,cn=Users, dc=us,dc=oracle,dc=com

d. When you see that the new entry was created successfully, click **Finish**. (Figure 18–6)

Figure 18–6 Oracle Directory Services Manager - Status



Create New Entry

Entry Properties Mandatory Properties Status

Status

The new entry "cn=mycrawladmin,cn=Users, dc=us,dc=oracle,dc=com" has been created successfully. Click the "Finish" button to exit the wizard.

18.4.2 Setting Up WebCenter Spaces for Oracle SES Search

This section describes how to configure WebCenter Spaces to work with Oracle SES, using WLST commands. After completing these steps you must restart the managed server on which WebCenter Spaces is deployed to effect your changes.

Note: Although some operations in this section can be run using Fusion Middleware Control, for consistency it is best to complete these operations using WLST.

For more information about using WLST, see Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool (WLST) Commands."

For more information about the WLST commands in this section, see *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*:

- `createSESConnection`
- `setSearchSESConfig`
- `setSearchConfig`
- `listAppRoles`
- `createAppRole`
- `grantPermission`
- `grantAppRole`
- `setSpacesCrawlProperties`
- `getSpacesCrawlProperties`
- `listDocumentsSpacesProperties`

---

1. Use WLST to configure the connection between WebCenter Spaces and Oracle SES.

   a. Use the WLST command `createSESConnection` to create a connection to Oracle SES, if a connection does not exist yet. For example:

   ```
   createSESConnection(appName='webcenter',
                       name='MySesConnection',
               url='http://myhost.com:7777/search/query/OracleSearch',
                       appUser='wpadmin',
                       appPassword='welcome1',
                       default=true)
   ```

   where `appUser` is the user name of the Oracle SES federation trusted entity created in Section 18.2.2, "Oracle SES - Configuration."

   b. Specify a data group (also known as source group) under which you will be searching Oracle SES. For example:

   ```
   setSearchSESConfig(appName='webcenter',
                      dataGroup='MySources')
   ```

   where `dataGroup` is the source group created in Section 18.4.5.5, "Additional Oracle SES Configuration."

   For more information on Oracle SES configuration, see Table 18–3.

   c. Increase the number of search results displayed in Oracle SES results. (Five is the default setting, but Oracle SES result sets generally are larger than five.) For example:

   ```
   setSearchConfig(appName='webcenter',
                   numResultsMain=20,
                   numResultsToolbar=20)
   ```

2. Create a *crawl application role* for WebCenter Spaces.

   a. See if the crawl application role exists with the following command:

   ```
   listAppRoles(appStripe='webcenter')
   ```

   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');
   ```

   Then grant `"view"` permissions to WebCenter 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.RelationshipPermiss
ion",
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")
```

b. Grant the crawl application role to the crawl admin user created in Section 18.4.1, "Setting Up Oracle SES for WebCenter Spaces." For example:

```
grantAppRole(appStripe="webcenter",
             appRoleName="webcenter#-#defaultcrawl",
             principalClass="weblogic.security.principal.WLSUserImpl",
             principalName="mycrawladmin");
```

3. Enable the Oracle SES crawlers in WebCenter Spaces.

   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 WebCenter Spaces crawler. By default, full crawls for the WebCenter 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.)

For example:

```
setSpacesCrawlProperties(appName='webcenter',
                         fullCrawlIntervalInHours=168,
                         spacesCrawlEnabled = true,
                         documentCrawlEnabled=true,
                         discussionsCrawlEnabled=true)
```

Notes: You can configure components like Oracle Content Manager and Oracle WebCenter Discussions and still use the default search adapters in WebCenter Spaces by setting `documentCrawlEnabled=false` or `discussionsCrawlEnabled=true`.

A clustered instance additionally requires the `server` parameter; for example, `server="WLS_Spaces1"`.

The following example specifies that WebCenter Spaces runs a full crawl through the WebCenter Spaces crawler every 8 days.

```
setSpacesCrawlProperties(appName='webcenter',fullCrawlIntervalInHours=192)
```

You also can use WLST to return the current crawl settings for WebCenter Spaces, such as the number of hours between full crawls (WebCenter Spaces crawler), and which Oracle SES crawlers are enabled (WebCenter Spaces crawler, Discussions crawler, and Document crawler). For example, the following command returns the current crawl settings for WebCenter Spaces.

```
getSpacesCrawlProperties(appName='webcenter')

WebCenter Spaces Crawl Properties:
-----------------
fullCrawlIntervalInHours: 124
spacesCrawlEnabled:       true
documentCrawlEnabled:     true
discussionsCrawlEnabled:  false
```

4. Use the `listDocumentsSpacesProperties` command to determine the unique name that the back-end Oracle Content Server is using to identify this WebCenter Spaces application and the connection name for the primary Oracle Content Server that WebCenter Spaces is using to store documents. For example:

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

The response should looks 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 "stanl18-ucm11g"
```

Note: Record the application name and the primary connection returned. These values are required later (in Section 18.4.5.2, "Setting Up Oracle SES to Search Documents") to set up Oracle SES to crawl WebCenter Spaces documents.

5. Restart the managed server on which the WebCenter Spaces application is deployed. See Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."

These steps complete WebCenter Spaces application configuration for Oracle SES. However, for Oracle SES searching to work, you must also configure the following:

- Section 18.4.3, "Setting Up Oracle Content Server for Oracle SES Search"
- Section 18.4.4, "Setting Up Oracle WebCenter Discussions for Oracle SES Search"
- Section 18.4.5, "Setting Up Oracle SES to Search WebCenter Spaces"

18.4.2.1 Enabling Oracle SES Crawlers Using Fusion Middleware Control

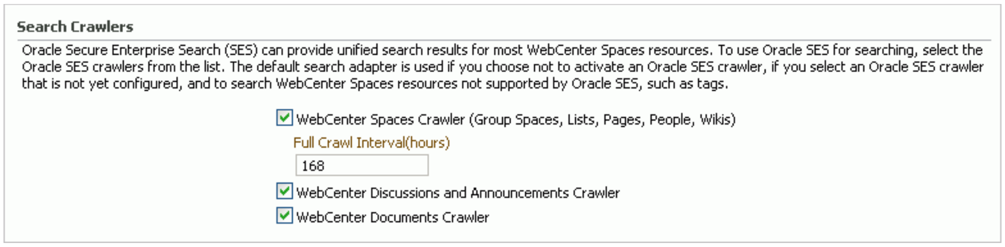
In addition to enabling crawlers using WLST commands, you also can enable or disable crawlers anytime using Fusion Middleware Control.

1. Log in to Fusion Middleware Control and navigate to the home page for WebCenter Spaces. For more information, see Section 6.2, "Navigating to the Home Page for WebCenter Spaces."
2. From the **WebCenter** menu, choose **Settings** > **Application Configuration**.
3. Select the crawlers you want to enable, and click **Apply** (Figure 18–1).

   You can specify an interval between full crawls for the WebCenter Spaces crawler. By default, full crawls for the WebCenter 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.)

   You do not need to restart the managed server on which the WebCenter application is deployed.

Figure 18–7 WebCenter Spaces Search Crawlers



Search Crawlers

Oracle Secure Enterprise Search (SES) can provide unified search results for most WebCenter Spaces resources. To use Oracle SES for searching, select the Oracle SES crawlers from the list. The default search adapter is used if you choose not to activate an Oracle SES crawler, if you select an Oracle SES crawler that is not yet configured, and to search WebCenter Spaces resources not supported by Oracle SES, such as tags.

☑ WebCenter Spaces Crawler (Group Spaces, Lists, Pages, People, Wikis)

Full Crawl Interval(hours)

168

☑ WebCenter Discussions and Announcements Crawler

☑ WebCenter Documents Crawler

18.4.3 Setting Up Oracle Content Server for Oracle SES Search

This section describes how to configure Oracle Content Server to be crawlable by Oracle SES (in particular, the Oracle Content Server that WebCenter Spaces uses for storing documents).

The following steps must be done from within Oracle Content Server.

1. In the Oracle Content Server console, install the SESCrawlerExport component on the content server, if not already done:

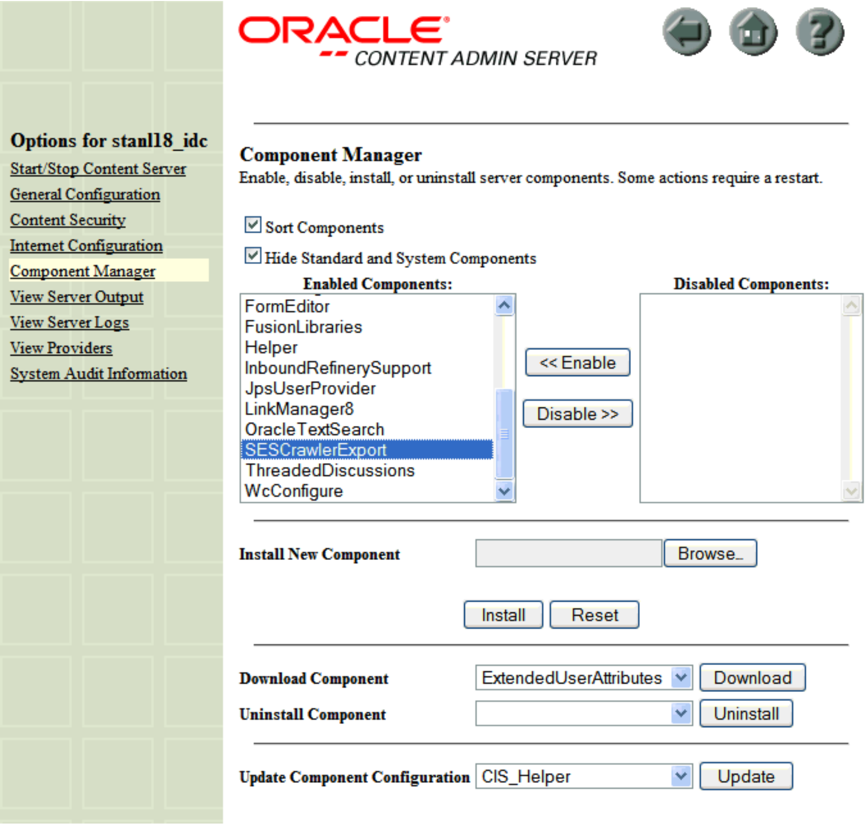
   a. Log on to Oracle Content Server as a system administrator. For example: `http://*host*:*port*/idc`.

   b. From the Administration dropdown menu, select **Admin Server**.

   c. Click the button with the instance name.

   d. Click **Component Manager** from the menu list on the left pane.

Figure 18–8 Oracle Content Server Component Manager



Component Manager

Enable, disable, install, or uninstall server components. Some actions require a restart.

☑ Sort Components

☑ Hide Standard and System Components

Enabled Components:

FormEditor
FusionLibraries
Helper
InboundRefinerySupport
JpsUserProvider
LinkManager8
OracleTextSearch
SESCrawlerExport
ThreadedDiscussions
WcConfigure

Disabled Components:

Install New Component

Download Component ExtendedUserAttributes

Uninstall Component

Update Component Configuration CIS_Helper

e. If the **SESCrawlerExport** is not listed under Enabled Components, then you must install it. In the Download section of the page, select SESCrawlerExport from the dropdown list and click **Download**. Or, in the Install New Component section, browse to find `SESCrawlerExport.zip` (generally, this is located in `$CONTENT_SERVER_HOME/custom/CS10gR35UpdateBundle/extras`), and click **Install**.

f. Enter configuration parameters. (You can change configuration parameters after installation on the Update Component Configuration page.)

Disable security on authentication and authorization APIs provided by the SESCrawlerExport. (Clear the **Disable the security on authentication/authorization APIs provided by the SESCrawlerExport** check box.) 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 Oracle Content Server.

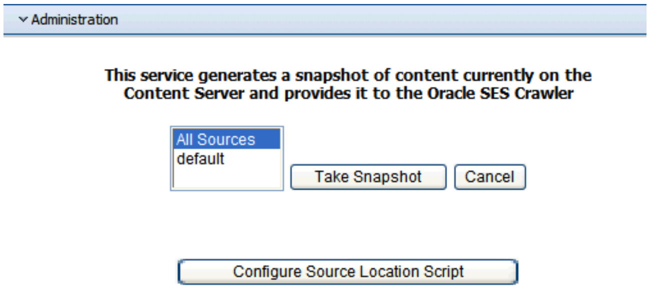
2. Take a snapshot of the Oracle Content Server repository.

a. Log on to Oracle Content Server as a system administrator. For example: `http://`*`host`*`:`*`port`*`/idc`.

b. From the Administration dropdown menu, select **SES Crawler Export**.

c. Select **All sources**, and click **Take Snapshot**.

Figure 18–9 Oracle Content Server Snapshot



This service generates a snapshot of content currently on the Content Server and provides it to the Oracle SES Crawler

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**.

For detailed information on Oracle Content Server configuration, see the `Deployment Guide.pdf` included with the product.

18.4.4 Setting Up Oracle WebCenter Discussions for Oracle SES Search

This section describes how to configure Oracle WebCenter Discussions to be crawlable by Oracle SES (in particular, the Oracle WebCenter Discussions Server that WebCenter Spaces uses for storing discussions and announcements).

Note: These steps is not required if you have a new installation of WebCenter (with an Oracle database) and Oracle WebCenter Discussions. 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 component has been installed on the system.

   - For Oracle and Microsoft SQL Server databases:

     Verify that the Oracle WebCenter Discussions back end has been configured properly by noting that the *`MyPrefix`*`_DISCUSSIONS` user is installed in RCU.

     Then verify that the Oracle WebCenter Discussions Crawler has been configured properly by noting that the *`MyPrefix`*`_DISCUSSIONS_CRAWLER` user is installed in RCU.

   - For IBM DB2 databases:

     Verify that the Oracle WebCenter Discussions back end has been configured properly by noting that the *`MyPrefix`*`_DS` user is installed in RCU. Then verify that the Oracle WebCenter 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 Discussions 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 Applications."

2. Run the following tool to upgrade the data in the Oracle WebCenter Discussions database schema, if you have not run the tool already:

```
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
```

18.4.5 Setting Up Oracle SES to Search WebCenter Spaces

The steps in this section must be performed in the Oracle SES administration tool.

The following steps are required:

1. Section 18.4.5.1, "Logging on to the Oracle SES Administration Tool"
2. Section 18.4.5.2, "Setting Up Oracle SES to Search Documents"

3. Section 18.4.5.3, "Setting Up Oracle SES to Search Discussions and Announcements"
4. Section 18.4.5.4, "Setting Up Oracle SES to Search Group Spaces, Lists, Pages, People, Wikis and Blogs"
5. Section 18.4.5.5, "Additional Oracle SES Configuration"

> **Tip:** For detailed information about Oracle SES configuration steps, see the Oracle SES documentation on the Oracle Fusion Middleware documentation library (in the WebCenter product area).

18.4.5.1 Logging on to the Oracle SES Administration Tool

To 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 user name `eqsys` and the password specified during installation.

18.4.5.2 Setting Up Oracle SES to Search Documents

To search WebCenter Spaces 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 an Oracle 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 to add indexable attributes for documents used in a WebCenter Spaces application.

   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`

      Click **Next**, and then click **Finish**.

   b. Create the Documents Service Instance.

      Again, on the Global Settings - Document Services page, click **Create.** This time, select **Select From Available Managers** with the **Secure Enterprise Search WebCenter UCM Plug-in**. Click **Next**, and, in addition to the entering an instance name, enter the following parameters:

      WebCenter Application Name: The unique name being used to identify this WebCenter Spaces application in the back-end Oracle Content Server.

      Connection Name: The name of the primary Oracle Content Server connection that WebCenter Spaces is using to store group space and personal space documents.

      WebCenter URL Prefix: The host and port where the WebCenter Spaces application is running; for example: `http://myhost:8888`

Note: Use the `listDocumentsSpacesProperties` command to determine the application name and connection name for WebCenter Spaces, as described in Section 18.4.2, "Setting Up WebCenter 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 Oracle Content Server source for documents.

   a. Go to **Home > Sources**.

   b. From the Source Type dropdown list, select **Oracle Content Server**. Click **Create**, and enter the following parameters:

   Source Name: `*unique_name*`

   Configuration URL: `*Content_Server_SES_Crawler_Export_endpoint*`; for example, `http://*host*:*port*/idc/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 Oracle Content Server is not protected by SSO, then enter `NATIVE`.

   If Oracle Content Server is protected by Oracle SSO, then enter `ORASSO`.

   User ID:

   If Authentication Type is `NATIVE`, then enter `sysadmin`.

   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 Oracle Content Server, and create a "local" version of the user (same name) in Oracle Content Server.

   Password: Password for this Oracle Content Server user.

   Realm:

   If Authentication Type is `NATIVE`, then enter "`Idc Security /idc/idcplg`", where `/idc/` is the context root you provided when you installing Oracle Content Server.

   If Authentication Type is `ORASSO`, then leave this parameter blank.

   Scratch Directory: 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**.

c. 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`*`/idc/idcplg`

Display URL Prefix: for example, `http://`*`host`*`:`*`port`*`/idc`

Authentication Type: `NATIVE`

Administrator User: Crawl admin user you registered in Section 18.4.1, "Setting Up Oracle SES for WebCenter Spaces"; for example, `mycrawladmin`

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 /idc/idcplg`", where `/idc/` is the context root you provided when you installing Oracle Content Server.

In Authentication Type is `ORASSO`, then leave this field blank.

d. 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

e. Click **Enable** and select the pipeline you created.

18.4.5.3 Setting Up Oracle SES to Search Discussions and Announcements

To search WebCenter Spaces 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 might 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`.

> **Notes:** There are slightly different steps for Oracle, Microsoft SQL Server, and IBM DB2 databases.

1. Required for IBM DB2 databases only:

   a. Copy the IBM driver files `db2jcc.jar` and `db2jcc_license_cu.jar` (obtainable from the IBM DB2 UDB client) into the `OracleSES_Home/search/lib/plugins/oracleapplications` folder in the Oracle SES instance.

   b. Modify the `drivers.properties` file to include the following line:

   ```
   "db2: com.ibm.db2.jcc.DB2Driver"
   ```

   c. Create a temporary directory called `tmp`, and then change to that directory and extract the contents of `appsjdbc.jar`:

   ```
   mkdir search/lib/plugins/oracleapplications/tmp
   cd search/lib/plugins/oracleapplications/tmp
   jar -xvf ../appsjdbc.jar
   ```

   > **Note:** The jar command comes from the `OracleSES_Home/jdk/bin` directory.

   d. In the directory `OracleSES_Home/search/lib/plugins/oracleapplications/tmp`, modify `META-INF/MANIFEST.MF` to change the line `"Class-Path: sqljdbc.jar"` to the following:

   ```
   "Class-Path: sqljdbc.jar db2jcc.jar db2jcc_license_cu.jar"
   ```

   e. 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**.)

   f. Remake the jar:

   ```
   jar cvfm ../appsjdbc.jar META-INF/MANIFEST.MF oracle/
   ```

2. Required for Microsoft SQL Server database only:

   Copy the Microsoft JDBC driver file `sqljdbc.jar` into directory `OracleSES_Home/search/lib/plugins/oracleapplications` in the Oracle SES instance.

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**. Click **Create**, and 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

- For an Oracle database, enter one of the following

`jdbc:oracle:thin:@host:port:sid`

`jdbc:oracle:thin@host:port/serviceId`

- For an IBM DB2 database, enter `jdbc:db2//host:port/database_name`

- For a Microsoft SQL Server database, enter `jdbc:sqlserver://host_or_IP_address:port;database_name`

User ID: Enter one of the following

- For an Oracle or Microsoft SQL Server database, the user `MyPrefix_DISCUSSIONS_CRAWLER` created during Oracle WebCenter Discussions installation

- For an IBM DB2 database, the user `MyPrefix_DC` created during Oracle WebCenter Discussions installation (where `MyPrefix` is five characters)

Password: Password for this user

View:

For an Oracle database, enter either `FORUMCRAWLER_VW` or `ANNOUNCECRAWLER_VW`: Use `FORUMCRAWLER_VW` for the source crawling discussion forums, and use `ANNOUNCECRAWLER_VW` for the source crawling announcements.

For a Microsoft SQL Server or IBM DB2 database, leave this parameter blank.

Query:

For an Oracle database, leave this parameter blank.

For a Microsoft SQL Server or IBM DB2 database, enter one of the following queries:

```
SELECT * FROM FORUMCRAWLER_VW
SELECT * FROM ANNOUNCECRAWLER_VW
```

Use `FORUMCRAWLER_VW` for the source crawling discussion forums, and use `ANNOUNCECRAWLER_VW` for the source crawling announcements.

URL Prefix: The URL prefix for the WebCenter Spaces application, including host and port; for example, `http://host:port/`

Grant Security Attributes: `FORUMID`

c. Click **Next**.

d. 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:

- For an Oracle database, enter one of the following:

`jdbc:oracle:thin:@`*`host:port:sid`*

`jdbc:oracle:thin@`*`host:port`*`/serviceId`

- For an IBM DB2 database, enter `jdbc:db2//`*`host:port/database_name`*

- For a Microsoft SQL Server database, enter `jdbc:sqlserver://`*`host_or_IP_address:port;database_name`*

User ID: Enter one of the following:

- For an Oracle or Microsoft SQL Server database, enter the user *`MyPrefix`*`_DISCUSSIONS_CRAWLER`

- For an 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 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.

e. Click **Create** to complete the source creation.

18.4.5.4 Setting Up Oracle SES to Search Group Spaces, Lists, Pages, People, Wikis and Blogs

In Oracle SES, you must first create the WebCenter source type and then set up a WebCenter source to search WebCenter Spaces objects like group spaces, lists, pages, people, wikis and blogs.

1. Create the WebCenter (Secure RSS) *source type* in Oracle SES. This source type only needs to be created one time in the Oracle SES instance.

   a. Go to the Global Settings - Source Types page. Click **Create**, and enter the following:

   Name: Enter a name for the source type; for example, `SecureWebCenterRss`

   Plug-in Manager Java Class Name: `oracle.search.plugin.rss.RSSSecureCrawlerMgr`

   Plug-in Jar File Name: `oracleapplications/rsscrawler.jar`

   > **Note:** The plug-in collects document attributes and contents to submit to the crawler. The crawler uses this information to index the documents.

b. Click **Next**, and on the following page click **Finish** to accept the default values.

2. Create the WebCenter source.

   a. Go to the **Home > Sources** page.

   b. From the **Source Type** dropdown list, select the source type name you entered in the previous step (for example, **SecureWebCenterRss**). This is the source type you created in the previous step. Click **Create**, and enter the following source parameters:

      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 18.4.1, "Setting Up Oracle SES for WebCenter Spaces"; for example, `mycrawladmin`

      Password: Password for the crawl admin user

      Realm: `jazn.com`

      Scratch Directory: Specify a directory on the system under which the Oracle SES instance resides.

      Oracle SSO Login URL:

      Leave this field blank.

      Oracle SSO Action URL:

      Leave this field blank.

      Click **Next**.

   c. On the Create User-Defined Source : Step 2 : Authorization page, enter the following parameters in the Authorization Manager section:

      Plug-in Class Name: `oracle.webcenter.search.auth.plugin.WebCenterAuthManager`

      Jar File Name: `webcenter/search-auth-plugin.jar`

      Click the **Get Parameters** button to display the following additional parameters:

      Authorization Endpoint: *`host:port_of_WebCenterSpaces`*`/sesUserAuth`; for example, `http://myhost:8888/sesUserAuth`

      Realm: `jazn.com`

      User ID: Crawl admin user you registered Section 18.4.1, "Setting Up Oracle SES for WebCenter Spaces"; 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.

   d. Click **Create** to complete the source creation.

Note: If WebCenter is fronted with an Oracle HTTP Server, then the Configuration URL and the Authorization Endpoint used in this example would require 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 application is deployed.

18.4.5.5 Additional Oracle SES Configuration

1. Create a *source group* that includes the names of the Oracle Content Server, Discussions, Announcements, and WebCenter services sources you created.

   a. Go to the Search - Source Groups page, and click **Create**.

   b. Enter the same source group name used in Section 18.4.2, "Setting Up WebCenter Spaces for Oracle SES Search."

   c. From the **Select Source Type** dropdown list, select each source type (Database, Oracle Content Server, Secure Rss), 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 example set up has the Oracle Internet Directory identity plug-in as the security filter.)

   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 Oracle Content Server, remember to go to the Oracle Content Server Administration page, select **SES Crawler Export**, and take a snapshot. For more information, see Section 18.4.3, "Setting Up Oracle Content Server for Oracle SES Search."

18.5 Troubleshooting Issues with Search

This section provides troubleshooting tips on administering the Search service. It includes the following subsections:

- Section 18.5.1, "Cannot Grant View Permissions to WebCenter Spaces"
- Section 18.5.2, "Oracle SES Cannot Search WebCenter Objects"
- Section 18.5.3, "Results Not Currently Available with Oracle SES Results"

18.5.1 Cannot Grant View Permissions to WebCenter Spaces

Problem

You get the following error when granting `"view"` permissions, as described in Section 18.4.2, "Setting Up WebCenter Spaces for Oracle SES Search."

```
Command FAILED, Reason: javax.naming.directory.AttributeInUseException: [LDAP: e
rror code 20 - uniquemember attribute has duplicate value.]; remaining name 'orc
lguid=F0CC506017B711DFBFFED9EA6A94EAEC,cn=Permissions,cn=JAAS Policy,cn=webcente
r,cn=wc_domain,cn=JPSContext,cn=jpsroot_webcenter_dadvmc0057'
```

Solution

This error appears if the permission is granted already. Ignore the error.

18.5.2 Oracle SES Cannot Search WebCenter Objects

Problem

The configuration for using Oracle SES to search WebCenter objects does not work.

Solution

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* 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 and Oracle SES use the same identity management system, such as Oracle Internet Directory. If you are using multiple crawler types (WebCenter Spaces crawler, Documents crawler, and Discussions crawler) on your Oracle SES instance, then each of those repositories (WebCenter Spaces, Oracle Content Server, and Oracle WebCenter Discussions) must share the same user base as Oracle SES.

   Additionally, for identity propagation to work, the Oracle SES identity management system must contain a user that represents applications or trusted federation entities.

   To test the Oracle SES is connection with a federated trusted entity user, see Section 18.3.5, "Testing Oracle SES Connections."

3. Monitor the crawl process in the Oracle SES administration tool by using a combination of the following:

   - 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.
   - Monitor your crawler statistics on the Home - Schedules - Crawler Progress Summary page and the Home - Statistics page.
   - Monitor your search statistics on the Home - General page and the Home - Statistics page.

   See the *Oracle Secure Enterprise Search Administrator's Guide* for tips to tune crawl performance.

18.5.3 Results Not Currently Available with Oracle SES Results

Problem

The "Results Not Currently Available" message appears after a search. This may appear inconsistently, such as after you click the **More** button on the search results dialog.

Solution

This message appears when the service times out. This largely depends on the load of the system. To alleviate this problem, adjust the `Execution Timeout` parameter.

For more information, see Section 18.3.1, "Registering Oracle SES Services."

19 Managing the Wiki and Blog Services

This chapter describes how to configure and manage the Wiki and Blog services for WebCenter Spaces and custom WebCenter applications deployed to Oracle WebLogic Server.

Always use Fusion Middleware Control or WLST command-line tool to review and configure back-end services for WebCenter applications. Any changes that you make to WebCenter applications, post deployment, are stored in the MDS metatdata store as customizations. For information, see Section 1.3.5, "Oracle WebCenter Configuration Considerations."

> **Note:** Changes that you make to WebCenter services configuration, through Fusion Middleware Control or using WLST, are not dynamic. So, for your changes to take effect you must restart the managed server to which your WebCenter application is deployed. For information, see Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."

This chapter includes the following sections:

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."

19.1 What You Should Know About the Wiki and Blog Server Connections

A wiki is a collection of useful content or information that users can browse and can update and remove, sometimes without the need for registration. This ease of interaction and the variety of operations makes wiki an effective tool for collaborative authoring, where multiple people create written content together using the wiki markup language. Blogs provide a useful tool for discussing and/or evangelizing any type of idea, strategy, or point of view. Blogs may be projected out to a select group of people or to a wider audience. Typically, blogs invite readers to comment on the overall concepts.

The Wiki service enables integration of wikis into WebCenter applications. The Blog service provides the ability to expose blogs on application pages.

Both the Wiki service and the Blog service rely on Oracle WebCenter Wiki and Blog Server at the back end. The Wiki and Blog services require a connection to the server. Both the services use the same connection to connect to the server.

19.2 Oracle WebCenter Wiki and Blog Server Prerequisites

This section contains the following subsections:

- Section 19.2.1, "Oracle WebCenter Wiki and Blog Server - Installation"
- Section 19.2.2, "Oracle WebCenter Wiki and Blog Server - Configuration"
- Section 19.2.3, "Oracle WebCenter Wiki and Blog Server - Security Considerations"
- Section 19.2.4, "Oracle WebCenter Wiki and Blog Server - Limitations"

19.2.1 Oracle WebCenter Wiki and Blog Server - Installation

Oracle WebCenter Wiki and Blog Server is a component of Oracle WebCenter. You can install Oracle WebCenter Wiki and Blog Server while installing Oracle WebCenter, or you can install it later by extending your existing WebCenter domain. For information about installing Oracle WebCenter Wiki and Blog Server, see *Oracle Fusion Middleware Installation Guide for Oracle WebCenter.*

19.2.2 Oracle WebCenter Wiki and Blog Server - Configuration

This section describes the basic administration and configuration tasks you can perform on Oracle WebCenter Wiki and Blog Server.

> **Note:** Depending on your requirements, you may need to perform only some of the configuration tasks listed in this section.

This section contains the following subsections:

- Section 19.2.2.1, "What You Should Know About Oracle WebCenter Wiki and Blog Server"
- Section 19.2.2.2, "Accessing the Oracle WebCenter Wiki and Blog Server"
- Section 19.2.2.3, "Setting Up Domains and Menus"
- Section 19.2.2.4, "Changing the Theme"
- Section 19.2.2.5, "Creating a User Interface Template"

- Section 19.2.2.6, "Unlocking a Page"
- Section 19.2.2.7, "Managing Users and Roles"
- Section 19.2.2.8, "Blocking an IP Address"
- Section 19.2.2.9, "Deleting Wiki Pages and Blog Entries"
- Section 19.2.2.10, "Specifying Configuration Parameters"
- Section 19.2.2.11, "Importing Templates and Attachments"
- Section 19.2.2.12, "Specifying Features Supported on Oracle WebCenter Wiki and Blog Server"
- Section 19.2.2.13, "Configuring `application_config_script`"
- Section 19.2.2.14, "Generating the Passcode"
- Section 19.2.2.15, "Backing Up and Restoring Wiki Content"

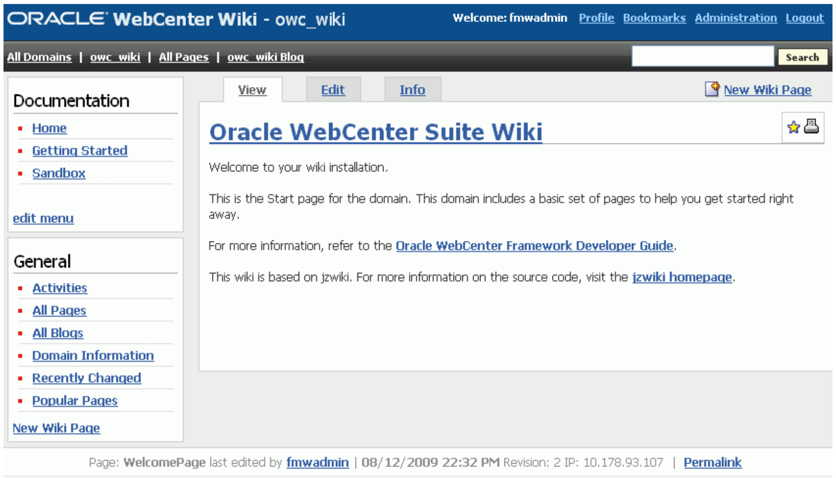
19.2.2.1 What You Should Know About Oracle WebCenter Wiki and Blog Server

When you log on to your Oracle WebCenter Wiki and Blog Server, the home page of the default wiki domain is displayed. The server displays a toolbar of useful links across the top of the page, a search feature, a domain-specific menu on the navigation panel on the left, and additional navigation under the **General** heading, as shown in Figure 19–1.

For administrators, Oracle WebCenter Wiki and Blog Server displays an extra **Administration** link on the top header.

> **Note:** The supported browsers for Oracle WebCenter Wiki and Blog Server are Internet Explorer 7.0 or later, Mozilla Firefox 2.0 or later, and Apple Safari 4.0 or later.

Figure 19–1 Oracle WebCenter Wiki and Blog Server Interface



Oracle WebCenter Suite Wiki

Welcome to your wiki installation.

This is the Start page for the domain. This domain includes a basic set of pages to help you get started right away.

For more information, refer to the Oracle WebCenter Framework Developer Guide.

This wiki is based on jzwiki. For more information on the source code, visit the jzwiki homepage.

Page: WelcomePage last edited by fmwadmin | 08/12/2009 22:32 PM Revision: 2 IP: 10.178.93.107 | Permalink

Note: The wiki and blog server provides the **logout** link. The link can be customized to any URL based on the single sign-on scheme used. To customize the link, you can modify the `logout_url` variable in the `application_config.script` file. Leaving `logout_url` blank renders the user session invalid and redirects to the login screen.

The `application_config.script` file is located in the `WEB-INF/classes` directory of your deployed Oracle WebCenter Wiki and Blog Server.

This section contains the following subsections:

- Section 19.2.2.1.1, "About the General Menu"
- Section 19.2.2.1.2, "About Administration Mode"

19.2.2.1.1 About the General Menu The General menu is a default menu and cannot be edited. You use the General menu to perform common operations on Oracle WebCenter Wiki and Blog Server.

Table 19–1 describes the links available in the General menu of a wiki domain.

Table 19–1 Links Available Under the General Menu

Link	Description
Activities	Displays the **Latest activities** page that lists recent activities related to wiki pages and blog entries. The **Latest activities** page summarizes activities on domain pages, including the thing acted upon (such as blog entry), the action performed (such as Deleted), a link to the changed object, the user name of the person performing the action, and the date and time the action was performed. The page lists the following activities: ■ Wiki pages added, updated, or deleted ■ Blog entries added, updated, or deleted ■ Blog comments added or deleted
All Pages	Displays a list of all wiki pages in the current domain.
All Blogs	Displays a list of all personal and domain blogs. You can access different blogs to add blog entries and manage blog authors.
Domain Information	Summarizes useful information about the current domain, such as details about popular pages and recently updated pages.
Recently Changed	Displays a list of recently updated wiki pages.
Popular Pages	Displays a list of wiki pages, in the current domain, with the most number of page views.
New Wiki Page	Enables you to create a new wiki page in the current domain.

19.2.2.1.2 About Administration Mode To configure Oracle WebCenter Wiki and Blog Server, you use Administration mode of the server. You access Administration mode by clicking the **Administration** link. (Figure 19–2)

Figure 19–2 Administration Link

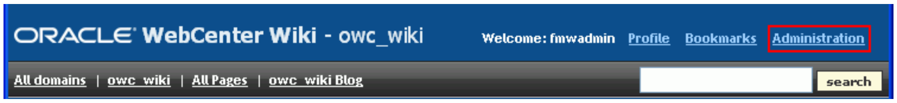
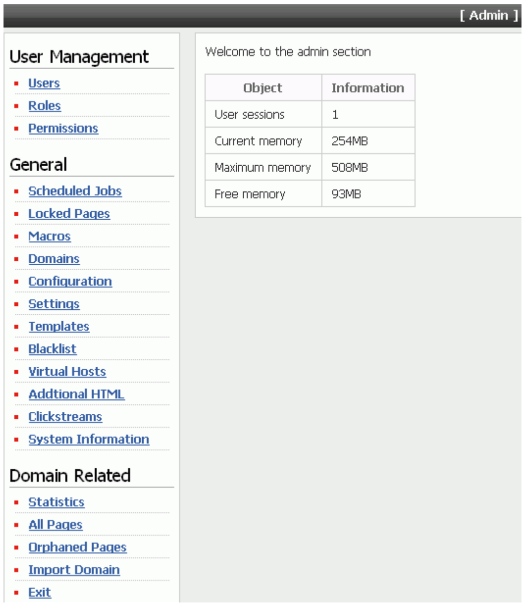

ORACLE WebCenter Wiki - owc_wiki
Welcome: fmwadmin
Profile
Bookmarks
Administration
All domains | owc_wiki | All Pages | owc_wiki Blog
search

Figure 19–3shows all the links available in Administration mode.

Figure 19–3 Administration Mode



Welcome to the admin section

Object	Information
User sessions	1
Current memory	254MB
Maximum memory	508MB
Free memory	93MB

Administration mode contains various links that you can use to configure settings specific to the current domain or the entire wiki and blog server. Table 19–2 describes the links available in Administration mode.

Table 19–2 Links in Administration Mode of Oracle WebCenter Wiki and Blog Server

Link	Description
User Management	
Users	Displays details, such as the name, e-mail address, status, and role of all wiki users. You can use this link to add new users, block or unblock users, reset their password, and edit their profile to assign them different roles. For more information, see Section 19.2.2.7.1, "Managing Users." **Note**: When you deploy Oracle WebCenter Wiki and Blog Server by leveraging single sign-on security, users are not initially imported from the security store. A user entry is created on Oracle WebCenter Wiki and Blog Server only upon first login by that user.
Roles	Enables you to add a new role and edit a role to manage permissions. For information about how to assign permissions to a role, see Section 19.2.2.7.2, "Managing Permissions for a Role."
Permissions	Displays a list of permissions that you can assign to various roles.
General	

Table 19–2 (Cont.) Links in Administration Mode of Oracle WebCenter Wiki and Blog

Link	Description
Scheduled Jobs	Displays a list of administrative jobs that you can run. For example, you can run `DailyIndexerJob` for updating the search index and `ActivityPublishJob` for publishing activities from the Activities list to the Activity Stream feature of the WebCenter Spaces People Connections service. For information about activities published, see the Activities row in Table 19–1. The `ActivityPublishJob` communicates with the Activity Stream in Oracle WebCenter by using the `WEBCENTER` schema. Therefore, you must ensure that the `WEBCENTER` schema is created in your Oracle WebCenter database. For information about schemas, see the section, "Create Schemas for Oracle WebCenter" in the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter*. The **Scheduled Jobs** link also shows the next time a job is scheduled to run. If you wish a job to run sooner, use the **run now** link.
Locked Pages	Displays details of pages that have been locked. Details include name of the user who locked the page, the time when the page was locked, and the time when the page will get unlocked automatically. To unlock a page, you can either wait for the time of the automatic unlock, or as an administrator, you can manually unlock a page by clicking the **remove lock** link. For information about how to unlock a page, see Section 19.2.2.6, "Unlocking a Page."
Macros	Enables you to execute complex or specialized functions on a wiki page. You can invoke a macro by using the `<macro:>` tag. Oracle WebCenter Wiki and Blog Server includes several sample macros, such as TaskMacro and Link. The **Macro** page provides a list and description of all sample macros.
Domains	Displays a list of all domains and domain details, such as page counts and the name of the domain home page. It also displays the total number of domains and pages on your wiki and blog server. The **Domains** link also enables you to add or delete a domain, edit details of a domain, and specify the members who can manage a domain. For information about how to manage domains, see Section 19.2.2.3, "Setting Up Domains and Menus."
Configuration	Enables you to configure your wiki and blog server by specifying details such as the default domain and wiki theme. For more information, see Section 19.2.2.10, "Specifying Configuration Parameters."
Settings	Enables you to specify your wiki and blog server settings. You can specify details such as whether attachments, page ratings, and trackbacks are supported. For more information, see Section 19.2.2.12, "Specifying Features Supported on Oracle WebCenter Wiki and Blog Server."
Templates	Enables you to add, view, edit, and delete templates used for creating wiki pages. For more information, see Section 19.2.2.5, "Creating a User Interface Template."

Table 19–2 (Cont.) Links in Administration Mode of Oracle WebCenter Wiki and Blog

Link	Description
Blacklist	Enables you to block certain IP addresses from adding or editing pages on your Oracle WebCenter Wiki and Blog Server. However, a blocked IP address can access the server to view pages. For more information, see Section 19.2.2.8, "Blocking an IP Address."
Virtual Hosts	Enables you to create multiple sites within Oracle WebCenter Wiki and Blog Server, differentiated by their host names.
Additional HTML	Enables you to define the additional HTML header and footer information that appears on every wiki page.
Clickstreams	Enables you to monitor the pages or functions that your users have accessed or clicked. Users are identified by their IP addresses. This link shows the IP addresses of users and the URLs accessed.
System Information	Displays the version number of your Oracle WebCenter Wiki and Blog Server. The version is the open source version number. The **Build** option refers to the Oracle version and the build number.
Domain Related	
Statistics	Displays statistics of the current domain for the specified time period. Domain statistics include the names of wiki pages viewed, the page view count, and the dates on which pages were last viewed within the specified date range.
All Pages	Displays details of all the pages within the current domain. You can use this link to delete a wiki page or to reduce the versions of that wiki page available on the server. For more information, see Section 19.2.2.9, "Deleting Wiki Pages and Blog Entries."
Orphaned Pages	Displays the pages that are not linked to any other page.
Export Domain	Enables you to publish wiki pages in a domain as HTML files so that the pages can be placed on a web server and accessed directly. **Note**: By default, the Export Domain link is not available. To access this link, you must enable the ExportDomain permission for the ADMIN role.
Import Domain	Enables you to point to a directory containing wiki pages, like wiki pages of the 10.1.3.2 version of the wiki and blog server, and import the domain into the database-based repository. For information about importing domains, see the section, "Migrating the Wiki Data" in the *Oracle Fusion Middleware Upgrade Guide for Oracle SOA Suite, WebCenter, and ADF*.
Exit	Exits Administration mode.

19.2.2.2 Accessing the Oracle WebCenter Wiki and Blog Server

You can access the Oracle WebCenter Wiki and Blog Server by using the following URL format:

```
http://host:port/owc_wiki
```

Where:

- `host:port` refer to the host and the port number of the server where you deployed Oracle WebCenter Wiki and Blog Server.
- `owc_wiki` refers to the deployment directory of your Oracle WebCenter Wiki and Blog Server.

For example, if the managed server where you deployed Oracle WebCenter Wiki and Blog Server is running on port 8001, you can access Oracle WebCenter Wiki and Blog Server by using the following path:

```
http://localhost:8001/owc_wiki
```

19.2.2.3 Setting Up Domains and Menus

Domains are an organizing model on Oracle WebCenter Wiki and Blog Server similar to folders on a file system. A wiki domain encompasses an identified group of wiki pages. It helps you organize wiki pages and secure them by role or specific users. Each wiki domain contains an associated blog, where blog authors can create blog entries and users can post comments.

As a wiki administrator, you can create, edit, or delete domains and manage domain members and blog authors. You can also create and edit domain menus to enable easy access to pages within each domain. This section discusses basic domain and menu administration tasks.

This section contains the following subsections:

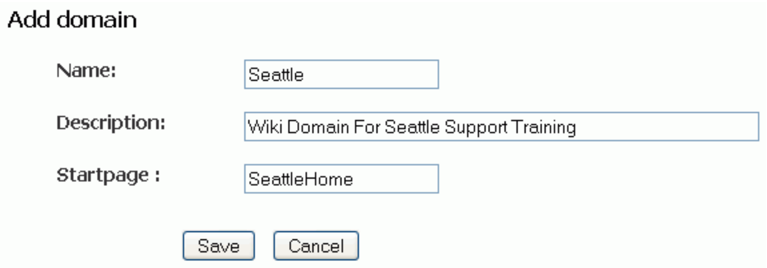
- Section 19.2.2.3.1, "Adding a Domain"
- Section 19.2.2.3.2, "Editing a Domain Menu"
- Section 19.2.2.3.3, "Managing Domain Members"
- Section 19.2.2.3.4, "Managing Blog Authors"

19.2.2.3.1 Adding a Domain To create a new domain:

1. Log on to Oracle WebCenter Wiki and Blog Server as an administrator and access Administration mode.
2. In the navigation panel on the left, under **General**, click **Domains**.

   The **Domains** page lists all the wiki domains on the server.
3. On the **Domains** page, click **add** to create a new domain.
4. Enter a domain name, a description, and a name for the home page, also called the start page, of your domain, as shown in Figure 19–4.

Figure 19–4 Adding a New Domain



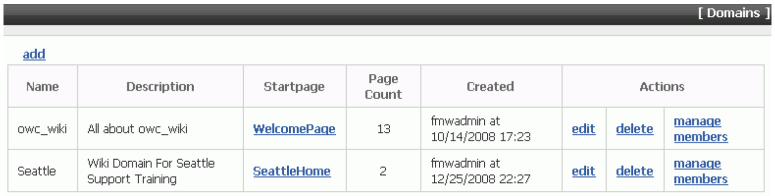
Add domain

Name:	Seattle
Description:	Wiki Domain For Seattle Support Training
Startpage :	SeattleHome

5. Click **Save**.

   The newly created domain is listed on the Domains page, as shown in Figure 19–5.

Figure 19–5 List of Domains



[Domains]

add

Name	Description	Startpage	Page Count	Created	Actions		
owc_wiki	All about owc_wiki	WelcomePage	13	fmwadmin at 10/14/2008 17:23	edit	delete	manage members
Seattle	Wiki Domain For Seattle Support Training	SeattleHome	2	fmwadmin at 12/25/2008 22:27	edit	delete	manage members

6. In the **Startpage** column, click the start page link of the new domain to navigate directly to the new domain.

   To exit Administration mode, under **General**, click **Exit**. This displays the wiki page of the last domain that you accessed before entering Administration mode.

   > **Note:** You can also create a domain by using the `scope` parameter in a wiki URL in any WebCenter application. If the specified domain does not exist, it is automatically created with the name specified in the `scope` parameter. The parameter also creates a start page named WelcomePage. For more information, see the "Integrating Oracle WebCenter Wiki and Blog Server" chapter in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*.

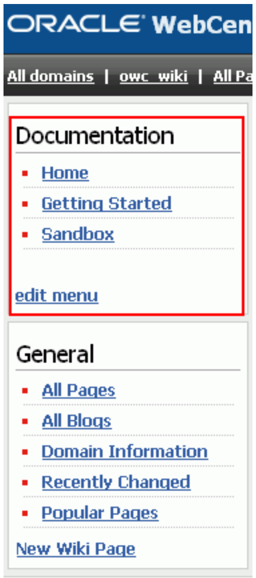
After creating a new domain, you can create wiki pages and blog entries in the domain. For information, see the "Working with Wikis and Blogs" chapter in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

19.2.2.3.2 Editing a Domain Menu As an administrator, you can create or edit the menu of a domain. The domain-specific menu appears at the top in the navigation panel. Figure 19–6 shows the menu of the default domain, `owc_wiki`.

A menu comprises menu topics, which display as headers. Menu topics contain menu items. For example, in the `owc_wiki` domain, **Documentation** is a menu topic and **Home** is a menu item. Menu topics display on the navigational panel in the order in which you create them.

A newly created domain contains an empty wiki page named **Menu**. You use this page to create or edit the domain's menu. You can edit the **Menu** wiki page by using the **edit menu** link on the navigation panel.

Figure 19–6 Domain Menu



Note: You can configure Oracle WebCenter Wiki and Blog Server to display the required wiki management tools. You use the query string parameter `inline` to control how much wiki capability to render. The navigation panel on the left and the **Menu** wiki page appear when `inline=0`. The **edit menu** link appears only when `inline=0` and the user is an administrator.

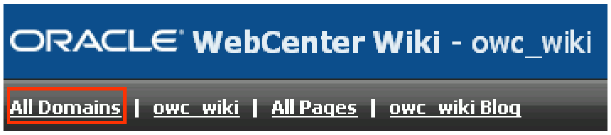
When using `inline=1`, the **Menu** wiki page does not appear. Instead a menu is auto-generated showing all wiki pages in the domain. For information about `inline` modes, see the "Integrating Oracle WebCenter Wiki and Blog Server" chapter in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*.

To modify the menu of a domain:

1. Log on to Oracle WebCenter Wiki and Blog Server as an administrator.
2. Click the **All Domains** link on the toolbar of links on the top-left corner of your wiki and blog server user interface. (Figure 19–7)

   You do not need to access Administration mode to edit a domain menu.

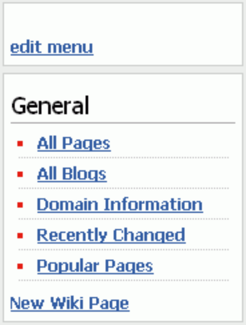
Figure 19–7 All Domains Link


ORACLE WebCenter Wiki - owc_wiki
All Domains | owc_wiki | All Pages | owc_wiki Blog

3. Click the start page link of the domain for which you wish to edit the menu.
4. Click the **edit menu** link. Figure 19–8 shows the blank menu of a newly created domain.

> **Tip:** When you click the **edit menu** link, the Edit Page displays. You can also access the Edit Page by clicking **All Pages** under **General** on the navigation panel. This displays a list of all wiki pages of the current domain. You can click the **Menu** wiki page to view the menu, and then click the **Edit** tab to edit the menu.

Figure 19–8 Menu of a New Domain



edit menu

General

- All Pages
- All Blogs
- Domain Information
- Recently Changed
- Popular Pages

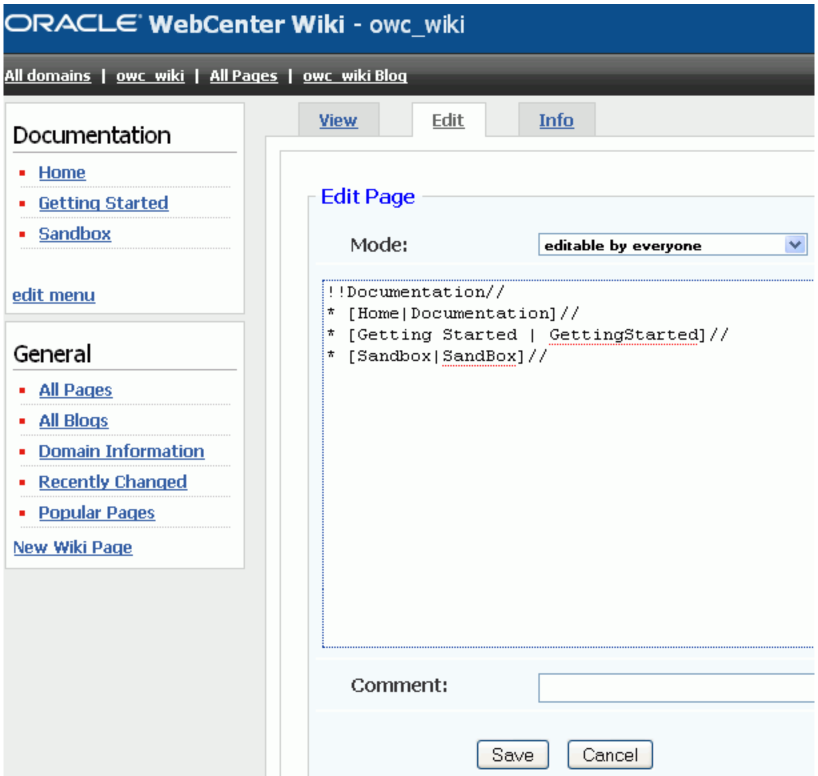
New Wiki Page

5. Specify the menu topic and menu items that you want to add or change. You edit the menu the same way you edit a wiki page. For information, see the "Editing a Wiki Page" section in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

   Within each menu topic, you can define menu items and link them to the required wiki pages or to the targets that are external to your wiki and blog server. When you create a menu item, you must provide a name and specify either the name of a wiki page or a URL. The name that you specify displays in the menu on the navigation panel.

   > **Tip:** When naming your page, ensure that you adhere to wiki markup standards, that is, you use the camel case notation for naming wiki pages. This notation uses an initial uppercase letter followed by lowercase letters, then another uppercase letter, and another series of lowercase letters, for example, `MyWikiPage`. To use an alternate name for your page, use the following convention:
   >
   > `[ *alternate name* | *wiki page name* ]`
   >
   > For example:
   >
   > `[ My Page | MyPage ]`
   >
   > For information about wiki markup language to format page content, see "Using Wiki Mark-Up" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

Figure 19–9 Editing a Domain Menu



Mode: editable by everyone

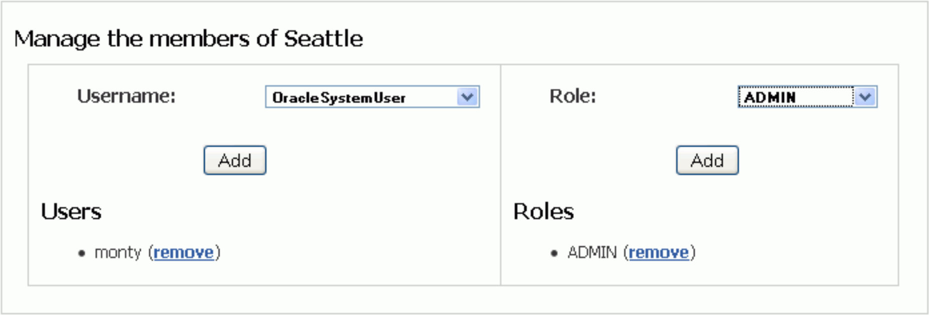
```
!!Documentation//
* [Home|Documentation]//
* [Getting Started | GettingStarted]//
* [Sandbox|SandBox]//
```

> **Tip:** After you edit a menu, it is good practice to change the mode to **only admins are allowed to edit** in the **Mode** dropdown list in the Edit tab. Although the **Edit menu** link is automatically removed from the menu, if the registered user is not an administrator, users may accidentally edit the menu page.

6. Click **Save**.

19.2.2.3.3 Managing Domain Members By default, all authorized wiki users can view and modify wiki pages in a wiki domain. However, you can restrict the permission to edit wiki pages in a domain by specifying domain members. You can add selected users and specific roles as domain members. Figure 19–10 shows that the user `monty` and the `Admin` role are defined as members of the **Seattle** wiki domain.

Figure 19–10 Adding Domain Members



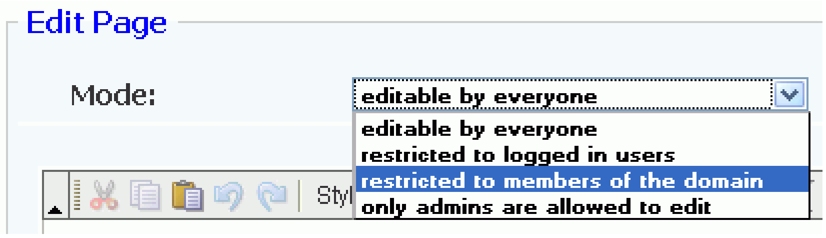
Username: OracleSystemUser

Role: ADMIN

- monty (remove)
- ADMIN (remove)

If members of a domain are defined, then while creating a wiki page in the domain, users can select the **restricted to members of the domain** option if they want only the domain members to be able to edit the wiki page. For example, for the Seattle wiki domain, the user monty and the ADMIN role are the members (Figure 19–10). While creating or editing a page in this domain, if the user selects the **restricted to members of the domain** option, then only **monty** and all users with the **ADMIN** role can edit that wiki page.

Figure 19–11 Restricting Access to Domain Members



Edit Page

Mode: editable by everyone

editable by everyone
restricted to logged in users
restricted to members of the domain
only admins are allowed to edit
Styl

To manage domain members:

1. In Administration mode, click **Domains**.
2. On the **Domains** page, click the **manage members** link of the domain for which you want to specify members.
3. From the **Username** list, select the user whom you want to add as a domain member.
4. Click **Add**.

   The new user's name displays in the **Users** section, as shown in Figure 19–10.
5. From the **Role** list, select the role to which you want to grant domain membership.
6. Click **Add**.

   The role assigned to the domain member displays in the **Roles** section, as shown in Figure 19–10.

   Repeat step 3 through 6 if you want to add any other user or role as a domain member.
7. Click the **remove** link next to a member's name under **Members** if you do not want that member to be able to manage the domain.

19.2.2.3.4 Managing Blog Authors By default, only a wiki administrator or the person who owns the blog can add blog entries. For a personal blog, the blog author is the person who owns that personal blog. In a domain (such as a blog associated with a WebCenter group space), the blog author is the domain creator, which is usually a wiki administrator.

A wiki administrator or the blog owner can specify additional users who can add blog entries. For information about enabling or disabling additional blog authors, see the section, "Adding and Removing Additional Blog Authors" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

Note: If a user creates a domain, the user does not automatically become the blog author for the domain blog. The user must be specifically added as a blog author.

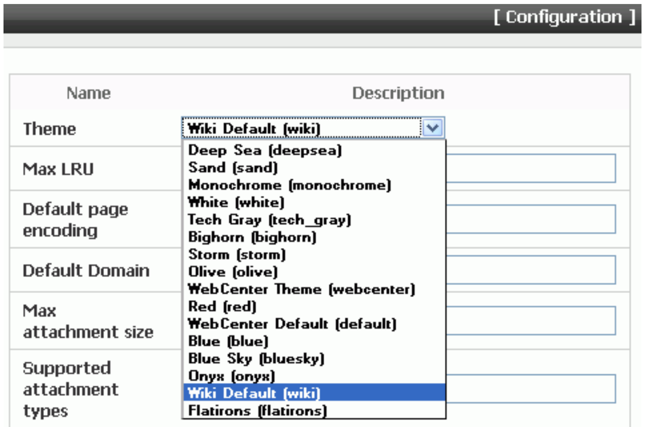
19.2.2.4 Changing the Theme

You can apply themes to change the look and feel of Oracle WebCenter Wiki and Blog Server.

To change the default theme:

1. In Administration mode, under **General**, click **Configuration**.
2. Select a theme from the **Theme** list.
3. Click **Save**.

Figure 19–12 Selecting a Theme



[Configuration]

Name	Description
Theme	Wiki Default (wiki)
Max LRU	
Default page encoding	
Default Domain	
Max attachment size	
Supported attachment types	

4. Click **Exit** to exit Administration mode and see your changes take effect.

> **Note:** Users can change the theme for a login session if they use a wiki or blog URL that includes the `theme` parameter.

19.2.2.5 Creating a User Interface Template

Templates enable you to set up a framework for users for creating pages. You can create new user interface templates as well as edit or delete the existing ones.

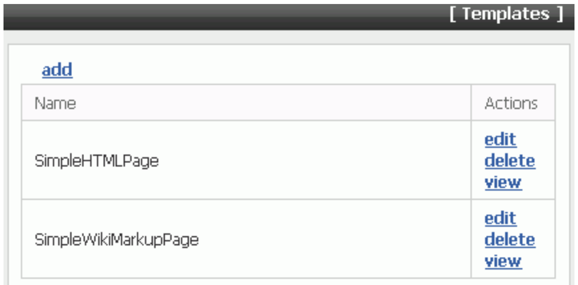
To create a template:

1. In Administration mode, under **General**, click **Templates**.

   The **Templates** page displays a list of existing templates. You can edit, view, or delete templates by clicking the appropriate link displayed in the **Actions** column, as shown in Figure 19–13.

2. Click **add** at the top-right corner of the **Templates** page to create a new template.

Figure 19–13 Managing Templates



[Templates]

add

Name	Actions
SimpleHTMLPage	edit delete view
SimpleWikiMarkupPage	edit delete view

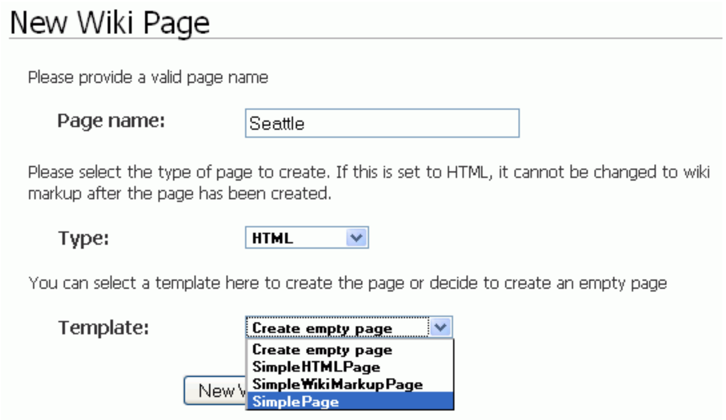
3. In the **Add template** page, in the **Name** field, enter the name of the template.

   While creating or editing a template, use the correct syntax. If the template is intended as a template for wiki markup, then use wiki markup. If it is intended to be a template for HTML pages, then use HTML. Template names should follow the same convention as wiki page names.

4. In the **Template** box, enter the content for the template.
5. Click **Save**.

After you create a new template, users can choose to use this new template while creating a new page, as shown in Figure 19–14.

Figure 19–14 Creating a Page Based on a Template



New Wiki Page

Please provide a valid page name

Page name: Seattle

Please select the type of page to create. If this is set to HTML, it cannot be changed to wiki markup after the page has been created.

Type: HTML

You can select a template here to create the page or decide to create an empty page

Template: Create empty page

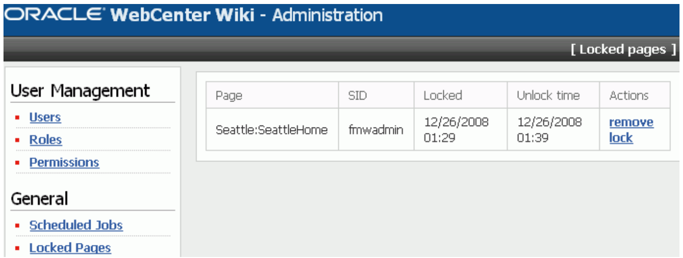
19.2.2.6 Unlocking a Page

Every time a user edits a wiki page, the page gets locked for a specified time period for that user before other users can modify that page. Sometimes as an administrator, you may need to unlock a page. For example, if a user starts editing a wiki page and then clicks away from that page without clicking the Save or the Cancel button, then the page is still considered locked for editing. If another user tries to edit the same page, a warning message displays that the page is currently being edited by some other user, and any changes may be overwritten by a newer version. As an administrator, you can unlock the page manually to remove this warning.

To unlock a page:

1. In Administration mode, under **General**, click the **Locked Pages** link.
2. On the Locked pages page, click the **remove lock** link for the page you want to unlock. (Figure 19–15)

Figure 19–15 Unlocking a Page



ORACLE WebCenter Wiki - Administration

[Locked pages]

User Management

- Users
- Roles
- Permissions

General

- Scheduled Jobs
- Locked Pages

Page	SID	Locked	Unlock time	Actions
Seattle:SeattleHome	fmwadmin	12/26/2008 01:29	12/26/2008 01:39	remove lock

> **Tip:** Details of a locked page are no longer displayed in Locked pages as soon as the page is unlocked, whether manually or automatically.

19.2.2.7 Managing Users and Roles

You can add users on Oracle WebCenter Wiki and Blog Server and assign them required roles. You can also create new roles and assign permissions to those roles.

This section contains the following subsections:

- Section 19.2.2.7.1, "Managing Users"
- Section 19.2.2.7.2, "Managing Permissions for a Role"

19.2.2.7.1 Managing Users To define the operations that a user can perform, you can assign specific roles to the user. To manage your users, you can edit user passwords, block users, add or delete the assigned roles, and add new users. This section describes the various tasks you can perform to manage your Oracle WebCenter Wiki and Blog users.

To assign a role to a user:

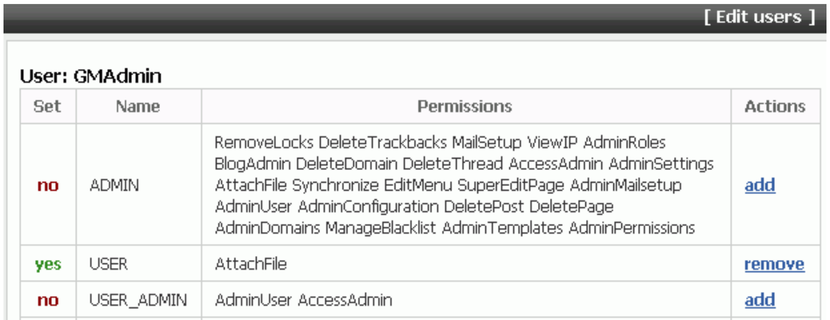
1. In Administration mode, under **User Management**, click **Users**.

   The **Users** page displays a list of all the users and roles assigned to them.

2. On the **Users** page, click the **edit** link for the user whose role you want to modify.

   The **Edit users** page displays a list of all the roles assigned to the user, permissions included in the assigned roles, and the roles that can be assigned to the user, as shown in Figure 19–16.

Figure 19–16 Assigning a Role to a User



[Edit users]

User: GMAdmin

Set	Name	Permissions	Actions
no	ADMIN	RemoveLocks DeleteTrackbacks MailSetup ViewIP AdminRoles BlogAdmin DeleteDomain DeleteThread AccessAdmin AdminSettings AttachFile Synchronize EditMenu SuperEditPage AdminMailsetup AdminUser AdminConfiguration DeletePost DeletePage AdminDomains ManageBlacklist AdminTemplates AdminPermissions	add
yes	USER	AttachFile	remove
no	USER_ADMIN	AdminUser AccessAdmin	add

3. To assign a role to the user, click the **add** link, in the **Actions** column, for the required role.

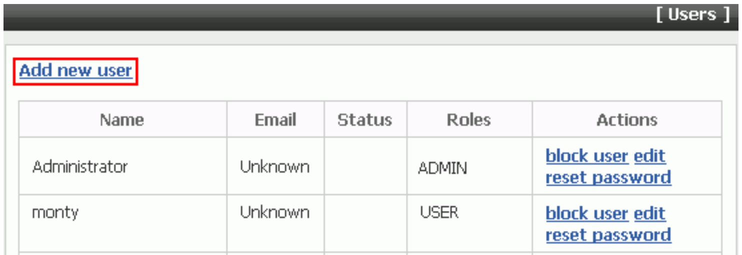
4. If you want to revoke a role from the user, click the **remove** link, in the **Actions** column, for the required role.

In Administration mode, you can block users and reset passwords. These features are useful only when the wiki and blog server is used as a standalone application. Changing user passwords through Administration mode changes passwords only in the local security store of Oracle WebCenter Wiki and Blog Server. If the server is integrated with another Oracle application through single sign-on or LDAP, then users are authenticated through single sign-on and passwords are stored in the external security store. In such a case, if a password needs to be changed, then you must change the password in the external security store.

When you deploy the wiki and blog server by leveraging single sign-on security, users are not initially imported from the external security store. Once a user is authenticated by the external security store, Oracle WebCenter Wiki and Blog Server checks whether the user exists in its local security store. If not, a user entry is created upon first login by that user and a default role, such as USER, is assigned to that user.

You can manually add a user by using the **Add new user** link on the **Users** page in Administration mode (Figure 19–17).

Figure 19–17 Adding a User



[Users]

Add new user

Name	Email	Status	Roles	Actions
Administrator	Unknown		ADMIN	block user edit reset password
monty	Unknown		USER	block user edit reset password

19.2.2.7.2 Managing Permissions for a Role For different wiki operations, you can create specific roles and assign required permissions to those roles. You can also modify existing roles to add or remove permissions. You can then assign the required roles to different users to define the operations that those users can perform.

To edit the permissions granted to a role:

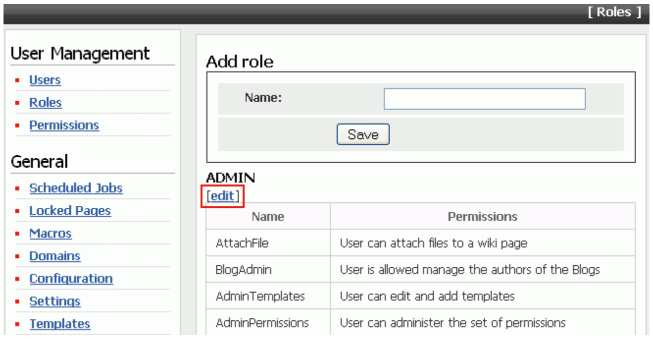
1. In Administration mode, under **User Management**, click **Roles**.

   The **Roles** page displays various roles and the permissions assigned to each role.

2. On the **Roles** page, click the **edit** link under the role that you want to modify. For example, to modify the ADMIN role, click **edit** under **ADMIN** (Figure 19–18).

   The Edit role page displays a list of all permissions that have been assigned or that can be assigned to the selected role (Figure 19–19).

Figure 19–18 Editing a Role



Add role

Name:

ADMIN
[edit]

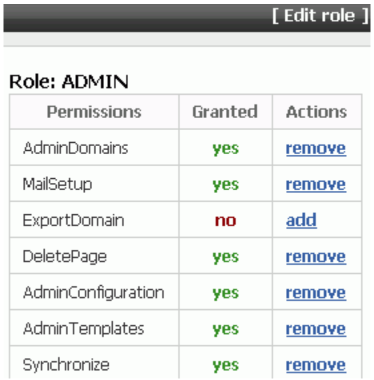
Name	Permissions
AttachFile	User can attach files to a wiki page
BlogAdmin	User is allowed manage the authors of the Blogs
AdminTemplates	User can edit and add templates
AdminPermissions	User can administer the set of permissions

> **Tip:** If you want to create a new role, then specify a role name in the **Name** field and then click **Save** on the **Roles** page (Figure 19–18). You can then click the **edit** link under the newly created role to add the required permissions.

3. In the **Actions** column, click the **add** link of the required permission to add that permission to the selected role, or click the **remove** link corresponding to a permission to remove that permission from the selected role. (Figure 19–19)

> **Tip:** You can view the description of each permission by clicking **Permissions** under **User Management** on the navigation panel in Administration mode.

Figure 19–19 Specifying Permissions for a Role



Role: ADMIN

Permissions	Granted	Actions
AdminDomains	yes	remove
MailSetup	yes	remove
ExportDomain	no	add
DeletePage	yes	remove
AdminConfiguration	yes	remove
AdminTemplates	yes	remove
Synchronize	yes	remove

4. Click the **Roles** link at the bottom of the Edit role page to return to the Roles page.

19.2.2.8 Blocking an IP Address

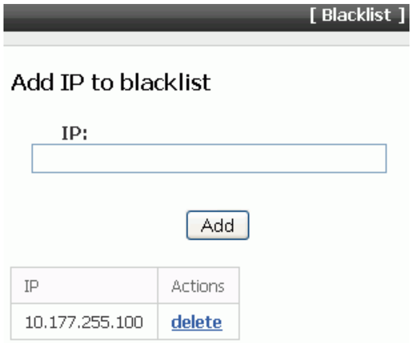
You can block selected IP addresses from creating or updating wiki pages on your Oracle WebCenter Wiki and Blog Server. However, a blocked IP address can still access the server to view wiki pages.

To block an IP address:

1. In Administration mode, under **General**, click **Blacklist**.
2. In the **IP** field, enter the IP address that you want to block.
3. Click **Add**.

   The IP address displays in the list of blocked IP addresses (Figure 19–20).

Figure 19–20 Blocking an IP Address



IP	Actions
10.177.255.100	delete

19.2.2.9 Deleting Wiki Pages and Blog Entries

As a wiki administrator, you can delete wiki pages and blog entries that are no longer required.

This section contains the following subsections:

- Section 19.2.2.9.1, "Deleting a Wiki Page"
- Section 19.2.2.9.2, "Deleting a Blog Entry"

19.2.2.9.1 Deleting a Wiki Page To delete a wiki page:

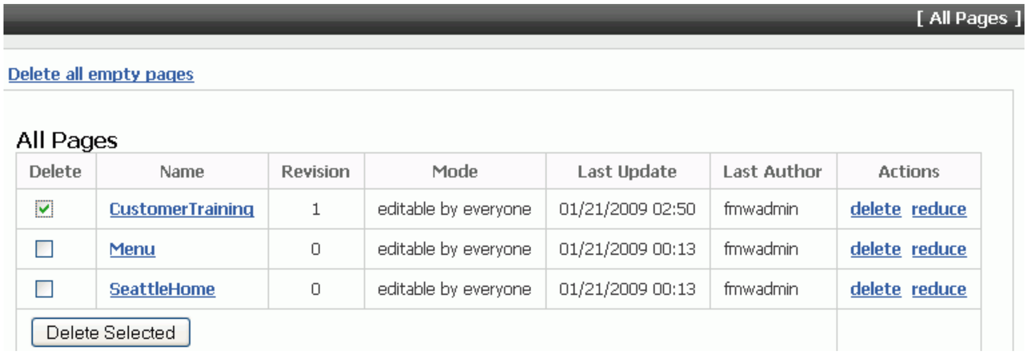
1. In the Administration mode, under **Domain Related**, click **All Pages**.

   This displays a list of all pages in the current domain.

   > **Note:** To delete wiki pages of a domain, you must first navigate to that domain and then access Administration mode.

2. On the **All Pages** page, in the **Actions** column, click the **delete** link corresponding to the wiki page that you want to delete, as shown in Figure 19–21. If you want to delete multiple pages, then select the checkboxes for those pages in the **Delete** column, and then click the **Delete Selected** button.

Figure 19–21 Deleting a Wiki Page



Delete	Name	Revision	Mode	Last Update	Last Author	Actions
☑	CustomerTraining	1	editable by everyone	01/21/2009 02:50	fmwadmin	delete reduce
□	Menu	0	editable by everyone	01/21/2009 00:13	fmwadmin	delete reduce
□	SeattleHome	0	editable by everyone	01/21/2009 00:13	fmwadmin	delete reduce

3. Click the **reduce** link corresponding to a wiki page if you want to reduce the versions of that wiki page available on the server. It makes the current or the latest version of a wiki page the only version and deletes all previous versions.

4. Click the **Delete all empty pages** link at the top on the All Pages page if you want to delete wiki pages that do not contain any text.

> **Note:** Users can delete the wiki pages that they created only if you select **true** for the **Allow users to delete pages they created** option. You access this option by selecting **Settings** under **General** in Administration mode. If this option is enabled, then a **Delete** icon is displayed to a user for the wiki pages that the user created.
>
> If the option is set to **false**, then only wiki administrators can delete wiki pages.

19.2.2.9.2 Deleting a Blog Entry A wiki administrator or users who have the permission to manage blogs can edit and delete blog entries. For information about how to delete blog entries, see the section, "Deleting a Blog Entry" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

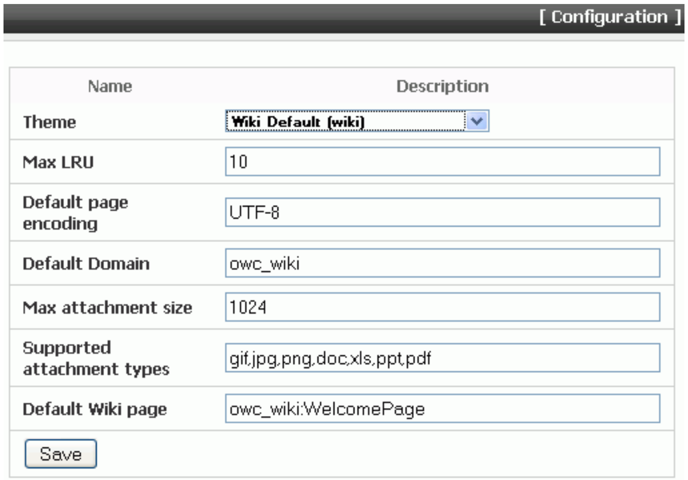
19.2.2.10 Specifying Configuration Parameters

You can use Administration mode to configure various parameters for your Oracle WebCenter Wiki and Blog Server. These configuration parameters include specifying the:

- Default server theme
- Maximum number of Last Recent Updates (LRU) pages listed
- Default page encoding format
- Default domain of the server
- Maximum attachment size in kilobytes (KB) supported on the server
- Attachment types supported on the server
- Default wiki page, that is the home page, of the server

To configure these settings, use the **Configuration** page, shown in Figure 19–22. You access this page by selecting **Configuration** under **General** in Administration mode.

Figure 19–22 Configuration Page



[Configuration]

Name	Description
Theme	Wiki Default (wiki)
Max LRU	10
Default page encoding	UTF-8
Default Domain	owc_wiki
Max attachment size	1024
Supported attachment types	gif,jpg,png,doc,xls,ppt,pdf
Default Wiki page	owc_wiki:WelcomePage

19.2.2.11 Importing Templates and Attachments

Oracle WebCenter Wiki and Blog Server supports only a database repository; templates and attachments are also stored in the database repository. In previous versions of Oracle WebCenter Wiki and Blog Server, regardless of the repository type configured for the server, templates and attachments were stored in a file-based repository.

If you migrate from any previous version of Oracle WebCenter Wiki and Blog Server configured to use a database repository, then during migration templates and attachments are migrated to the database repository of your server. If you migrate from a previous version of Oracle WebCenter Wiki and Blog Server configured to use a file-based repository, then templates and attachments are migrated to a file-based repository and not to the database repository of your Oracle WebCenter Wiki and Blog Server. To make these templates and attachments available in your Oracle WebCenter Wiki and Blog Server, you must manually migrate them to the database repository.

To import attachments for a wiki page, the user who owns that wiki page or you as an administrator must reupload the attachments on the wiki page. When you reupload an attachment, the attachment gets stored in the database repository. Note that attachments must be reuploaded for each wiki page individually.

To migrate templates:

1. In Administration mode of your Oracle WebCenter Wiki and Blog Server 11.1.1.2.0, click **Templates**.
2. Click **import**.
3. On the **Import Templates** page, in the **Folder** field, enter the path to templates. For example,

   `*$APPLICATIONS_DIRECTORY*/owc_wiki/templates`.

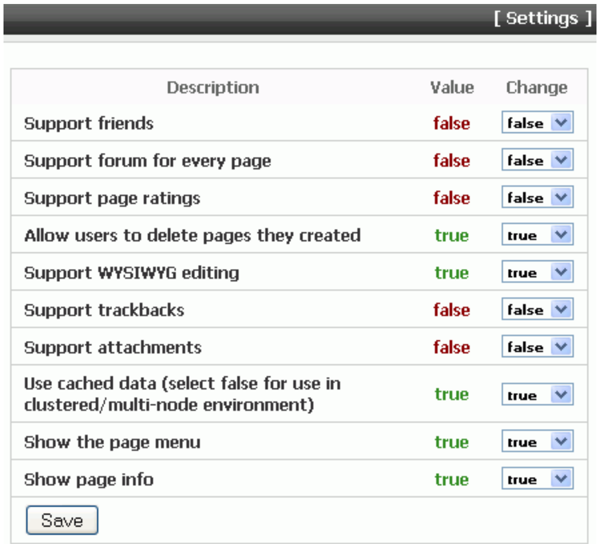
   Where, *`$APPLICATIONS_DIRECTORY`* is the directory where you installed Oracle WebCenter Wiki and Blog Server 11.1.1.2.0. That is, *`APPLICATIONS_DIRECTORY`* = *`MW_HOME`*`/user_projects/applications/`*`WEBCENTER_DOMAIN_NAME`*.
4. Click **Import Templates**. The existing file-based templates are individually re-created in the wiki database repository.

19.2.2.12 Specifying Features Supported on Oracle WebCenter Wiki and Blog Server

As an administrator, you can choose to enable or disable certain features on your Oracle WebCenter Wiki and Blog Server. For example, you can specify whether attachments, page menu, and remote synchronization are supported.

To set your wiki and blog server features, in Administration mode, click the **Settings** link, and then select the value for the specified features as **true** or **false**, as shown in Figure 19–23.

Figure 19–23 Wiki and Blog Server Settings



[Settings]

Description	Value	Change
Support friends	false	false
Support forum for every page	false	false
Support page ratings	false	false
Allow users to delete pages they created	true	true
Support WYSIWYG editing	true	true
Support trackbacks	false	false
Support attachments	false	false
Use cached data (select false for use in clustered/multi-node environment)	true	true
Show the page menu	true	true
Show page info	true	true

Table 19–3 describes the settings that you can configure on Oracle WebCenter Wiki and Blog Server.

Table 19–3 Oracle WebCenter Wiki and Blog Server Settings

Setting	Description
Support friends	Provides the ability to keep a set of bookmarked links to blogs of users whom you consider your friends.
Support forum for every page	Enables discussion forums associated with each wiki page.
Allow users to delete pages they created	Enables users to delete the wiki pages that they created. If this option is set to `false`, then only a wiki administrator can delete a wiki page.
Support WYSIWYG editing	Enables users to perform WYSIWYG editing, that is, view the result of their changes as they make the changes on wiki pages.
Support trackbacks	Enables a way for wiki authors to keep track of links to their pages.
Support attachments	Enables users to upload attachments to a wiki page. With this setting enabled, an Attachments tab appears on wiki pages.
Use cached data (select false for use in clustered/multi-node environment)	Enables use of cached data. You can enable this feature in a single-server environment to gain performance improvements from caching. Caches are not shared in a clustered environment. It is recommended that you disable this feature in a clustered or multi-node environment.
Show the page menu	Displays the domain-specific menu in the navigation panel on the wiki and blog server.
Show page info	Enables page information displayed in the footer of wiki pages.

19.2.2.13 Configuring `application_config_script`

You can configure the `application_config_script` file to enable or disable various features on your Oracle WebCenter Wiki and Blog Server. The `application_config_script` file is located in the `WEB-INF/classes` directory of your deployed Oracle WebCenter Wiki and Blog Server.

Table 19–4 describes the entries that you can configure in `application_config_script`.

Table 19–4 application_config_script Configuration Settings

Entry	Description

`index_cron`	Specifies the schedule for search indexing.
	Use the following format:
	`SecondsOfDay MinutesOfDay HourOfDay DayOfMonth MonthOfYear ?`
	An asterisk in any of these parameters implies "all". For example, to run search indexing every day at 2:30 a.m., use the following entry:
	`0 30 2 * * ?`

`index_on_startup`	Performs a full search indexing on server startup if `index_on_startup=true`. Running this search ensures that the search index is properly synchronized with the wiki and blog server data when the server is running.

`activity_job_cron`	Specifies the schedule for activity job publishing. Use the following format:
	`SecondsOfDay MinutesOfDay HourOfDay DayOfMonth MonthOfYear ?`
	An asterisk in any of these parameters implies "all". For example, to run activity publish job every day at 2:30 a.m., use the following entry:
	`0 30 2 * * ?`
	To disable the job, use the following value:
	`0 0 0 0 0 ?`

`custom_analyzer`	Specifies the fully qualified class name of the custom search analyzer to be used for tokenizing wiki content. For example, if you are using the Chinese Sandbox, then the entry should look like: `custom_analyzer : org.apache.lucene.analysis.cn.ChineseAnalyzer`

Note: Oracle WebCenter 11*g* Release 1 (11.1.1.2.0) does not provide the feature to publish the wiki activity data to Analytics. Therefore, in the `application_config_script` file, by default, the `support_analytics` entry is set to `false`.

19.2.2.14 Generating the Passcode

Oracle WebCenter Wiki and Blog Server provides Web Services that enable interaction with WebCenter applications. All Web Services methods are protected to prevent unauthorized access. Every method contains a String key parameter to ensure authorized access. This key is generated as a function of a user's name and a preconfigured passcode. The passcode is an arbitrary string that you create in the credential store of the WebCenter domain in which Oracle WebCenter Wiki and Blog Server is deployed.

> **Note:** You may skip this section if you do not plan to use Oracle WebCenter Wiki and Blog Server Web Services.

To create the passcode, you must create a password credential key named `wsPasscode` in the credential map named `owc_wiki`. In this key, you need to specify the user name as `owc_wiki` and the desired passcode. The passcode must be shared with trusted application developers wishing to use Web Services. For information about Oracle WebCenter Wiki and Blog Server Web Services, see the "Oracle Wiki Server Web Services Interface" section in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*.

> **Note:** In Oracle WebCenter Wiki and Blog Server 11*g*, Release 1 (11.1.1.1.0), the default value of passcode for Web Services configuration was `owCwIKi`. The passcode was stored as cleartext in `web.xml` of the server. In Oracle WebCenter Wiki and Blog Server 11*g*, Release 1 (11.1.1.2.0), there is no default passcode and the passcode is stored in a credential store.

You can create the password credential key by using the WLST command `createCred` or by using Oracle Enterprise Manager Fusion Middleware Control Console.

To generate the passcode by using the `createCred` WLST command:

```
createCred
(map="mapname",key="keyname",user="username",password="password",desc="description
")
```

For example:

```
createCred(map="owc_wiki",key="wsPasscode",user="owc_wiki",password="123456",desc=
"OWC Wiki Web Services passcode")
```

To create the passcode by using Fusion Middleware Control Console:

1. Start Fusion Middleware Control Console. For information, see Section 6.1, "Displaying Fusion Middleware Control Console."
2. Right-click the domain in which Oracle WebCenter Wiki and Blog Server is deployed. Next, select **Security** and then click **Credentials**.
3. On the **Credentials** page, click the **Create Map** button to create a credential map for your wiki and blog server.
4. In the Create Map dialog, in the **Map Name** field, enter `owc_wiki` as the credential map name.
5. Click **OK**.
6. Select the newly created credential map, `owc_wiki`.
7. Click the **Create Key** button.
8. In the Create Key dialog, ensure that `owc_wiki` is selected in the **Select Map** list, and **Password** is selected in the **Type** list.

9. In the **Key** field, enter `wsPasscode` as the name of the key.
10. In the **User Name** field, enter a user name.
11. In the **Password** field, enter the desired passcode.
12. Click **OK**.
13. Restart the server to which Oracle WebCenter Wiki and Blog Server is deployed.

19.2.2.15 Backing Up and Restoring Wiki Content

Oracle WebCenter Wiki and Blog Server uses a database repository. You can back up all your wiki content stored in the database by using SQL scripts or any database backup tool. You can also back up the wiki configuration file, `application_config.script`, which is located at the following path:

```
$APPLICATIONS_DIRECTORY/owc_wiki/WEB-INF/classes/application_config.script
```

19.2.3 Oracle WebCenter Wiki and Blog Server - Security Considerations

You can configure Oracle WebCenter Wiki and Blog Server to leverage single sign-on (SSO) using Oracle Access Manager (OAM), Oracle Single Sign-On (OSSO), or SAML-based single sign-on solution to secure Oracle WebCenter Wiki and Blog Server. For general information about configuring SSO, see Chapter 26, "Configuring WebCenter Applications and Components to Use SSO." For information specific to configuring the Wiki and Blog Server for OAM, see Section 26.1.7.3, "Configuring the Wiki Server."

You may also want to secure the browser connection to the Wiki and Blog Server using SSL to provide message encryption. For information about securing the browser connection to the Wiki and Blog Server, see Section 27.4, "Securing the Browser Connection to the Wiki Service with SSL."

When you integrate wikis and blogs into your WebCenter applications, users defined for your applications must match the users created on the Oracle WebCenter Wiki and Blog Server. Once a user is authenticated, if the user does not exist on Oracle WebCenter Wiki and Blog Server, the user is created and a default role is assigned to the user.

19.2.4 Oracle WebCenter Wiki and Blog Server - Limitations

Wiki pages on Oracle WebCenter Wiki and Blog Server do not support global preference settings and bi-directional languages.

19.3 Registering Oracle WebCenter Wiki and Blog Server

You can register multiple Oracle WebCenter Wiki and Blog Server connections with a WebCenter application, but only one of the connections is active at a time.

To start using a new (active) connection, you must restart the managed server on which the WebCenter application is deployed.

This section contains the following subsections:

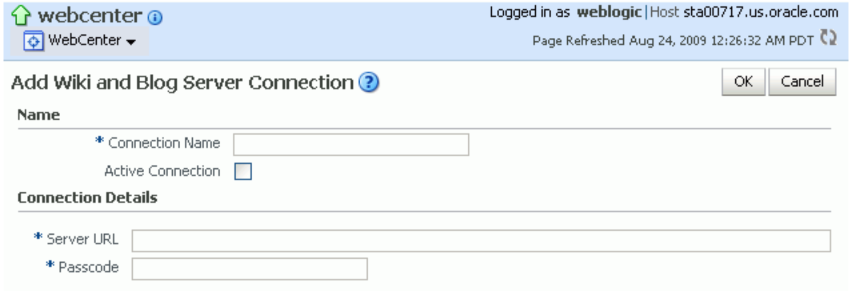
- Section 19.3.1, "Registering Oracle WebCenter Wiki and Blog Server Using Fusion Middleware Control"
- Section 19.3.2, "Registering Oracle WebCenter Wiki and Blog Server Using WLST"

19.3.1 Registering Oracle WebCenter Wiki and Blog Server Using Fusion Middleware Control

To register a connection to Oracle WebCenter Wiki and Blog Server:

1. Log in to Fusion Middleware Control and navigate to the home page for WebCenter Spaces or the custom WebCenter application. For more information, see:
   - Section 6.2, "Navigating to the Home Page for WebCenter Spaces"
   - Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"
2. Do one of the following:
   - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings** > **Service Configuration**.
   - For WebCenter applications - From the **Application Deployment** menu, choose **WebCenter** > **Service Configuration**.
3. From the list of services on the WebCenter Service Configuration page, select **WikiServer**.
4. To register a connection to the wiki and blog server, click **Add** (Figure 19–24).

Figure 19–24 Registering a Wiki and Blog Server Connection


webcenter
WebCenter
Logged in as weblogic | Host sta00717.us.oracle.com
Page Refreshed Aug 24, 2009 12:26:32 AM PDT
OK
Cancel

Add Wiki and Blog Server Connection

Name

* Connection Name

Active Connection □

Connection Details

* Server URL

* Passcode

5. On the **Add Wiki and Blog Server Connection** page, in the **Name** section, enter a unique name for the connection, and indicate whether the connection is the active (or default) connection for the application (Table 19–5).

Table 19–5 Wiki and Blog Connection - Name

Field	Description
Name	Enter a unique name for the connection. The name must be unique (across all connection types) within the WebCenter application.
Active Connection	Select the checkbox to use this connection in the WebCenter application for Wiki and Blog services. While you can register multiple wiki and blog server connections, only one connection is used by the Wiki and Blog services— the default (or active) connection.

6. In the Connection Details section, enter connection details for your Oracle WebCenter Wiki and Blog Server. For details, see Table 19–6.

Table 19–6 Wiki and Blog Connection - Connection Details

Field	Description
Server URL	Enter the base URL of the server providing Wiki and Blog services. The server must be an Oracle WebCenter Wiki and Blog Server. Use the format: `protocol://host:port` For example: `http://mywiki.com:8001`
Passcode	Enter the passcode that is required to call methods in Oracle WebCenter Wiki and Blog Server Web Services. The passcode is an arbitrary string that the administrator sets up in Oracle WebCenter Wiki and Blog Server after installation to prevent unauthorized access. Contact the administrator to obtain the server's passcode.

7. Click **OK** to save this connection.
8. To start using the new (active) connection, you must restart the managed server to which the WebCenter application is deployed. For more information, see Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."

19.3.2 Registering Oracle WebCenter Wiki and Blog Server Using WLST

Use the `createWikiserverConnection` WLST command to create a wiki and blog server connection for a named WebCenter application. For command syntax and examples, see the section "createWikiserverConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

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

> **Note:** To start using the new (active) connection, you must restart the managed server to which the WebCenter 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*.

19.4 Choosing the Active Wiki and Blog Server Connection

You can register multiple wiki and blog server connections with a WebCenter application but only one connection is active at a time.

For WebCenter Spaces and custom WebCenter applications, the *active connection* becomes the back-end wiki and blog server for:

- Wiki and blog pages (created through page styles)
- Wiki search adapter
- Wiki Oracle SES crawl adapter

This section contains the following subsections:

- Section 19.4.1, "Choosing the Active Wiki and Blog Server Connection Using Fusion Middleware Control"

- Section 19.4.2, "Choosing the Active Wiki and Blog Server Connection Using WLST"

19.4.1 Choosing the Active Wiki and Blog Server Connection Using Fusion Middleware Control

To change the active connection:

1. Log in to Fusion Middleware Control and navigate to the home page for WebCenter Spaces or the custom WebCenter application. For more information, see:
   - Section 6.2, "Navigating to the Home Page for WebCenter Spaces"
   - Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"
2. Do one of the following:
   - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings** > **Service Configuration**.
   - For WebCenter applications - From the **Application Deployment** menu, choose **WebCenter** > **Service Configuration**.
3. From the list of services on the WebCenter Services Configuration page, choose **WikiServer**.

   The Manage Wiki and Blog 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 (active) connection you must restart the managed server to which the WebCenter application is deployed. For more information, see Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."

19.4.2 Choosing the Active Wiki and Blog Server Connection Using WLST

Use the WLST command `setWikiserverConnection` with `default=true` to activate an existing wiki and blog server connection. Use the `listDefaultWikiserverConnection` command to find out the active or default connection used by the Wiki and Blog services. For command syntax and examples, see the sections, "setWikiserverConnection" and "listDefaultWikiserverConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

To start using the new (active) connection, you must restart the managed server to which the WebCenter application is deployed. For more information, see "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

19.5 Modifying the Wiki and Blog Server Connection Details

You can modify the wiki and blog server connection details at any time.

To start using the modified (active) connection, you must restart the managed server to which the WebCenter application is deployed.

This section contains the following subsections:

- Section 19.5.1, "Modifying Wiki and Blog Server Connection Details Using Fusion Middleware Control"
- Section 19.5.2, "Modifying Wiki and Blog Server Connection Details Using WLST"

19.5.1 Modifying Wiki and Blog Server Connection Details Using Fusion Middleware Control

To update wiki and blog server connection details:

1. Log in to Fusion Middleware Control and navigate to the home page for WebCenter Spaces or the custom WebCenter application. For more information, see:
   - Section 6.2, "Navigating to the Home Page for WebCenter Spaces"
   - Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"
2. Do one of the following:
   - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings** > **Service Configuration**.
   - For WebCenter applications - From the **Application Deployment** menu, choose **WebCenter** > **Service Configuration**.
3. From the list of services on the WebCenter Service Configuration page, choose **WikiServer**.
4. Select the connection name, and click **Edit**.
5. Edit the connection details, as required. For detailed parameter information, see Table 19–6.
6. Click **OK** to save your changes.
7. To start using the updated (active) connection, you must restart the managed server to which the WebCenter application is deployed. For information, see Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments".

19.5.2 Modifying Wiki and Blog Server Connection Details Using WLST

Use the WLST command `setWikiserverConnection` to edit the wiki and blog server connection details. For command syntax and examples, see the section, "setWikiserverConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

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

Note: To start using the updated (active) connection, you must restart the managed server to which the WebCenter 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*.

19.6 Deleting Wiki and Blog Server Connections

You can delete wiki and blog server connections at any time, but be careful when deleting the active connection. If you delete the active connection, none of the wiki and blog server web services will work because they all require Oracle WebCenter Wiki and Blog Server at the back end.

This section contains the following subsections:

- Section 19.6.1, "Deleting a Wiki and Blog Server Connection Using Fusion Middleware Control"
- Section 19.6.2, "Deleting a Wiki and Blog Server Connection Using WLST"

19.6.1 Deleting a Wiki and Blog Server Connection Using Fusion Middleware Control

To delete a wiki and blog server connection:

1. Log in to Fusion Middleware Control and navigate to the home page for WebCenter Spaces or the custom WebCenter application. For more information, see:
   - Section 6.2, "Navigating to the Home Page for WebCenter Spaces"
   - Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"
2. Do one of the following:
   - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings** > **Service Configuration**.
   - For WebCenter applications - From the **Application Deployment** menu, choose **WebCenter** > **Service Configuration**.
3. From the list of services on the **WebCenter Services Configuration** page, select **WikiServer**.
4. Select the connection name, and click **Delete**.
5. To effect this change, you must restart the managed server to which the WebCenter application is deployed. For more information, see Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."

Note: Before restarting the managed server, mark another connection as active; otherwise the service will be disabled.

19.6.2 Deleting a Wiki and Blog Server Connection Using WLST

Use the WLST command `deleteConnection` to remove a connection. For command syntax and examples, see the section, "deleteConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

Ensure that another connection is marked active; otherwise, the service will be disabled.

For information about how to run WLST commands, see Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool (WLST) Commands."

Note: To effect this change, you must restart the managed server to which the WebCenter 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*.

19.7 Testing Wiki and Blog Server Connections

Try accessing your Oracle WebCenter Wiki and Blog Server with the following URL format:

```
http://host:port/owc_wiki
```

This should show the home page of the default wiki domain.

19.8 Monitoring Oracle WebCenter Wiki and Blog Server

You can monitor Oracle WebCenter Wiki and Blog Server by viewing the log file, `owc_wiki.log`. This file is located in the following directory:

```
$APPLICATIONS_DIRECTORY/owc_wiki
```

Where:

- *`$APPLICATIONS_DIRECTORY`* is the directory where you installed Oracle WebCenter Wiki and Blog Server. That is, *`APPLICATIONS_DIRECTORY`* = *`MW_HOME`*`/user_projects/applications/`*`WEBCENTER_DOMAIN_NAME`*.
- `owc_wiki` is the directory where your Oracle WebCenter Wiki and Blog Server is deployed.

To change the log level, modify the `jlo_logging.xml` file located at the following path:

```
$APPLICATIONS_DIRECTORY/owc_wiki/WEB-INF/classes
```

You can change the targets of the loggers in this file. The following targets are supported: `trace`, `info`, `debug`, `warn`, `error`, and `fatal`. You can also use two special targets: `off` (to switch off all the targets) or `all` (to switch on all the targets). For more information about the jLo logger, see:

`http://jlo.jzonic.org/GettingStarted.html`

Note: You can change the location of the log file by using the jLo handlers. For more information, see:

`http://jlo.jzonic.org/AllHandlers.html`

19.9 Troubleshooting Issues with Wiki and Blogs

This section describes a possible issue that you may face after configuring OAM-SSO on Oracle WebCenter Wiki and Blog Server.

Problem

After configuring OAM-SSO on Oracle WebCenter Wiki and Blog Server, when you log out, the server does not redirect to the login page properly.

Solution

Ensure that the `logout_url` property is set accurately in the `application_config.script` file, which is located in the `Web-INF/classes` directory of your deployed Oracle WebCenter Wiki and Blog Server.

The link can be customized to any URL based on the single sign-on scheme used. Leaving `logout_url` blank renders the user session invalid and redirects to the login screen.

20

Managing the Worklist Service

This chapter describes how to configure and manage the Worklist service for WebCenter Spaces and custom WebCenter applications deployed on Oracle WebLogic Server.

Always use Fusion Middleware Control or WLST command-line tool to review and configure back-end services for WebCenter applications. Any changes that you make to WebCenter applications, post deployment, are stored in MDS metatdata store as customizations. See Section 1.3.5, "Oracle WebCenter Configuration Considerations."

> **Note:** Changes that you make to WebCenter services configuration, through Fusion Middleware Control or using WLST, are not dynamic so you must restart the managed server on which the WebCenter application is deployed for your changes to take effect. See Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."

This chapter includes the following sections:

- Section 20.1, "What You Should Know About BPEL Connections"
- Section 20.2, "BPEL Server Prerequisites"
- Section 20.3, "Setting Up Worklist Connections"
- Section 20.4, "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."

20.1 What You Should Know About BPEL Connections

Both the Worklist service and the WebCenter Spaces workflows require a connection to a BPEL (Business Process Execution Language) server. These WebCenter services can share the same BPEL server connection or each connect to different BPEL servers.

- **Worklist service** - allows multiple connections so that WebCenter users can monitor and manage assignments and notifications from a range of BPEL servers. For more information, see Section 20.3, "Setting Up Worklist Connections."

- **WebCenter Spaces workflows** - requires a single connection to the BPEL server included with the Oracle SOA Suite. For more information, see Section 9.1.1, "Specifying the BPEL Server Hosting WebCenter Spaces Workflows."

20.2 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
  ```

  Users must be identical in both identity stores (LDAP).
- 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.
- While configuring the BPEL server to LDAP, in the OID Authenticator, use the value `dc=example,dc=com`.
- No configuration-related exceptions must exist. Use the WLST command `listWorklistConnections` to display the configured connections and validate the connection details.
- If the Oracle SOA Suite BPEL's managed server is configured to use a shared identity store and that store does not contain the required user by default, then the user must be configured, as described in Section 20.4.2.2, "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 20.4, "Troubleshooting Issues with Worklists."

This section includes the following subsections:

- Section 20.2.1, "BPEL Server - Installation and Configuration"
- Section 20.2.2, "BPEL Server - Security Considerations"
- Section 20.2.3, "BPEL Server - Limitations in WebCenter"

20.2.1 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 applications by setting up connections to the BPEL server. No further configuration is required on Oracle SOA or Oracle WebCenter.

20.2.2 BPEL Server - Security Considerations

The Worklist service displays tasks for the currently authenticated user. For WebCenter 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 (same user name and password) on both the WebCenter 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 (with the same password) on both the BPEL server and within your application.

To access BPEL task details from the WebCenter Worklist component, without incurring additional login prompts, WebCenter and Oracle SOA Suite servers must be configured to a shared Oracle Single Sign-On server. For more information, see Section 26.2, "Configuring Oracle Single Sign-On (OSSO)."

For information on configuring WS-Security between SOA and WebCenter Spaces, see Chapter 28, "Configuring WS-Security for WebCenter Applications and Components."

20.2.3 BPEL Server - Limitations in WebCenter

Worklist task flows function inside authenticated pages only. If Worklist task flows are placed on unsecured pages, that is, public pages, a security error message displays.

20.3 Setting Up Worklist Connections

This section includes the following subsections:

- Section 20.3.1, "What You Should Know About Worklist Connections"
- Section 20.3.2, "Registering Worklist Connections"
- Section 20.3.3, "Activating a Worklist Connection"
- Section 20.3.4, "Modifying Worklist Connection Details"
- Section 20.3.5, "Deleting Worklist Connections"
- Section 20.3.6, "Testing Worklist Connections"

20.3.1 What You Should Know About Worklist Connections

The Worklist service enables WebCenter applications to show authenticated users a list of BPEL worklist items currently assigned to them through the Worklist task flow. BPEL worklist items are open BPEL tasks from one or more BPEL worklist repositories.

A connection to every BPEL server that delivers worklist items is required. Multiple worklist connections are allowed so that WebCenter users can monitor and manage assignments and notifications from a range of BPEL servers.

Worklist connection details are stored in `connections.xml`. Another file, `adf-config.xml`, identifies which connections are actively used by the Worklist service.

If 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 application's diagnostic log.

WebCenter Spaces

WebCenter Spaces requires a BPEL server connection to support its internal workflows, that is, group space membership notifications and group space subscription requests. The BPEL server providing this functionality is always a BPEL server included with the Oracle SOA Suite. For more information, see Section 9.1.1, "Specifying the BPEL Server Hosting WebCenter Spaces Workflows."

The Worklist service can share the SOA instance connection and by doing so, display worklist items relating to group space activity in each user's Worklist task flow.

20.3.2 Registering Worklist Connections

This section includes the following subsections:

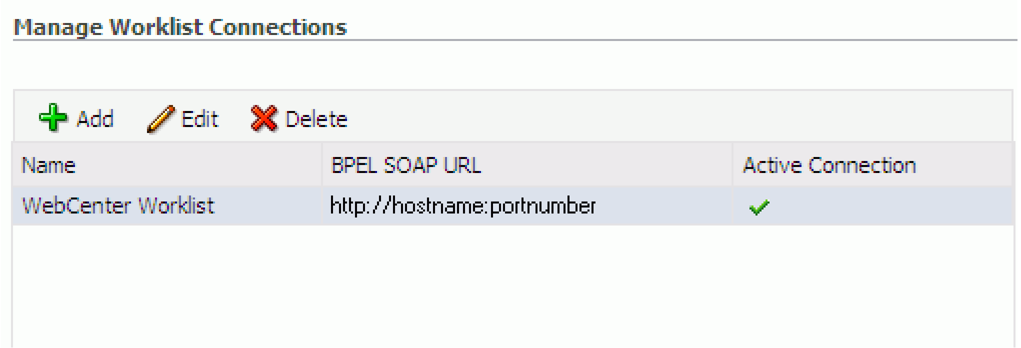
- Section 20.3.2.1, "Registering Worklist Connections Using Fusion Middleware Control"
- Section 20.3.2.2, "Registering Worklist Connections Using WLST"

20.3.2.1 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 WebCenter Spaces or the custom WebCenter application. For more information, see:
   - Section 6.2, "Navigating to the Home Page for WebCenter Spaces"
   - Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"
2. Do one of the following:
   - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings** > **Service Configuration**.
   - For WebCenter applications - From the **Application Deployment** menu, choose **WebCenter** > **Service Configuration**.
3. From the list of services on the WebCenter Service Configuration page, select **Worklist**.
4. To register a new connection, click **Add** (Figure 20–1).

Figure 20–1 Configuring Worklist Connections



Manage Worklist Connections

Name	BPEL SOAP URL	Active Connection
WebCenter Worklist	http://hostname:portnumber	✓

5. Enter a unique name for the Worklist connection and activate the connection to use the connection immediately (Table 20–1).

Table 20–1 Worklist Connection - Name

Field	Description
Name	Enter a unique name for the connection. The name must be unique (across all connection types) within the WebCenter application. This name may be displayed to users working with the worklist feature in the WebCenter application. Users may organize their worklist assignments through various sorting and grouping options. The option "Group By Worklist Server" displays the name you specify here so it's important to enter a meaningful name that other users will easily recognize, for example, `Human Resources`.
Active Connection	Select to activate this worklist connection in the WebCenter application. Once activated, worklist items from the associated BPEL server display in users' worklists. Multiple worklist connections may be active at a time, enabling WebCenter users to monitor and manage assignments and notifications from a range of BPEL servers. If you need to disable a connection for any reason, deselect this option. (Edit mode only.) Check boxes indicate whether other components share this connection: **WebCenter Spaces Application** Indicates whether WebCenter Spaces uses this BPEL server connection for internal workflows, such as Group Space membership notifications, Group Space subscription requests, and more. The BPEL server that provides this functionality is the BPEL server included with the Oracle SOA Suite. For more information, see Section 9.1.1, "Specifying the BPEL Server Hosting WebCenter Spaces Workflows." Before modifying connection properties, consider impact to any other components that share this connection.

6. Enter connection details for the BPEL server (Table 20–2).

Table 20–2 Worklist Connection - Connection Details

Field	Description

BPEL Soap URL	Enter the URL required to access the BPEL server. Use the format:
	`protocol://host:port`
	For example:
	`http://mybpelserver.com:8001`
	Note: WebCenter Spaces uses the BPEL server included with the Oracle SOA Suite to implement group space subscription 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 9.1.1, "Specifying the BPEL Server Hosting WebCenter Spaces Workflows."

SAML Token Policy URI	Select the SAML (Security Assertion Markup Language) token policy this connection uses for authentication. 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. Options available are: ■ **SAML Token Client Policy** (oracle/wss10_saml_token_client_policy) - Select to verify your basic configuration without any additional security. This is the default setting. ■ **SAML Token With Message Protection Client Policy** (oracle/wss10_saml_token_with_message_protection_client_policy) - Select to increase the security using SAML-based BPEL Web Services. If selected, you must configure keystores both in your WebCenter application and in the BPEL application. For information about configuring the BPEL server's Worklist connection to use this policy, see Section 28.1.3, "Configuring the BPEL Server for a Simple Topology."

7. Click **OK** to save this connection.
8. To start using the new (active) connection you must restart the managed server on which the WebCenter application is deployed. For more information, see Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."

20.3.2.2 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 20.3.3.2, "Activating a Worklist Connections Using WLST."

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

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

20.3.3 Activating a Worklist Connection

In WebCenter applications, multiple Worklist connections may be active at a time. Multiple connections enable WebCenter users to monitor and manage assignments and notifications from a multiple BPEL servers. From time to time you may need to temporarily disable an active connection, or enable an existing connection.

This section includes the following subsections:

- Section 20.3.3.1, "Activating a Worklist Connections Using Fusion Middleware Control"
- Section 20.3.3.2, "Activating a Worklist Connections Using WLST"

20.3.3.1 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 WebCenter Spaces or the custom WebCenter application. For more information, see:
   - Section 6.2, "Navigating to the Home Page for WebCenter Spaces"
   - Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"
2. Do one of the following:
   - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings** > **Service Configuration**.
   - For WebCenter applications - From the **Application Deployment** menu, choose **WebCenter** > **Service Configuration**.
3. From the list of services on the WebCenter Services Configuration page, 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 application.

   Once activated, worklist items from the associated BPEL server display in Worklist task flows. If you need to disable a connection for any reason, deselect this option.
6. Click **OK** to update the connection.
7. To start using the new (active) connection you must restart the managed server on which the WebCenter application is deployed. For more information, see

Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."

20.3.3.2 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.

Use `listWorklistConnections` to see which connections are currently active. If the `listWorklistConnections` command indicates an invalid connection name, a connection was removed from `connections.xml` using the `deleteConnection` command but it was not removed from `adf-config.xml` with `removeWorklistConnection`. To resolve this issue, you can either re-create the named connection using `createBPELConnection`, or run the `removeWorklistConnection` command.

For syntax details and examples, see "removeWorklistConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

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

> **Note:** To start using the active connection you must restart the managed server on which the WebCenter 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*.

20.3.4 Modifying Worklist Connection Details

This section includes the following subsections:

- Section 20.3.4.1, "Modifying Worklist Connection Details Using Fusion Middleware Control"
- Section 20.3.4.2, "Modifying Worklist Connection Details Using WLST"

20.3.4.1 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 WebCenter Spaces or the custom WebCenter application. For more information, see:
   - Section 6.2, "Navigating to the Home Page for WebCenter Spaces"
   - Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"
2. Do one of the following:
   - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings** > **Service Configuration**.

- For WebCenter applications - From the **Application Deployment** menu, choose **WebCenter** > **Service Configuration**.

3. From the list of services on the WebCenter Services Configuration page, 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 20–2, " Worklist Connection - Connection Details".
6. Click **OK** to update the connection.
7. To start using the updated (active) connection you must restart the managed server on which the WebCenter application is deployed. For more information, see Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."

20.3.4.2 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 1.12.3.1, "Running Oracle WebLogic Scripting Tool (WLST) Commands."

> **Note:** To start using the updated (active) connection you must restart the managed server on which the WebCenter application is deployed. For more information, see the section, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

20.3.5 Deleting Worklist Connections

Before you delete a Worklist connection, verify whether the WebCenter Spaces workflows use the same connection.

This section includes the following subsections:

- Section 20.3.5.1, "Deleting Worklist Connections Using Fusion Middleware Control"
- Section 20.3.5.2, "Deleting Worklist Connections Using WLST"

20.3.5.1 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 WebCenter Spaces or the custom WebCenter application. For more information, see:
   - Section 6.2, "Navigating to the Home Page for WebCenter Spaces"
   - Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"
2. Do one of the following:

- For WebCenter Spaces - From the **WebCenter** menu, choose **Settings** > **Service Configuration**.
- For WebCenter applications - From the **Application Deployment** menu, choose **WebCenter** > **Service Configuration**.

3. From the list of services on the WebCenter Services Configuration page, 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 application is deployed. For more information, see Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."

20.3.5.2 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` 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 1.12.3.1, "Running Oracle WebLogic Scripting Tool (WLST) Commands."

20.3.6 Testing Worklist Connections

To test a Worklist connection, log in to the SOA BPEL Worklist application with valid user credentials. A Worklist application is accessible through a URL in the following format:

```
protocol://host:port/integration/worklistapp
```

For example:

```
http://mybpelserver.com:8001/integration/worklistapp
```

You can also verify the status of the `wsm-pm` application, that manages the SAML policy Web service authentication mechanism used by the Worklist service. To list `wsm-pm` policies, log in to both the SOA BPEL server and the server running the Worklist task flow, using the following URL format:

```
protocol://SOA_server_host:port/wsm-pm/validator
```

For example:

```
http://mypbelserver.com:8001/wsm-pm/validator
http://myWorklistHostingServer.com:8888/wsm-pm/validator
```

20.4 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 20.4.1, "Unavailability of the Worklist Service Due to Application Configuration Issues"
- Section 20.4.2, "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.

20.4.1 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 20.4.1.1, "adf-config.xml Refers to a Non-Existent BPEL Connection"
- Section 20.4.1.2, "adf-config.xml Has No Reference to a BPEL Connection"
- Section 20.4.1.3, "No Rows Yet Message Displays"

20.4.1.1 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 20.3, "Setting Up Worklist Connections."

During development, refer to the chapter "Integrating the Worklist Service" in *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*.

To find out which connections names are referenced and to validate the Worklist service configuration, run the WLST command, `listWorklistConnections(appName='myApp', verbose=true)`. For more information, see "listWorklistConnections" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

20.4.1.2 adf-config.xml Has No Reference to a BPEL Connection

There is no reference to a Worklist service connection in the application's `adf-config.xml`, but this connection exists in the `connections.xml` file.

Problem

In diagnostic log files for the managed server on which the application is running, you see entries such as the following:

```
[2009-03-23T10:23:56.943+00:00] [DefaultServer] [WARNING]
[WCS-32009] [oracle.webcenter.worklist.config] [tid:
[ACTIVE].ExecuteThread: '21' for queue: 'weblogic.kernel.Default
(self-tuning)'] [userId: user] [ecid:
0000I0mqx8Fk3FLN2o2ye19lqBV000008,0] [APP: Worklist#V2.0] The
Worklist service does not have a ConnectionName configuration
entry in adf-config.xml that maps to a BPELConnection in
connections.xml, therefore the Worklist service was not
configured for this application.
```

Solution

Configure a connection to at least one BPEL server so that the Worklist service can query worklist items.

Post deployment, create Worklist connections through WLST or Fusion Middleware Control. For information, see Section 20.3, "Setting Up 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*.

20.4.1.3 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*.

20.4.2 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. 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 20.4.2.1, "Users Mismatch in Identity Stores"
- Section 20.4.2.2, "Shared User Directory Does Not Include the weblogic User"
- Section 20.4.2.3, "Issues with the wsm-pm Application"
- Section 20.4.2.4, "Clocks are Out of Sync for More Than Five Minutes"
- Section 20.4.2.5, "Worklist Service Timed Out or is Disabled"

20.4.2.1 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-sece
xt-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:
0000I0nB64fFk3FLN2o2ye19lrBX00000O,0:1:3:1]
[WEBSERVICE_PORT.name: TaskQueryServicePortSAML] [APP:
soa-infra] [J2EE_MODULE.name:
/integration/services/TaskQueryService] [WEBSERVICE.name:
TaskQueryService] [J2EE_APP.name: soa-infra] Web service
authentication failed.
```

Solution

The same users must exist in identity stores of both managed servers. For information, see the section "Setting Security for the Worklist Service in *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*.

This can be easily accomplished 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.

20.4.2.2 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="SOAAdmin")
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.

20.4.2.3 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.

20.4.2.4 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.

20.4.2.5 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(InternalExecutorSer
vice.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.

21

Managing Portlet Producers

This chapter describes how to register, edit, delete, and deploy portlet producers.

This chapter includes the following sections:

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 1.12, "Oracle WebCenter Administration Tools."

21.1 What You Should Know About Portlet Producers

Consider the following while working with portlet producers:

- Several out-of-the-box producers are provided with Oracle WebCenter: OmniPortlet, Web Clipping, Rich Text Portlet, and WSRP Tools. The following EAR files are packaged with Oracle WebCenter:
  - `portalTools.ear` - OmniPortlet and Web Clipping
  - `wsrp-tools.ear` - Rich Text Portlets and 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 168 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* to install it in the production environment.
- When you create a connection to a portlet producer, the producer is registered with the WebCenter application and the connection is added to the `connections.xml` file. For WRSP 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, "Oracle WebCenter Configuration Considerations." For detailed information about MDS, see the chapter "Managing the Oracle Metadata Repository" in the *Oracle Fusion Middleware Administrator's Guide*.
- Portlet producer registration is dynamic. New portlet producers and updates to existing producers are immediately available in the WebCenter application; it is not necessary to restart the WebCenter application or the managed server.
- To migrate producers from one instance to another, use the migration utilities described in the appendix "Portlet Preference Store Migration Utilities" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*.
- For information on securing portlet producers, see Section 29.1, "Securing a WSRP Producer" and Section 29.2, "Securing a PDK-Java Producer."

21.2 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 21.2.1, "Registering a WSRP Producer Using Fusion Middleware Control"
- Section 21.2.2, "Registering a WSRP Producer Using WLST"

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*.

21.2.1 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 your custom WebCenter application (or WebCenter Spaces). For more information, see:
    - Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications".
    - Section 6.2, "Navigating to the Home Page for WebCenter Spaces"

2. Do one of the following:
   - For custom WebCenter applications - From the **Application Deployment** menu, choose **WebCenter** > **Register Producer**.
   - For WebCenter Spaces - From the **WebCenter** menu, choose **Register Producer**.
3. In the **Add Portlet Producer Connection** section, enter connection details for the WSRP producer.

   For detailed parameter information, see Table 21–1.

Table 21–1 WSRP Producer Connection Parameters

Field	Description
Connection Name	Enter a unique name to identify this portlet producer registration within the WebCenter application. The name must be unique across all WebCenter connection types. The name you specify here appears in the Oracle Composer (under the *Portlets* folder).
Producer Type	Indicate the type of this producer. Select **WSRP Producer**.
WSDL URL	The registration URL for the WSRP producer. The syntax varies according to your WSRP implementation. For example, possible URL formats for a portlet deployed to the Oracle WSRP container include: http://*host_name*:*port_number*/*context_root*/portlets/wsrp2?WSDL http://*host_name*:*port_number*/*context_root*/portlets/wsrp1?WSDL http://*host_name*:*port_number*/*context_root*/portlets/?WSDL (WSRP 1.0 for backward compatibility) Where: ■ `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. In WebCenter Spaces, only v2 WSDLs are supported for Oracle WebLogic Portal Producers. For example: `http://myhost.com:7778/MyPortletApp/portlets/wsrp2?WSDL` For WSRP producers, you can obtain this registration URL by accessing the producer test page at: http://*host_name*:*port_number*/*context_root*/info
Use Proxy?	Select if the WebCenter application must use an HTTP proxy when contacting this producer. If selected, enter values for **Proxy Host** and **Proxy Port**. A proxy is required when the WebCenter application and the remote portlet producer are separated by a firewall and an HTTP proxy is needed to communicate with the producer.

Table 21–1 (Cont.) WSRP Producer Connection Parameters

Field	Description
Proxy Host	Enter the address for the proxy server. Do not prefix `http://` to the proxy server name.
Proxy Port	Enter the port number on which the proxy server listens. The default port is `80`.
Default Execution Timeout (Seconds)	Enter a suitable timeout for design time operations. For example, the maximum time the producer may take to register, deregister, or display portlets on WebCenter pages. Individual portlets may define their own timeout period, which takes precedence over the value expressed here. This default is `30` seconds.

4. Use the **Security** section to specify the type of security token to use for the identity propagation/assertion.

   The security token with the propagated or asserted user information is represented as an XML element in the SOAP header. The security token and the SOAP message body are then digitally signed to prove the authenticity of the SOAP message origin from the WebCenter application. WebCenter Spaces supports three types of security tokens: *Username Tokens Without Password*, *Username Tokens With Password*, and *SAML Tokens*.

   Note: PeopleSoft WSRP producers support two profiles: *Username Token With Password* and *SAML Token With Message Integrity*. Oracle Portal (as a consumer) supports three profiles: *Username Token Without Password*, *Username Token With Password*, *SAML Token With Message Integrity*. Other Oracle WSRP producers support all profiles. For other WSRP containers, check with the specific vendor to determine the token formats they support.

   For detailed parameter information, see Table 21–2.

Table 21–2 WSRP Producer Security Connection Parameters

Field	Description
Token Profile	Select the type of token profile to use for authentication with this WSRP producer. Select from: ■ **None**—No security on this connection. If you select None, no WS-Security header is attached to the SOAP message. ■ **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. This policy does not require any keystore configuration. ■ **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. ■ **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. When you select this policy, you must also specify the Recipient Alias. ■ **WSS 1.0 Username 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 Basic128 suite of asymmetric key technologies. Specifically, RSA key mechanism for message confidentiality, SHA-1 hashing algorithm for message integrity, and AES-128 bit encryption. Use this token profile if the WSRP producer has a different identity store. You must define an external application pertaining to the producer and associate the external application with this producer. The external application defined here is used to retrieve and propagate the user credentials to the producer. The producer verifies this against the identity store configured for the external application. When you select this policy, you must also specify the Recipient Alias.

Table 21–2 (Cont.) WSRP Producer Security Connection Parameters

Field	Description
Token Profile (cont.)	■ **WSS 1.0 Username 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 (username 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 Basic128 suite of asymmetric key technologies. Specifically, RSA key mechanisms for message confidentiality, SHA-1 hashing algorithm for message integrity, and AES-128 bit encryption. When you select this policy, you must also specify the Recipient Alias. ■ **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 Basic128 suite of asymmetric key technologies for endorsing signatures.
Configuration	Select: ■ **Default** to use a default token profile configuration. ■ **Custom** to provide a custom Oracle Web Service Manager configuration. Additional security options display (including all the keystore properties) when you select **Custom**.
Issuer Name	Enter the name of the issuer of the SAML Token. For example: `www.example.com` 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. Valid for: WSS 1.0 SAML Token With Message Integrity, WSS1.0 SAML Token With Message Protection, WSS 1.0 SAML Token, and WSS 1.1 SAML Token with Message Protection

Table 21–2 (Cont.) WSRP Producer Security Connection Parameters

Field	Description
Default User	Enter a user name to assert to the remote producer when the user is not authenticated with the WebCenter application. When unauthenticated, the identity *anonymous* is associated with the application user. The value *anonymous* 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 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. The WSRP producer must be configured with `strict-authentication` to support *anonymous* to a default user mapping. The `strict-authentication` flag is defined in the producer's `oracle-portlet.xml` file. For more information, see the appendix "oracle-portlet.xml Syntax" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*. You must also add a grant to the policy store as described in Section 21.2.3, "Adding a Grant to the Policy Store for a Mapped User Identity." 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.
Associated External Application (Username With Password)	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. An external application is required to support producers using the security option *Username With Password*. The external application stores and supplies the user credentials. See also Section 22.2, "Registering External Applications." Valid for: WSS 1.0 Username With Password only.

5. Use the **Keystore** section to specify the location of the key store that contains the certificate and private key that is used for signing some parts (security token and SOAP message body) of the SOAP message.

   For detailed parameter information, see Table 21–3.

Table 21–3 WSRP Producer Key Store Connection Parameters

Field	Description
Recipient Alias	Specify the key store alias that is associated with the producer's certificate. This certificate is used to encrypt the message to the producer.
Store Path	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. The keystore should be created using JDK's keytool utility.
Password	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.

Table 21–3 (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 to use for encryption.
Encryption Key Password	Enter the password for accessing the encryption key.

6. Click **OK**.

   The new producer appears in the connection table.

21.2.2 Registering a WSRP Producer Using WLST

Use the WLST command `registerWSRPProducer` to create a connection to a WSRP portlet producer and register the producer with your WebCenter application. For command syntax and examples, see 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 1.12.3.1, "Running Oracle WebLogic Scripting Tool (WLST) Commands."

21.2.3 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.

21.3 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
```

21.4 Registering Oracle PDK-Java Producers

This section describes how to register PDK-Java producers for a deployed WebCenter application using Fusion Middleware Control and WLST commands. This section includes the following subsections:

- Section 21.4.1, "Registering an Oracle PDK-Java Producer Using Fusion Middleware Control"
- Section 21.4.2, "Registering an Oracle PDK-Java Producer Using WLST"

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*.

21.4.1 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 your custom WebCenter application (or WebCenter Spaces):
   - Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"
   - Section 6.2, "Navigating to the Home Page for WebCenter Spaces"
2. Do one of the following:

- For custom WebCenter applications - From the **Application Deployment** menu, choose **WebCenter** > **Register Producer**.
- For WebCenter Spaces - From the **WebCenter** menu, choose **Register Producer**.

3. In the **Add Portlet Producer Connection** section, enter connection details for the Oracle PDK-Java producer.

   For detailed parameter information, see Table 21–4, " Oracle PDK-Java Producer Connection Parameters".

Table 21–4 Oracle PDK-Java Producer Connection Parameters

Field	Description
Connection Name	Enter a unique name that identifies this portlet producer registration within the WebCenter application. The name must be unique across all WebCenter connection types. The name you specify here appears in the Oracle Composer (under the *Portlets* 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:
	`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
	▪ `context_root` is the Web application's context root.
	▪ `providers` is static text.
	For example:
	`http://myHost.com:7778/myEnterprisePortlets/providers`

Service ID	Enter a unique identifier for this producer.
	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.
	For example, the following URL endpoint requires `sample` as the service ID:
	`http://domain.example.com:7778/axyz/providers`
	However, the following URL endpoint, does not require a service ID:
	`http://domain.example.com:7778/axyz/providers/sample`
	The service ID is used to look up a file called `<service_id>.properties`, 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, `_default.properties` is used.

Table 21–4 (Cont.) Oracle PDK-Java Producer Connection Parameters

Field	Description
Use Proxy?	Select this checkbox if the WebCenter application must use an HTTP proxy when contacting this producer. If selected, enter values for **Proxy Host** and **Proxy Port**. A proxy is required if the WebCenter application and the remote portlet producer are separated by a firewall and an HTTP proxy is needed for communication with the producer.
Proxy Host	Enter the host name for the proxy server. Do not prefix `http://` to the proxy server name.
Proxy Port	Enter the port number on which the proxy server listens. The default port is `80`.
Associated External Application	If one of this producer's portlets requires authentication, select **Associate Producer with an External Application**, and then select the relevant external application from the dropdown list. See also Section 22.2, "Registering External Applications."
Establish Session?	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. Message authentication uses sessions, so if you specify a shared key, you must also select this option. For sessionless communication between the producer and the server, do not select this option.
Default Execution Timeout (Seconds)	Enter a suitable timeout for design time operations. For example, the maximum time the producer may take to register, deregister, or display portlets on WebCenter pages. This defaults to `30` seconds. Individual portlets may define their own timeout period, which takes precedence over the value expressed here.
Subscriber ID	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 (WebCenter application in this instance) passes the value for Subscriber ID to the producer. If the producer does not see the expected value for Subscriber ID, it might reject the registration call.
Shared Key	Enter a shared key to use for producers that are set up to handle encryption. 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. 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.

4. Click **OK**.

   The new producer appears in the connection table.

21.4.2 Registering an Oracle PDK-Java Producer Using WLST

Use the WLST command `registerPDKJavaProducer` to create a connection to a PDK-Java portlet producer and register the producer with your WebCenter application. For command syntax and examples, see 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 1.12.3.1, "Running Oracle WebLogic Scripting Tool (WLST) Commands."

21.5 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/axyz/providers/sample
```

21.6 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 applications, you must also migrate producer customizations and personalizations to the producer's new location. Use the WLST commands `exportProducerMetadata` and `importProducerMetadata` to migrate portlet client metadata to a different location. For more information, see Section 31.2.3, "Exporting Portlet Client Metadata (Custom WebCenter Applications)" and Section 31.2.4, "Importing Portlet Client Metadata (Custom WebCenter Applications)."

> **Note:** If you want to migrate all the metadata for a particular producer (rather than portlet customizations and personalizations only), then use the producer migration tool. For more information, see Section 31.1.3.15, "Exporting Portlet Producers" and Section 31.1.3.16, "Importing Portlet Producers."

This section includes the following subsections:

- Section 21.6.1, "Editing Producer Registration Details Using Fusion Middleware Control"

- Section 21.6.2, "Editing Producer Registration Details Using WLST"
- Section 21.6.3, "Migrating WSRP Producer Metadata to a New WSDL URL"

21.6.1 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 your custom WebCenter application (or WebCenter Spaces):
   - Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"
   - Section 6.2, "Navigating to the Home Page for WebCenter Spaces"
2. Do one of the following:
   - For custom WebCenter applications - From the **Application Deployment** menu, choose **WebCenter** > **Service Configuration**.
   - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings** > **Service Configuration**.
3. From the list of services on the WebCenter Service Configuration page, 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 21–1, " WSRP Producer Connection Parameters"
   - Table 21–4, " Oracle PDK-Java Producer Connection Parameters"
6. Click **OK**.

21.6.2 Editing Producer Registration Details Using WLST

Use the following WLST commands to edit portlet producer connections:

- **WSRP producers** - `setWSRPProducer`
- **PDK-Java producers** - `setPDKJavaProducer`

For command syntax and examples, see the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

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

21.6.3 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. Before importing the producer metadata, you must deregister the existing producer and then reregister the producer with the new URL endpoint. If you do not reregister the producer, "`Portlet Unavailable`" messages display in your WebCenter application.

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. Use Fusion Middleware Control or the WLST command `deregisterWSRPProducer` to remove the existing producer connection, and the producer's metadata, from the WebCenter application. For more information, see Section 21.7, "Deregistering Producers."
4. Use Fusion Middleware Control or the WLST command `registerWSRPProducer` to reregister the WSRP producer with the same name but the new WSDL URL. For more information, see Section 21.2, "Registering WSRP Producers."
5. 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*.

21.7 Deregistering Producers

You can deregister producers at any time but, before doing so, consider any impact to the WebCenter application as portlets associated with 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 30.2, "Viewing Performance Information."

When you deregister a producer, registration data is removed from both the WebCenter application and the remote producer:

- WebCenter 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 application pages. In place of the portlet, WebCenter 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 22.5, "Deleting External Application Connections."

This section includes the following subsections:

- Section 21.7.1, "Deregistering Producers Using Fusion Middleware Control"
- Section 21.7.2, "Deregister Producers Using WLST"

21.7.1 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 your custom WebCenter application (or WebCenter Spaces):
   - Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"
   - Section 6.2, "Navigating to the Home Page for WebCenter Spaces"
2. Do one of the following:
   - For custom WebCenter applications - From the **Application Deployment** menu, choose **WebCenter** > **Service Configuration**.
   - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings** > **Service Configuration**.
3. From the list of services on the WebCenter Service Configuration page, 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 application.

21.7.2 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:

- **Out-of-the-box producers** - `deregisterOOTBProducers`
- **Sample producers** - `deregisterSampleProducers`

For command syntax and examples, see the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

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

21.8 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*.

This section includes the following subsections:

- Section 21.8.1, "Understanding Portlet Producer Application Deployment"
- Section 21.8.2, "Converting a JSR 168 Portlet Producer EAR File into a WSRP EAR File"
- Section 21.8.3, "Deploying Portlet Producer Applications Using Oracle JDeveloper"
- Section 21.8.4, "Deploying Portlet Producer Applications Using Fusion Middleware Control"

- Section 21.8.5, "Deploying Portlet Producer Applications Using Oracle WebLogic Server Administration Console"
- Section 21.8.6, "Deploying Portlet Applications Using WLST"

For more information about deploying applications, see the chapter "Deploying Application" in *Oracle Fusion Middleware Administrator's Guide*.

21.8.1 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 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 1.12, "Oracle WebCenter Administration Tools."

21.8.2 Converting a JSR 168 Portlet Producer EAR File into a WSRP EAR File

To deploy JSR 168 portlets to the WSRP Oracle Portlet Container, the portlet application EAR files must be converted into a WSRP application, which contains the necessary WSDL documents. To convert the JSR 168 portlet producer EAR file into a WSRP EAR file, run the WSRP producer predeployment tool located in the Middleware directory at *`WC_ORACLE_HOME`*`/webcenter/modules/oracle.portlet.server_11.1.1`, as follows:

```
java -jar wsrp-predeploy.jar source EAR  target EAR
```

For JSR 168 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 168 EAR file.
- `target EAR` file is the name of the new EAR file to be created. If the file name for the targeted EAR file is not specified, then a new EAR file called `WSRP-`*`source EAR`* is produced.

In the following example Web proxy is specified:

```
java -Dhttp.proxyHost=myhttpproxy.com -Dhttp.proxyPort=80 -jar wsrp-predeploy.jar
wsrp-samples.ear
```

This example produces `WSRP-wsrp-samples.ear`.

The `wsrp-predeploy.jar` predeployment tool makes all the necessary changes to a JSR 168 portlet to be able to deploy it to the Oracle portlet container and expose it as a WSRP producer. Here are some examples of what the predeployment tool does:

- Creates the `wsdldeploy` directory in the `java.io.tmpdir` folder.
  - On UNIX, the default value of this property is `/tmp` or `/var/tmp`
  - On Microsoft Windows, the default value of this property is `c:\temp`.
- Unpacks the EAR file into `wsdldeploy/EAR`.
- Unpacks the WAR files into `wsdldeploy/[warfilename.war]/`.
- Inserts `WEB-INF/`*`WSDLs`* into the unpacked application.
- Modifies `WEB-INF/web.xml` in the unpackaged WAR files.
- Inserts or modifies `WEB-INF/webservices.xml` in the WAR files.
- Inserts or modifies `WEB-INF/oracle-webservices.xml` in the WAR files.
- Repackages the WARs and builds a new EAR file.

21.8.3 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*.

21.8.4 Deploying Portlet Producer Applications Using Fusion Middleware Control

For information about deploying a portlet producer application using Fusion Middleware Control, see Section 7.1.4.2, "Deploying Applications Using Fusion Middleware Control."

21.8.5 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 7.1.4.4, "Deploying Applications Using the WLS Administration Console."

21.8.6 Deploying Portlet Applications Using WLST

For information on deploying a portlet application using the WLST command, see Section 7.1.4.3, "Deploying Applications Using WLST."

21.9 Troubleshooting Portlet Producer Issues

This section includes the following sub sections:

- Section 21.9.1, "Producer Registration Fails for a Custom WebCenter Application"
- Section 21.9.2, "Portlet Unavailable: WSM-00101 Exception"

21.9.1 Producer Registration Fails for a Custom WebCenter Application

This section describes producer registration and portlet unavailability issues.

Problem

You are unable to register a WSRP producer.

Solution

Ensure the following:

- Back-end producer is up and running. To test the producer, access the WSDL URL of the producer through a browser window. See, Section 21.3, "Testing WSRP Producer Connections."
- Producer application is packaged accurately. If not, then register the producer at design time (in JDeveloper), as described in the section "Registering Portlet Producers with a WebCenter Application" in the chapter "Consuming Portlets" in *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*, and redeploy the application, as described in Section 7.1, "Deploying Custom WebCenter Applications." After redeployment, verify that the packaged application includes the MBean, `ProducerManager`:

  1. In Fusion Middleware Control, from the **Application Deployment** menu, select **System MBean Browser**.
  2. In the Navigator, expand **Application Defined MBeans** > **oracle.webcenter.portlet** > **Application**: *application_name* > **Producer Manager > Producer Manager**.

- `PortletServletContextListener` is added to the `web.xml` file.

  For applications that support post deployment registration of producers, the producer must be registered at least once at design time. This adds `PortletServletContextListener` to the `web.xml` file, which registers the appropriate runtime MBeans to enable post deployment registration of producers. For example, see the text in **bold** in the following `web.xml` snippet:

  ```
  <listener>
     <description>
        WebCenter Portlet Context Listener
     </description>
     <display-name>
        WebCenterPortletContextListener
     </display-name>
     <listener-class>
        oracle.webcenter.portlet.listener.PortletServletContextListener
     </listener-class>
  </listener>
  ```

21.9.2 Portlet Unavailable: WSM-00101 Exception

Setting up the **User Name with Password** token profile in a WSRP portlet producer throws the exception `WSM-00101`.

Problem

If you configure the **User Name with Password Token** profile for a WSRP producer through Fusion Middleware Control (or WLST) while portlets associated with this producer are in use, the portlets display the following exception in the WebCenter application:

```
oracle.wsm.common.sdk.WSMException: WSM-00101:
The specified Keystore file
/keys/user_projects/domains/pv_0309/config/fmwconfig/default-keystore.jks
cannot be found; it either does not exist or its path is not included in the
application classpath.
```

Solution

Ensure that you have configured the default keystore in your portlet producer. For information, see Section 29.1.3, "Setting Up the Keystores."

22

Managing External Applications

An external application is any application that implements its own authentication process. Specifically, it is an application that does not take part in your WebCenter application's single sign-on process.

You can use Fusion Middleware Control or the WLST command-line tool to register and manage external applications for WebCenter application deployments. All external application changes that you make for WebCenter applications, post deployment, are stored in the MDS repository as customizations.

> **Note:** External application configuration through Fusion Middleware Control or WLST is dynamic. Configuration changes are immediately reflected in the WebCenter application; it is not necessary to restart the application or the managed server.

This chapter includes the following sections:

- Section 22.1, "What You Should Know About External Applications"
- Section 22.2, "Registering External Applications"
- Section 22.3, "Modifying External Application Connection Details"
- Section 22.4, "Testing External Application Connections"
- Section 22.5, "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."

22.1 What You Should Know About External Applications

If your WebCenter application interacts with an application that handles its own authentication, you can associate that application with an external application definition to allow for credential provisioning. In doing so, you use an external application definition to provide a means of accessing content from these independently authenticated applications.

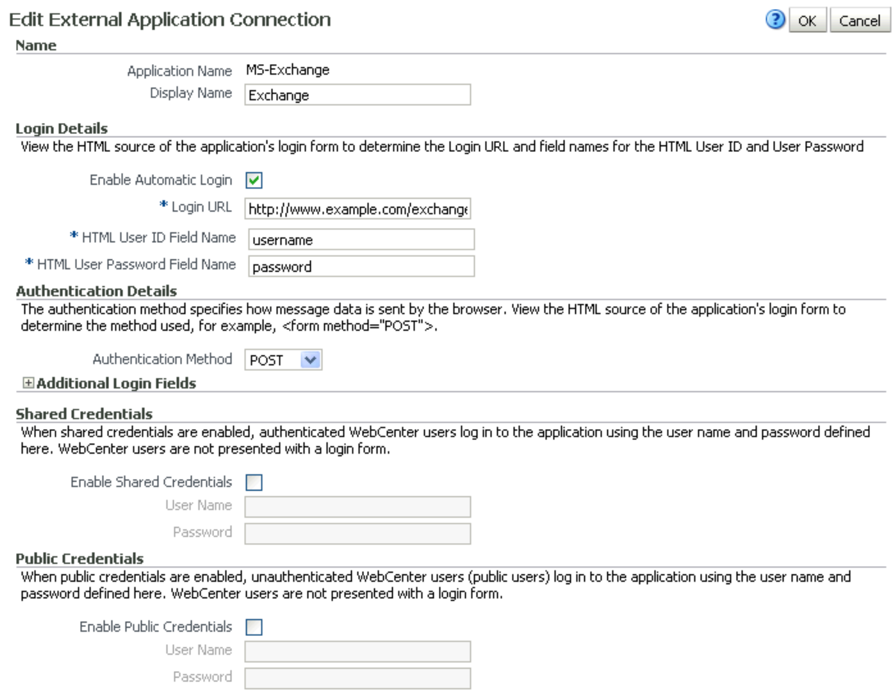
To replicate a single sign-on experience from the end user's perspective, the external application service captures the user name and password, and any other credentials for the external application, and supplies it to the WebCenter service or application requiring the credentials. The WebCenter service or other application then uses this information to log in on behalf of the end user. This username and password combination is securely stored in a credential store configured for the WebLogic domain where the application is deployed.

The user provides login credentials when prompted, and these credentials are mapped to the WebCenter application user and stored in the credential store configured for the domain. The credential store subsequently supplies that information during authentication to the external application. Unless the external application's credentials change, the user supplies the credentials only once as the mapped information is read from the credential store for future requests.

> **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 custom WebCenter application can be specified before deployment through a wizard in Oracle JDeveloper, or after deployment through Fusion Middleware Control Console (Figure 22–1) 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 24, "Configuring the Identity Store," and Chapter 25, "Configuring the Policy and Credential Store."

Figure 22–1 Edit External Application



Edit External Application Connection

Name

Application Name MS-Exchange

Display Name Exchange

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 http://www.example.com/exchange

* HTML User ID Field Name username

* HTML User Password Field Name password

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 POST

⊞**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

22.2 Registering External Applications

You can register external applications for WebCenter applications through Fusion Middleware Control or using WLST commands.

Before registering an external application, access the application's login page and examine the HTML source for the application's login form. All the registration details you require are located in the `<form tag>`.

For example, the underlying code for the *Yahoo! Mail* login form looks something like this:

```
<form method=post action="https://login.yahoo.com/config/login?"
autocomplete="off" name="login_form">
...
<td><input name="login" size="17"</td>
...
<td><input name="passwd" size="17"</td>
...
```

In this example, to provide WebCenter users with a direct link to the *Yahoo! Mail* application, the following sample registration information is required:

Registration Information	Sample Value	HTML Source
Login URL	`https://login.yahoo.com/config/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 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*.

This section includes the steps for:

- Section 22.2.1, "Registering External Applications Using Fusion Middleware Control"
- Section 22.2.2, "Registering External Applications Using WLST"

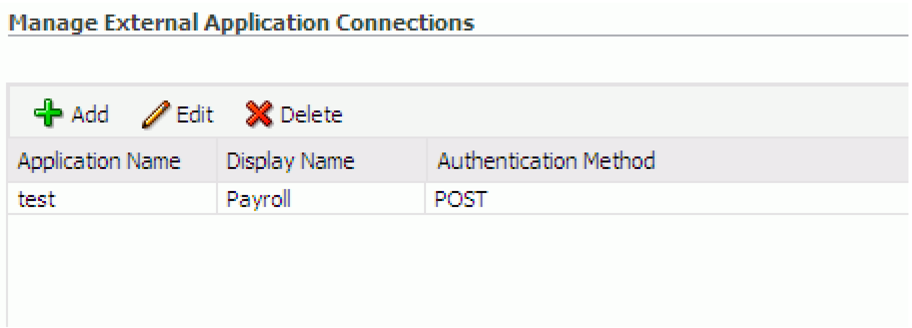
22.2.1 Registering External Applications Using Fusion Middleware Control

To register an external application:

1. Login to Fusion Middleware Control and navigate to the home page for your WebCenter application (or WebCenter Spaces):
   - Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications".
   - Section 6.2, "Navigating to the Home Page for WebCenter Spaces"

2. Do one of the following:
   - For custom WebCenter applications: from the **Application Deployment** menu, choose **WebCenter** > **Service Configuration**.
   - For WebCenter Spaces: from the **WebCenter** menu, choose **Settings** > **Service Configuration**.
3. From the list of services on the WebCenter Service Configuration page, choose **External Applications**.
4. To register a new external application, click **Add** (Figure 22–2).

Figure 22–2 Configuring External Application Connections



Manage External Application Connections

Application Name	Display Name	Authentication Method
test	Payroll	POST

5. Enter a unique name for the external application and a display name that WebCenter users working with this external application will see.

   See also, Table 22–1.

Table 22–1 External Application Connection - Name

Field	Description
Application Name	Enter a name for the application. The name must be unique (across all connection types) within the WebCenter application. For example: `yahoo` **Note:** Once registered, you cannot edit the Application Name.
Display Name	Enter a user friendly name for the application that WebCenter users will recognize. WebCenter end-users working with this external application will see the display name you specify here. For example: `My Yahoo` If you leave this field blank, the Application Name is used.

6. Enter login details for the external application.

   For details, see Table 22–2.

Table 22–2 External Application Connection - Login Details

Field	Description
Enable Automatic Login	Select to allow automatically log users in to this application. Choosing this option requires you to complete the `Login URL`, `HTML User ID Field Name`, and `HTML User Password Field Name` fields 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. **Note:** Automated login is not supported for: ■ 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 `j_security_check` for authentication. ■ External sites that do not support UTF8 encoding.
Login URL	Enter the login URL for the external application. To determine the URL, navigate to the application's login page and record the URL. For example: `http://login.yahoo.com/config/login` **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. When omitted, the external application is not available for display in the WebCenter Spaces Application pane. See Section 36.2, "Making an Application Available to WebCenter Users."
HTML User ID Field Name	Enter the name that identifies the "user name" or "user ID" field on the login form. **Tip:** To find this name, look at the HTML source for the login page. This property does not specify user credentials. **Note:** You must complete this field if the Authentication Method is GET or POST. Leave this field blank if the application uses basic authentication (see **Authentication Method**).
HTML User Password Field Name	Enter the name that identifies the "password" field on the login form. **Tip:** To find this name, look at the HTML source for the login page. **Note:** You must complete this field if the Authentication Method is GET or POST. Leave this field blank if the application uses basic authentication (see **Authentication Method**).

7. Select the authentication method used by the external application.

   For details, see Table 22–3.

Table 22–3 External Application Connection - Authentication Details

Field	Description
Authentication Method	Select the form submission method used by the external application. Choose from one of the following: ■ **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. 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, `<form method="POST" action="https://login.yahoo.com/config/login?" AutoComplete="off">`

8. Specify additional login fields and details, if required.

   For details, see Table 22–4, " External Application Connection - Additional Login Fields".

Table 22–4 External Application Connection - Additional Login Fields

Field	Description
Additional Login Fields	If your application requires additional login criteria, expand **Additional Login Fields**. For example, in addition to *user name* and *password*, the Lotus Notes application requires two additional fields - *Host* and *MailFilename*. Click **Add** to specify an additional field for the login form. For each new field, do the following: ■ **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. Click **Delete** to remove a login field.

9. Specify shared and public user credentials, if required.

   For details, see Table 22–5.

Table 22–5 External Application Connection - Shared User and Public User Credentials

Field	Description
Enable Shared Credentials	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. When shared credentials are specified, every user accessing this external application, through the WebCenter application, is authenticated using the user name and password defined here. WebCenter users are not presented with a login form. Because WebCenter users do not need to define personal credentials of their own, external applications with shared credentials are not listed in the external application's change password task flows such as *My Accounts* (see also *User's Guide -Managing Your Application Login Credentials*).
Enable Public Credentials	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. When public credentials are specified, public users accessing this external application through the WebCenter application's public pages are logged in using the username and password defined here. If public credentials are not specified, public users will see an authorization error indicating this external application is not accessible to public users.

10. Click **OK** to register the application.

In WebCenter Spaces, registered applications for automated login are not available to WebCenter users immediately. The WebCenter Spaces administrator decides which registered applications to expose through the Applications pane, see Section 36.2, "Making an Application Available to WebCenter Users."

22.2.2 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 1.12.3.1, "Running Oracle WebLogic Scripting Tool (WLST) Commands."

22.3 Modifying External Application Connection Details

This section shows you how to modify the external application connection details by:

- Section 22.3.1, "Modifying External Application Connection Using Fusion Middleware Control"

- Section 22.3.2, "Modifying External Application Connection Using WLST"

22.3.1 Modifying External Application Connection Using Fusion Middleware Control

To update external application connection details:

1. Log in to Fusion Middleware Control and navigate to the home page for your custom WebCenter application (or WebCenter Spaces):
   - Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications".
   - Section 6.2, "Navigating to the Home Page for WebCenter Spaces"
2. Do one of the following:
   - For custom WebCenter applications - from the **Application Deployment** menu, choose **WebCenter** > **Service Configuration**.
   - For WebCenter Spaces - from the **WebCenter** menu, choose **Settings** > **Service Configuration**.
3. From the list of services on the WebCenter Service Configuration page, choose **External Applications**.
4. Select the name of the external application you want to modify, and click **Edit**.
5. Edit connection details, as required. For detailed parameter information, see Table 22–2.

   Note that you cannot edit the name of the external application.
6. Click **OK** to save your changes.

22.3.2 Modifying External Application Connection Using WLST

Use the WLST command `setExtAppConnection` to edit existing external application connection details. For command syntax and examples, see `setExtAppConnection` in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

> **Note:** To edit details relating to an additional login field, use `setExtAppField`. To edit existing shared or public credentials, use `setExtAppCredential`.
>
> To delete an additional login field, use `removeExtAppField`. To delete shared or public credentials, use `removeExtAppCredential`.

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

22.4 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*.

22.5 Deleting External Application Connections

Take care when deleting an external application connection as WebCenter application users will no longer have access to that application, and any services dependent on the external application may not function correctly.

In WebCenter Spaces, links to external applications are not automatically removed from the Applications pane when an external application is deleted. To prevent unsuccessful access attempts, administrators are advised to remove links to unavailable applications. For details, see Section 36.6, "Removing Links from the Applications Pane."

This section includes the following subsections:

- Section 22.5.1, "Deleting External Application Connections Using Fusion Middleware Control"
- Section 22.5.2, "Deleting External Application Connections Using WLST"

22.5.1 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 WebCenter application (or WebCenter Spaces):
   - Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications".
   - Section 6.2, "Navigating to the Home Page for WebCenter Spaces"
2. Do one of the following:
   - For WebCenter applications - from the **Application Deployment** menu, choose **WebCenter** > **Service Configuration**.
   - For WebCenter Spaces - from the **WebCenter** menu, choose **Settings** > **Service Configuration**.
3. From the list of services on the WebCenter Service Configuration page, choose **External Applications**.
4. Select the name of the external application you want to remove, and click **Delete**.

22.5.2 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 1.12.3.1, "Running Oracle WebLogic Scripting Tool (WLST) Commands."

Part V

Advanced Systems Administration for Oracle WebCenter

Part V contains the following chapters:

23

Managing Security

This chapter provides an introduction to securing custom WebCenter applications, and describes the security configuration that is in place when custom WebCenter applications and WebCenter Spaces 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 23.1, "Introduction to WebCenter Application Security"
- Section 23.2, "Default Security Configuration"
- Section 23.3, "Troubleshooting Security Configuration Issues"

Audience

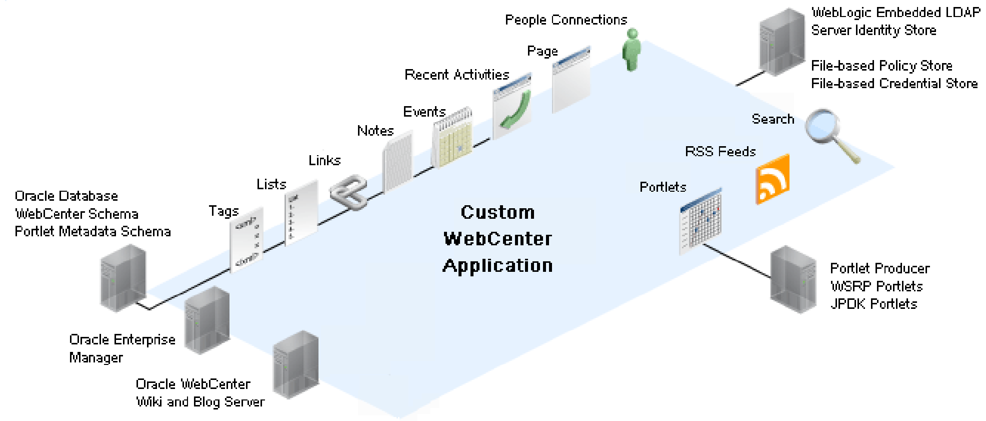
The content of this chapter is intended for Fusion Middleware administrators (users granted the `Admin` role through the Oracle WebLogic Server Administration Console). Users with the `Monitor` or `Operator` roles can view security information but cannot make changes. See also, Section 1.8, "Understanding Administrative Operations, Roles, and Tools."

23.1 Introduction to WebCenter Application Security

The recommended security model for Oracle WebCenter is based on Oracle ADF Security, which implements the Java Authentication and Authorization Service (JAAS) model. For more information about Oracle ADF Security, see the *Oracle Fusion Middleware Fusion Developer's Guide for Oracle Application Development Framework*.

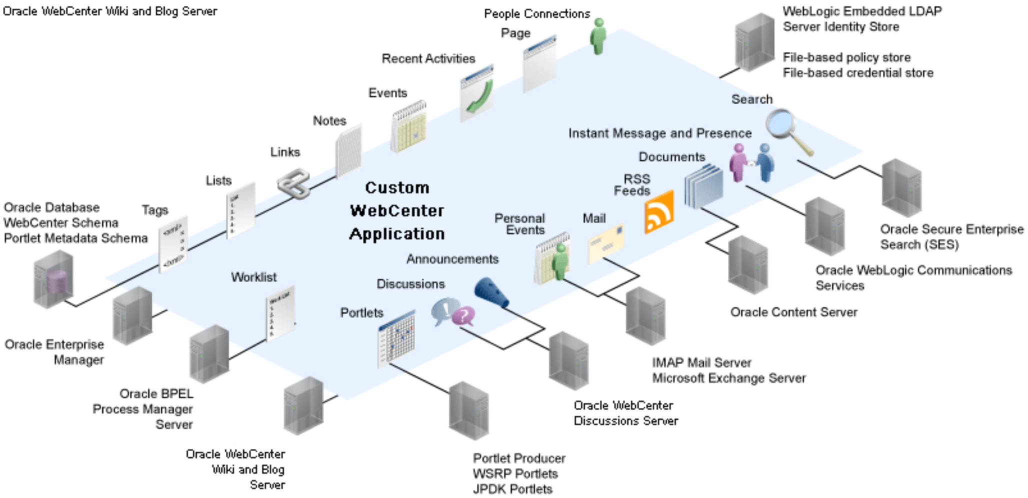
Figure 23–1 shows the relationship between a WebCenter application deployment and its services, servers, portlets, portlet producers, its identity, credential and policy stores, and Oracle Enterprise Manager.

Figure 23–1 Basic WebCenter Application Architecture



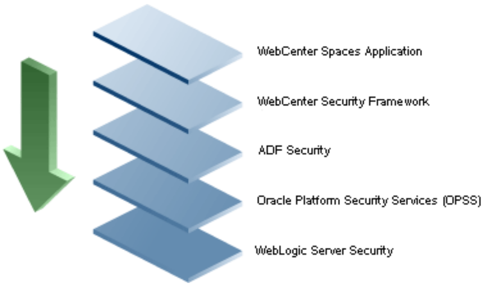
The diagram in Figure 23–2 shows a basic WebCenter application after deployment with its back-end server connections.

Figure 23–2 WebCenter Application Architecture with Back-end Server Connections


Oracle WebCenter Wiki and Blog Server
People Connections
Page
Recent Activities
Events
Notes
Links
Lists
Tags
WebLogic Embedded LDAP Server Identity Store
File-based policy store
File-based credential store
Search
Instant Message and Presence
Documents
RSS Feeds
Mail
Personal Events
Custom WebCenter Application
Oracle Database
WebCenter Schema
Portlet Metadata Schema
Announcements
Discussions
Worklist
Portlets
Oracle Secure Enterprise Search (SES)
Oracle WebLogic Communications Services
Oracle Content Server
Oracle Enterprise Manager
Oracle BPEL Process Manager Server
IMAP Mail Server
Microsoft Exchange Server
Oracle WebCenter Discussions Server
Oracle WebCenter Wiki and Blog Server
Portlet Producer
WSRP Portlets
JPDK Portlets

The diagram in Figure 23–3 shows the security layers for the WebCenter Spaces application.

Figure 23–3 WebCenter Spaces Security Layers


WebCenter Spaces Application
WebCenter Security Framework
ADF Security
Oracle Platform Security Services (OPSS)
WebLogic Server Security

The security layers for a custom WebCenter application could have the same four bottom layers (WebCenter Security Framework, ADF Security, OPSS, and WebLogic Server Security) depending on how the application was structured. The application layer will, of course, depend on the implementation.

WebCenter Spaces Application Security

WebCenter Spaces provides support for:

- Application role management and privilege mapping
- Self-registration
- Group space security management
- Account management
- External application credential management

WebCenter Security Framework

WebCenter Security Framework provides support for:

- Service Security Extension Framework
- Permission-based authorization
- Role-mapping based authorization
- External applications and credential mapping

ADF Security

ADF Security provides support for:

- Page authorization
- Task flow authorization
- Secure connection management
- Credential mapping APIs
- Logout invocation, including logout from SSO-enabled configurations with Oracle Access Manager and Oracle SSO
- Secured login URL for ADF Security-based applications (the adfAuthentication servlet)

Oracle Platform Security Services (OPSS)

OPSS provides support for:

- Anonymous-role support
- Authenticated-role support
- Identity store, policy store, and credential store
- Identity Management Services
- Oracle Web Service Manager Security

WebLogic Server Security

WebLogic Server Security provides support for:

- WebLogic authenticators
- Identity asserters

- J2EE container security
- SSL

23.2 Default Security Configuration

This section describes the security configuration that is in place when custom WebCenter applications and WebCenter Spaces are deployed, and the tasks that must be carried out after deployment:

- Section 23.2.1, "Administrator Accounts"
- Section 23.2.2, "Application Roles and Enterprise Roles in WebCenter Spaces"
- Section 23.2.3, "Default Identity and Policy Stores"
- Section 23.2.4, "Default Policy Store Permissions and Grants"
- Section 23.2.5, "Post-deployment Security Configuration Tasks"

23.2.1 Administrator Accounts

Custom WebCenter 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 WebCenter Spaces 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 WebCenter 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 24.6, "Granting the WebCenter Spaces Administrator Role to a WebCenter Spaces User."

23.2.2 Application Roles and Enterprise Roles in WebCenter Spaces

Application roles and permissions are defined within WebCenter Spaces and are stored in an application-specific stripe of the policy store. Consequently, WebCenter Spaces roles apply only to WebCenter Spaces; WebCenter Spaces roles and permissions do not extend to other applications.

Application roles differ from roles that appear in the identity store portion of the embedded LDAP server or in roles defined by the enterprise LDAP provider. Application roles are specific to an application and defined in the application policy store.

Enterprise roles, which are stored in the enterprise identity store, apply at the enterprise level. That is, the roles and permissions that you or a system administrator define within the enterprise identity store do not imply permissions within WebCenter Spaces.

Within WebCenter Spaces you can 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.

23.2.3 Default Identity and Policy Stores

By default, WebCenter applications are configured to use a file-based embedded LDAP identity store to store application-level user IDs, and a file-based LDAP policy store to store policy grants.

Although secure, the embedded LDAP identity store is not a "production-class" store and should be replaced with an external LDAP-based identity store such as Oracle Internet Directory for enterprise production environments.

The default file-based policy store can only be used for single-node WebCenter Spaces configurations. For multi-node configurations, you must reassociate the policy and credential store with an external LDAP-based store (such as Oracle Internet Directory) as described in Chapter 25, "Configuring the Policy and Credential Store."

The policy store can only be configured to use Oracle Internet Directory 11gR1 and 10.1.4.3, and OVD 11gR1 with the Local Store Adapter (LSA).

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 be configured to use the following LDAP servers:

- Oracle Internet Directory (OID) 11gR1 and 10.1.4.3
- Oracle Virtual Directory (OVD) 11gR1 and 10.1.4
- Sun iPlanet version 4.1.3
- Active Directory shipped as part of Windows 2000
- Open LDAP version 2.0.7
- Novell NDS version 8.5.1

For more information on reconfiguring the identity, policy and credential stores, see Chapter 24, "Configuring the Identity Store" and Chapter 25, "Configuring the Policy and Credential Store."

> **Note:** Oracle WebCenter Discussions requires an external LDAP-based identity store. Consequently, if you want to use the Discussions service (which relies on Oracle WebCenter Discussions) you must reassociate the identity store with one of the external LDAP servers listed above.
>
> For WebCenter Spaces, both WebCenter Spaces and Oracle Content Server must share the same LDAP server. For more information, see Section 24.7, "Configuring the Oracle Content Server to Share the WebCenter Spaces Identity Store LDAP Server."

23.2.3.1 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.

23.2.4 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 23.2.4.1, "Permission-based Authorization"
- Section 23.2.4.2, "Role-mapping Based Authorization"
- Section 23.2.4.3, "Default Policy Store Permissions for WebCenter Spaces"
- Section 23.2.4.4, "Default Code-based Grants"

23.2.4.1 Permission-based Authorization

Permission-based authorization is used for services, such as Lists, where access control is implemented within the WebCenter application using Oracle Platform Security Services (OPSS). WebCenter Spaces provides extensive user and role management tools with which you can create application roles, and define what permissions should be granted to those roles. For information on managing users and roles in WebCenter Spaces, see Section 34.3, "Managing Application Roles and Permissions."

23.2.4.2 Role-mapping Based Authorization

Services that need to access "remote" (back-end) resources require role-mapping based authorization. For example, for the Discussions service, role mapping is required when the users of a WebCenter application (mapping to one or more group space roles) must be mapped to another set of roles on the Oracle WebCenter Discussions Server.

In WebCenter Spaces:

- Default application and group space roles for WebCenter Spaces are mapped to the corresponding service roles. For default mappings, see Table 34–4 and Table 34–5.
- When a new user is granted an application or group space role, a similar grant (privilege) is granted in the back-end server. For example, when user Pat is granted `Discussions-Manage` permissions in WebCenter Spaces, Pat is granted corresponding permissions in the back-end discussion server. See also, Section 34.1.4, "Understanding Discussions Server Role and Permission Mapping."

23.2.4.3 Default Policy Store Permissions for WebCenter Spaces

The tables in this section describe out-of-the-box permissions and roles for WebCenter Spaces:

- Table 23–1 shows the default permissions for pre-seeded application roles in the WebCenter Spaces policy store. Application roles determine what users can do in their *personal space*.
- Table 23–2 shows the default permissions for group space roles that come pre-seeded with out-of-the-box group space templates: Community of Interest (COI), Group Project, Blank. When a new group space is created, these group space roles and their corresponding permissions are added to the policy store at runtime.

Table 23–1 Default Application Roles and Permissions in WebCenter Spaces

	Default Application Roles		
Permissions	**Administrator**	**Spaces-User**	**Public-User**
Application			
Manage	✔		
Configure	✙		
View	✙	✔	✔
Group Spaces			
Manage	✔		
Configure	✙		
View	✙		
Create	✙	✔	
Group Space Templates			
Manage	✔		
View	✙		
Create	✙	✔	
Pages			
Manage	✔		
Delete	✙		
Edit	✙		
Personalize	✙		
View	✙		
Create	✙	✔	
Discussions			
Manage	✔		
Links			
Manage	✔		
Delete	✙		
Create	✙		
People Connections			
Manage	✔		
Edit	✙	✔	
Share	✙	✔	

Table 23–2 Default Group Space Roles and Permissions in WebCenter Spaces

Default Roles	Moderator			Participant			Viewer			Spaces-User	Public-User
Template	**COI**	**Project**	**Blank**	**COI**	**Project**	**Blank**	**COI**	**Project**	**Blank**		
Group Space Access											
Manage	✔	✔	✔								
Configure	✚	✚	✚								
View	✚	✚	✚	✔	✔	✔	✔	✔	✔		
Group Space Services (Pages, Events, Links, Lists, Notes)											
Manage	✔	✔	✔								
Design	✔	✔	✔		✔	✔					
Contribute	✔	✔	✔	✔	✔	✔					
View	✔	✔	✔	✔	✔	✔	✔	✔	✔		
Announcements											
Manage	✔	✔								n/a	
Edit	✚	✚		✔	✔					n/a	
View	✚	✚		✔	✔		✔	✔		n/a	
Discussions											
Manage	✔	✔								n/a	
Edit	✚	✚		✔	✔					n/a	
View	✚	✚		✔	✔		✔	✔		n/a	
Documents											
Manage	✔	✔								n/a	
Delete	✔	✔		✔	✔					n/a	
View	✔	✔		✔	✔		✔	✔		n/a	
Create	✔	✔		✔	✔					n/a	

Legend	Description
✔	Shows an explicitly granted permission or action.
✚	Shows an implied permission because of an explicitly granted permission. The permission implementation itself does the implication.

23.2.4.4 Default Code-based Grants

WebCenter applications make internal calls to APIs on the security platform that are secured with permission checks. To facilitate this, the WebCenter 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`), and CRUD on application roles. In the case of WebCenter Spaces, CRUD permission are granted by default, out of the box.

Similarly, WebCenter applications must pre-authorize access to various operations that it wants to expose using the WebCenter permissions (described in Table 23–1 and Table 23–2), and then invoke the OPSS APIs as privileged actions.

23.2.5 Post-deployment Security Configuration Tasks

After deploying your custom WebCenter application or WebCenter Spaces, consider the following security-related configuration tasks for your site:

- **Reassociating the identity store to use an external LDAP**

  By default, WebCenter applications use an embedded LDAP for its identity store. Although secure, the out-of-the-box embedded LDAP may not scale appropriately for large enterprise production environments. For instructions on how to configure the identity store to use an external LDAP such as Oracle Internet Directory (OID), see Chapter 24, "Configuring the Identity Store."

  > **Note:** Oracle Content Server and Oracle WebCenter Discussions rely on external LDAP-based identity stores. Consequently, if you want to use the Documents service (which relies on Oracle Content Server) or the Discussions service (which relies on Oracle WebCenter Discussions) you must reassociate the identity store to use an external LDAP server. For more information on reconfiguring the identity store, see Chapter 24, "Configuring the Identity Store."

- **Reassociating the policy store to use an external LDAP**

  By default, custom WebCenter applications use a file-based `system-jazn-data.xml` policy store to store policy grants. You should consider using an LDAP-based policy store. For information on how to configure the policy store to use an LDAP server, see Chapter 25, "Configuring the Policy and Credential Store."

- **Configuring WS-Security**

  Although the use of WS-Security adds complexity to the configuration and management of a WebCenter application and the set of producers it consumes, it helps ensure the security of the information being published by the WebCenter application. Adding WS-Security provides authentication for the consumer, and message-level security.

  For information on how to configure WS-Security for WebCenter applications and components, see Chapter 28, "Configuring WS-Security for WebCenter Applications and Components."

- **Configuring SSO**

  Single Sign-On (SSO) allows users to log in once across WebCenter applications and components rather than having to log in for each sub-application (for example, for accessing a wiki page in WebCenter Spaces). Users do not have to maintain a separate user ID and password for each application or component that they access. However, you can still configure a variety of authentication methods, so that more sensitive applications can be protected using more stringent methods. WebCenter supports four single sign-on solutions: Oracle Access Manager (OAM), Oracle Single Sign-on (OSSO), a SAML-based single sign-on solution for Oracle WebCenter applications only, and an SSO solution for Microsoft clients, using Windows authentication based on the Simple and Protected Negotiate (SPNEGO) mechanism and the Kerberos protocol. For a discussion of these solutions and an overview of single sign-on, see Chapter 26, "Configuring WebCenter Applications and Components to Use SSO."

- **Configuring SSL**

Secure Sockets Layer (SSL) provides additional security for connections between WebCenter applications or components by providing an additional authentication layer, and by encrypting the data exchanged. For connections between applications or components where the data 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 27, "Securing WebCenter Applications and Components with 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.

23.3 Troubleshooting Security Configuration Issues

This section includes the following sub-sections:

- Section 23.3.1, "Webcenter Spaces Does Not Find Users in LDAP Provider"
- Section 23.3.2, "Group Space Gets Created with Errors When Logged in as OID User"
- Section 23.3.3, "Users Cannot Self-Register when WebCenter Spaces Configured with Active Directory"
- Section 23.3.4, "User Made Administrator Does Not Have Administrator Privileges"
- Section 23.3.5, "OmniPortlet Producer Authorization Exception in SSO Environment"

23.3.1 Webcenter Spaces 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 WebCenter Spaces, but when you try to assign the administrator role, in WebCenter 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 24, "Configuring the Identity Store." Restart the Administration Server and Managed Servers for the domain.

23.3.2 Group Space Gets Created with Errors When Logged in as OID User

Problem

When logged in to WebCenter as an OID user (for example, `orcladmin`), and you try to create a group space, the group 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 `<MIDDLEWARE_HOME>/user_projects/domains/WebCenter/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 `WLS_Spaces` server.

23.3.3 Users Cannot Self-Register when WebCenter Spaces Configured with Active Directory

Problem

Users cannot self-register with Active Directory after configuring WebCenter 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.

23.3.4 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`.

23.3.5 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 is configured with SSO.

Solution

Grant the required permissions to `ssofilter.jar` by connecting to the Oracle WebCenter Administration Server using WLST (for more information, see Section 1.12.3.1, "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="*")
```

24

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 Content Server and contains the following subsections:

- Section 24.1, "Reassociating the Identity Store with an External LDAP"
- Section 24.2, "Tuning the Identity Store for Performance"
- Section 24.3, "Adding Users to the Embedded LDAP Identity Store"
- Section 24.4, "Managing Users and Roles"
- Section 24.5, "Moving the Administrator Account to an External LDAP Server"
- Section 24.6, "Granting the WebCenter Spaces Administrator Role to a WebCenter Spaces User"
- Section 24.7, "Configuring the Oracle Content Server to Share the WebCenter Spaces Identity Store LDAP Server"

Caution: Before reassociating the identity store, be sure to back up the relevant configuration files:

- `config.xml`
- `jps-config.xml`
- `system-jazn-data.xml`

As a precaution, you should also back up the `boot.properties` file for the Administration Server for the domain.

Note that for custom WebCenter applications, the steps for Granting the WebCenter Spaces Administrator Role to a WebCenter Spaces User and Migrating the WebCenter Discussions Server to Use an External LDAP are not required. For more information about the identity store, see the *Oracle Fusion Middleware 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."

24.1 Reassociating the Identity Store with an External LDAP

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 23.2, "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).

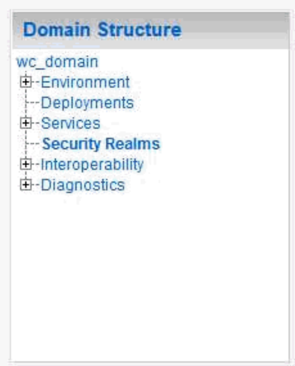
To reassociate the identity store with OID:

1. Log in to the WebLogic Server Administration Console.

   For information on logging into the WebLogic Server Administration Console, see Section 1.12.2, "Oracle WebLogic Server Administration Console."

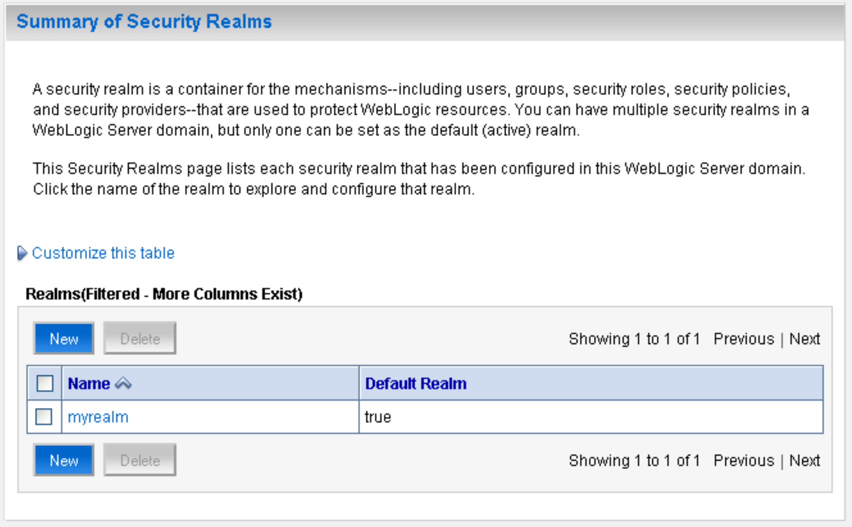
2. In the Domain Structure pane (see Figure 24–1), click **Security Realms**.

Figure 24–1 Domain Structure Pane



The Summary of Security Realms pane displays (see Figure 24–10).

Figure 24–2 Summary of Security Realms pane



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.

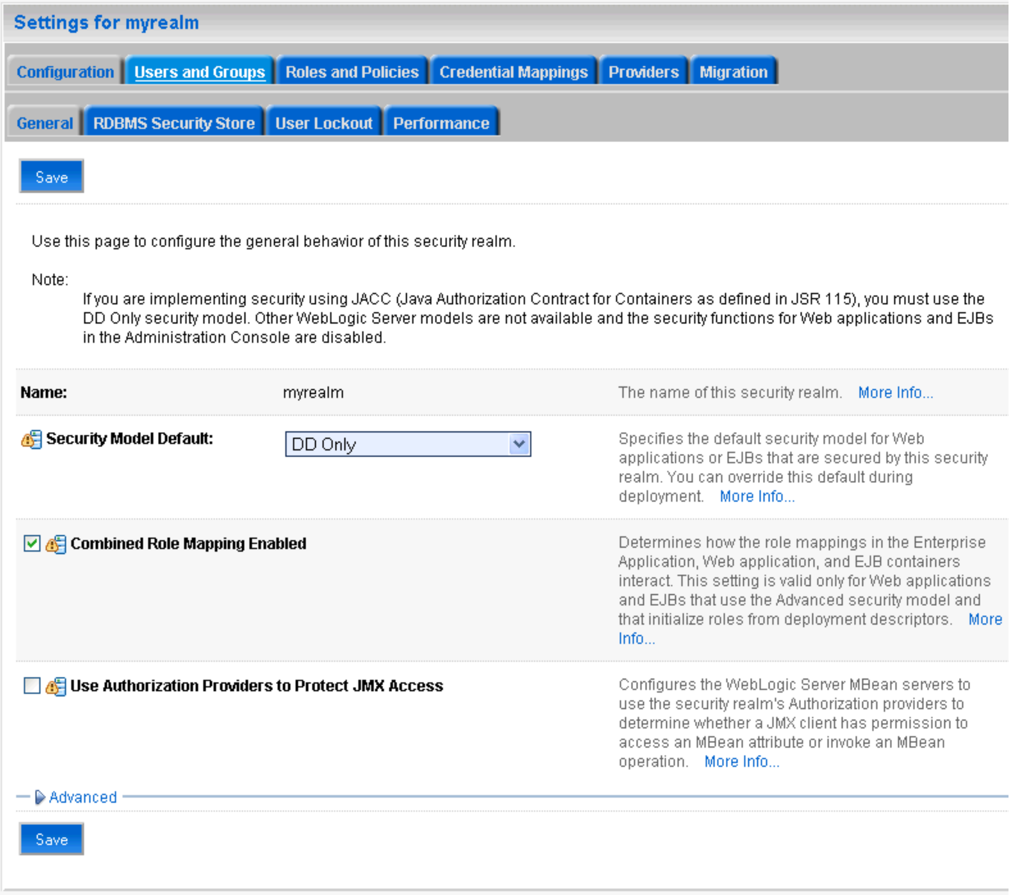
Realms(Filtered - More Columns Exist)

□	Name	Default Realm
□	myrealm	true

3. In the Name column, click the realm for which you want to reassociate the identity store.

The Realm Settings pane displays (see Figure 24–3).

Figure 24–3 Realm Settings Pane



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...

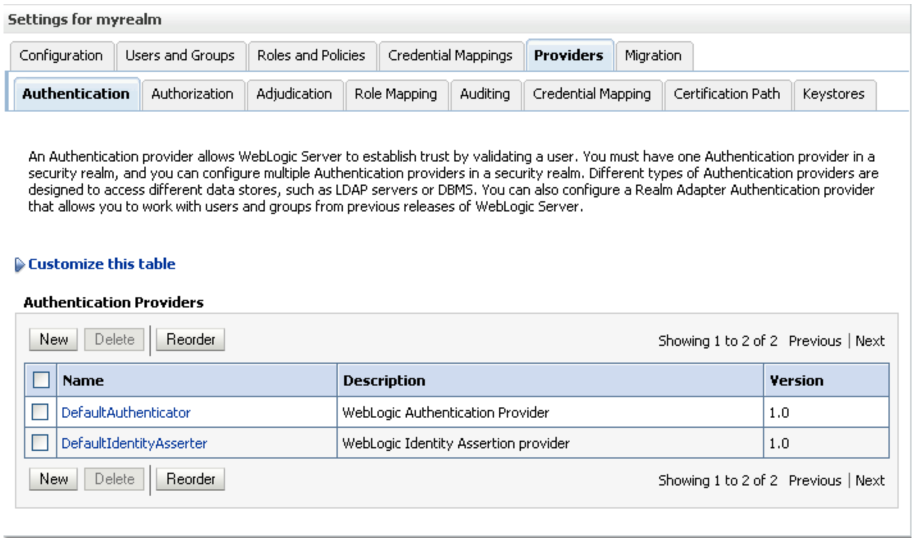
☐ **Use Authorization Providers to Protect JMX Access**

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...

4. Open the **Providers** tab.

   The Providers Settings pane displays (see Figure 24–4).

Figure 24–4 Settings Pane - Providers



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.

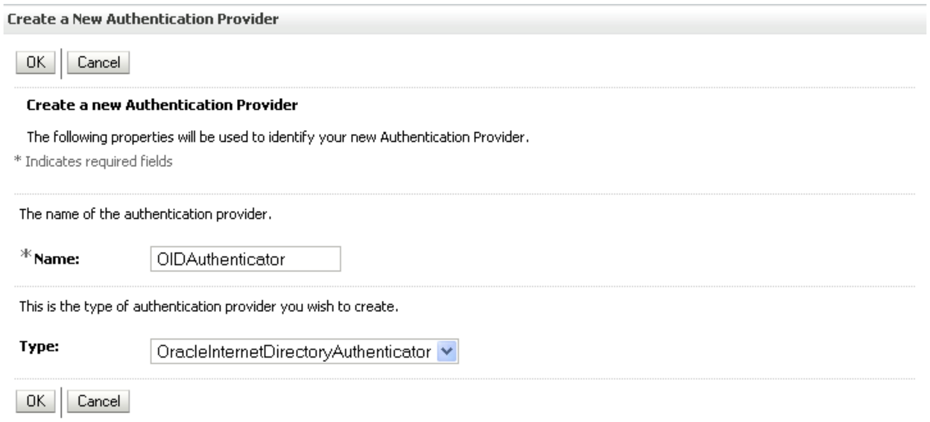
Authentication Providers

□	Name	Description	Version
□	DefaultAuthenticator	WebLogic Authentication Provider	1.0
□	DefaultIdentityAsserter	WebLogic Identity Assertion provider	1.0

5. Click **New** to add a new provider.

   The Create a New Authentication Provider pane displays (see Figure 24–5).

Figure 24–5 Create a New Authentication Provider Pane



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:** OIDAuthenticator

This is the type of authentication provider you wish to create.

Type: OracleInternetDirectoryAuthenticator

6. Enter a name for the provider (for example `OIDAuthenticator` for a provider that authenticates the user for the Oracle Internet Directory).

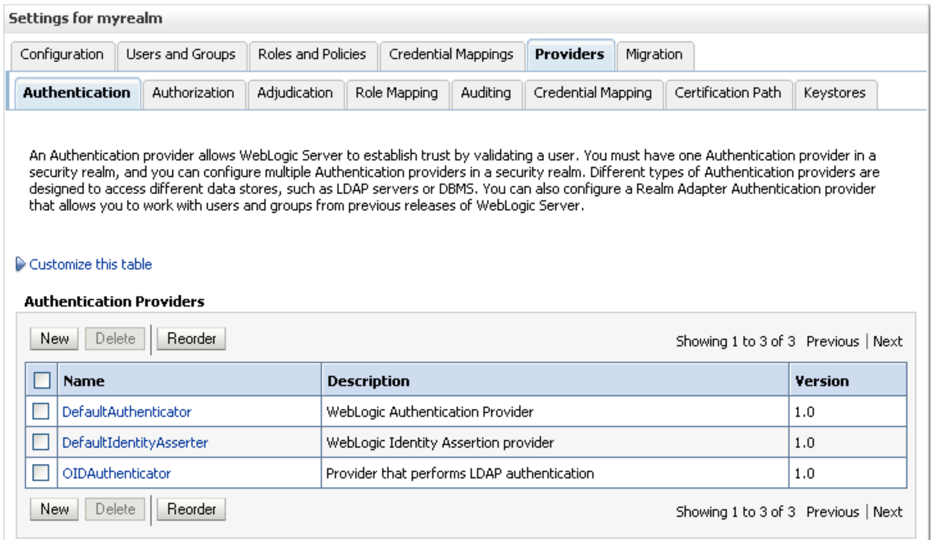
7. Select the authenticator appropriate for your LDAP directory from the list of authenticators.

   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 24–6).

Figure 24–6 Settings Pane - Authentication Providers



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.

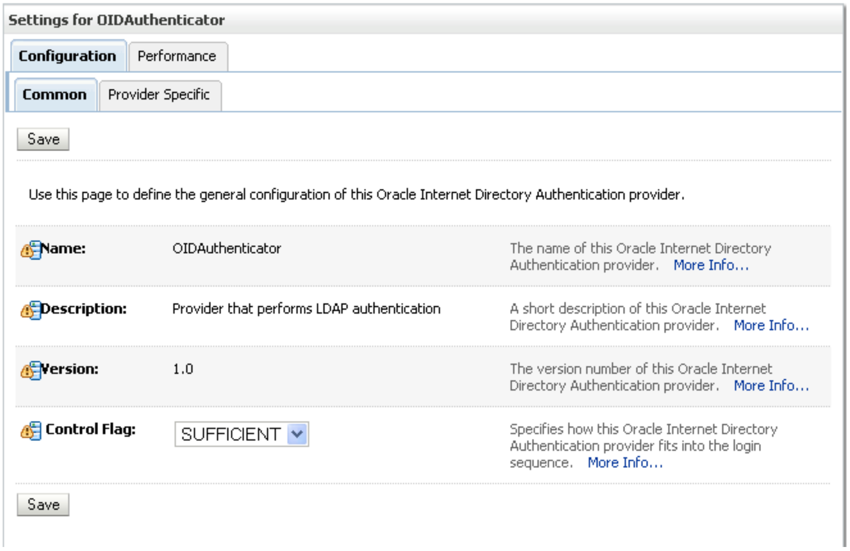
Authentication Providers

□	Name	Description	Version
□	DefaultAuthenticator	WebLogic Authentication Provider	1.0
□	DefaultIdentityAsserter	WebLogic Identity Assertion provider	1.0
□	OIDAuthenticator	Provider that performs LDAP authentication	1.0

9. In the list of Authentication Providers, click the newly created provider.

   The Settings Pane for the new authentication provider displays (see Figure 24–7).

Figure 24–7 Settings Pane for Authenticator



Use this page to define the general configuration of this Oracle Internet Directory Authentication provider.

Name:	OIDAuthenticator	The name of this Oracle Internet Directory Authentication provider. 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...

10. Set the Control Flag to `SUFFICIENT`.

    Setting the Control Flag to `SUFFICIENT` indicates that if a user can be authenticated successfully by this authenticator, then the authentication provider should accept that authentication and should not invoke any additional authenticators.

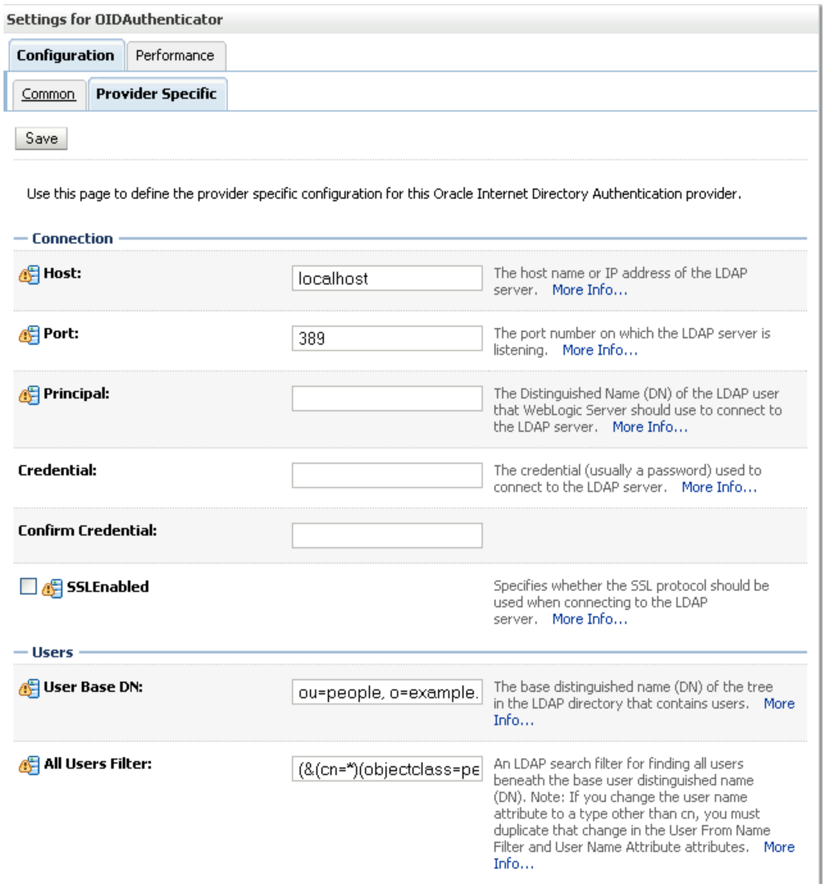
> **Note:** If the authentication fails, it falls through to the next authenticator in the chain. Therefore, be sure all subsequent authenticators also have their control flag set to `SUFFICIENT`.

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 24–8).

Figure 24–8 Provider Specific Pane



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.

Parameter	Value	Description
Host:		The LDAP server's server ID (for example, <*ldap_host*>`example.com`)
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`)

Parameter	Value	Description
Group Base DN:		Specify the DN that points to your Groups node (for example, `cn=groups,dc=example,dc=com`) For Active Directory only, set the Group Base DN to `cn=builtin,`*`<realm>`* (for example, `cn=builtin, dc=newexchange,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))`	For Active Directory only, set this value to `(&(sAMAccountName=%u)(objectclass=user)).`
User Name Attribute:	uid	

If you modify a username attribute to something other than the default set for the LDAP server in the authenticator, you must also edit the `jps-config.xml` file to correspond to these values. Specifically, the **username.attr** and **user.login.attr** properties (highlighted below) must be added for user lookups to function correctly:

```
<!-- JPS WLS LDAP Identity Store Service Instance -->
<serviceInstance name="idstore.ldap" provider="idstore.ldap.provider">
<property name="idstore.config.provider"
value="oracle.security.jps.wls.internal.idstore.WlsLdapIdStoreConfigProvider"/>
<property name="username.attr" value="uid"/>
<property name="user.login.attr" value="uid"/>
</serviceInstance>
```

For the permissible values for other LDAPs, such as Active Directory, see the appendix "OPSS System and Configuration Properties" in the *Oracle Fusion Middleware Security Guide*.

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 24.5, "Moving the Administrator Account to an External LDAP Server."

    Note: WebCenter Spaces uses only the first authenticator to authenticate users in the identity store.

16. Restart the Administration Server and the managed server for the changes to take effect.

24.2 Tuning the Identity Store for Performance

For a production environment, Oracle recommends that you add the following configuration entry to the `jps-config.xml` file for best performance:

```
<serviceInstance provider="idstore.ldap.provider" name="idstore.ldap">
<property
value="oracle.security.jps.wls.internal.idstore.WlsLdapIdStoreConfigProvider"
name="idstore.config.provider"/>
<property name="CONNECTION_POOL_CLASS"
value="oracle.security.idm.providers.stdldap.JNDIPool"/>
</serviceInstance>
```

24.3 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.

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 24.1, "Reassociating the Identity Store with an External LDAP") to avoid having to migrate the users from the embedded LDAP to the newly configured external LDAP.

WebCenter Spaces supports self-registration. New users who self-register with WebCenter Spaces are added directly to the identity store. For more information about self-registration, see Section 34.4, "Allowing Self-Registration."

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 24.3.1, "Adding Users to the Identity Store Using the WLS Administration Console"
- Section 24.3.2, "Adding Users to the Identity Store Using an LDIF File"

24.3.1 Adding Users to the Identity Store Using the WLS Administration Console

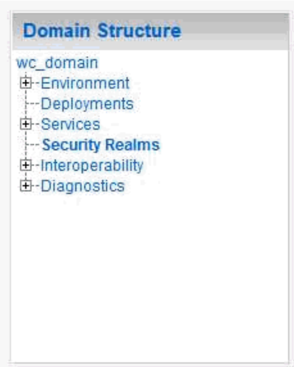
To add users to the embedded LDAP identity store from the WebLogic Server Administration Console:

1. Log in to the WebLogic Server Administration Console.

For information on logging into the WebLogic Server Administration Console, see Section 1.12.2, "Oracle WebLogic Server Administration Console."

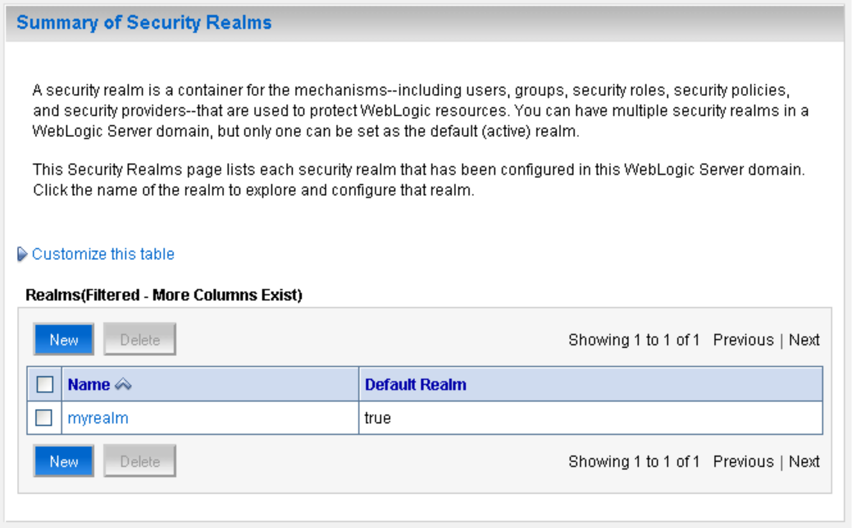
2. In the Domain Structure pane (see Figure 24–9), click **Security Realms**.

Figure 24–9 Domain Structure Pane



The Summary of Security Realms pane displays (see Figure 24–10).

Figure 24–10 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.

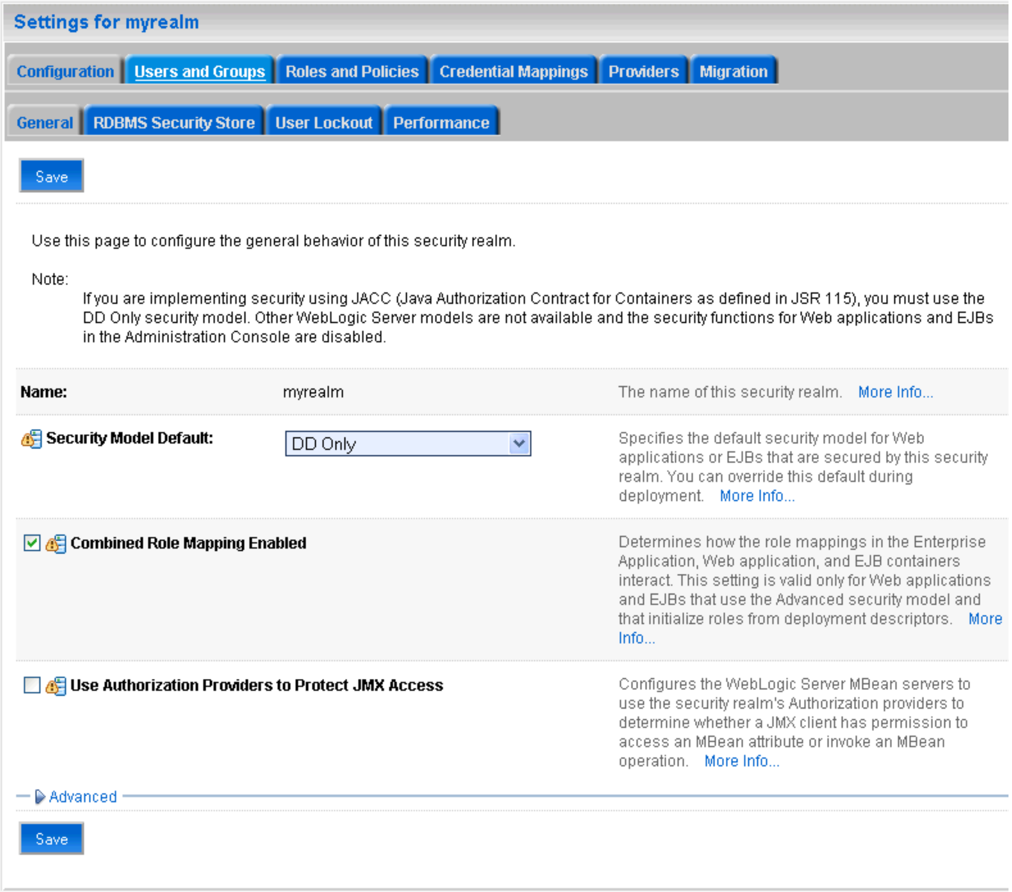
Realms(Filtered - More Columns Exist)

□	Name	Default Realm
□	myrealm	true

3. In the Name column, click the realm to which you want to add users.

   The Realm Settings pane displays (see Figure 24–11).

Figure 24–11 Realm Settings Pane



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...

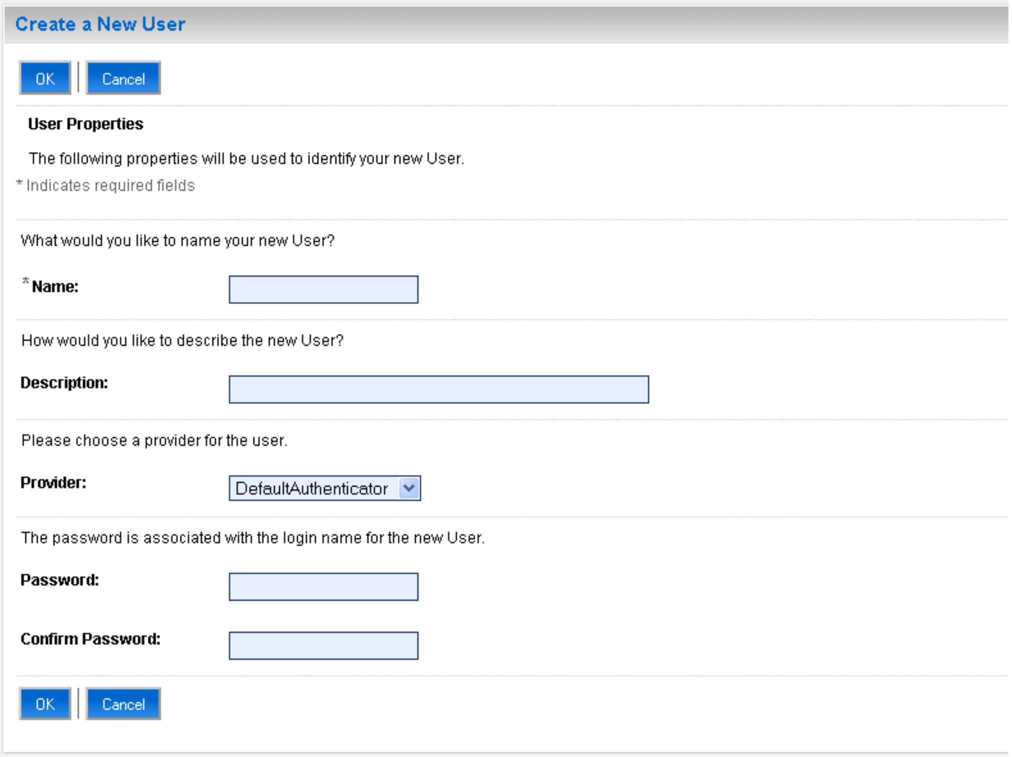
Security Model Default: DD Only — Specifies the default security model for Web applications or EJBs that are secured by this security realm. You can override this default during deployment. More Info...

☑ **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...

4. Click the **Users and Groups** tab to display the list of current users.
5. Click **New** to add a new user.

Figure 24–12 Create a New User Page



Create a New User

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: DefaultAuthenticator

The password is associated with the login name for the new User.

Password:

Confirm Password:

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.

24.3.2 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.

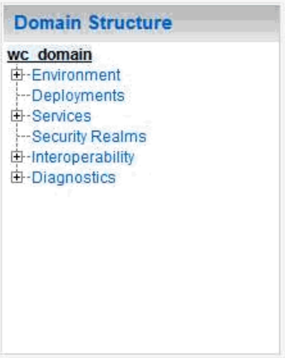
To reset the access credential for the embedded LDAP:

1. Log in to the WebLogic Server Administration Console.

   For information on logging into the WebLogic Server Administration Console, see Section 1.12.2, "Oracle WebLogic Server Administration Console."

2. In the Domain Structure pane (see Figure 24–13), click **wc_domain**.

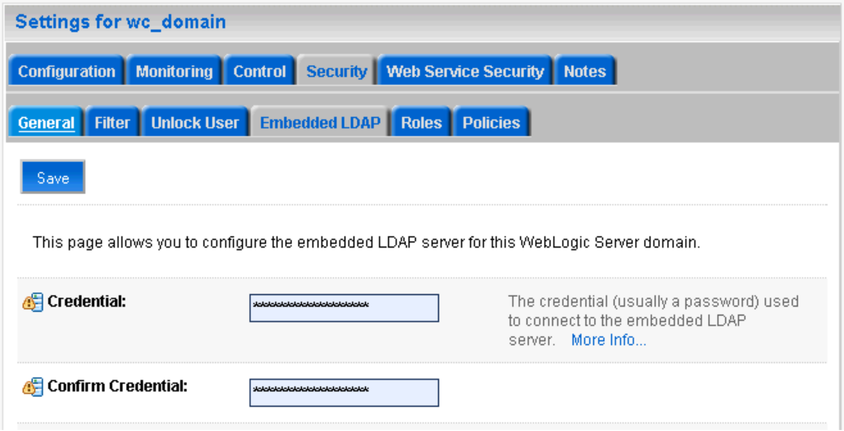
Figure 24–13 Domain Structure Pane (wc_domain)



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 24–14).

Figure 24–14 Settings Pane with Embedded LDAP Settings



Settings for wc_domain

This page allows you to configure the embedded LDAP server for this WebLogic Server domain.

Credential: ******************* The credential (usually a password) used to connect to the embedded LDAP server.

Confirm Credential: *******************

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

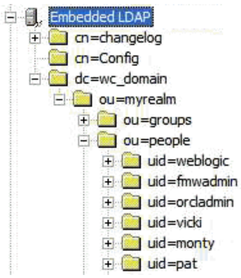
Create an LDIF File

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 24–15.

Figure 24–15 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 WebCenter 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: WebCenter 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 Fusion Middleware User Reference for Oracle Identity Management*.

```
ldapadd -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
```

24.4 Managing Users and Roles

WebCenter Spaces provides a *Users tab* from which an administrator can add users defined in the identity store, and assign roles to those users within WebCenter Spaces. For information about managing users and user roles for WebCenter Spaces, see Chapter 34, "Managing Users and Roles for WebCenter Spaces."

> **Caution:** The "Allow Password Change" property, which specifies whether users can change their passwords within WebCenter Spaces, should be carefully controlled for corporate identity stores. WebCenter Spaces administrators can set this property from the Profile Management Settings page in WebCenter Spaces. For more information, see Section 16.3.4, "Configuring Profile."

The user interface and management tools with which to manage users and user roles for custom WebCenter applications depends on what has been implemented for the particular deployment. For more information about role-mapping for ADF-security based WebCenter applications, see the section *What You May Need to Know About Application Roles and Enterprise Roles* in the *Oracle Fusion Middleware Fusion Developer's Guide for Oracle Application Development Framework*.

24.5 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 24.5.1, "Migrating the WebCenter 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 WebCenter 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 24.5.2, "Changing the Administrator Group Name."

24.5.1 Migrating the WebCenter Discussions Server to Use an External LDAP

If you've installed Oracle WebCenter Discussions Server and choose **not to move** the administrator account to an external LDAP (as described in Section 24.5, "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 24.3, "Adding Users to the Embedded LDAP Identity Store."

3. Log in to the Oracle WebCenter Discussions Server Admin Console with the boot-identity account (that is, weblogic) at:

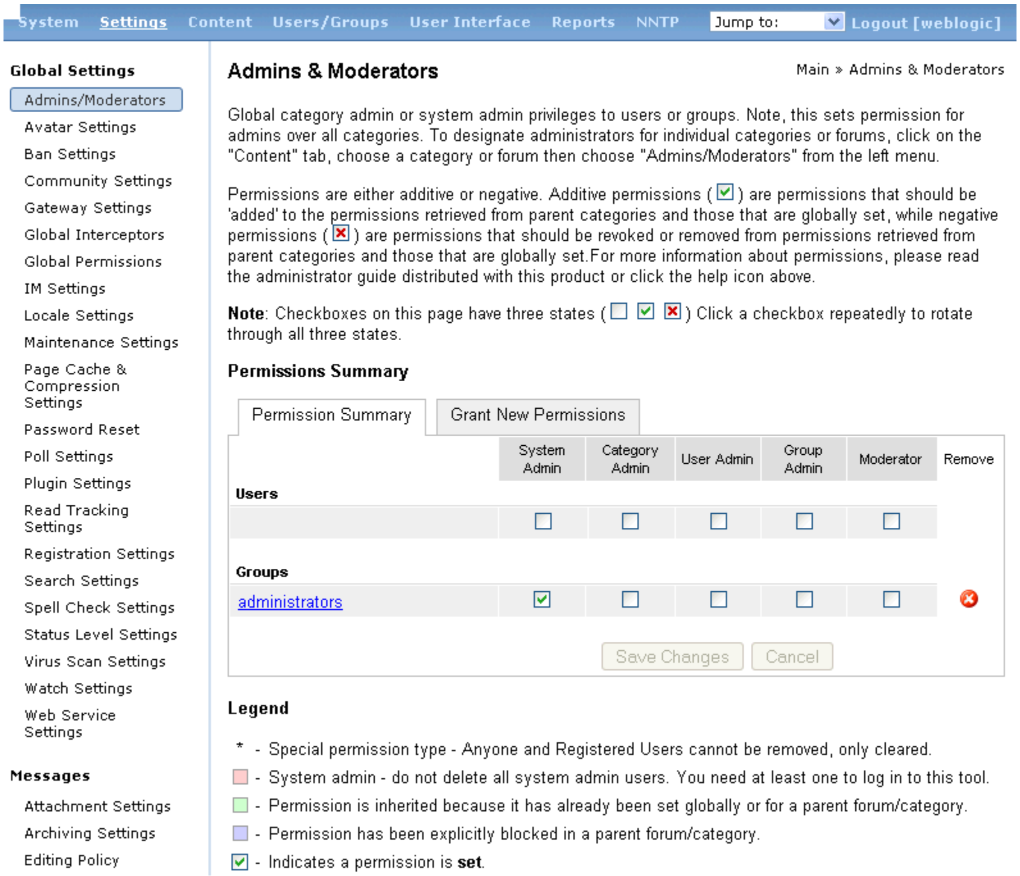
   ```
   http://host:port/owc_discussions/admin
   ```

   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 24–16).

Figure 24–16 Admins & Moderators Page



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						
	□	□	□	□	□	
Groups						
administrators	☑	□	□	□	□	☒

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.

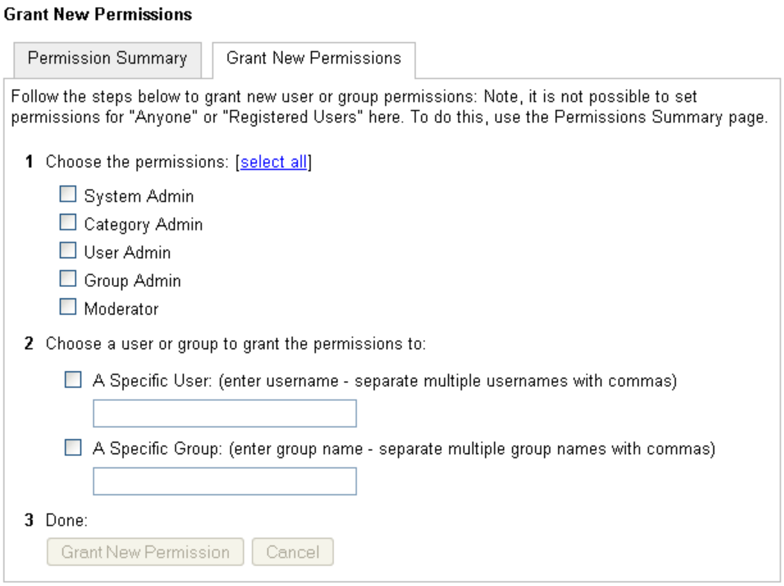
🟦 - Permission has been explicitly blocked in a parent forum/category.

☑ - Indicates a permission is **set**.

5. Click **Grant New Permissions**.

   The Grant New Permissions pane displays (see Figure 24–17).

Figure 24–17 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.

1 Choose the permissions: [select all]

□ System Admin
□ Category Admin
□ User Admin
□ Group Admin
□ Moderator

2 Choose a user or group to grant the permissions to:

□ A Specific User: (enter username - separate multiple usernames with commas)

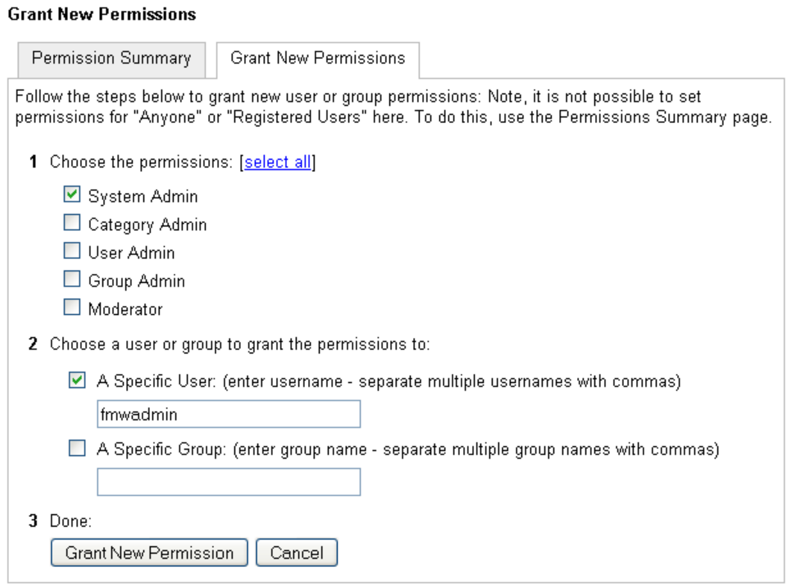
□ A Specific Group: (enter group name - separate multiple group names with commas)

3 Done:

Grant New Permission | Cancel

6. Grant System Admin privileges to the user you created, as shown in Figure 24–18.

Figure 24–18 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.

1 Choose the permissions: [select all]

☑ System Admin
☐ Category Admin
☐ User Admin
☐ Group Admin
☐ Moderator

2 Choose a user or group to grant the permissions to:

☑ A Specific User: (enter username - separate multiple usernames with commas)

fmwadmin

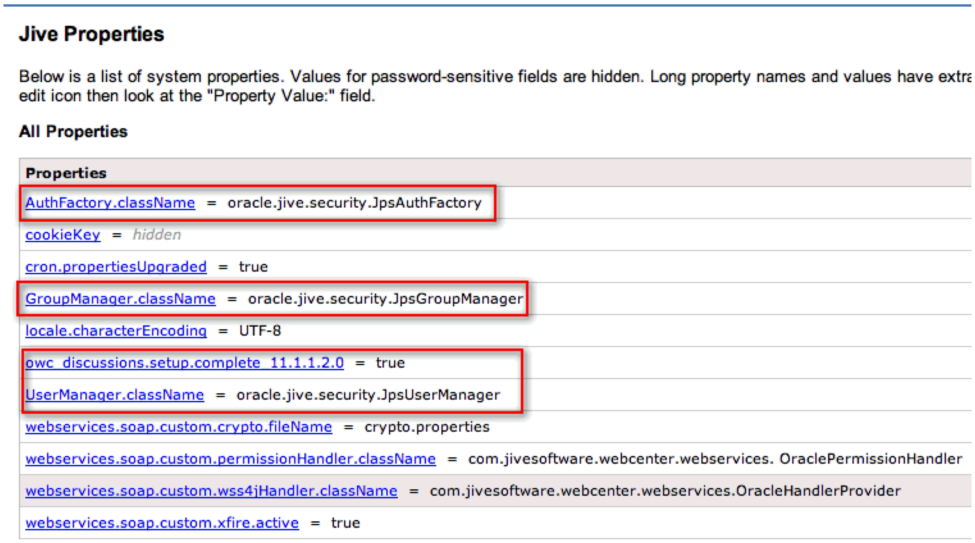
☐ A Specific Group: (enter group name - separate multiple group names with commas)

3 Done:

7. Click **System** > **System Properties**.

   The Jive Properties page displays (see Figure 24–19).

Figure 24–19 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
owc_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

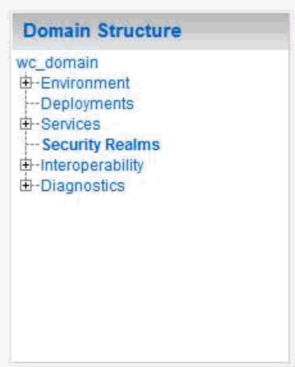
8. Check that the properties marked in red have been added and are set as shown in Figure 24–20.

9. Log in to the WebLogic Server Administration Console.

   For information on logging in to the WebLogic Server Administration Console, see Section 1.12.2, "Oracle WebLogic Server Administration Console."

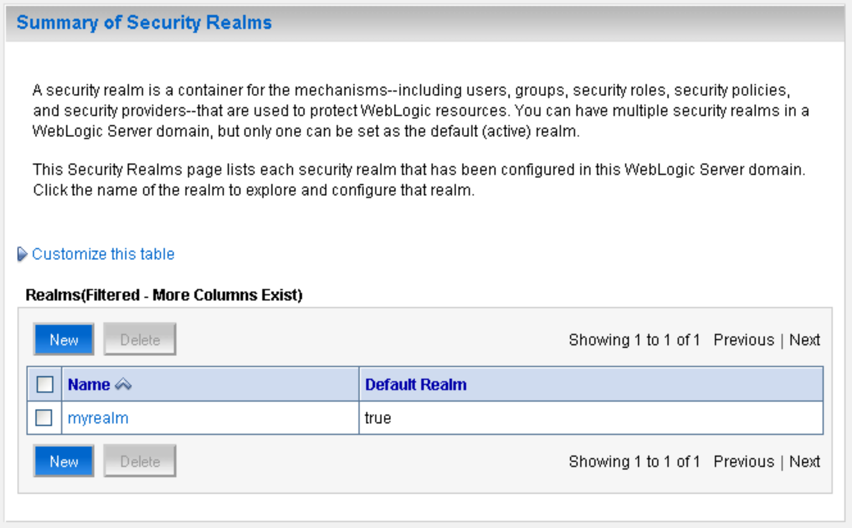
10. In the Domain Structure pane (see Figure 24–20), click **Security Realms**.

Figure 24–20 Domain Structure Pane



The Summary of Security Realms pane displays (see Figure 24–21).

Figure 24–21 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

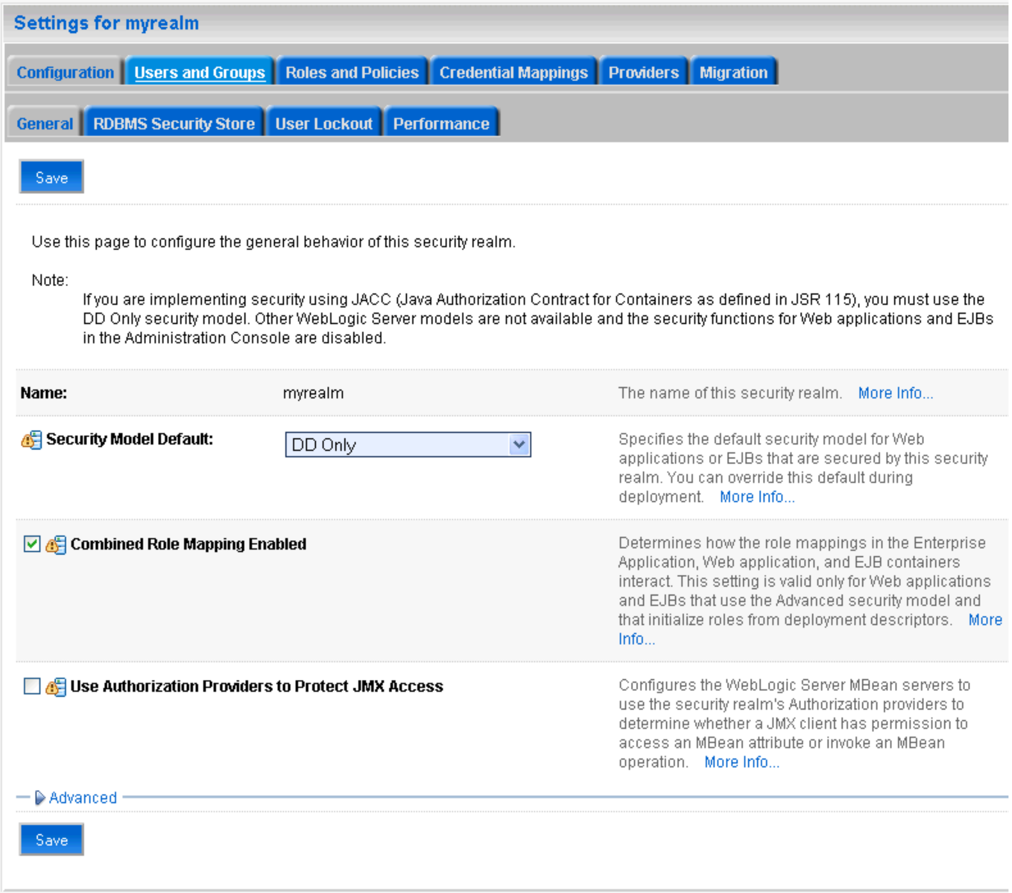
Realms(Filtered - More Columns Exist)

□	Name	Default Realm
□	myrealm	true

11. In the Name column, click the realm for which you want to change the administrator group name.

    The Realm Settings pane displays (see Figure 24–22).

Figure 24–22 Realm Settings Pane



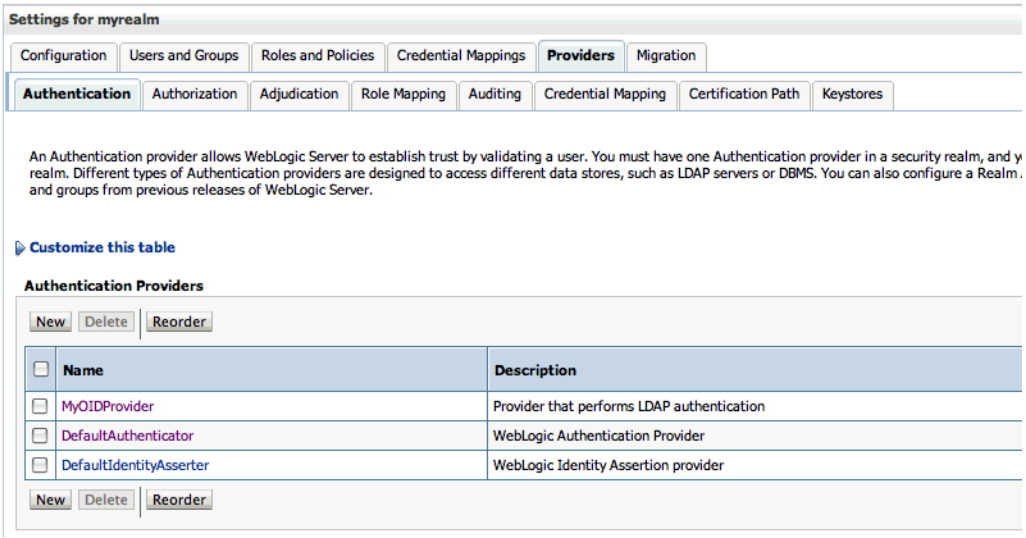
Use this page to configure the general behavior of this security realm.

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...

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 24–23:

Figure 24–23 Providers Tab with Reordered Authentication Providers



An Authentication provider allows WebLogic Server to establish trust by validating a user. You must have one Authentication provider in a security realm, and y 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 and groups from previous releases of WebLogic Server.

Authentication Providers

☐	Name	Description
☐	MyOIDProvider	Provider that performs LDAP authentication
☐	DefaultAuthenticator	WebLogic Authentication Provider
☐	DefaultIdentityAsserter	WebLogic Identity Assertion provider

13. Restart the domain Administration Server and discussions server.

24.5.2 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.

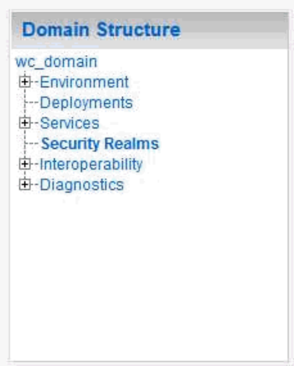
To update the role definition for the WebLogic Server global Admin role:

1. Log in to the WebLogic Server Administration Console.

   For information on logging into the WebLogic Server Administration Console, see Section 1.12.2, "Oracle WebLogic Server Administration Console."

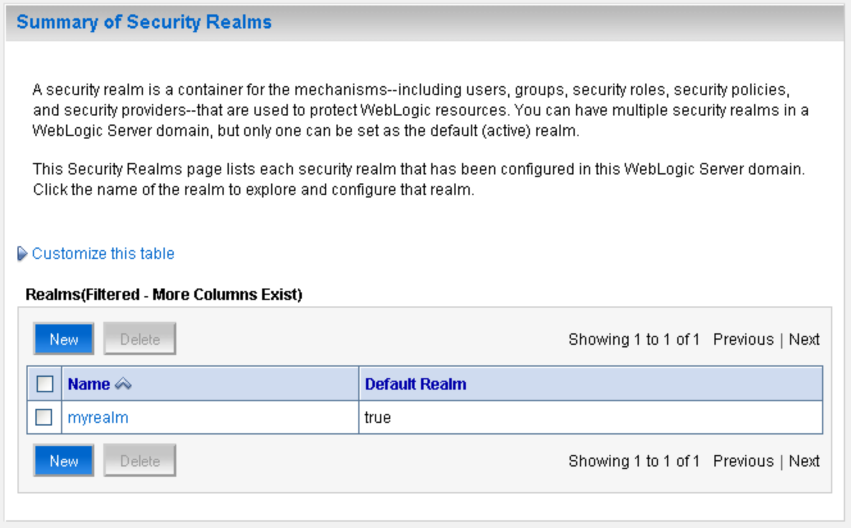
2. In the Domain Structure pane (see Figure 24–24), click **Security Realms**.

   Figure 24–24 Domain Structure Pane

   The Summary of Security Realms pane displays (see Figure 24–25).

Figure 24–25 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.

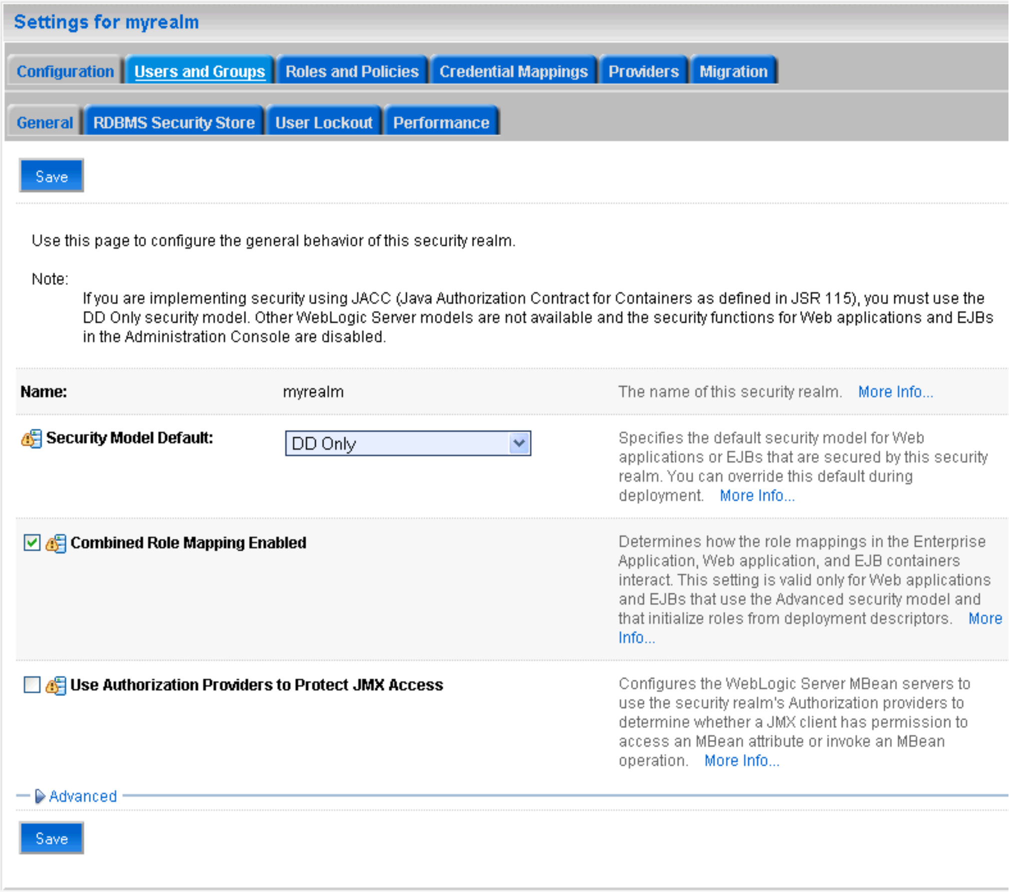
Realms(Filtered - More Columns Exist)

□	Name	Default Realm
□	myrealm	true

3. In the Name column, click the realm for which you want to change the administrator group name.

   The Realm Settings pane displays (see Figure 24–26).

Figure 24–26 Realm Settings Pane



Settings for myrealm

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...

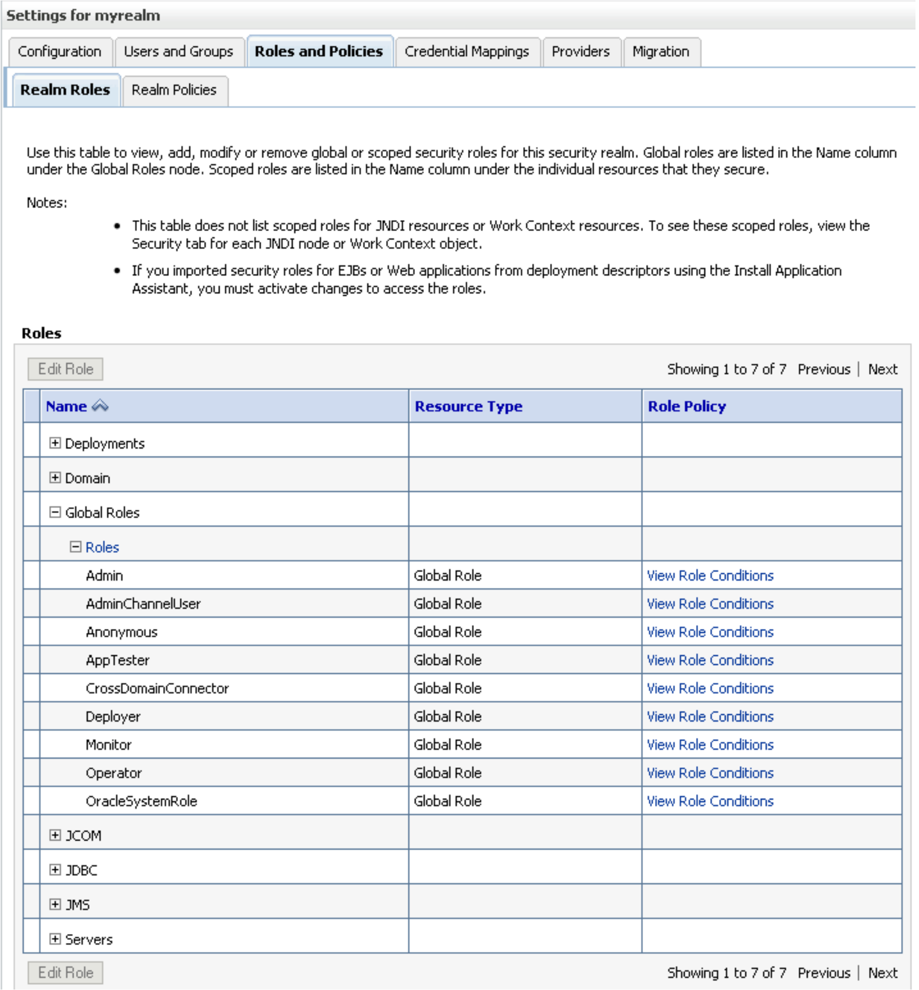
☑ Combined Role Mapping Enabled — Determines how the role mappings in the Enterprise Application, Web application, and EJB containers interact. This setting is valid only for Web applications and EJBs that use the Advanced security model and that initialize roles from deployment descriptors. More Info...

□ 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...

4. Open the Roles and Policies tab, and then the Realm Roles subtab.

   The Realm Roles settings pane displays (see Figure 24–27).

Figure 24–27 Realm Roles Settings Pane



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

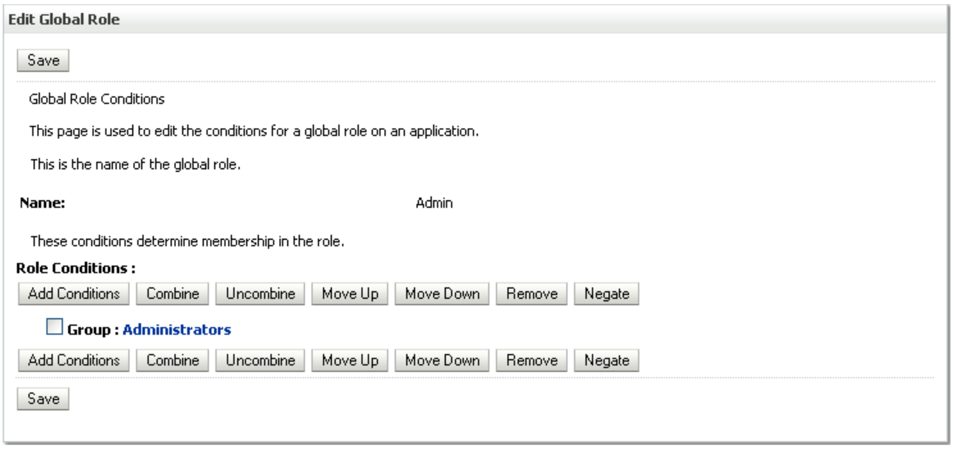
Name	Resource Type	Role Policy
⊞ Deployments		
⊞ Domain		
⊟ Global Roles		
⊟ Roles		
Admin	Global Role	View Role Conditions
AdminChannelUser	Global Role	View Role Conditions
Anonymous	Global Role	View Role Conditions
AppTester	Global Role	View Role Conditions
CrossDomainConnector	Global Role	View Role 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		

5. Expand the Global Roles node, and then the Roles node.

6. Click **View Role Conditions** for the `Admin` role.

   The Edit Global Role page displays (see Figure 24–28).

Figure 24–28 Edit Global Role Page



Global Role Conditions

This page is used to edit the conditions for a global role on an application.

This is the name of the global role.

Name: Admin

These conditions determine membership in the role.

Role Conditions :

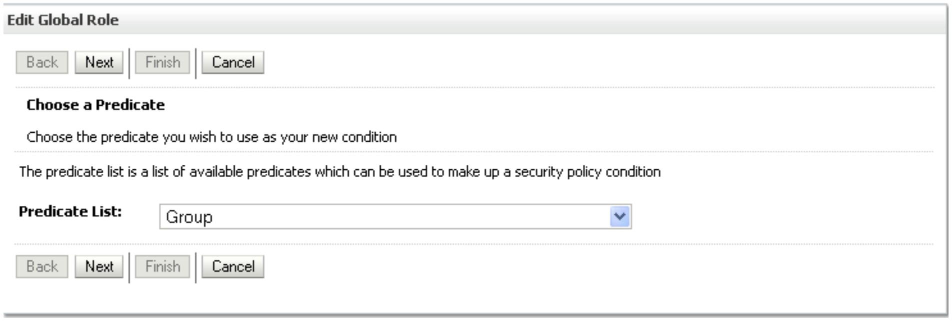
□ **Group : Administrators**

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 24–29).

Figure 24–29 Edit Global Role Page - Predicate List



Choose a Predicate

Choose the predicate you wish to use as your new condition

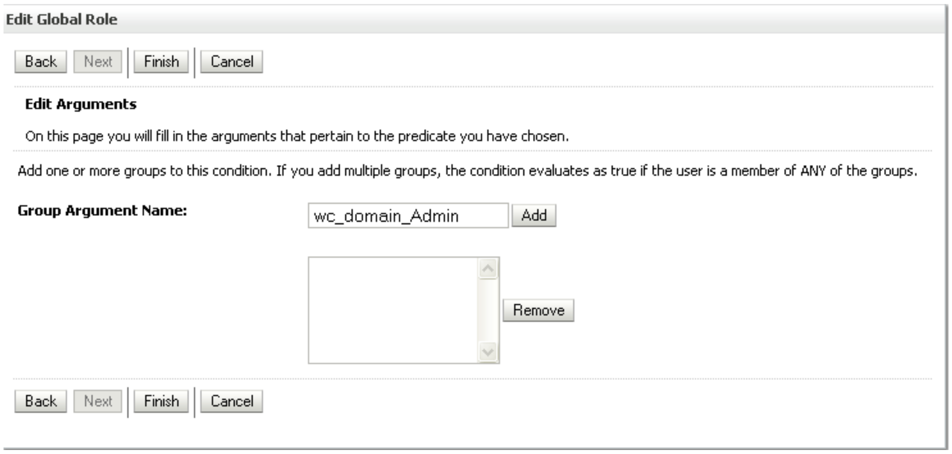
The predicate list is a list of available predicates which can be used to make up a security policy condition

Predicate List: Group

8. Select `Group` from the **Predicate List** list and click **Next**.

   The Edit Global Role - Arguments page displays (see Figure 24–30).

Figure 24–30 Edit Global Role Page - Arguments



Edit Global Role

Edit Arguments

On this page you will fill in the arguments that pertain to the predicate you have chosen.

Add one or more groups to this condition. If you add multiple groups, the condition evaluates as true if the user is a member of ANY of the groups.

Group Argument Name: wc_domain_Admin

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.

24.6 Granting the WebCenter Spaces Administrator Role to a WebCenter Spaces User

WebCenter Spaces only recognizes users in the identity store that is mapped by the first authenticator. Since the WebCenter Spaces Administrator account is initially created only in the embedded LDAP server, if an external LDAP such as Oracle Internet Directory is configured as the primary authenticator for WebCenter Spaces, you must also create a user in that LDAP and grant that user the WebCenter Spaces Administrator role.

You can grant a user the WebCenter Administrator role using Fusion Middleware Control or WLST as shown below in the sections on:

- Section 24.6.1, "Granting the WebCenter Spaces Administrator Role Using Fusion Middleware Control"
- Section 24.6.2, "Granting the WebCenter 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*.

24.6.1 Granting the WebCenter Spaces Administrator Role Using Fusion Middleware Control

This section describes how to grant the WebCenter Spaces administrator role to a user account other than the default "weblogic" account.

To grant the WebCenter Spaces Administrator role using Fusion Middleware Control:

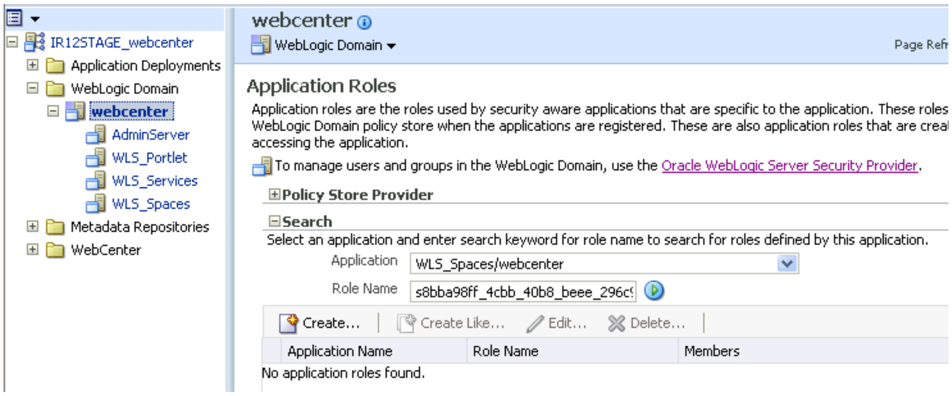
1. Log into Fusion Middleware Control and select the WebLogic domain for WebCenter Spaces.

For information on logging into Fusion Middleware Control, see Section 6, "Starting Enterprise Manager Fusion Middleware Control."

2. From the WebLogic Domain menu, select **Security -> Application Roles**.

   The Application Roles page displays (see Figure 24–31).

Figure 24–31 Application Roles Page



Application Roles

Application roles are the roles used by security aware applications that are specific to the application. These roles WebLogic Domain policy store when the applications are registered. These are also application roles that are creat accessing the application.

To manage users and groups in the WebLogic Domain, use the Oracle WebLogic Server Security Provider.

Policy Store Provider

Search

Select an application and enter search keyword for role name to search for roles defined by this application.

Application: WLS_Spaces/webcenter

Role Name: s8bba98ff_4cbb_40b8_beee_296c9

Application Name	Role Name	Members

No application roles found.

3. Search for the Administration application role by selecting the **Application** name for WebCenter Spaces (`WLS_Spaces/webcenter`), and providing the following internal identifier used by WebCenter Spaces as the **Role Name**:

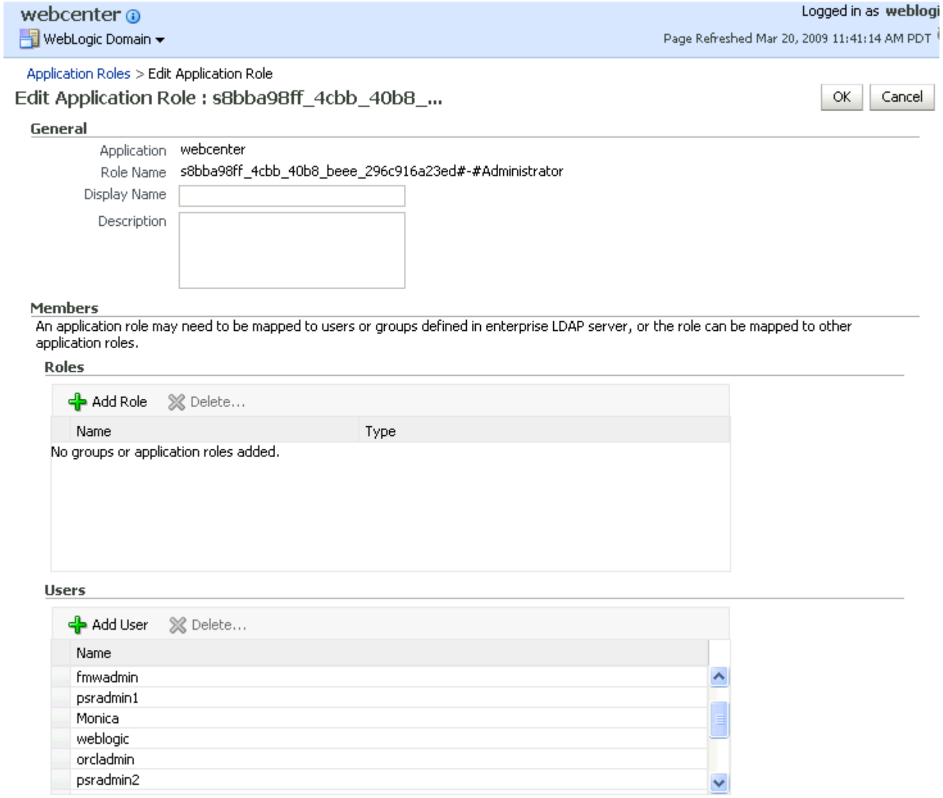
```
s8bba98ff_4cbb_40b8_beee_296c916a23ed#-#Administrator
```

   The search should return `s8bba98ff_4cbb_40b8_beee_296c916a23ed#-#Administrator`, which is the administrator role identifier.

4. Click the administrator role name (`s8bba98ff_4cbb_40b8_beee_296c916a23ed#-#Administrator`) in the Role Name column.

   The Edit Application Role page displays (see Figure 24–32).

Figure 24–32 Edit Application Role Page



Edit Application Role : s8bba98ff_4cbb_40b8_...

General

Application: webcenter

Role Name: s8bba98ff_4cbb_40b8_beee_296c916a23ed#-#Administrator

Display Name:

Description:

Members

An application role may need to be mapped to users or groups defined in enterprise LDAP server, or the role can be mapped to other application roles.

Roles

Name	Type
No groups or application roles added.	

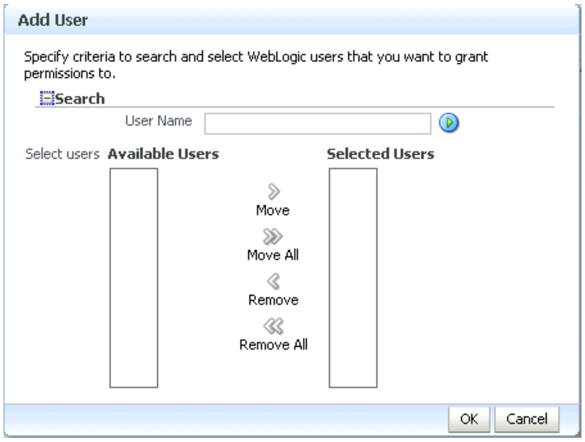
Users

Name
fmwadmin
psradmin1
Monica
weblogic
orcladmin
psradmin2

5. Click **Add User**.

   The Add User pop-up displays (see Figure 24–33).

Figure 24–33 Add User Pop-up



Specify criteria to search and select WebLogic users that you want to grant permissions to.

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**.

10. Restart the `WLS_Spaces` managed server.

    When you login to WebCenter Spaces, the Administration link should appear and you should be able to perform all administrator operations. See also, Section 32.1, "Logging into WebCenter Spaces as an Administrator."

24.6.2 Granting the WebCenter Spaces Administrator Role Using WLST

To grant the WebCenter Administrator role using WLST:

1. Start WLST as described in Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool (WLST) Commands."

2. Connect to the WebCenter Spaces Administration Server for the target domain with the following command:

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

    Where:

    - *`user_name`* is the name of the user account with which to access the Administration Server (for example, `weblogic`)
    - *`password`* is the password with which to access the Administration Server
    - *`host_id`* is the host ID of the Administration Server
    - *`port`* is the port number of the Administration Server (for example, `7001`).

3. Grant the WebCenter Spaces administrator application role to the user in Oracle Internet Directory using the `grantAppRole` command as shown below:

    ```
    grantAppRole(appStripe="webcenter",
    appRoleName="s8bba98ff_4cbb_40b8_beee_296c916a23ed#-#Administrator",
    principalClass="weblogic.security.principal.WLSUserImpl",
    principalName="wc_admin")
    ```

    Where *`wc_admin`* is the name of the administrator account to create.

4. To test the new account, log into WebCenter Spaces using the new account name.

    The Administration link should appear, and you should be able to perform all administrator operations. See also, Section 32.1, "Logging into WebCenter Spaces as an Administrator."

5. After granting the WebCenter Spaces Administrator role to new accounts, remove this role from accounts that no longer need it or should no longer have it using the WLST `revokeAppRole` command. For example, if WebCenter Spaces was installed with a different administrator user name than "weblogic", the administrator role should be given to that user and should be revoked from the default "weblogic".

    ```
    revokeAppRole(appStripe="webcenter",
    appRoleName="s8bba98ff_4cbb_40b8_beee_296c916a23ed#-#Administrator",
    principalClass="weblogic.security.principal.WLSUserImpl",
    principalName="weblogic")
    ```

24.7 Configuring the Oracle Content Server to Share the WebCenter Spaces Identity Store LDAP Server

Oracle Content Server (OCS) must be configured to use the same identity store LDAP server as Oracle WebCenter Spaces. For more information on configuring the OCS, see Section 11.2.1.2.1, "Configuring the Identity Store," and also "Configuring the Identity Store Service" in the *Oracle Fusion Middleware Security Guide*.

25

Configuring the Policy and Credential Store

For most environments, and especially production environments, you must reassociate your policy store with an external LDAP such as Oracle Internet Directory (OID). Note that when using an external LDAP-based store, the credential store and policy store must be configured to use the same LDAP server (either Oracle Internet Directory 11gR1 or 10.1.4.3).

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 as described in the following sections:

- Section 25.1, "Creating a root Node"
- Section 25.2, "Reassociating the Credential and Policy Store Using Fusion Middleware Control"
- Section 25.3, "Reassociating the Credential and Policy Store Using WLST"
- Section 25.4, "Managing Credentials"
- Section 25.5, "Configuring Self-Registration By Invitation in WebCenter Spaces"

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."

25.1 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.

25.2 Reassociating the Credential and Policy Store Using Fusion Middleware Control

When initially installed, WebCenter Spaces and Enterprise Manager are already associated and deployed in the same domain.

Before reassociating the policy and credential store with Oracle Internet Directory, you must first have created the root node as described in Section 25.1, "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.

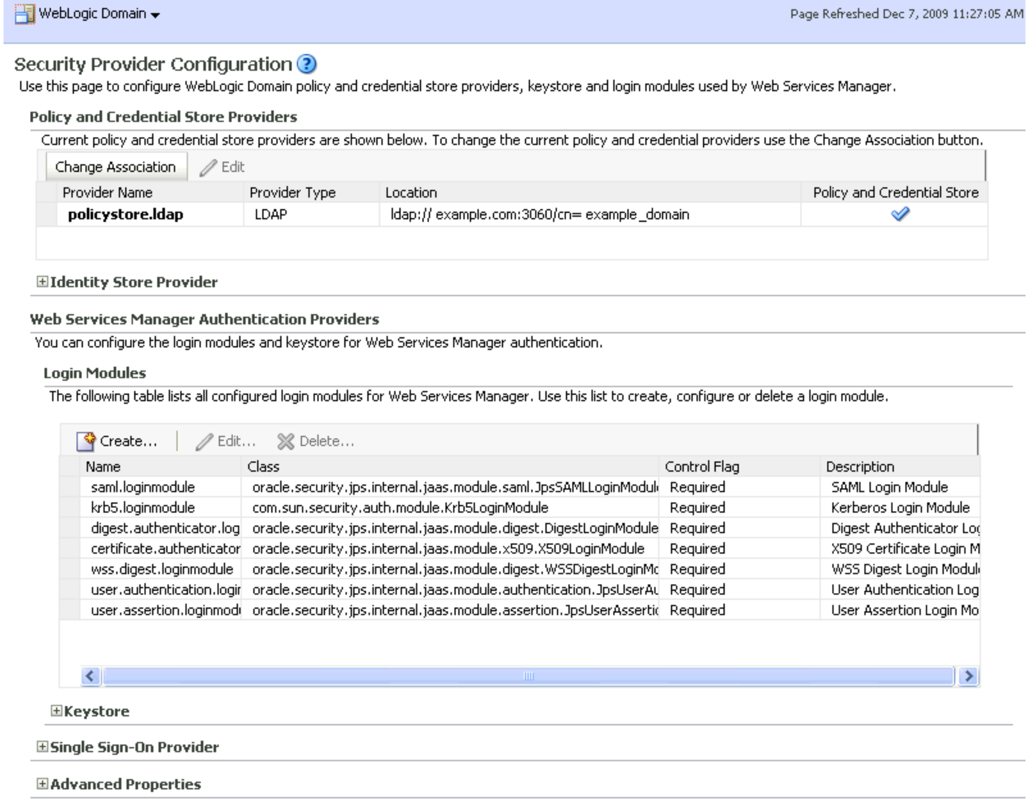
   For information on logging into Fusion Middleware Control, see Section 6, "Starting Enterprise Manager Fusion Middleware Control."

2. In the Navigation pane, click your domain.

3. From the WebLogic Domain menu, select **Security > Security Provider Configuration**.

   The Security Provider Configuration page displays (see Figure 25–1).

Figure 25–1 Security Provider Configuration Page



Security Provider Configuration

Use this page to configure WebLogic Domain policy and credential store providers, keystore and login modules used by Web Services Manager.

Policy and Credential Store Providers

Current policy and credential store providers are shown below. To change the current policy and credential providers use the Change Association button.

Provider Name	Provider Type	Location	Policy and Credential Store
policystore.ldap	LDAP	ldap:// example.com:3060/cn= example_domain	✓

⊞Identity Store Provider

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.JpsSAMLLoginModul	Required	SAML 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 Lo
certificate.authenticator	oracle.security.jps.internal.jaas.module.x509.X509LoginModule	Required	X509 Certificate Login M
wss.digest.loginmodule	oracle.security.jps.internal.jaas.module.digest.WSSDigestLoginMc	Required	WSS Digest Login Modul
user.authentication.logi	oracle.security.jps.internal.jaas.module.authentication.JpsUserAu	Required	User Authentication Log
user.assertion.loginmod	oracle.security.jps.internal.jaas.module.assertion.JpsUserAsserti	Required	User Assertion Login Mo

⊞Keystore

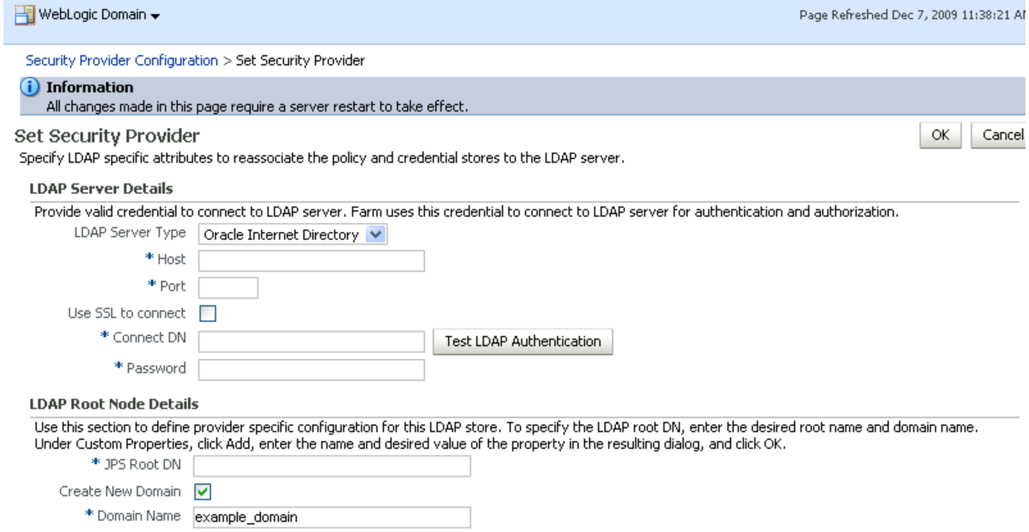
⊞Single Sign-On Provider

⊞Advanced Properties

4. On the Security Provider Configuration page, click **Change Association...** to add the new Oracle Internet Directory provider.

   The Set Security Provider page displays (see Figure 25–2).

Figure 25–2 Set Security Provider Page



Security Provider Configuration > Set Security Provider

Information

All changes made in this page require a server restart to take effect.

Set Security Provider

Specify LDAP specific attributes to reassociate the policy and credential stores to the LDAP server.

LDAP Server Details

Provide valid credential to connect to LDAP server. Farm uses this credential to connect to LDAP server for authentication and authorization.

LDAP Server Type	Oracle Internet Directory
* Host	
* Port	
Use SSL to connect	□
* Connect DN	
* Password	

LDAP Root Node Details

Use this section to define provider specific configuration for this LDAP store. To specify the LDAP root DN, enter the desired root name and domain name. Under Custom Properties, click Add, enter the name and desired value of the property in the resulting dialog, and click OK.

* JPS Root DN	
Create New Domain	☑
* Domain Name	example_domain

5. Under LDAP Server Details, select **Oracle Internet Directory** as the LDAP Server Type.

6. In the **Host** and **Port** fields, enter the host name and the LDAP port for Oracle Internet Directory.
7. Set the **User DN** field to `cn=orcladmin,` and enter the associated password in the **Password** field.
8. Under LDAP Root Node Details, set the **JPS Root DN** field to the one you added to the `root.ldif` file (for example, `cn=root_webcenter_abcd99`). Be sure to include the `cn=`.
9. Click **OK** to begin the reassociation. Restart the WebLogic server when prompted after migration.

25.3 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 25.1, "Creating a root Node."

1. Start WLST as described in Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool (WLST) Commands."
2. Connect to the Administration Server for the target domain with the following command:

   ```
   connect('username>,'password', 'host_id:port')
   ```

   where:

   - *`username`* is the administrator account name used to access the Administration Server (for example, `weblogic`)
   - *`password`* is the administrator password used to access the Administration Server (for example, `weblogic`)
   - *`host_id`* is the server ID of the Administration Server (for example, `example.com`)
   - *`port`* is the port number of the Administration Server (for example, `7001`).

3. Reassociate the policy and credential store using the `reassociateSecurityStore` command:

   ```
   reassociateSecurityStore(domain="domain_name", admin="admin_name",
   password="password",
   ldapurl="ldap_uri", servertype="ldap_srvr_type", jpsroot="root_webcenter_xxxx")
   ```

   Where:

   - *`domain_name`* specifies the domain name where reassociation takes place.
   - *`admin_name`* specifies the administrator's user name on the LDAP server. The format is `cn=usrName`.
   - *`password`* specifies the password associated with the user specified for the argument `admin`.
   - *`ldap_uri`* specifies the URI of the LDAP server. The format is `ldap://host:port`, if you are using a default port, or `ldaps://host:port`, if you are using a secure LDAP port. The secure port must have been configured to handle an anonymous SSL connection, and it is distinct from the default (non-secure) port.

- *ldap_srvr_type* specifies the kind of the target LDAP server. 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")
```

25.4 Managing Credentials

Administrators can manage credentials for the WebCenter domain credential store using Fusion Middleware Control and WLST commands. For more information, see "Managing Credentials" in the *Oracle Fusion Middleware Security Guide*.

25.5 Configuring Self-Registration By Invitation in WebCenter Spaces

WebCenter Spaces supports self-registration by invitation, as described in Section 34.4.1, "Enabling Self-Registration By Invitation-Only." The self-registration 'by-invitation' feature requires that the WebCenter 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 WebCenter 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 Security Guide*.

26

Configuring WebCenter Applications and Components to Use SSO

This chapter describes the available single sign-on (SSO) solutions for your WebCenter application to use, and how each is configured.

Oracle Access Manager (OAM), part of Oracle's enterprise class suite of products for identity management and security, provides a wide range of identity administration and security functions, including several single sign-on options for WebCenter Spaces and custom WebCenter applications. OAM is the recommended single sign-on solution for Oracle WebCenter 11g installations.

For deployment environments that are already invested in Oracle 10g infrastructure, and where the Oracle Application Server Single Sign-On (OSSO) server is used as the primary SSO solution, WebCenter 11g can also be configured to use OSSO for single sign-on.

For smaller scale Oracle WebCenter 11g installations, where you do not have an enterprise-class single sign-on infrastructure like Oracle Access Manager or Oracle SSO, and you only need to provide a single sign-on capability within WebCenter Spaces and its associated Web applications like Wiki, Discussions, RSS and Worklist, you can configure a SAML-based SSO solution. If you need to provide single sign-on with other enterprise applications, this solution is not recommended.

If your enterprise uses Microsoft desktop logins that authenticate with a Microsoft domain controller with user accounts in Active Directory, then configuring SSO with Microsoft Clients may also be an option to consider.

The following subsections describe the setup required for each of these SSO solutions:

- Section 26.1, "Configuring Oracle Access Manager (OAM)"
- Section 26.2, "Configuring Oracle Single Sign-On (OSSO)"
- Section 26.3, "Configuring SAML-based Single Sign-on"
- Section 26.4, "Configuring SSO with Microsoft Clients"

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."

26.1 Configuring Oracle Access Manager (OAM)

Oracle Access Manager (OAM) provides flexible and extensible authentication and authorization, and provides audit services. This section describes how to configure WebCenter Spaces and custom WebCenter applications for OAM single sign-on authentication, including how to configure the WebLogic server side and the WebCenter application as the partner application participating in SSO.

Much of the configuration can be done using scripts (recommended). To use the scripts, follow the instructions in Section 26.1.2, "Configuring OAM Using Scripts," and complete the instructions in Section 26.1.3, "Configuring the Webtier Components" and Section 26.1.6, "Configuring the Policy Manager," and any additional configurations as appropriate in Section 26.1.7, "Additional Configurations."

To perform the configuration manually, complete the instructions in all of the subsections, exception for Section 26.1.2, "Configuring OAM Using Scripts."

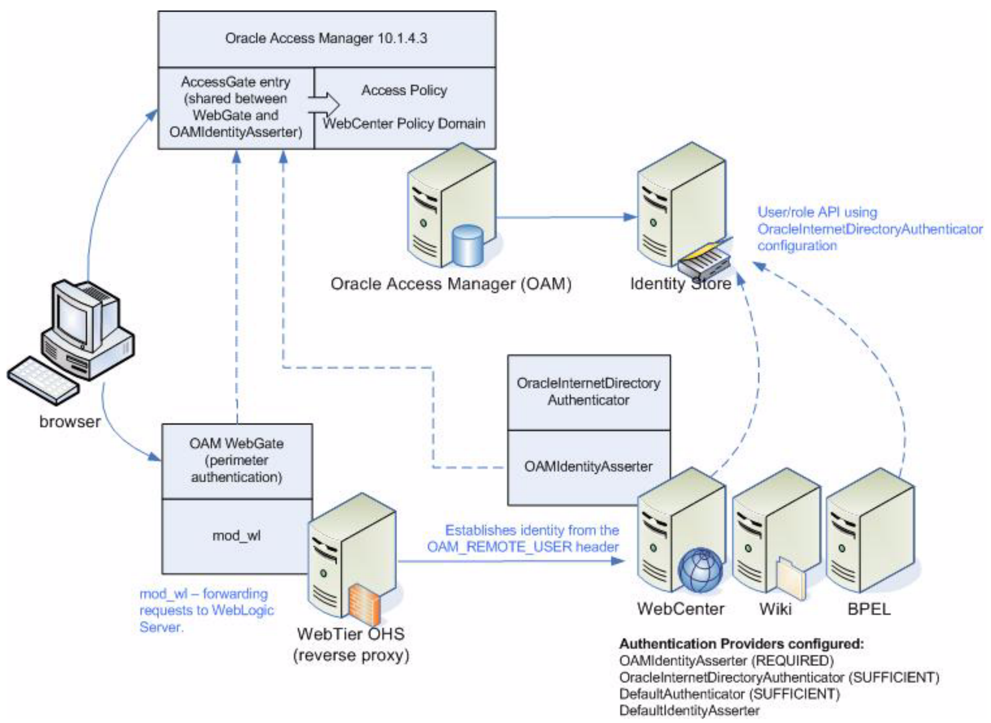
The scripted and equivalent manual configuration steps are presented in the following subsections:

- Section 26.1.1, "OAM Components and Topology"
- Section 26.1.2, "Configuring OAM Using Scripts"
- Section 26.1.3, "Configuring the Webtier Components"
- Section 26.1.4, "Manually Configuring the Access System"
- Section 26.1.5, "Manually Defining the WebCenter Policy Domain"
- Section 26.1.6, "Configuring the Policy Manager"
- Section 26.1.7, "Additional Configurations"

26.1.1 OAM Components and Topology

Figure 26–1 shows the components and topology required to set up single sign-on with Oracle Access Manager for a WebCenter application.

Figure 26–1 OAM Single Sign-On Components and Topology


Oracle Access Manager 10.1.4.3
AccessGate entry (shared between WebGate and OAMIdentityAsserter)
Access Policy
WebCenter Policy Domain
Oracle Access Manager (OAM)
Identity Store
User/role API using OracleInternetDirectoryAuthenticator configuration
browser
OracleInternetDirectory Authenticator
OAMIdentityAsserter
OAM WebGate (perimeter authentication)
mod_wl
Establishes identity from the OAM_REMOTE_USER header
mod_wl – forwarding requests to WebLogic Server.
WebTier OHS (reverse proxy)
WebCenter
Wiki
BPEL
Authentication Providers configured:
OAMIdentityAsserter (REQUIRED)
OracleInternetDirectoryAuthenticator (SUFFICIENT)
DefaultAuthenticator (SUFFICIENT)
DefaultIdentityAsserter

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.

26.1.2 Configuring OAM Using Scripts

These steps assume that you've installed Oracle WebCenter (see Section 2.3, "Installing WebCenter Spaces"). By default, an Oracle WebCenter installation creates a WebLogic Server domain, including an Administration Server and three managed servers: WLS_Spaces, WLS_Services and WLS_Portlet.

1. Install the WebTier, which contains the Oracle HTTP Server (OHS) and `mod_wl` (see the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter* for information on how to install the WebTier).
2. Configure the module mod_wl in the WebTier OHS so that it forwards requests to the Oracle WebLogic Server for WebCenter, as described in Section 26.1.3.1, "Configure mod_weblogic (mod_wl_ohs.conf)."
3. Determine which access server to use.

a. Log onto the Access Manager.

b. Click **Access System Console**.

c. Open the Access System Configuration tab.

d. Click **Access Server Configuration** to display a list of all access servers.

e. Click an access server in the list to see server details.

   The host name and port are the values you need for the `oam_aaa_host` and `oam_aaa_port` parameters respectively in the script.

4. Run the following command.

   The `oamcfgtool.jar` is available in `ORACLE_HOME/modules/oracle.oamprovider_11.1.1/oamcfgtool.jar` in the WebCenter installation. Values in bold are the ones that you must supply based on the settings of your WebCenter and OAM instances.

```
java -jar ORACLE_HOME/modules/oracle.oamprovider_11.1.1/oamcfgtool.jar
mode=CREATE app_domain="your_domain_name"
protected_uris="/webcenter/adfAuthentication,/webcenter/content,/owc_wiki/user/
login.jz,/owc_wiki/adfAuthentication,/integration/worklistapp,
/workflow/sdpmessagingsca-ui-worklist/faces/adf.task-flow,/workflow/WebCenterWo
rklistDetail/faces/adf.task-flow,
/workflow/sdpmessagingsca-ui-worklist,/rss/rssservlet,/owc_discussions/login!wi
thRedirect.jspa,
/owc_discussions/login!default.jspa,/owc_discussions/login.jspa,/owc_discussion
s/admin,/rest,/cmisrestprelim"
public_uris="/webcenter,/owc_wiki,/owc_discussions,/rss,/workflow"
app_agent_password=<Password to be provisioned for App Agent>
ldap_host=<Hostname of LDAP server> ldap_port=<Port of LDAP server>
ldap_userdn=<DN of LDAP Admin User, usually "cn=orcladmin">
ldap_userpassword=<Password of LDAP Admin User> oam_aaa_host=<HOST of OAM
server> oam_aaa_port=<Port of OAM server>
```

   We recommend that you register your domain (for **<your_domain_name>**) as something like "`webtier.example.com`", where "`webtier.example.com`" is your Webtier, so that you can easily distinguish the various policies in OAM.

   If your command ran successfully, you should see something like the following output depending on the values you used:

```
Processed input parameters
Initialized Global Configuration
Successfully completed the Create operation.
Operation Summary:
Policy Domain : webtier.example.com
Host Identifier: webtier.example.com
Access Gate ID : webtier.example.com_AG
```

   You can also run the Validate command to validate your configurations:

```
java -jar 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.

5. Check the Policy Domain settings.
   a. Log on to the Oracle Access Manager.
   b. Click **Policy Manager**.
   c. Click **My Policy Domains**.

      You should see the domain you just created in the list of policy domains. In the URL prefixes column, you should also see the URIs you specified during the creation of this domain.
   d. Click the domain you just created and open the Resources tab.

      The URIs you specified should display. You can also open other tabs to view and verify other settings, and manually add additional resources later, if required.
6. Check the Access Gate Configurations.
   a. Click **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.
7. Run the WebGate Installer as described in the section on "Installing the WebGate" in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*.

   The InstallShield Wizard will prompt you for several inputs during the installation. Supply the information requested based on the settings for your environment.
8. Continue with the steps for configuring the Policy Manager in Section 26.1.6, "Configuring the Policy Manager," and any further configurations, as required, in Section 26.1.7, "Additional Configurations."

26.1.3 Configuring the Webtier Components

This section includes the following subsections:

- Configure mod_weblogic (mod_wl_ohs.conf)
- Create an AccessGate Entry
- Install WebGate on the WebTier

26.1.3.1 Configure mod_weblogic (mod_wl_ohs.conf)

Configure the module `mod_wl` in the WebTier OHS so that it forwards requests to the Oracle WebLogic Server for WebCenter, by uncommenting lines at `WT_ORACLE_HOME/instances/<your_instance>/config/OHS/ohs1/mod_wl_ohs.conf`. This file is included by the `httpd.conf` file.

To configure Web Tier OHS to work with multiple non-clustered servers, use the example below in `mod_wl_ohs.conf`. Ensure that the WebLogic port numbers match your configuration.

```
<IfModule mod_weblogic.c>
MatchExpression  /webcenter   WebLogicHost=webcenter.example.com|WebLogicPort=8888
MatchExpression  /rss         WebLogicHost=webcenter.example.com|WebLogicPort=8888
MatchExpression  /owc_wiki    WebLogicHost=webcenter.example.com|WebLogicPort=8890
MatchExpression  /owc_discussions
WebLogicHost=webcenter.example.com|WebLogicPort=8890
MatchExpression /workflow WebLogicHost=soa.example.com|WebLogicPort=8888
MatchExpression /integration/worklistapp
WebLogicHost=soa.example.com|WebLogicPort=8888
MatchExpression /integration/services
WebLogicHost=soa.example.com|WebLogicPort=8888
MatchExpression /soa-infra WebLogicHost=soa.example.com|WebLogicPort=8888
MatchExpression /rest WebLogicHost=webcenter.example.com|WebLogicPort=8888
MatchExpression /cmisrestprelim
WebLogicHost=webcenter.example.com|WebLogicPort=8888
</IfModule>
```

Note: The entries in the MatchExpression list above map the incoming paths to the appropriate WebLogic Server managed servers on which the corresponding applications reside.

26.1.3.2 Create an AccessGate Entry

An AccessGate entry must be created on the Access Manager to be shared by the OAM Identity Assertion Provider (IAP), and the WebGate performing perimeter authentication on the webtier reverse proxy.

Note: If you are doing the configuration using the oamcfgtool scripted installation, this step is not required, as the installation script does it automatically.

To create an AccessGate entry:

1. Log in to the Access Server Console using your browser to navigate to:

   http://*host*:*port*/access/oblix

   Where *host* is the host ID of the server hosting the Access Manager (for example, oam.example.com), and *port* is the HTTP port number (for example, 8888).

2. Open the Access System Configuration page.
3. Click **Add New AccessGate** to create an AccessGate entry.
4. Click **List Access Servers** on the Details pane and bind the AccessGate to the Access Server that has been set up for OAM Single Sign-on.

Some of the settings specified here will be needed for WebGate installation and OAM Identity Assertion Provider (IAP) setup. Table 26–1 shows settings for a typical AccessGate entry.

Table 26–1 Sample Settings for AccessGate Entry

Setting	Value
AccessGate Name	webcenter-access-gate
Description	
State	Enabled

Table 26–1 (Cont.) Sample Settings for AccessGate Entry

Setting	Value
Hostname	webtier.example.com
Port	9010
Access Gate Password	<Not Displayed>
Debug	Off
Maximum user session time (seconds)	3600
Idle Session Time (seconds)	3600
Maximum Connections	1
Transport Security	Open
IPValidation	On
IPValidationException	
Maximum Client Session Time (hours)	24
Failover threshold	1
Access server timeout threshold	
Sleep For (seconds)	60
Maximum elements in cache	100000
Cache timeout (seconds)	1800
Impersonation username	
Impersonation password	<Not Displayed>
ASDK Client	
Access Management Service	On
Web Server Client	
Primary HTTP Cookie Domain	.example.com
Preferred HTTP Host	webtier.example.com:9010
Deny On Not Protected	Off
CachePragmaHeader	no-cache
CacheControlHeader	no-cache
LogOutURLs	

26.1.3.3 Install WebGate on the WebTier

This section describes how to install the WebGate.

To install the WebGate:

1. Copy the ZIP file (`Oracle_Access_Manager10_1_4_3_0_linux_GCClib.zip`) containing the

two gcc libraries required for the installation (libgcc_s.so.1 and libstdc++.so.5) to a /tmp directory.

2. Run the installation as root. For example, from the /tmp directory run:

   ```
   sudo -u root ./Oracle_Access_Manager10_1_4_3_0_linux_OHS11g_WebGate
   ```

3. Follow the installation runtime instructions, providing the installation directory, information of the AccessGate that you created earlier and the absolute path to the httpd.conf file of the web server. For example:

   ```
   WT_ORACLE_HOME/instances/<your_instance>/config/OHS/ohs1/httpd.conf
   ```

   Information for the AccessGate can be found in the Access System Console. For more information, see Section 26.1.3.2, "Create an AccessGate Entry."

4. After the installation a new section is inserted in the httpd.conf file between the following entries:

   ```
   #** BEGIN WEBGATE SPECIFIC ***
   #** END Oblix NetPoint Specific ***
   ```

   Check to see if the content is consistent with your environment.

26.1.4 Manually Configuring the Access System

To configure the Access System, you must add a host identifier:

1. Log in to the Access Server Console using your browser to navigate to:

   ```
   http://host:port/access/oblix
   ```

   Where *host* is the host ID of the server hosting the Access Manager (for example, oam.example.com), and *port* is the HTTP port number (for example, 8888).

2. Open the Access System Configuration page.

3. On the navigation pane, click **Host Identifiers**.

4. Add a host identifier for the webtier and enter the **Host Identifier name** (for example, webtier), a **Description**, and all **Hostname variations**. The hostname variations should include all the ways that a browser could issue a request to the webtier. For example, webtier and webtier.example.com if the webtier is using the default port; and additionally webtier:8080 and webtier.example.com:8080 if the webtier is not using the default port.

26.1.5 Manually Defining the WebCenter Policy Domain

This section describes the steps to set up the WebCenter Policy Domain that will configure the WebCenter application for OAM SSO authentication.

To configure the WebCenter Policy Domain:

1. Log in to the Access Server Console using your browser to navigate to:

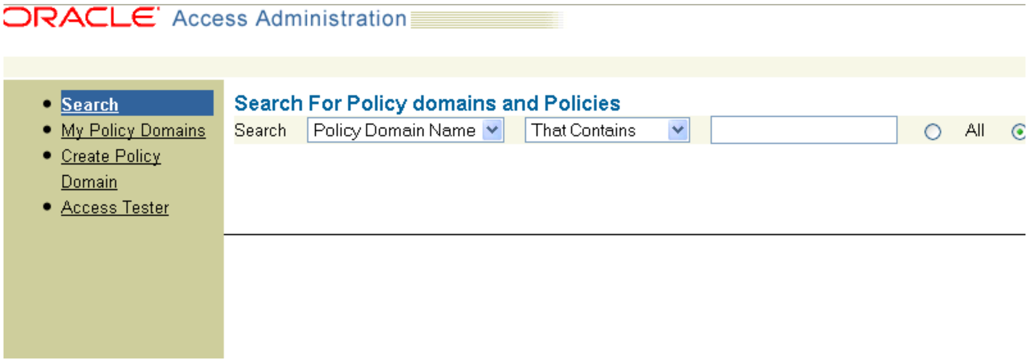
   ```
   http://host:port/access/oblix
   ```

   where *host* is the host ID of the server hosting the Access Manager (for example, oam.example.com), and *port* is the HTTP port number (for example, 8888).

2. Click **Policy Manager**.

   The Policy Manager pane displays (see Figure 26–2).

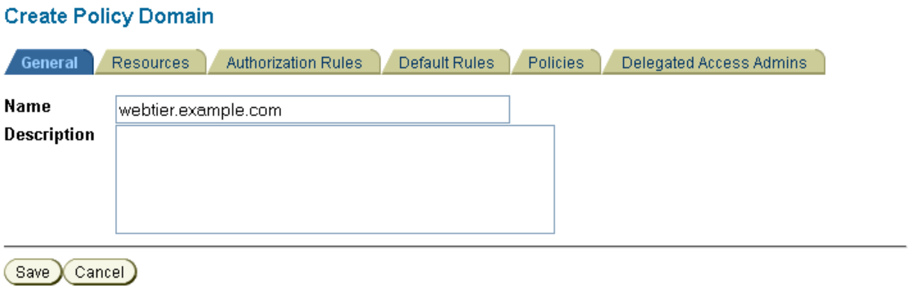
Figure 26–2 Policy Manager Pane



3. Click **Create Policy Domain** in the Navigation pane to create a policy domain to protect the WebCenter resources.

   The Create Policy Domain page displays (see Figure 26–3).

Figure 26–3 Create Policy Domain Page



Name: webtier.example.com

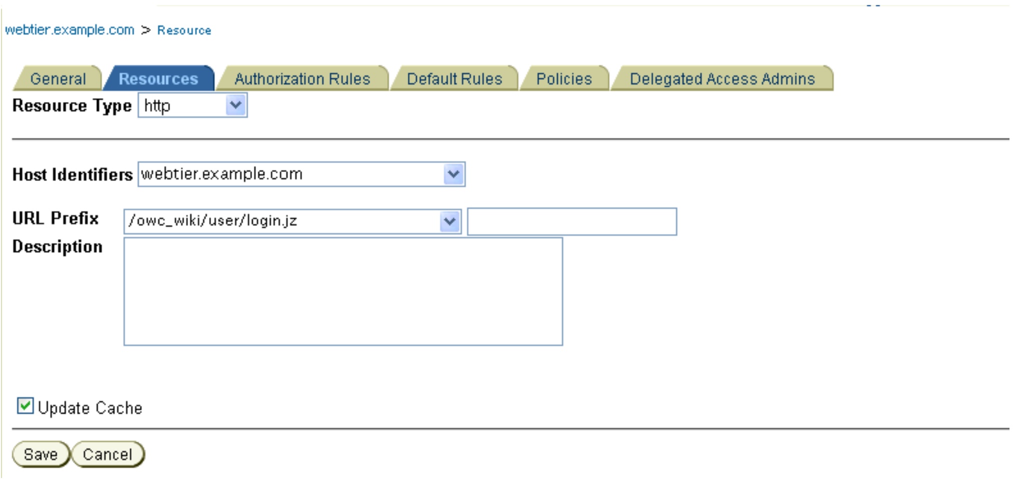
Description:

4. Enter a **Name** (for example, `webtier.example.com`) and **Description** for the policy domain and click **Save**.

5. Open the Resources tab and click **Add**.

   The Resource page displays (see Figure 26–4).

Figure 26–4 Policy Domain Resource Page



Resource Type: http

Host Identifiers: webtier.example.com

URL Prefix: /owc_wiki/user/login.jz

Description:

☑ Update Cache

6. 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 webtier.

   c. Enter the **URL Prefix** for the resources you want to protect. The following resources can be protected:

```
/adf.task-flow
/faces/adf.task-flow
/integration/worklistapp
/owc_discussions/login!withRedirect.jspa
/owc_discussions/login!default.jspa
/owc_discussions/login.jspa
/owc_discussions/admin
/owc_wiki/user/login.jz
/owc_wiki/acl
/owc_wiki/adfAuthentication
/owc_wiki/admin
/owc_wiki/attachments
/owc_wiki/default
/owc_wiki/domain
/owc_wiki/export
/owc_wiki/index_dir
/owc_wiki/install
/owc_wiki/js
/owc_wiki/layouts
/owc_wiki/macro
/owc_wiki/page
/owc_wiki/pages
/owc_wiki/remote
/owc_wiki/tags
/owc_wiki/templates
/owc_wiki/user
/owc_wiki/vhost
/owc_wiki/wp
/rss/rssservlet
/rest
/cmisrestprelim
/webcenter/adfAuthentication
/webcenter/content
```

```
/workflow/sdpmessagingsca-ui-worklist
/workflow/WebCenterWorklistDetail/faces
/workflow/sdpmessagingsca-ui-worklist
```

d. Enter a **Description** for the resource.

e. Ensure that **Update Cache** is selected, and then click **Save**.

f. Enter the **URL Prefix** for the context roots of the public resources. The following context roots should be added if the corresponding component is installed:

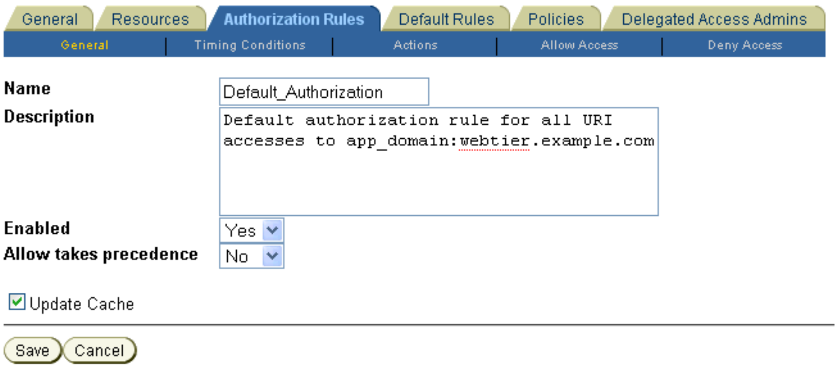
```
/owc_discussions
/owc_wiki
/rss
/webcenter
/workflow
```

7. Enter a **Description** for each context root, ensure that **Update Cache** is selected, and then click **Save**.

8. Open the Authorization Rules tab and click **Add**.

   The Authorization Rules page displays (see Figure 26–5).

Figure 26–5 Authorization Rules Page



Name	Default_Authorization
Description	Default authorization rule for all URI accesses to app_domain:webtier.example.com
Enabled	Yes
Allow takes precedence	No

☑ Update Cache

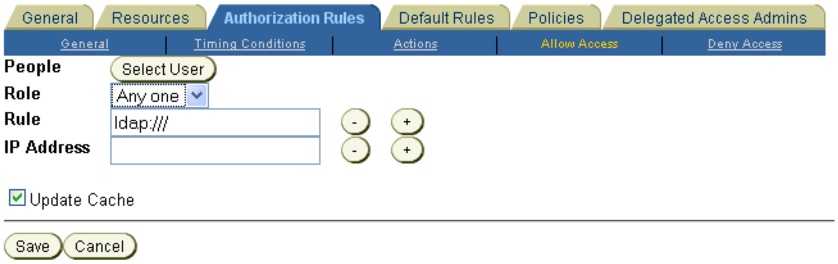
9. Enter a **Name** for the new rule (for example, `Default_Authorization`) and **Description**.

10. Select `Yes` for **Enabled**, and `No` for **Allow takes precedence**, and click **Save**.

11. Click **Allow Access** on the Authorization Rules tab and click **Add**.

    The Allow Access page displays (see Figure 26–6).

Figure 26–6 Allow Access Page



People

Role: Any one

Rule: ldap:///

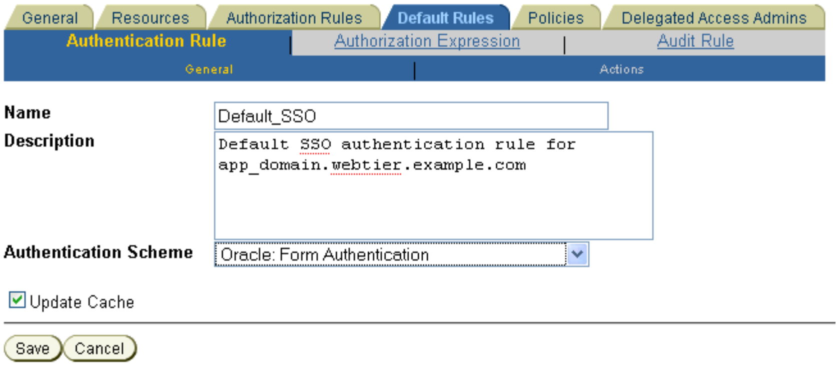
IP Address

☑ Update Cache

12. In the **Role** drop down list, select `Any one` and click **Save**.
13. Open the Default Rules tab and click **Add**.

    The Access Manager Authentication Rule page displays (see Figure 26–7).

Figure 26–7 Access Manager Authentication Rules Page



Name: Default_SSO

Description: Default SSO authentication rule for app_domain.webtier.example.com

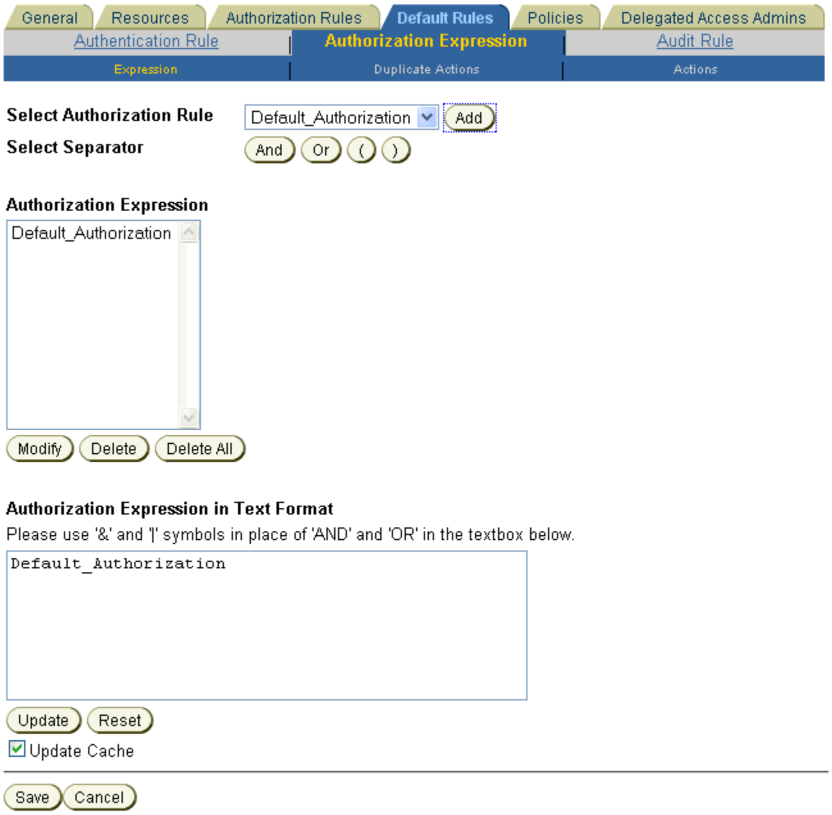
Authentication Scheme: Oracle: Form Authentication

☑ Update Cache

14. Enter a **Name** (for example, `Default_SSO`) and **Description** for the rule.
15. Set the **Authentication Scheme** to `Oracle: Form Authentication` (or a form-based authentication scheme that was previously created) and click **Save**.
16. Click **Authorization Expression** on the Default Rules tab, and click **Add**.

    The Authorization Expression page displays (see Figure 26–8).

Figure 26–8 Authorization Expression Page



Select Authorization Rule: Default_Authorization

Select Separator

Authorization Expression

Default_Authorization

Authorization Expression in Text Format

Please use '&' and '|' symbols in place of 'AND' and 'OR' in the textbox below.

```
Default_Authorization
```

☑ Update Cache

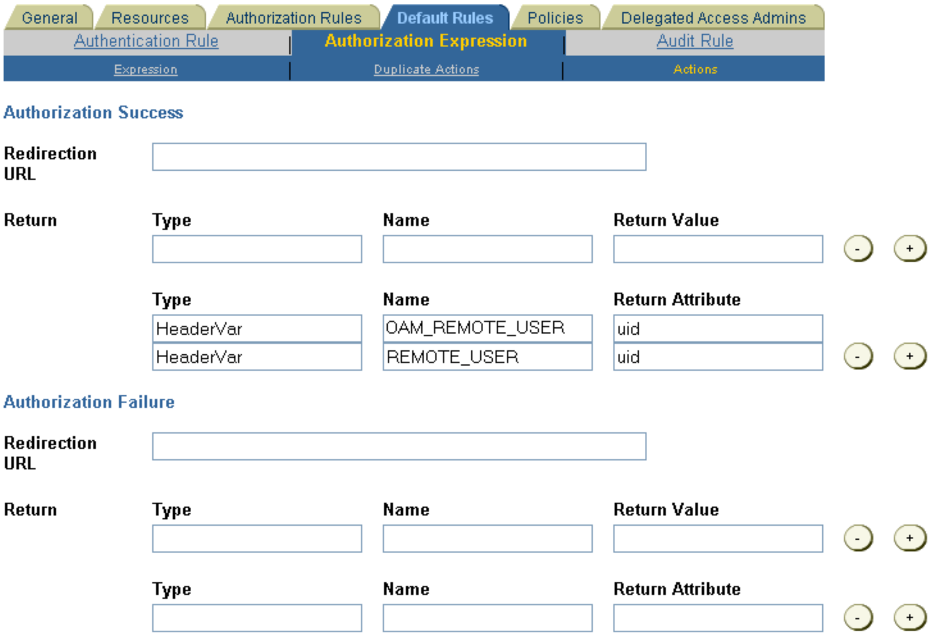
17. Add the `Default-Authorization` authorization rule (or the rule you created previously) to the Authorization Expression and click **Add** to add it to the Authorization Expression list.

18. Click **Save**.

19. Click **Actions** on the Authorization Expression subtab and click **Add**.

    The Actions page displays (see Figure 26–9).

Figure 26–9 Actions Page



Authorization Success

Redirection URL

Return

Type	Name	Return Value

Type	Name	Return Attribute
HeaderVar	OAM_REMOTE_USER	uid
HeaderVar	REMOTE_USER	uid

Authorization Failure

Redirection URL

Return

Type	Name	Return Value

Type	Name	Return Attribute

20. Under Authorization Success, specify what actions should be invoked when the authorization succeeds. Add two **Return Attribute** entries, specifying the **Return Type**, **Name** and **Return Attribute** as:

    - `HeaderVar`, OAM_REMOTE_USER, `uid`
    - `HeaderVar`, `REMOTE_USER`, `uid`

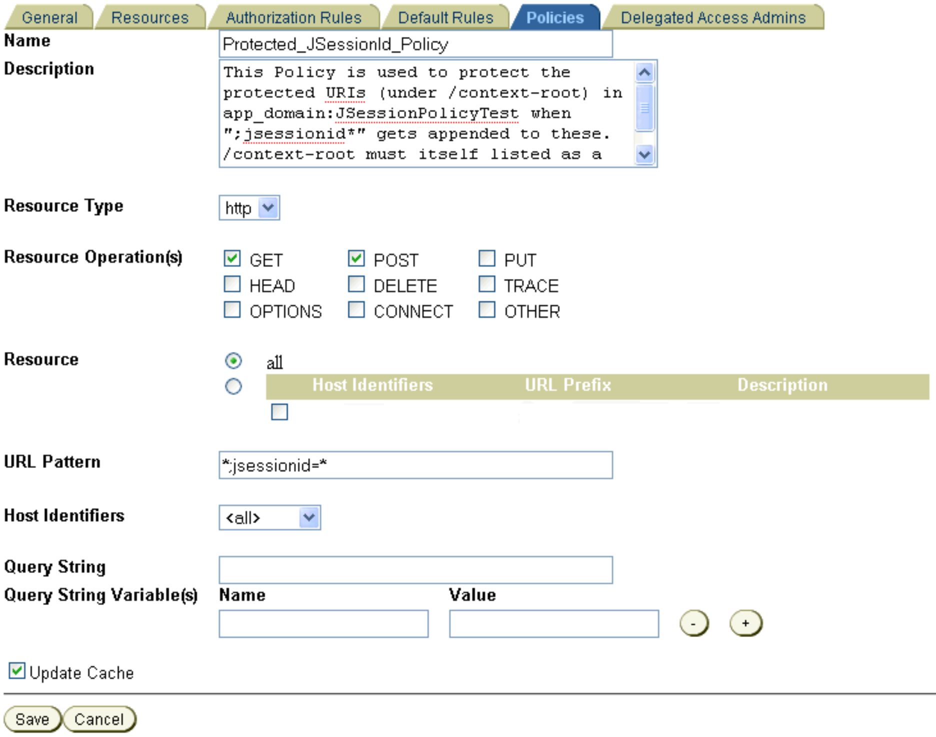
    > **Note:** Be careful not to put these values under the row for **Return Value**. The settings should be placed under **Return Attribute**.

21. Click **Save**.

22. Open the Policies tab and click **Add**.

    The Policies page displays (see Figure 26–10).

Figure 26–10 Policies Page



Name: Protected_JSessionId_Policy

Description:

```
This Policy is used to protect the
protected URIs (under /context-root) in
app_domain:JSessionPolicyTest when
";jsessionid*" gets appended to these.
/context-root must itself listed as a
```

Resource Type: http

Resource Operation(s): ☑ GET ☑ POST □ PUT □ HEAD □ DELETE □ TRACE □ OPTIONS □ CONNECT □ OTHER

Resource: ● all ○

	Host Identifiers	URL Prefix	Description
□			

URL Pattern: *;jsessionid=*

Host Identifiers: <all>

Query String:

Query String Variable(s): Name Value

☑ Update Cache

23. Use the settings below to add a new policy to protect protected URIs under `/context-root` in `app_domain:JSessionPolicyTest` when `;jsessionid*` is appended to them as shown in Figure 26–10. Note that `/context-root` must itself also be listed as a resource.

    - **Policy Name**: `Protected_JSessionId_Policy`
    - Description: This policy is used to protect protected URIs under /context-root in `app_domain:JSessionPolicyTest` when `;jsessionid*` is appended to them.
    - Resource Type: `http`
    - Resource Operation(s): `GET / POST`
    - Resource: Select `all`
    - URL Pattern: Enter `*;jsessionid=*`
    - Host Identifiers: Select the **Host Identifier** (the host identifier of the WebCenter webtier) to which to apply the policy (for example, `webtier.example.com`)

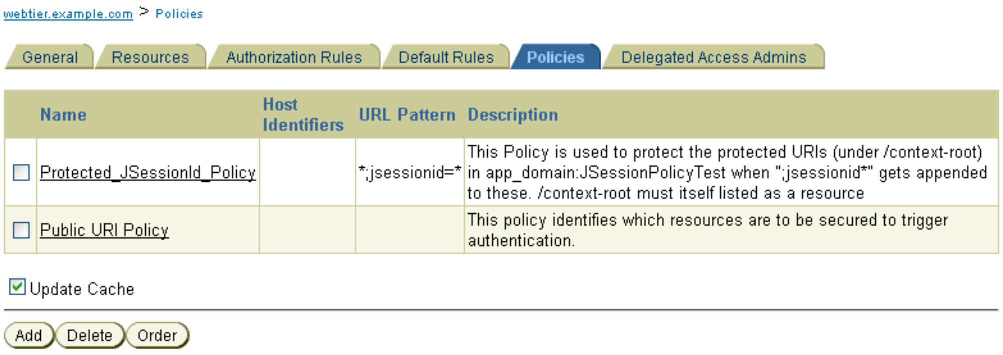
    The Authentication Rule and Authorization Expression settings under the corresponding tabs can be left as Default.

24. Click **Save**.

25. Open the Policies tab again.

    A list of policies for the current domain displays (see Figure 26–11).

Figure 26–11 Policies List



	Name	Host Identifiers	URL Pattern	Description
□	Protected_JSessionId_Policy		*;jsessionid=*	This Policy is used to protect the protected URIs (under /context-root) in app_domain:JSessionPolicyTest when ";jsessionid*" gets appended to these. /context-root must itself listed as a resource
□	Public URI Policy			This policy identifies which resources are to be secured to trigger authentication.

☑ Update Cache

26. Click **Add** and use the following settings to add the policy that will identify which resources are to be secured to trigger authentication.

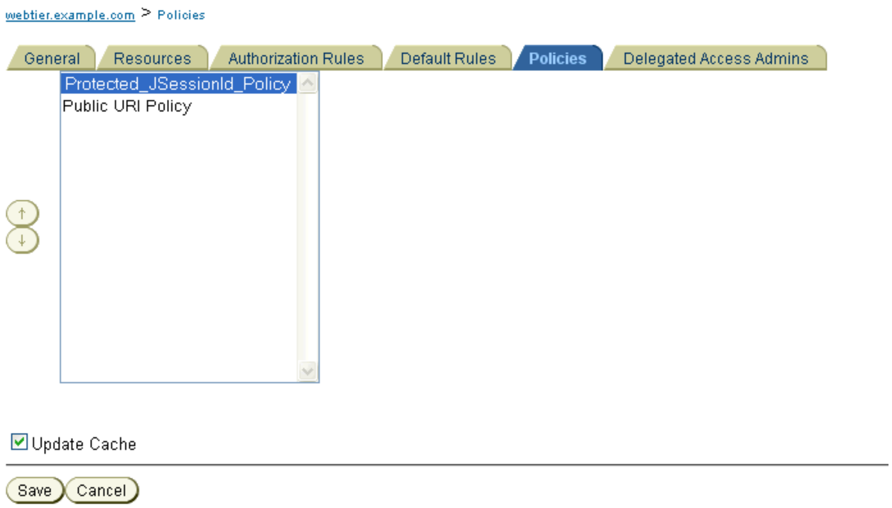
    - **Policy Name**: Enter a name (for example, `Public URI Policy`)
    - Description: Enter a description (for example "This policy identifies which resources are to be secured to trigger authentication.")
    - Resource Type: Select `http`.
    - Resource Operation(s): Select `GET / POST`.
    - Resource: Select the context roots you added in step 6. Note that /webcenter must always be selected.
    - Host Identifiers: Select the **Host Identifier** (the host identifier of the WebCenter webtier) to which to apply the policy (for example, `webtier.example.com`).

27. Click **Save**.

28. Open the Policies tab again and click **Order**.

    A tool you can use to set the order for policies currently defined for the domain displays (see Figure 26–12).

Figure 26–12 Order Tool



☑ Update Cache

29. Use the Order tool to ensure that `Protected_JSessionId_Policy` is at the top of the list.

30. Click **Save**.

26.1.6 Configuring the Policy Manager

This section includes the following subsections:

- Section 26.1.6.1, "Configuring the Oracle Internet Directory Authenticator"
- Section 26.1.6.2, "Configuring the OAM Identity Asserter"
- Section 26.1.6.3, "Configuring the Default Authenticator and Setting the Provider Order"
- Section 26.1.6.4, "Configuring the Application for Oracle Access Manager SSO"

26.1.6.1 Configuring the Oracle Internet Directory Authenticator

Assuming Oracle Internet Directory is backing the OAM identity store, an Oracle Internet Directory authenticator (`OracleInternetDirectoryAuthenticator`) should be configured for the LDAP server that is used as the identity store of OAM, and the provider should be set to `SUFFICIENT`.

To configure the Oracle Internet Directory authenticator:

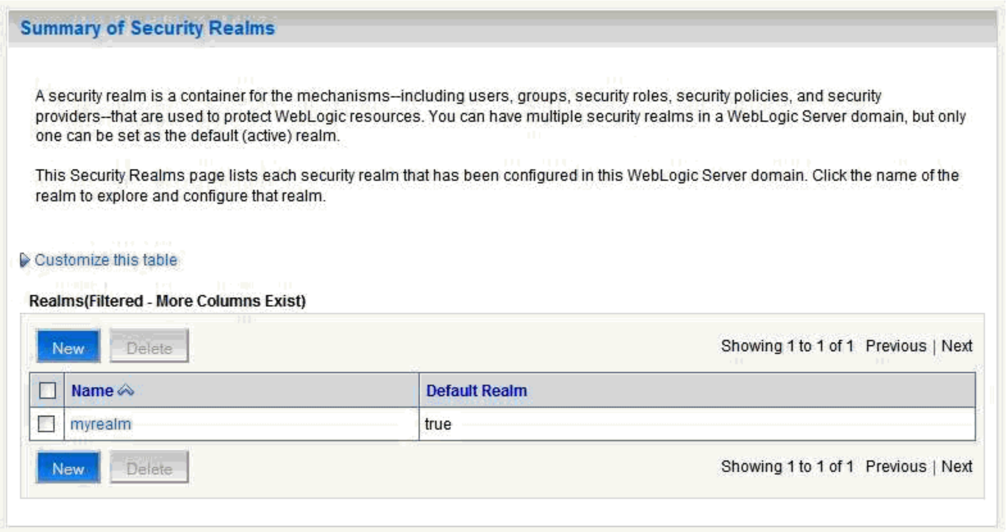
1. Log in to the WebLogic Server Administration Console.

   For information on logging in to the WebLogic Server Administration Console, see Section 1.12.2, "Oracle WebLogic Server Administration Console."

2. From the Domain Structure pane, click **Security Realms**.

   The Summary of Security Realms pane displays (see Figure 26–13).

Figure 26–13 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.

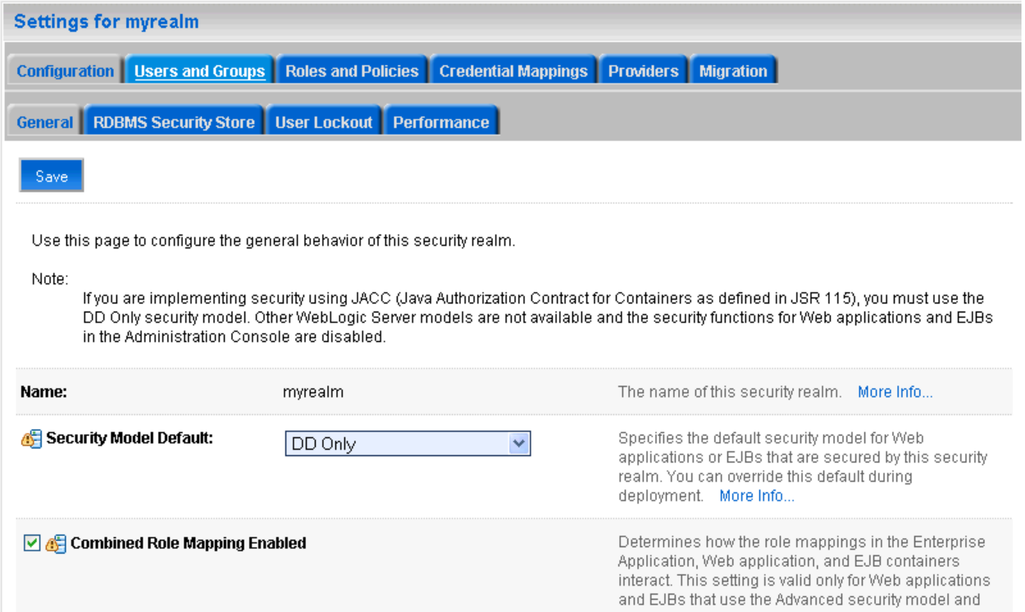
Realms(Filtered - More Columns Exist)

□	Name	Default Realm
□	myrealm	true

3. Click the realm entry for which to configure the OAM authenticator.

   The Settings pane for the realm displays (see Figure 26–14).

Figure 26–14 Settings Pane



Use this page to configure the general behavior of this security realm.

Note:

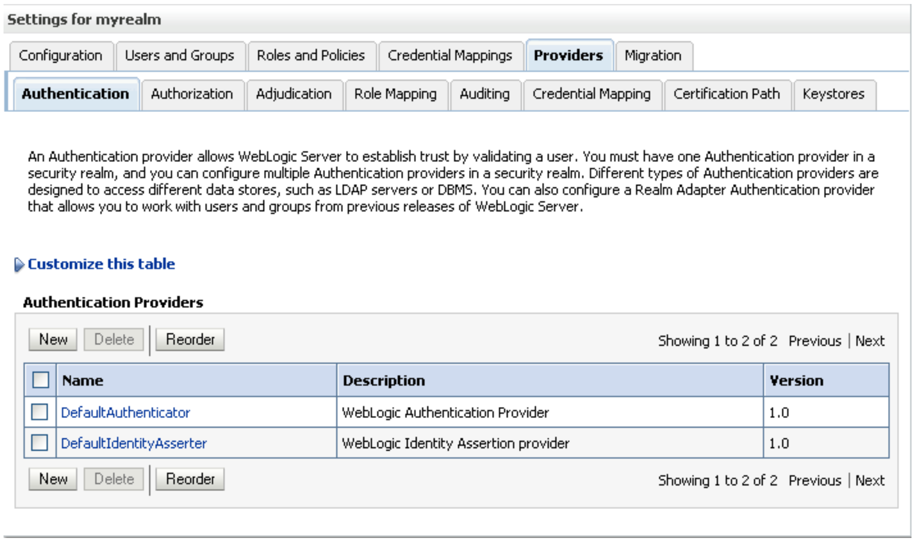
If you are implementing security using JACC (Java Authorization Contract for Containers as defined in JSR 115), you must use the DD Only security model. Other WebLogic Server models are not available and the security functions for Web applications and EJBs in the Administration Console are disabled.

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. Open the Providers tab.

   The Provider Settings display (see Figure 26–15).

Figure 26–15 Settings Pane - Providers



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.

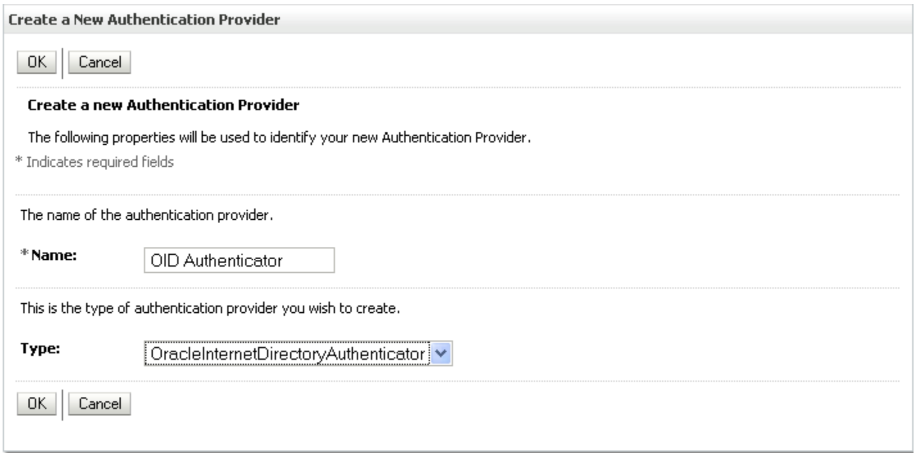
Authentication Providers

□	Name	Description	Version
□	DefaultAuthenticator	WebLogic Authentication Provider	1.0
□	DefaultIdentityAsserter	WebLogic Identity Assertion provider	1.0

5. Click **New** to create a provider.

   The Create a New Authentication Provider pane displays (see Figure 26–16).

Figure 26–16 Create a New Authentication Provider Pane



Create a New Authentication Provider

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:** OID Authenticator

This is the type of authentication provider you wish to create.

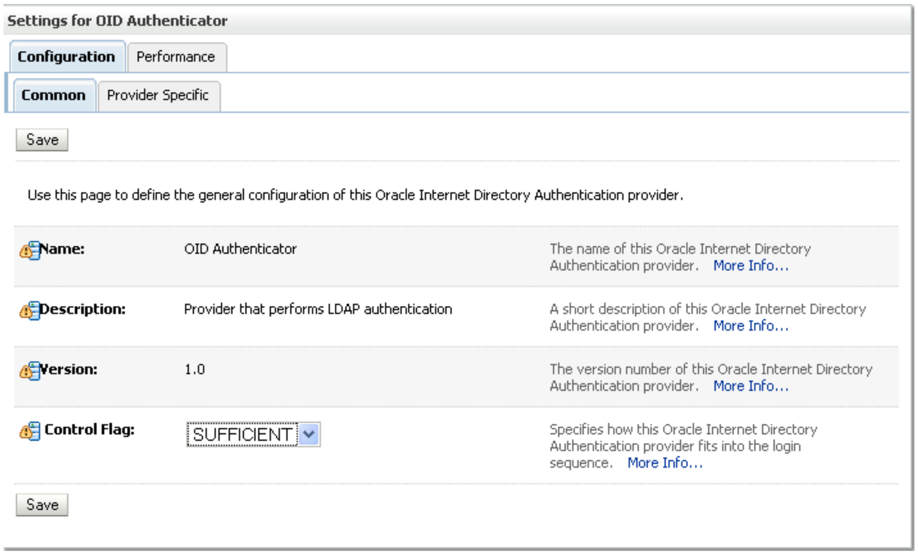
Type: OracleInternetDirectoryAuthenticator

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 26–17).

Figure 26–17 Common Settings Pane



Settings for OID Authenticator

Use this page to define the general configuration of this Oracle Internet Directory Authentication provider.

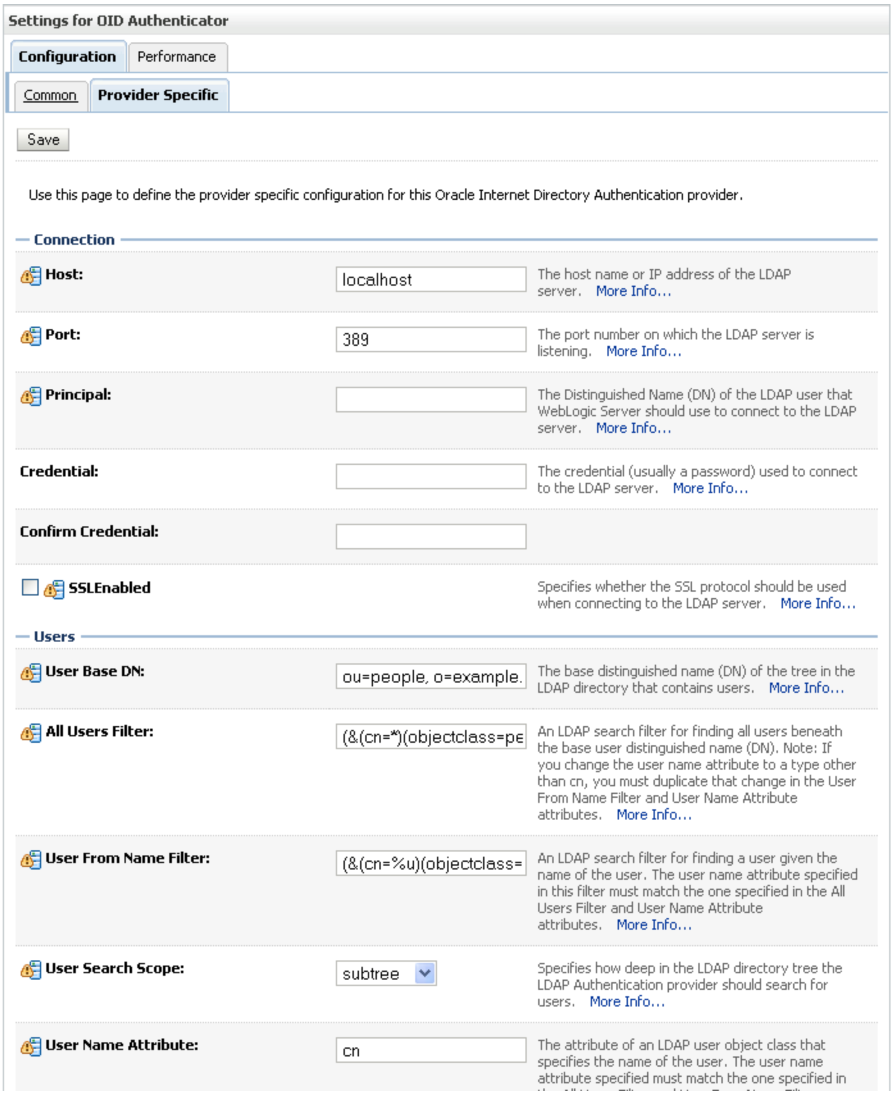
Name:	OID Authenticator	The name of this Oracle Internet Directory Authentication provider. More Info...
Description:	Provider that performs LDAP authentication	A short description of this Oracle Internet Directory Authentication provider. More Info...
Version:	1.0	The version number of this Oracle Internet Directory Authentication provider. More Info...
Control Flag:	SUFFICIENT	Specifies how this Oracle Internet Directory Authentication provider fits into the login sequence. More Info...

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 26–18).

Figure 26–18 Provider Specific Settings for OID Authenticator



Settings for OID Authenticator

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 would be same as #1.d in OAM Access Manager Setup

Field	Value	Comment
All Users Filter:	"(&(uid=*)(objectclass =person))"	
User Name Attribute:	"uid"	
Group Base DN:		Group search base - Same as User Base DN

11. Click **Save**.
12. Restart the WebCenter Administration Server and managed server and validate the configuration by navigating to the Realm Settings page in the WebLogic Server Administration Console and opening the Users and Groups tab.

26.1.6.2 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:

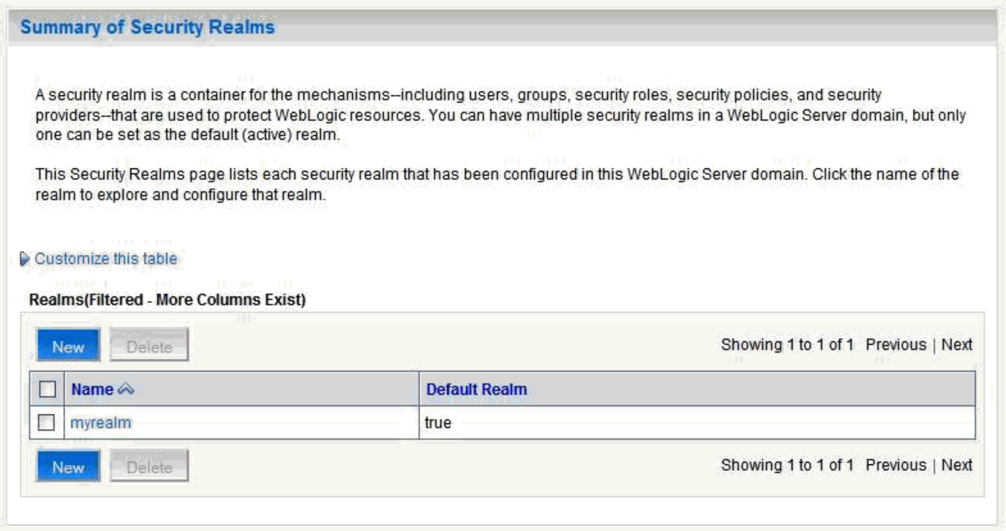
1. Log in to the WebLogic Server Administration Console.

   For information on logging in to the WebLogic Server Administration Console, see Section 1.12.2, "Oracle WebLogic Server Administration Console."

2. From the Domain Structure pane, click **Security Realms**.

   The Summary of Security Realms pane displays (see Figure 26–19).

Figure 26–19 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.

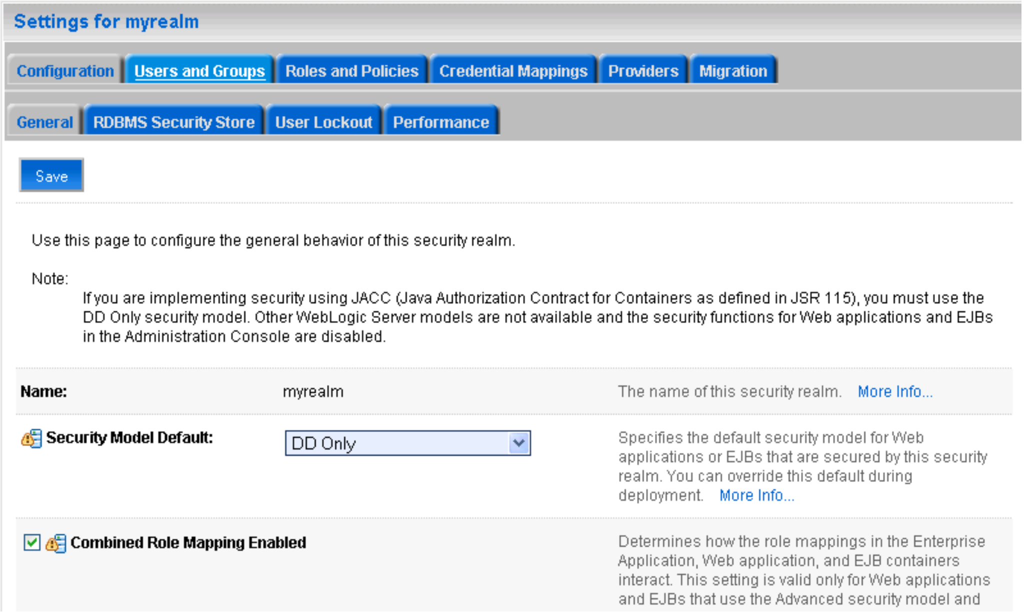
Realms(Filtered - More Columns Exist)

□	Name	Default Realm
□	myrealm	true

3. Click the realm entry for which to configure the OAM identity asserter.

   The Settings pane for the realm displays (see Figure 26–20).

Figure 26–20 Settings Pane



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...

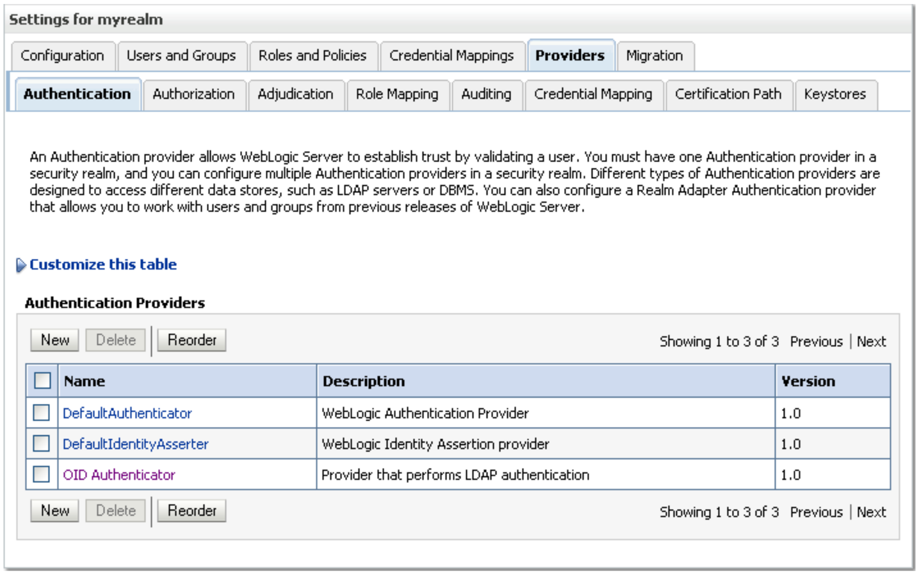
Security Model Default: DD Only — Specifies the default security model for Web applications or EJBs that are secured by this security realm. You can override this default during deployment. More Info...

☑ **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. Open the Providers tab.

   The Provider Settings display (see Figure 26–21).

Figure 26–21 Settings Pane - Providers



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.

Authentication Providers

Showing 1 to 3 of 3

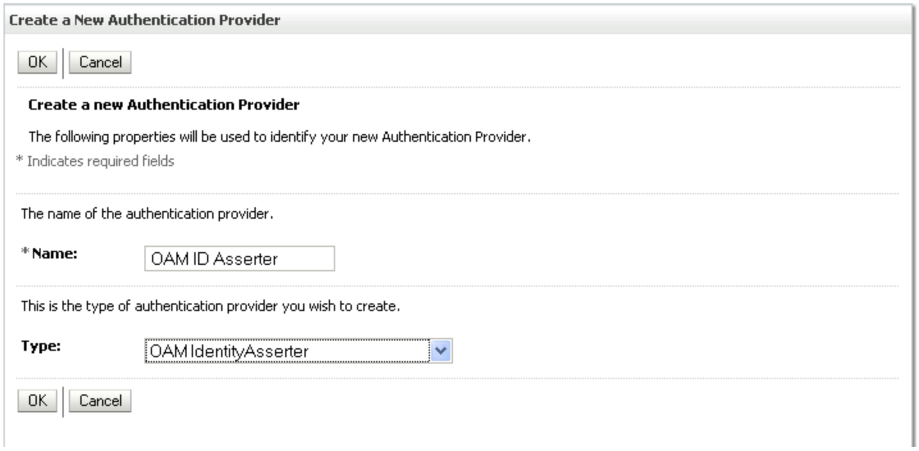
□	Name	Description	Version
□	DefaultAuthenticator	WebLogic Authentication Provider	1.0
□	DefaultIdentityAsserter	WebLogic Identity Assertion provider	1.0
□	OID Authenticator	Provider that performs LDAP authentication	1.0

Showing 1 to 3 of 3

5. Click **New** to create a provider.

   The Create a New Authentication Provider pane displays (see Figure 26–22).

Figure 26–22 Create a New Authentication Provider Pane



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:** OAM ID Asserter

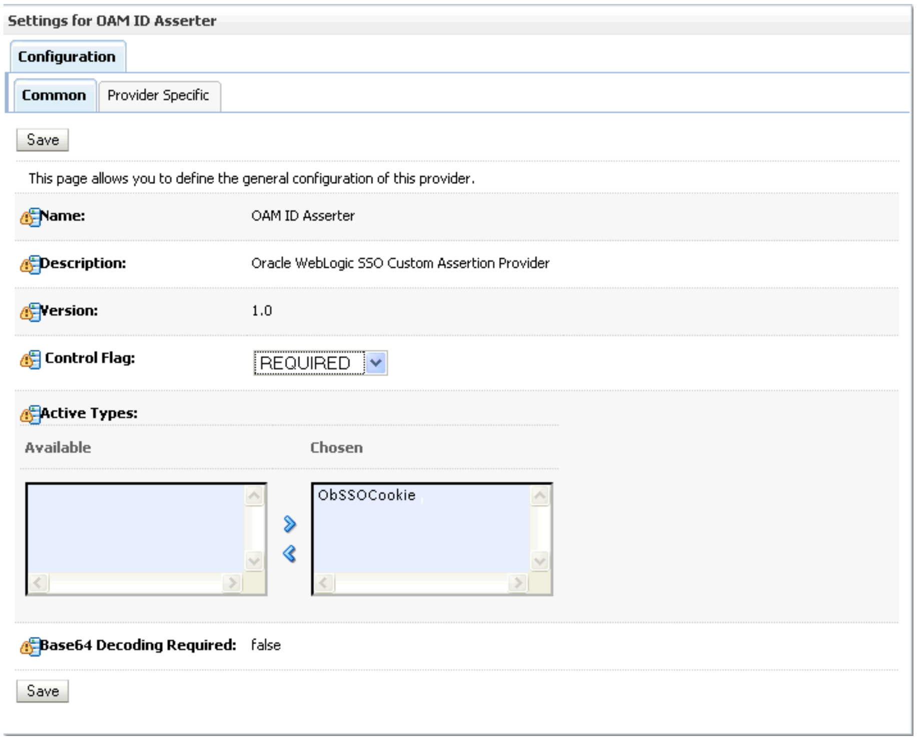
This is the type of authentication provider you wish to create.

Type: OAMIdentityAsserter

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 26–23).

Figure 26–23 Common Settings Pane



This page allows you to define the general configuration of this provider.

Name: OAM ID Asserter

Description: Oracle WebLogic SSO Custom Assertion Provider

Version: 1.0

Control Flag: REQUIRED

Active Types:

Available:

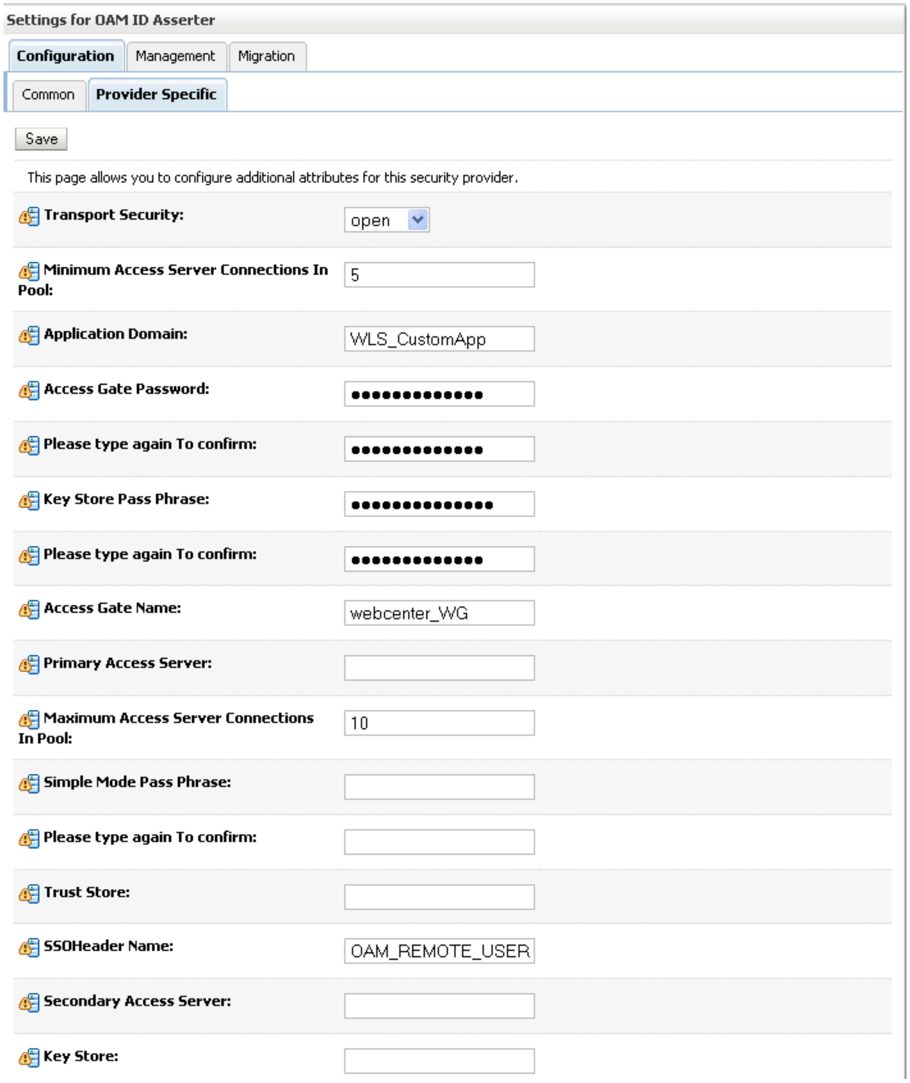
Chosen: ObSSOCookie

Base64 Decoding Required: false

8. Set the control flag to `REQUIRED` and check that `ObSSOCookie` is set for **Active Types**.
9. Click **Save**.
10. Open the Provider Specific tab.

The Provider Specific Settings pane for the OAMIdentityAsserter displays (see Figure 26–24).

Figure 26–24 Provider Specific Settings for the OAMIdentityAsserter



This page allows you to configure additional attributes for this security provider.

Transport Security:	open
Minimum Access Server Connections In Pool:	5
Application Domain:	WLS_CustomApp
Access Gate Password:	••••••••••••••
Please type again To confirm:	••••••••••••••
Key Store Pass Phrase:	•••••••••••••••
Please type again To confirm:	••••••••••••••
Access Gate Name:	webcenter_WG
Primary Access Server:	
Maximum Access Server Connections In Pool:	10
Simple Mode Pass Phrase:	
Please type again To confirm:	
Trust Store:	
SSOHeader Name:	OAM_REMOTE_USER
Secondary Access Server:	
Key Store:	

11. Complete the fields as shown in the table below. Leave the rest of the fields set to their default values.

Field	Value	Comment
Primary Access Server:		The OAM server endpoint information in HOST:PORT format
Access Gate Name:		Name of the Access Gate
Access Gate Password:		Provide the Access Gate password and confirm in the field below.

12. Click **Save** to save your settings.

26.1.6.3 Configuring the Default Authenticator and Setting the 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 26–21).
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

26.1.6.4 Configuring the Application for Oracle Access Manager SSO

Configure the applications for SSO by adding a setting to EXTRA_JAVA_PROPERTIES.

There is a system property that tells WebCenter and ADF that the application is configured in SSO mode and some special handling is required. The following system property is required in this mode:

Field	Value	Comment
oracle.webcenter.spaces.osso	true	This flag tells WebCenter 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. Add the property to the EXTRA_JAVA_PROPERTIES variable, as follows:

```
EXTRA_JAVA_PROPERTIES="-Dweblogic.security.SSL.ignoreHostnameVerification=true
-Doracle.mds.bypassCustRestrict=true
-Djps.update.subject.dynamic=true -Doracle.webcenter.spaces.osso=true
-noverify ${EXTRA_JAVA_PROPERTIES}"
```

After making this change, restart the following servers:

- WebCenter's Administration Server
- All the domain's managed servers
- WebTier OHS

26.1.7 Additional Configurations

The configurations described in the following sections may be necessary or helpful in providing additional security for your site:

- Section 26.1.7.1, "Configuring the WebLogic Server Administration Console and Enterprise Manager"
- Section 26.1.7.2, "Configuring the Discussions Server for SSO"

- Section 26.1.7.2.1, "Creating a Discussions Server Connection for WebCenter Spaces"
- Section 26.1.7.3, "Configuring the Wiki Server"
- Section 26.1.7.4, "Restricting Access with Connection Filters"

26.1.7.1 Configuring the WebLogic Server Administration Console and Enterprise Manager

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 Access Server Console using your browser to navigate to:

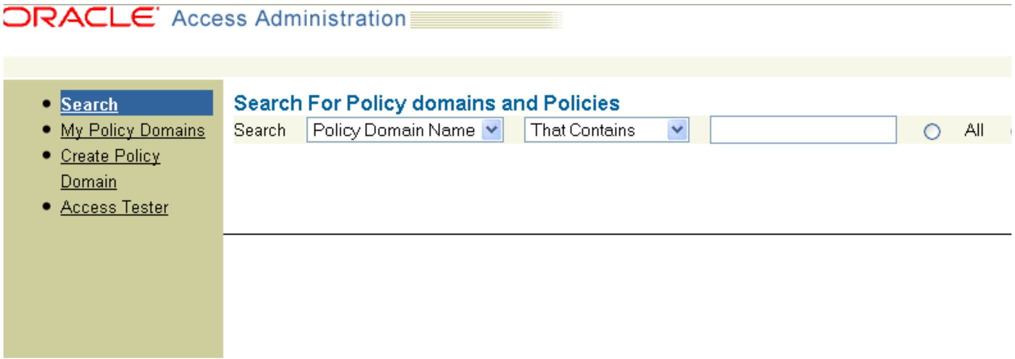
   ```
   http://host:port/access/oblix
   ```

   Where *host* is the host ID of the server hosting the Access Manager (for example, `oam.example.com`), and *port* is the HTTP port number (for example, `8888`).

2. Click **Policy Manager**.

   The Policy Manager pane displays (see Figure 26–25).

Figure 26–25 Policy Manager Pane

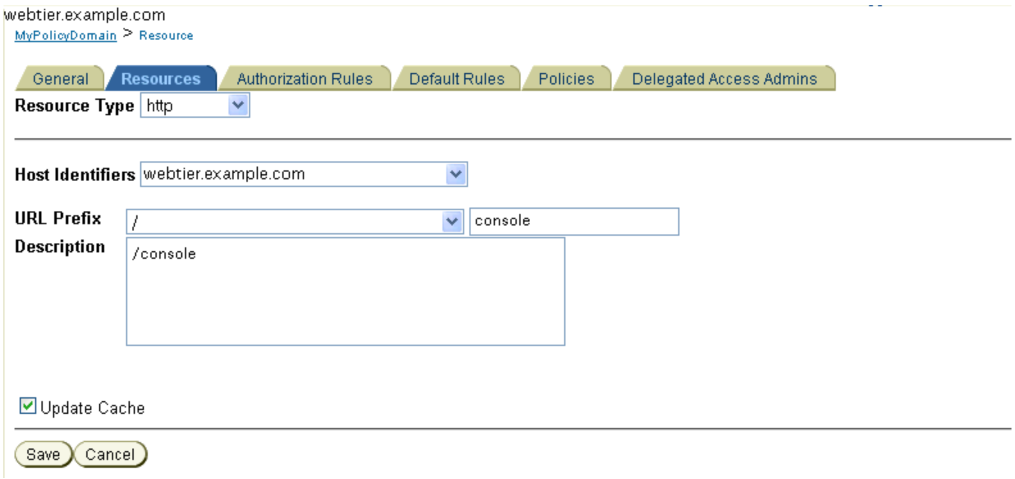


3. Search for the policy domain that you created earlier to protect WebCenter resources in Section 26.1.5, "Manually Defining the WebCenter Policy Domain."

4. Open the Resources tab and click **Add**.

   The Resource page displays (see Figure 26–26).

Figure 26–26 Policy Domain Resource Page



webtier.example.com

MyPolicyDomain > Resource

Resource Type: http

Host Identifiers: webtier.example.com

URL Prefix: / console

Description: /console

☑ Update Cache

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 webtier.
   c. Enter the **URL Prefix** for the WebLogic Server Administration Console or Enterprise Manager.
   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, using the actual host ID for the WebCenter Administration Server for `WebLogicHost`.

```
<IfModule mod_weblogic.c>
  MatchExpression  /webcenter
WebLogicHost=example.com|WebLogicPort=8888
  MatchExpression  /rss
WebLogicHost=example.com|WebLogicPort=8888
  MatchExpression  /owc_wiki
WebLogicHost=example.com|WebLogicPort=8890
  MatchExpression  /owc_discussions
WebLogicHost=example.com|WebLogicPort=8890
  MatchExpression /rest
WebLogicHost=example.com|WebLogicPort=8888
  MatchExpression /cmisrestprelim
WebLogicHost=example.com|WebLogicPort=8888
  MatchExpression  /console
WebLogicHost=example.com|WebLogicPort=7001
  MatchExpression  /em
WebLogicHost=example.com|WebLogicPort=7001
</IfModule>
```

7. Restart the Oracle HTTP Server for your changes to take effect.

   You should now be able to access the 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.

26.1.7.2 Configuring the Discussions Server for SSO

This section describes how to configure Oracle WebCenter Discussions 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 WebCenter Spaces, as described in Section 24.1, "Reassociating the Identity Store with an External LDAP." If you've chosen not to move the default administrator account to an external LDAP, be sure to also follow the instructions in Section 24.5.1, "Migrating the WebCenter Discussions Server to Use an External LDAP."

To set up the discussions server for SSO:

1. Log in to the Oracle WebCenter Discussions Server Admin Console at:

   ```
   http://host:port/owc_discussions/admin
   ```

   Where *host* and *port* are the host ID and port number of the `WLS_Services` managed server.

2. Open the System Properties page and edit (if it already exists) or add the `owc_discussions.sso.mode` property, setting it's value to `true`.

3. Edit or add the `jiveURL` property to point to the base URL of the SSO server. For example:

   ```
   jiveURL = example.com:8890/owc_discussions
   ```

26.1.7.2.1 Creating a Discussions Server Connection for WebCenter Spaces

To create a discussions server connection for WebCenter Spaces:

1. Log in to Fusion Middleware Control and select the WebLogic domain for WebCenter Spaces.

   For information on logging in to Fusion Middleware Control, see Section 6, "Starting Enterprise Manager Fusion Middleware Control."

2. In the Navigation pane, open the WebCenter node, and then the WebCenter Spaces node, and click `WebCenter Spaces (WLS_Spaces).`

3. Register the discussion server as described in Section 12.3.1, "Registering Discussions Servers Using Fusion Middleware Control."

   For **Server URL**, enter `http://<host>:<port>/owc_discussions .`

4. Restart the `WLS_Spaces` managed server.

   When you log in to WebCenter Spaces, you automatically sign on to the discussion server as well.

26.1.7.3 Configuring the Wiki Server

Wiki page functionality is supported as an iFrame, which you can embed in a Web page, and OAM single sign-on is supported this way. Since the Oracle WebCenter Wiki and Blog Server does not require or support an identity store, there is no need to configure the LDAP.

To add a wiki page to a WebCenter identity store, follow the steps below:

1. Log in to WebCenter Spaces, and open a group space.
2. Add a page, choosing `Web Page` as the **Style**.
3. When the page is created, click the **Edit** icon.

   The Component properties dialog displays.
4. Enter the following URL in the **Source** box:

   ```
   http://host:OHS
   port/owc_wiki/page/show.jz?inline=1&scope=#{communityContext.communityName}
   ```

   Where *`host`* is the host ID of the `WLS_Spaces` server, and *`OHS_port`* is the port number of the Oracle HTTP Server. The OHS port is used so the call goes through the WebGate which initiates SSO.

   After specifying the component properties you see the wiki page contents.
5. Save the changes.

26.1.7.4 Restricting Access with Connection Filters

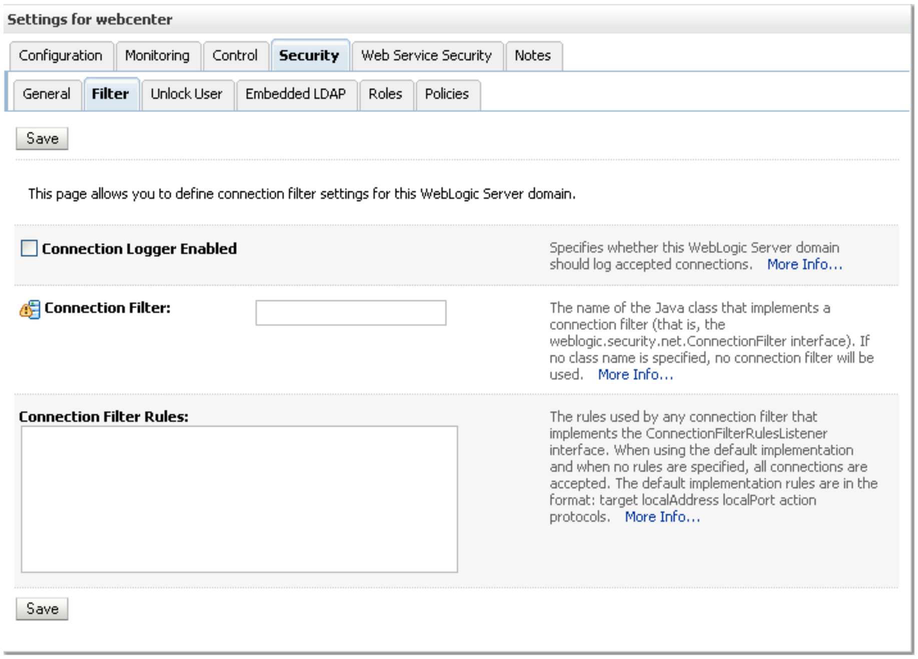
Follow the steps below to only allow users to access WebCenter and other services through the WebTier OHS ports so that they can be properly authenticated.

1. Log in to the WebLogic Server Administration Console.

   For information on logging in to the WebLogic Server Administration Console, see Section 1.12.2, "Oracle WebLogic Server Administration Console."
2. In the Domain Structure pane, select the domain you want to configure (for example, `webcenter`).
3. Open the Security tab and the Filter subtab.

   The Security Filter Settings pane displays (see Figure 26–27).

Figure 26–27 Security Filter Settings Page



Settings for webcenter

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...

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 through the OHS port:

   ```
   http://host:OHS_port/webcenter
   ```

26.2 Configuring Oracle Single Sign-On (OSSO)

In a default installation, WebCenter uses the HTTP ports in the Managed Server created for WebCenter. To configure WebCenter with Oracle Single Sign-On, WebCenter needs Oracle HTTP Server and the associated Module `mod_osso` to integrate with Oracle Single Sign-On (OSSO).

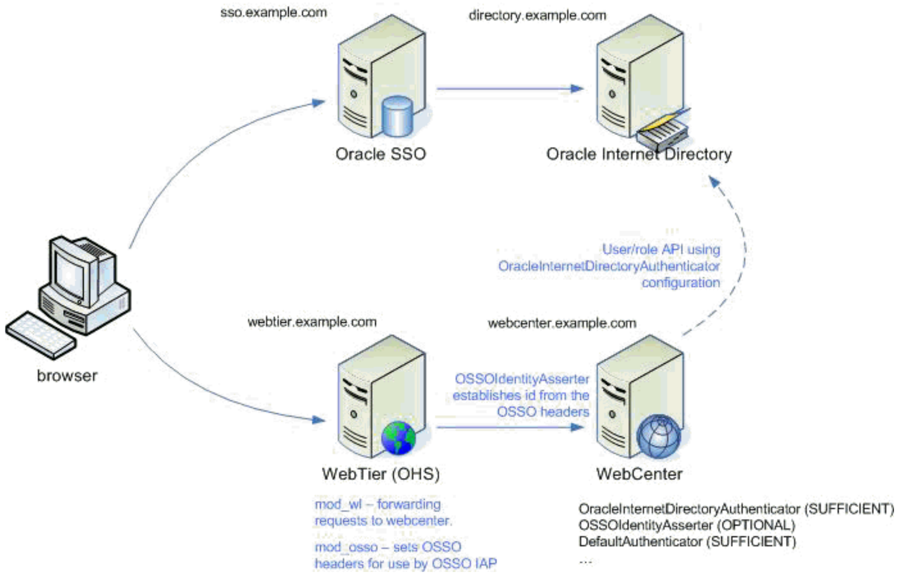
> **Note:** The BPEL Console does not support SSO integration. When WebCenter is configured for SSO, login to BPEL must still be done through the standard login page on the BPEL Console.

This section includes the following subsections

26.2.1 OSSO Components and Topology

In a default installation, WebCenter uses the HTTP ports of the Managed Server created for WebCenter. To configure WebCenter with Oracle Single Sign-On, WebCenter needs the Oracle HTTP Server and the associated Module `mod_osso`, to integrate with Oracle SSO. The diagram below (Figure 26–28) shows the overall architecture of this integration:

Figure 26–28 OSSO Components and Topology



26.2.2 Configuring the Oracle HTTP Server and Associated mods

This section describes how to load and configure the Oracle HTTP Server and associated mods.

To load and configure the Oracle HTTP Server and associated mods:

1. Install the WebTier, which contains Oracle HTTP Server (OHS) and associated mods (`mod_osso` and `mod_wl`).

2. Configure the module `mod_wl` in WebTier OHS so that it forwards requests to the Oracle WebLogic Server for WebCenter.

   Uncomment the lines at `WT_ORACLE_HOME/instances/<your_instance>/config/OHS/ohs1/mod_wl_ohs.conf`. This file is included by the `httpd.conf` file and looks like the following:

   ```
   LoadModule weblogic_module   WT_ORACLE_HOME/ohs/modules/mod_wl_ohs.so
   <IfModule mod_weblogic.c>
   ```

```
MatchExpression /webcenter WebLogicHost=webcenter.example.com|WebLogicPort=8888
MatchExpression /rss WebLogicHost=webcenter.example.com|WebLogicPort=8888
MatchExpression /owc_wiki WebLogicHost=webcenter.example.com|WebLogicPort=8890
MatchExpression /owc_discussions
WebLogicHost=webcenter.example.com|WebLogicPort=8890
MatchExpression /workflow WebLogicHost=soa.example.com|WebLogicPort=8888
MatchExpression /integration WebLogicHost=soa.example.com|WebLogicPort=8888
MatchExpression /rest WebLogicHost=webcenter.example.com|WebLogicPort=8888
MatchExpression /cmisrestprelim
WebLogicHost=webcenter.example.com|WebLogicPort=8888
</IfModule>
```

26.2.3 Configuring the OSSOIdentityAsserter

Include the OSSO Identity Assertion Provider (IAP) provider in the Oracle WebLogic domain for WebCenter. Use the WebLogic Server Administration Console to add the OSSO IAP to your domain as shown in the steps below.

To configure the OSSOIdentityAsserter:

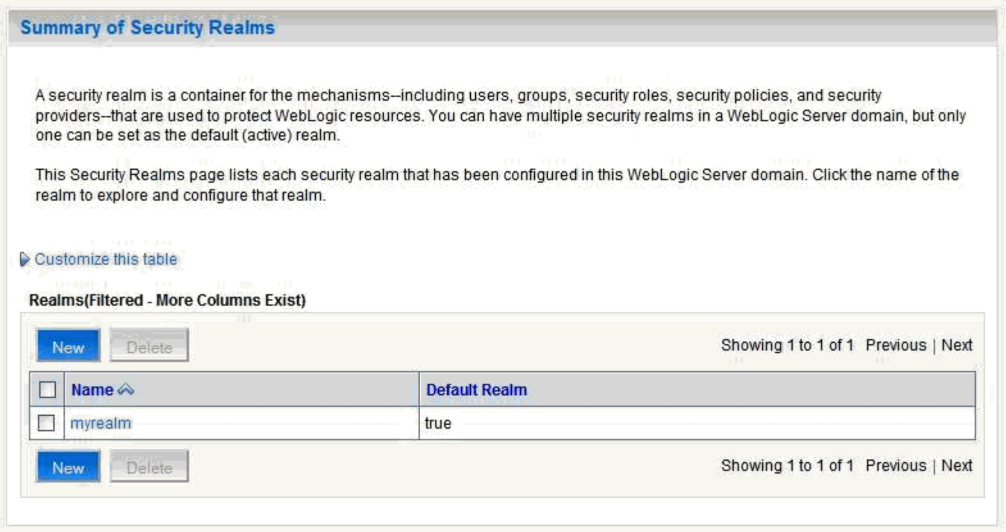
1. Log in to the WebLogic Server Administration Console.

   For information on logging in to the WebLogic Server Administration Console, see Section 1.12.2, "Oracle WebLogic Server Administration Console."

2. From the Domain Structure pane, click **Security Realms**.

   The Summary of Security Realms pane displays (see Figure 26–29).

Figure 26–29 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.

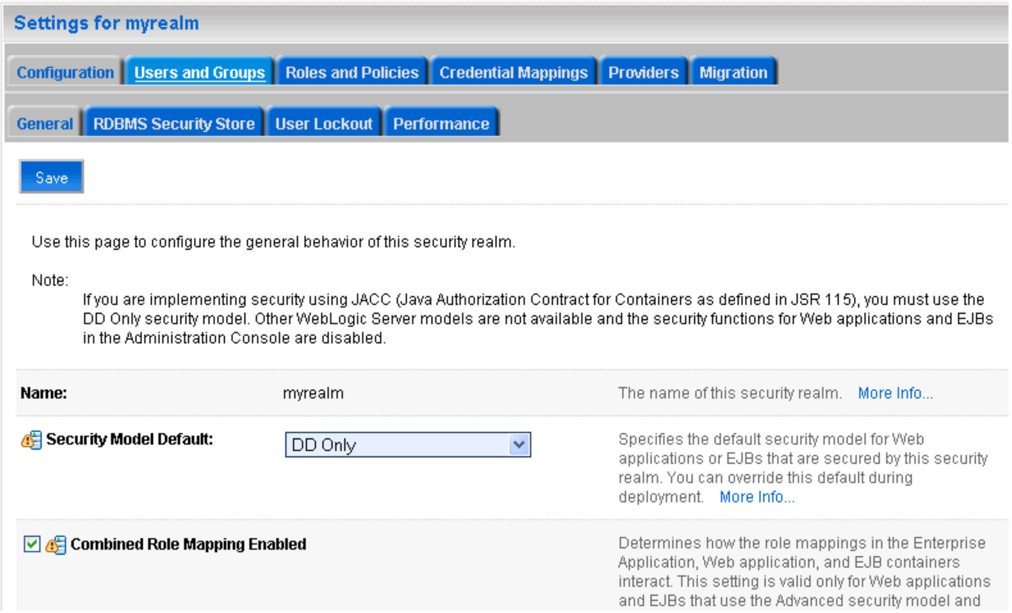
Realms(Filtered - More Columns Exist)

□	Name	Default Realm
□	myrealm	true

3. Click the realm entry to which to add the provider.

   The Settings pane for the realm displays (see Figure 26–30).

Figure 26–30 Settings Pane



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...

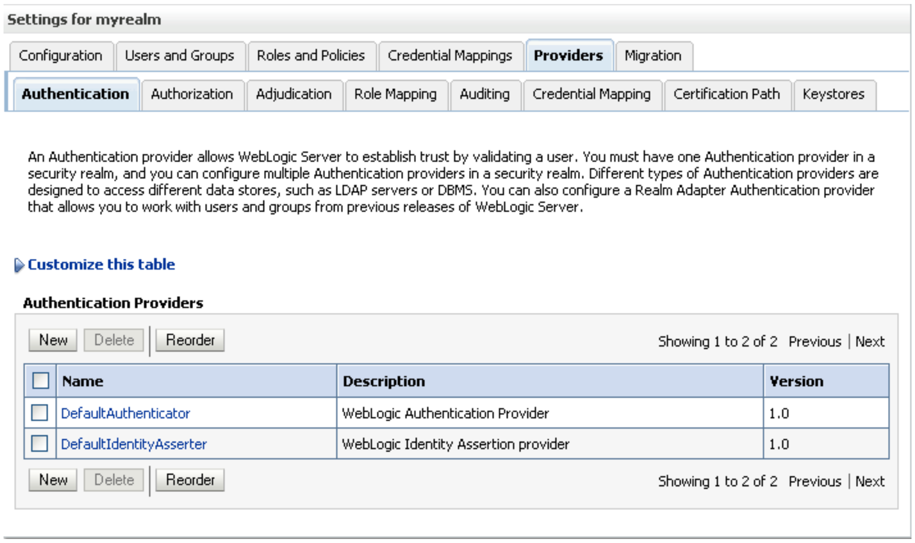
Security Model Default: DD Only — Specifies the default security model for Web applications or EJBs that are secured by this security realm. You can override this default during deployment. More Info...

☑ **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 26–31).

Figure 26–31 Settings Pane - Providers



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.

Authentication Providers

Showing 1 to 2 of 2

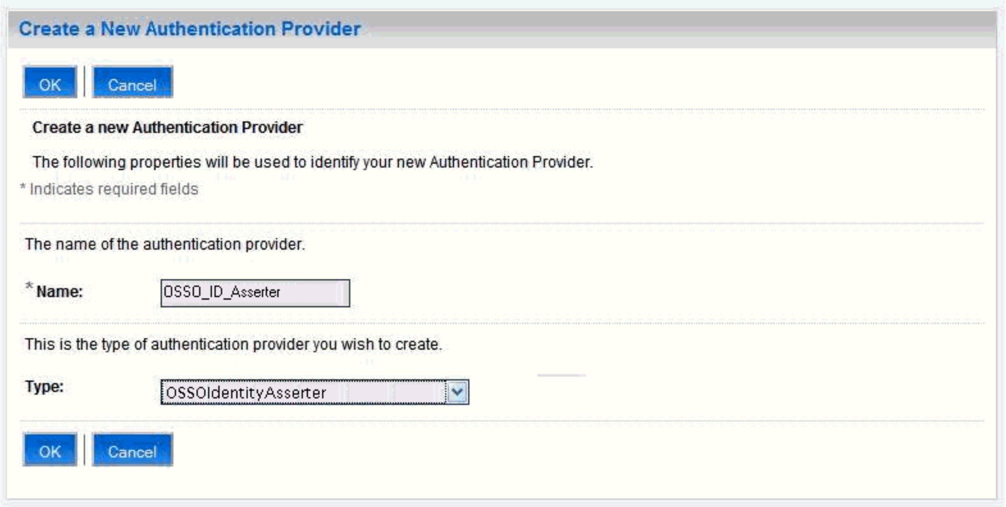
□	Name	Description	Version
□	DefaultAuthenticator	WebLogic Authentication Provider	1.0
□	DefaultIdentityAsserter	WebLogic Identity Assertion provider	1.0

Showing 1 to 2 of 2

5. Click **New** to create a provider.

   The Create a New Authentication Provider pane displays (see Figure 26–32).

Figure 26–32 Create a New Authentication Provider Pane



Create a New Authentication Provider

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: OSSO_ID_Asserter

This is the type of authentication provider you wish to create.

Type: OSSOIdentityAsserter

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 24, "Configuring the Identity Store."

   For OID, the provider list should appear as follows:

   - **OracleInternetDirectoryAuthenticator** (`SUFFICIENT`)
   - **OSSOIdentityAsserter** (`OPTIONAL`)
   - **DefaultAuthenticator** (`SUFFICIENT`)
   - **DefaultIdentityAsserter** (`OPTIONAL`)

   Also ensure that the default `jpsContext` in WebCenter's `jps-config.xml` file is set to the `idstore.ldap` serviceInstance.

26.2.4 Registering OHS with Oracle SSO

Register the module `mod_osso` in the WebTier OHS with the SSO Server as a partner application by following the steps below.

To register OHS with Oracle SSO:

1. Run `ssoreg` from the SSO server to generate an `osso.conf` file and manually copy it to the partner application (*`WT_ORACLE_HOME`*).

   The following example shows how you would register a remote partner application on a SSO Server. Note that *`ORACLE_HOME`* here is the *`ORACLE_HOME`* of the OSSO installation on the SSO server.

```
bash-3.00$ ORACLE_HOME/sso/bin/ssoreg.sh -site_name
webtier.example.com:80 -config_mod_osso TRUE -mod_osso_url
```

```
http://webtier.example.com -remote_midtier  -config_file
webtier.example.com.osso.conf
```

Running this command creates a `webtier.example.com.osso.conf` file.

2. Copy the `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. Add a static rule to the `mod_osso.conf` file to protect the `/webcenter` URL with Oracle SSO.

   The `mod_osso.conf` file should look similar to this:

```
LoadModule osso_module WT_ORACLE_HOME/ohs/modules/mod_osso.so
 <IfModule mod_osso.c>
    OssoIpCheck off
    OssoIdleTimeout off
    OssoSecureCookies Off

    # whatever the location of your real osso.conf file is, that was generated
from the ssoreg.sh command.
    OssoConfigFile /OracleWebTier/webtier.example.com.osso.conf

#______-
# Notes
#______-
# 1. Here's what you need to add to protect a resource,
#    e.g. <ApacheServerRoot>/htdocs/private:
# 2. if an application is protected by SSO then no matter what Apache will
always
#    send no-cache headers practically undoing whatever the Apache
configuration or
#    the ADF faces Cache library do. To allow caching for SSO protected
resources
#    add "OssoSendCacheHeaders off " as following.

    <Location /webcenter/adfAuthentication*>
      OssoSendCacheHeaders off
      require valid-user
      AuthType Osso
    </Location>
    <Location /owc_wiki/user/login.jz>
      OssoSendCacheHeaders off
      require valid-user
      AuthType Osso
    </Location>
    <Location /rss/rssservlet>
      OssoSendCacheHeaders off
      require valid-user
      AuthType Osso
    </Location>
    <Location /owc_discussions/login!withRedirect.jspa>
      OssoSendCacheHeaders off
      require valid-user
      AuthType Osso
    </Location>
    <Location /owc_discussions/login!default.jspa>
```

```
      OssoSendCacheHeaders off
      require valid-user
      AuthType Osso
    </Location>
    <Location /owc_discussions/login.jspa>
      OssoSendCacheHeaders off
      require valid-user
      AuthType Osso
    </Location>
    <Location /owc_discussions/admin>
      OssoSendCacheHeaders off
      require valid-user
      AuthType Osso
    </Location>
    <Location /owc_wiki/adfAuthentication>
      OssoSendCacheHeaders off
      require valid-user
      AuthType Osso
    </Location>
    <Location /integration/worklistapp>
      OssoSendCacheHeaders off
      require valid-user
      AuthType Osso
    </Location>
    <Location /workflow/WebCenterWorklistDetail>
      OssoSendCacheHeaders off
      require valid-user
      AuthType Osso
    </Location>
    <Location /workflow/sdpmessagingsca-ui-worklist>
      OssoSendCacheHeaders off
      require valid-user
      AuthType Osso
    </Location>
    <Location /rest>
      OssoSendCacheHeaders off
      require valid-user
      AuthType Osso
    </Location>
    <Location /cmisrestprelim>
      OssoSendCacheHeaders off
      require valid-user
      AuthType Osso
    </Location>
</IfModule>
#
# If you would like to have short hostnames redirected to
# fully qualified hostnames to allow clients that need
# authentication via mod_osso to be able to enter short
# hostnames into their browsers uncomment out the following
# lines
#
#PerlModule Apache::ShortHostnameRedirect
#PerlHeaderParserHandler Apache::ShortHostnameRedirect
```

Ensure that you change the **`OssoConfigFile`** parameter to point to the location (and filename if you've changed it) of your `osso.conf` file.

4. Restart the WebTier so that the configuration changes to `mod_osso` and `mod_wl` to take effect.

5. For the Worklist service changes to take effect, run the following command on the WebCenter Administration server:

   ```
   setBPELConnection('webcenter','WebCenter-Worklist',
   'http://webcenter-stage.example.com')
   ```

6. To only allow users to access WebCenter and other services through the WebTier OHS ports so that they can be properly authenticated, follow the steps in Section 26.1.7.4, "Restricting Access with Connection Filters."
7. Complete the configuration for Oracle Single Sign-on (OSSO) by adding a setting to EXTRA_JAVA_PROPERTIES as described in Section 26.1.6.4, "Configuring the Application for Oracle Access Manager SSO."

26.2.5 Configuring the Discussions Server for SSO

This section describes how to configure Oracle WebCenter Discussions 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 WebCenter Spaces, as described in Section 24.5.1, "Migrating the WebCenter Discussions Server to Use an External LDAP."

To set up the discussions server for SSO:

1. Log in to the Oracle WebCenter Discussions Server Admin Console at:

   ```
   http://host:port/owc_discussions/admin
   ```

   Where *host* and *port* are the host ID and port number of the WLS_Services managed server.
2. Open the System Properties page and edit (if it already exists) or add the owc_discussions.sso.mode property, setting it's value to true.
3. Edit or add the jiveURL property to point to the base URL of the SSO server. For example:

   ```
   jiveURL = example.com:8890/owc_discussions
   ```

26.3 Configuring SAML-based Single Sign-on

Security Assertion Markup Language (SAML) enables cross-platform authentication between Web applications or Web Services running in a WebLogic Server domain and Web browsers or other HTTP clients. WebLogic Server supports single sign-on (SSO) based on SAML. When users are authenticated at one site that participates in a single sign-on (SSO) configuration, they are automatically authenticated at other sites in the SSO configuration and do not need to log in separately.

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 since REST applications (including the `/rest` webapp and `/cmisrestprelim` webapp) do not have a single access point and SAML 1.1 standard does not support wildcards in the Source Redirect URIs (in the asserting party configuration), SAML single sign-on for REST is not supported.

Note also that if you set up SAML-based single sign-on with WebCenter Spaces as the source application and Oracle WebCenter Discussions as the destination application, you can access administration pages of the Discussions application from the WebCenter Spaces Manage Group Space Services screen or Configure WebCenter Services screen. However, since the Oracle WebCenter Discussion administration pages do not participate in SSO, if you access administration pages directly, you are required to log in to Oracle WebCenter Discussions again.

This SSO mechanism can be used for departmental WebCenter installations for which there is no existing Oracle SSO or Oracle Access Manager single sign-on infrastructure, but single sign-on between only WebCenter Spaces and its services is required. For High Availability and large enterprise deployments, the Oracle Access Manager SSO configuration is recommended.

This section describes how to set up SAML 1.1-based single sign-on for Oracle WebCenter Spaces and the Wiki and Worklist services running on different managed servers within the same domain.

This section includes the following subsections:

- Section 26.3.1, "SAML Components and Topology"
- Section 26.3.2, "Configuring SAML-based Single Sign-on"

26.3.1 SAML Components and Topology

Figure 26–34 shows the components and their interaction in a SAML-based single sign-on configuration that includes WebCenter Spaces and the Wiki service.

A SAML-based single sign-on solution consists of the following components:

- **SAML Credential Mapper** - The SAML Credential Mapping provider acts as a producer of SAML security assertions, allowing WebLogic Server to act as a source site for using SAML for single sign-on. The SAML Credential Mapping provider generates valid SAML 1.1 assertions for authenticated subjects based on the configuration of the target site or resource.
- **Inter Site Transfer Service (ITS)** - an addressable component that generates identity assertions and transfers the user to the destination site.
- **Assertion Retrieval Service (ARS)** - an addressable component that returns the SAML assertion that corresponds to the artifact. The assertion ID must have been allocated at the time assertion was generated.
- **SAML Identity Asserter** - The SAML Identity Assertion provider acts as a consumer of SAML security assertions, allowing WebLogic Server to act as a

destination site for using SAML for single sign-on. The SAML Identity Assertion provider processes valid SAML 1.1 assertions for authenticated subjects obtained from the source site or resource.

- **Assertion Consumer Service (ACS)** - an addressable component that receives assertions and/or artifacts generated by the ITS and uses them to authenticate users at the destination site
- **SAML Relying party** - A SAML Relying Party is an entity that relies on the information in a SAML assertion produced by the SAML source site. You can configure how WebLogic Server produces SAML assertions separately for each Relying Party or use the defaults established by the Federation Services source site configuration for producing assertion.
- **SAML Asserting party** - A SAML Asserting Party is a trusted SAML Authority (an entity that can authoritatively assert security information in the form of SAML Assertions).

Figure 26–33 shows the components and flow for a POST-configured SAML SSO configuration that includes both a WebCenter and SOA domain. The flow is similar for other destination applications participating in single sign-on such as RSS, Worklist applications, and Discussions.

Figure 26–33 Detailed SAML Single Sign-on Components and Topology (POST Profile Configured)

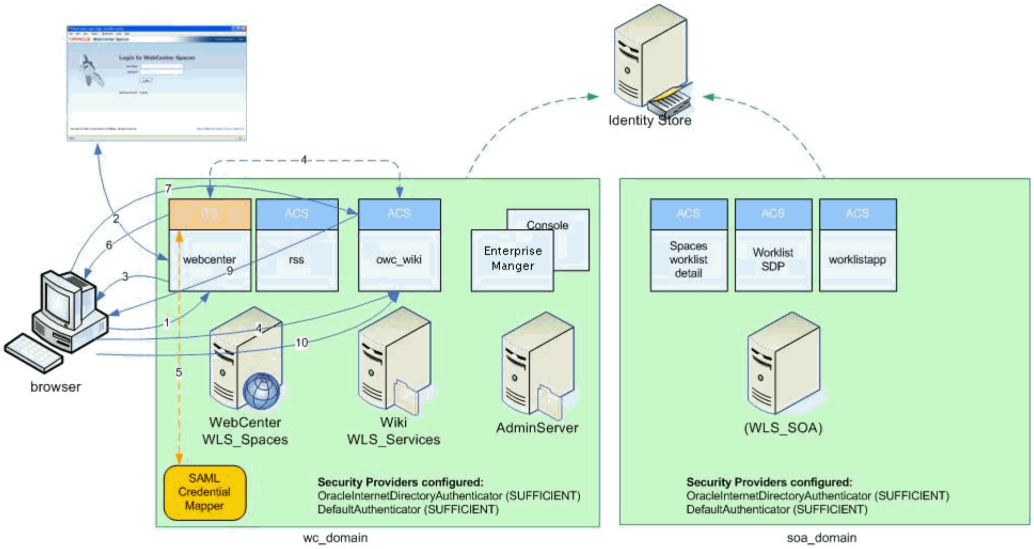
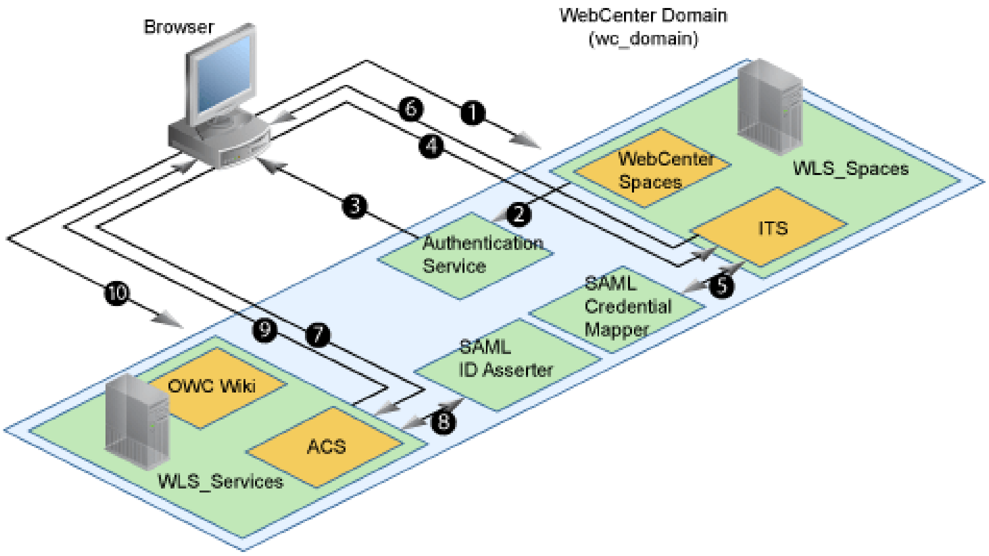


Figure 26–34 shows a simplified version of the components and flow for a POST-configured SAML SSO configuration, including the SAML SSO flow between WebCenter Spaces and the OWC Wiki application.

Figure 26–34 SAML Single Sign-on Components and Topology (POST Profile Configured)



The steps in the flow are:

1. The user's browser accesses WebCenter Spaces (source site), hosted on a WebLogic managed server (`WLS_Spaces`) in the WebCenter domain (`wc_domain`), by supplying user credentials.
2. WebCenter Spaces passes the user credentials to the authentication service provider.
3. If authentication is successful, the authenticated session is established, and the WebCenter Spaces welcome page is displayed.
4. From the welcome page, the user then clicks on a link on the page to access a secured Web page of the Wiki service (destination site), hosted on a different WebLogic Server (`WLS_Services`) in the same domain. This triggers a call to the Inter-Site Transfer Service (ITS) servlet configured. In this case, the ITS servlet is hosted within the source site (that is, on the WebCenter Spaces application on the `WLS_Spaces` managed server) that shares the same JSESSIONID cookie as WebCenter Spaces.
5. The ITS servlet calls the SAML Credential Mapper configured in the WebCenter domain (`wc_domain`) to request a caller assertion. The SAML Credential Mapper returns the assertion. It also returns the URL of the destination site application Web page (a secured Web page of the Wiki service) and path to the appropriate POST form (if the source site is configured to use the POST profile).
6. The SAML ITS servlet generates a SAML response containing the generated assertion, signs it, base-64 encodes it, embeds it in the HTML form, and returns the form to the user's browser.
7. The user's browser POSTs the form to the destination site's Assertion Consumer Service (ACS). In this case, the ACS Servlet is hosted in destination site (the Wiki service) and shares its login cookie.
8. The assertion is validated.
9. If the assertion is successful, the user is redirected to the target (the secured Web page of the Wiki service).

10. The user is logged in on the destination site Wiki service without having to reauthenticate.

26.3.2 Configuring SAML-based Single Sign-on

This section describes how to configure WebCenter Spaces and services for SAML-based single sign-on. You can either use a set of automated scripts, or do the configuration manually. This section provides the steps for both approaches, along with a set of common prerequisites, and a set of steps to check that your single sign-on is working.

This section includes the following sub-sections:

- Section 26.3.2.1, "Common Prerequisites"
- Section 26.3.2.2, "Configuring SAML-based SSO Using Scripts"
- Section 26.3.2.3, "Configuring SAML-based SSO Manually"
- Section 26.3.2.4, "Checking Your Configuration"

26.3.2.1 Common Prerequisites

This section describes the common set of steps for configuring SAML-based single sign-on. These steps must be carried out first regardless of whether you're using the scripts or doing the configuration manually.

The prerequisites for SAML-based SSO are described in the following sub-sections:

- Section 26.3.2.1.1, "Preparing WebCenter Spaces and Services for SAML SSO"
- Section 26.3.2.1.2, "Generating and Registering Certificates"
- Section 26.3.2.1.3, "Setting Up SSL"

26.3.2.1.1 Preparing WebCenter Spaces and Services for SAML SSO

Install WebCenter Spaces and related applications as required for your environment. After installing WebCenter Spaces and the Wiki and Worklist services, test the single sign-on configuration as described in the steps below.

To install and check the default WebCenter Spaces and Wiki service login:

1. Install WebCenter Spaces, and select the Wiki service and Discussions service, and any other service applications to be configured for SSO (RSS is automatically deployed when you install WebCenter Spaces). For information on installing WebCenter Spaces, see "Installing WebCenter Spaces, Portlet Producers, Discussions, and Wiki and Blogs" in the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter*.

   When the installation is complete, WebCenter Spaces is hosted on the `WLS_Spaces` Managed Server, and Wiki and Discussions services are hosted on the `WLS_Services` Managed Server. Record the host and port that the Wiki service is running on so, later on, you can construct the URL and test single sign-on.

2. Log in to WebCenter Spaces and create a page with a link to the Wiki service:

   a. Log in to WebCenter Spaces as a user with create page permissions.

   b. In a group space, choose **Create Page** from the **Page Actions** menu.

   c. Enter an appropriate title for the page (for example, "Wiki"), choose the **Web page** template, and click **Create**.

- **d.** Click the **Edit** icon for the Web page component.
- **e.** Change the source to be the URL specified below:

  ```
  http://host:port/owc_wiki/page/show.jz?inline=1&scope=#{communityContext.co
  mmunityName}
  ```

  Where *host* is the Wiki server host ID and *port* is the Wiki server port number.
- **f.** Click OK.
- **g.** Save the page.

When you click the link, notice that you are challenged to log in by the Wiki service. Once you have completed the remainder of the steps, this is not required. You are automatically logged in to the Wiki server.

3. For the Worklist service, install SOA (which includes the BPEL server). For information on installing SOA, see *Oracle Fusion Middleware Installation Guide for Oracle SOA Suite and Oracle Business Process Management Suite*.
4. Configure a connection between WebCenter Spaces and the BPEL server, as described in Section 20.3, "Setting Up Worklist Connections."
5. To test the BPEL server connection used by the Worklist service:
   - **a.** Log in to WebCenter Spaces, create a group space, and add your administrator account as a moderator.
   - **b.** Log in to WebCenter Spaces with your administrator account.

     You should see a new item in the Worklist task flow indicating that you have been added as a moderator for the group space.
   - **c.** Click the link.

     Note that you are challenged to log in. After you have completed the rest of the steps you automatically log in to the BPEL server on the SOA domain.
6. Deploy the SAML SSO version of the Oracle WebCenter Discussions Server:

   By default, the .EAR file that is deployed for the Oracle WebCenter Discussions Server supports form-based Oracle SSO or Oracle Access Manager SSO. Therefore, to configure the Oracle WebCenter Discussions Server for SAML-based single sign-on, you must deploy the SAML SSO version of the discussion server .EAR file.

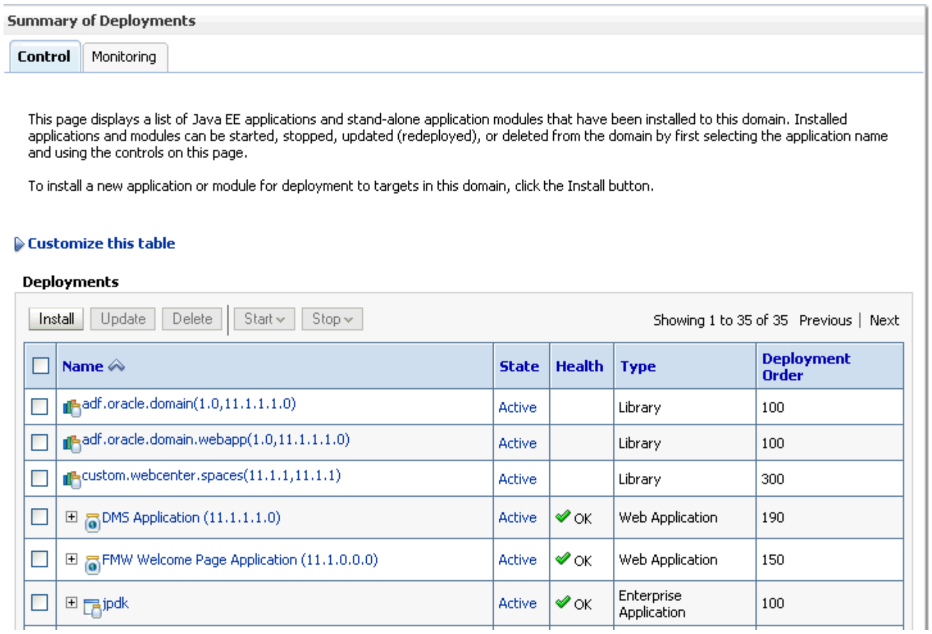
   > **Note:** Before configuring the discussions server for SSO, ensure that it is configured to use the same identity store LDAP as WebCenter Spaces, as described in Section 24.1, "Reassociating the Identity Store with an External LDAP." If you've chosen not to move the default administrator account to an external LDAP, be sure to also follow the instructions in Section 24.5.1, "Migrating the WebCenter Discussions Server to Use an External LDAP."

   - **a.** Log in to the WebLogic Server Administration Console as an administrator.

     For information on logging in to the WebLogic Server Administration Console, see Section 1.12.2, "Oracle WebLogic Server Administration Console."
   - **b.** In the Domain Structure pane, click **Deployments**.

The Deployments Summary pane displays (see Figure 26–35).

Figure 26–35 Deployment Summary Pane



Summary of Deployments

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.

Deployments

□	Name	State	Health	Type	Deployment Order
□	adf.oracle.domain(1.0,11.1.1.1.0)	Active		Library	100
□	adf.oracle.domain.webapp(1.0,11.1.1.1.0)	Active		Library	100
□	custom.webcenter.spaces(11.1.1,11.1.1)	Active		Library	300
□	⊞ DMS Application (11.1.1.1.0)	Active	✓ OK	Web Application	190
□	⊞ FMW Welcome Page Application (11.1.0.0.0)	Active	✓ OK	Web Application	150
□	⊞ jpdk	Active	✓ OK	Enterprise Application	100

c. On the Deployment Summary page, select `owc_discussions stop and delete` and click **Install**.

d. Using the Install Application Assistant **Path** field, locate the SSO enabled owc_discussions .EAR file (`owc_discussions_samlsso.ear`, typically in `$WC_ORACLE_HOME/discussionserver`).

e. Select the `owc_discussions_samlsso.ear` file and click **Next**.

f. Select **Install this deployment as an application** and click **Next**.

g. Set the **Name** to `owc_discussions`.

h. Deploy the .EAR file.

i. Log in to the Discussions Server Administration Console as an administrator (see Section 26.1.7.2, "Configuring the Discussions Server for SSO" for more information on logging in to the Discussions Server Administration Console).

j. Open the System Properties page and edit (if it already exists) or add the `owc_discussions.sso.mode` property, setting it's value to `true`.

k. Restart the `WLS_Services` Managed Server (where the discussions server is deployed).

7. To test RSS access from WebCenter Spaces, click the RSS link from **Recent Documents** or **Lists**.

26.3.2.1.2 Generating and Registering 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. Navigate to the `JAVA_HOME/bin` directory.
2. Using `keytool`, generate the key with the following command:

   ```
   keytool -genkey -keypass key_password -keystore keystore_name -storepass
   keystore_password -keyalg rsa -alias alias -validity days_valid
   ```

   Where:

   - *`key_password`* is the password to apply to the generated key
   - *`keystore_name`* is the name of the custom keystore
   - *`keystore_password`* is the password for the custom keystore
   - *`alias`* is the alias name (for example, `testalias`)
   - *`days_valid`* is the number of days for which the key password is valid (for example, `360`).
3. Run the keytool command with `-export` option to generate a key file calling it, for example, `testalias.der`.

   ```
   keytool -export -keystore keystore_name -storepass keystore_password -alias
   alias -file testalias.der
   ```

   where:

   - *`keystore_name`* is the name of the custom keystore
   - *`keystore_password`* is the password for the custom keystore
   - *`alias`* is the alias name (for example, `testalias`)
   - 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 in to the WebLogic Server Administration Console.

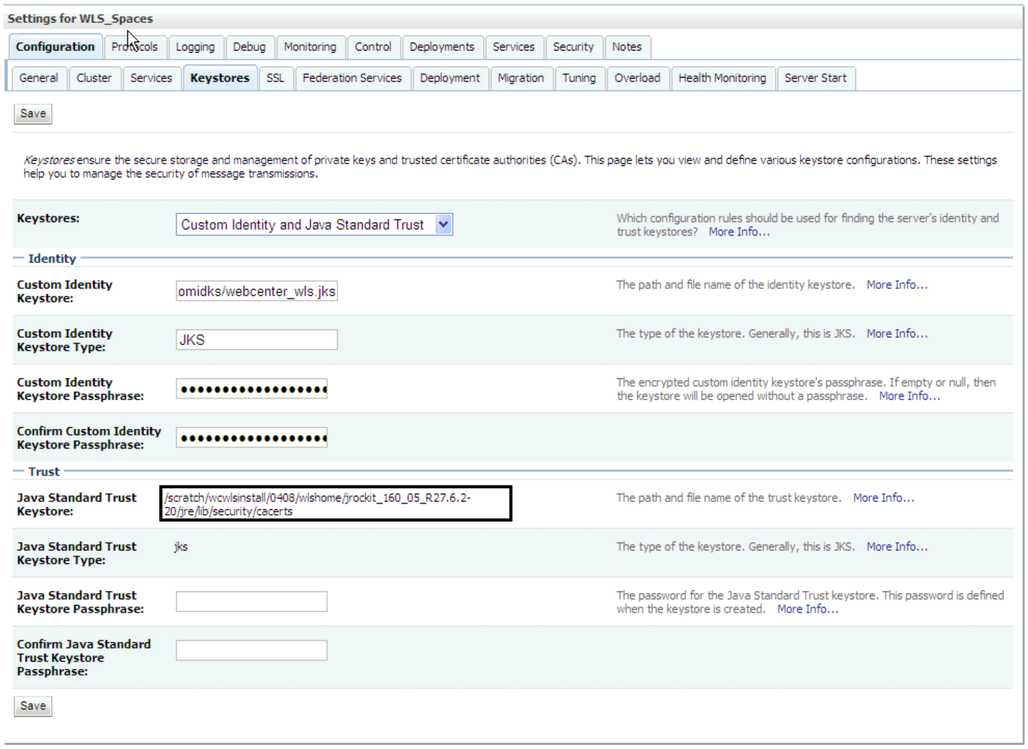
     b. In the Domain Structure pane, expand Environments and click `Servers`.

     c. In the list of servers, click `WLS_Spaces`.

     d. Open the Configuration tab, and the Keystores subtab.

     The Keystores Settings pane displays (see Figure 26–36).

Figure 26–36 Keystores Settings Pane



Settings for WLS_Spaces

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:	omidks/webcenter_wls.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:	/scratch/wcwlsinstall/0408/wlshome/jrockit_160_05_R27.6.2-20/jre/lib/security/cacerts	The path and file name of the trust keystore. More Info...
Java Standard Trust Keystore Type:	jks	The type of the keystore. Generally, this is JKS. More Info...
Java Standard Trust Keystore Passphrase:		The password for the Java Standard Trust keystore. This password is defined when the keystore is created. More Info...
Confirm Java Standard Trust Keystore Passphrase:		

- **e.** Note down the location of the server in the **Java Standard Trust Keystore** field (shown in Figure 26–39).

  Note that the `cacerts` file may be "read only", in which case you must change its permissions so that it's writable.

- Import the self-signed certificate generated above in this trust store:

  ```
  keytool -importcert -trustcacerts -alias alias -file certificate_file
  -keystore cacerts -storepass changeit
  ```

  Where:

  – *`alias`* is the WebCenter Spaces alias (for example, `webcenter_wls`)

  – *`certificate_file`* is the file name for the certificate to export the key to (for example, `webcenter_wls.cer`)

To register the keystore using the WebLogic Server Administration Console

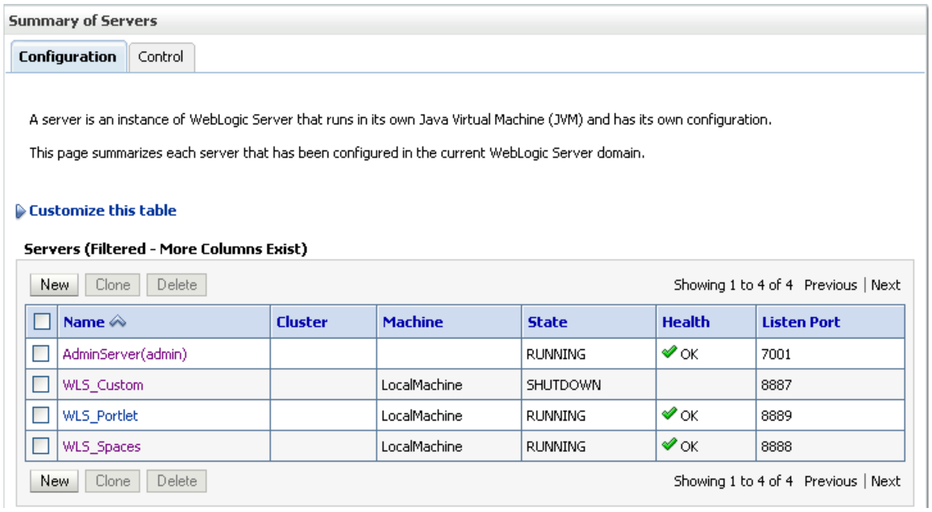
1. Log in to the WebLogic Server Administration Console.

   For information on logging in to the WebLogic Server Administration Console, see Section 1.12.2, "Oracle WebLogic Server Administration Console."

2. In the Domain Structure pane, expand **Environment** and click **Servers**.

   The Summary of Servers pane displays (see Figure 26–37).

Figure 26–37 Summary of Servers Pane



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.

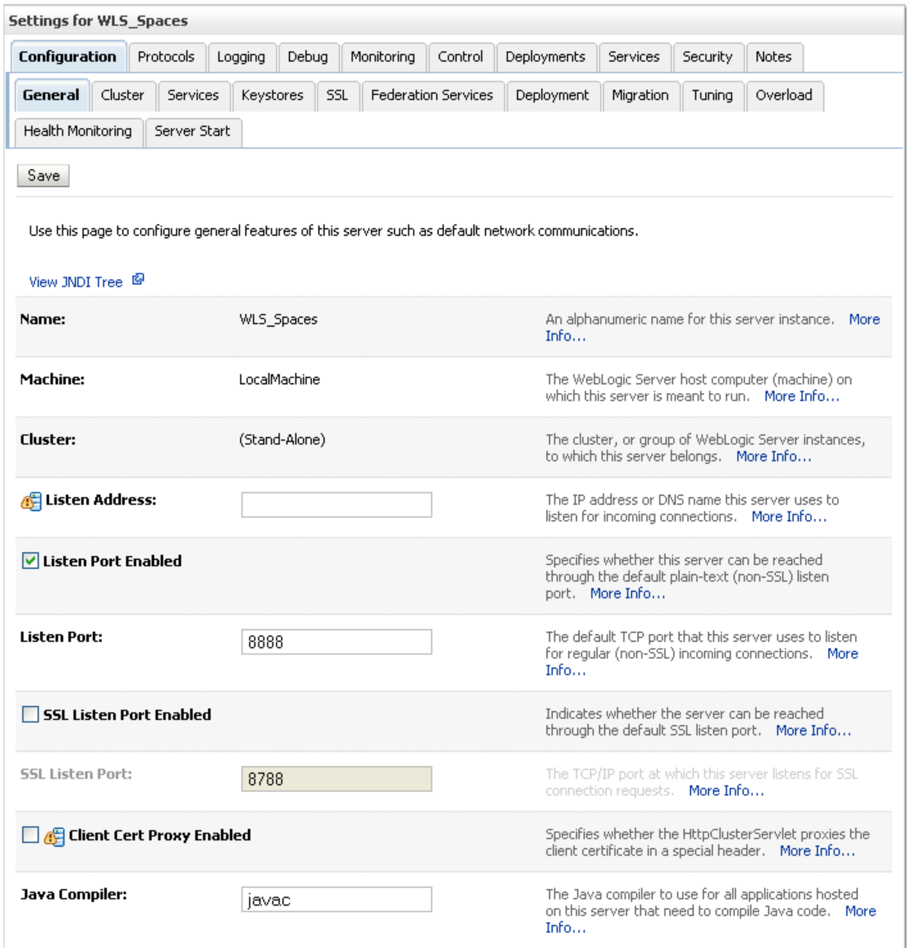
Servers (Filtered - More Columns Exist)

□	Name	Cluster	Machine	State	Health	Listen Port
□	AdminServer(admin)			RUNNING	✓ OK	7001
□	WLS_Custom		LocalMachine	SHUTDOWN		8887
□	WLS_Portlet		LocalMachine	RUNNING	✓ OK	8889
□	WLS_Spaces		LocalMachine	RUNNING	✓ OK	8888

3. Click the WebCenter Spaces server (`WLS_Spaces`) to configure the identity and trust keystore.

   The Settings pane for the WebCenter Spaces server displays (see Figure 26–38).

Figure 26–38 Settings Pane for WebCenter Spaces Server



Settings for WLS_Spaces

Configuration | Protocols | Logging | Debug | Monitoring | Control | Deployments | Services | Security | Notes
General | Cluster | Services | Keystores | SSL | Federation Services | Deployment | Migration | Tuning | Overload
Health Monitoring | Server Start
Save

Use this page to configure general features of this server such as default network communications.

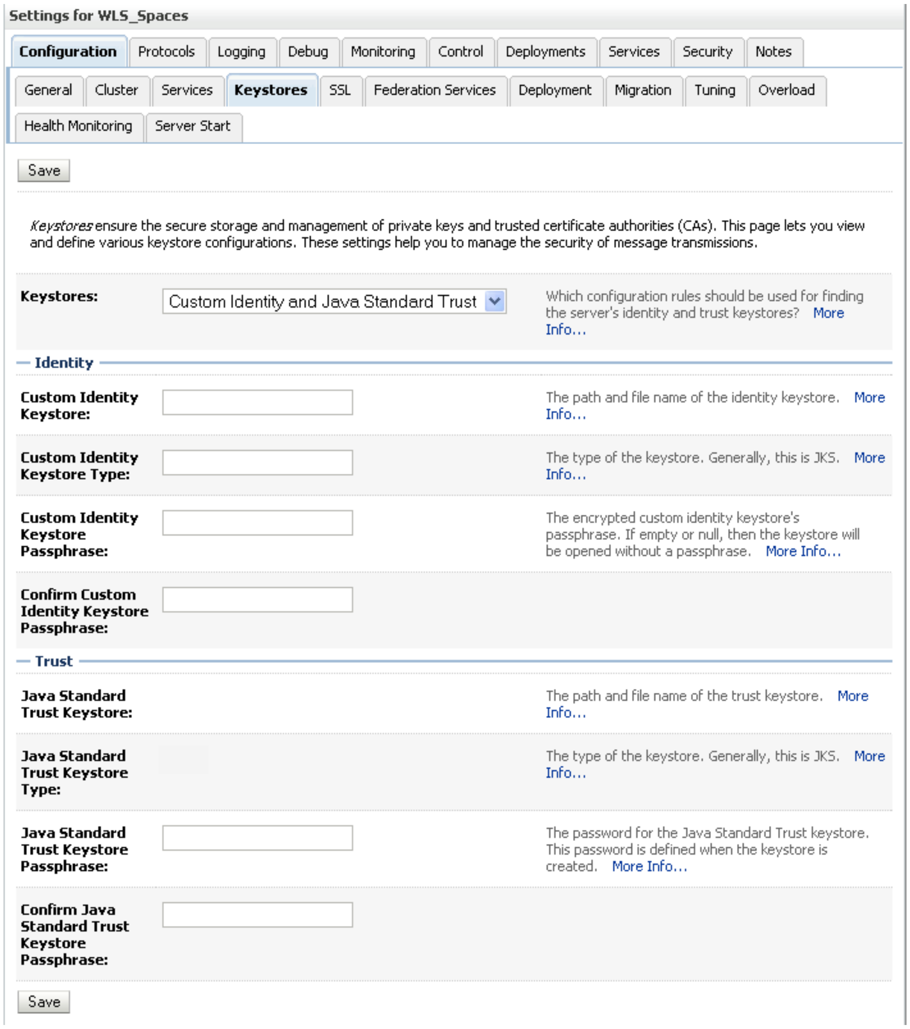
View JNDI Tree

Name:	WLS_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:		The IP address or DNS name this server uses to listen for incoming connections. More Info...
☑ **Listen Port Enabled**		Specifies whether this server can be reached through the default plain-text (non-SSL) listen port. More Info...
Listen Port:	8888	The default TCP port that this server uses to listen for regular (non-SSL) incoming connections. More Info...
☐ **SSL Listen Port Enabled**		Indicates whether the server can be reached through the default SSL listen port. More Info...
SSL Listen Port:	8788	The TCP/IP port at which this server listens for SSL connection requests. More Info...
☐ **Client Cert Proxy Enabled**		Specifies whether the HttpClusterServlet proxies the client certificate in a special header. More Info...
Java Compiler:	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 26–39).

Figure 26–39 Keystores Pane



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...

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:

Java Standard Trust Keystore: — The path and file name of the trust keystore. More Info...

Java Standard Trust Keystore Type: — 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:

5. For **Keystores**, select **Custom Identity and Java Standard Trust**.

6. In the Identity section, enter the path to the **Custom Identity Keystore** you created, choose JKS as the **Type**, and enter and confirm the **Custom Identity Keystore Passphrase**.

7. In the Trust section, enter the path to the trust keystore in Java Standard Trust Keystore, enter `JKS` as the **Type**, and enter and confirm the **Java Standard Trust Keystore Passphrase**.

8. Click **Save**.

26.3.2.1.3 Setting Up SSL

If the WebCenter installation requires SSL for providing transport-level security, then SSL should be configured before configuring single sign-on as described in Section 26, "Configuring WebCenter Applications and Components to Use SSO." Note that setting up SSL is not related to enabling SSO.

26.3.2.2 Configuring SAML-based SSO Using Scripts

After installing WebCenter 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

The manual configuration details for each of the above configuration steps are also described in Section 26.3.2.3, "Configuring SAML-based SSO Manually."

This section includes the following sub-sections:

- Section 26.3.2.2.1, "The Single Sign-on Script"
- Section 26.3.2.2.2, "Using the Scripts"

26.3.2.2.1 The Single Sign-on Script

The scripts are contained in a ZIP file (`saml_scripts.zip`) that can be downloaded from OTN at:

```
http://www.oracle.com/technology/products/webcenter/files/saml_s
cripts.zip
```

The ZIP file contains the scripts to configure SAML 1.1 SSO for WebCenter Spaces and related applications. The following files are contained in the ZIP file:

wcsamlsso.properties

This properties file 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, WebCenter Spaces server and URL, and so forth, of the WebCenter 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 domain
- `keyFile` - Key file to decrypt the weblogic user account and password for the WebCenter domain
- `adminURL` - WebLogic Admin URL to connect to WLST
- `usesSSL` - Indicates whether WebCenter Spaces is configured to use SSL
- `url` - WebCenter URL. If `usesSSL` is "`true`", then change "`http`" to "`https`"
- `serverName` - Server where WebCenter Spaces is deployed, typically `WLS_Spaces`

- `certAlias` - Alias of certificate to sign SAML assertions
- `certPassword` - Encrypted password of certificate to sign SAML assertions

services_config

This section captures the login information, admin URL, certificate file path, and so forth, of the Services domain required for the Identity Asserter and Destination Site Federation Services configuration. Only complete this section if your setup has Wiki and/or 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 Wiki/Discussions is configured to use SSL
- `serverName` - Server where Wiki and Discussions are deployed (typically the `WLS_Services` Managed Server)
- `certAlias` - Alias of certificate to verify SAML assertions
- `certPath` - Path to exported certificate to verify SAML assertions

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

wiki_config

Specify whether your configuration has Wiki installed.

- `url` - OWC Wiki URL. If `usesSSL` in **services_config** is "`true`", then change "`http`" to "`https`"

rss_config

This section must be completed.

- `url` - RSS URL. If `usesSSL` in **spaces_config** is "`true`", then change "`http`" to "`https`"

forum_config

Specify whether your configuration has Discussions installed.

- `url` - OWC Discussions URL. If `usesSSL` in **services_config** is "`true`", then change "`http`" to "`https`"

worklist_config

Specify whether SOA is installed and Worklist is configured for WebCenter Spaces.

- `worklist_detail` - Worklist Detail application URL. If `usesSSL` in **soa_config** is "`true`", then change "`http`" to "`https`"
- `worklist_sdp` - Worklist SDP application URL. If `usesSSL` in **soa_config** is "`true`", then change "`http`" to "https"
- `worklist_integration` - Worklist Integration application URL. If `usesSSL` in **soa_config** is "`true`", then change "`http`" to "https"

wcsamlsso.py

Script file that contains utility functions invoked by rest of the configuration scripts

configureSpaces.py

Executable script to configure SAML 1.1 Credential Mapper, SAML 1.1 Identity Asserter and Source and Destination site federation services on the WebCenter domain

configureServices.py

Executable script to configure SAML 1.1 Identity Asserter and Destination site federation services on the Services domain

configureSOA.py

Executable script to configure SAML 1.1 Identity Asserter and Destination site federation services on the SOA domain

configureSSO.py

Executable script to configure asserting and relying parties for all related applications used in WebCenter Spaces (that is, RSS, Wiki, Discussions, and Worklist). If your setup does not have one or more of the six applications, then Oracle recommends that you run the specific scripts to configure individual applications described below.

configureRSS.py

Executable script to configure asserting and relying parties for the RSS application

configureWiki.py

Executable script to configure asserting and relying parties for the Wiki application

configureForum.py

Executable script to configure asserting and relying parties for the Discussions application

configureWorklistIntegration.py

Executable script to configure asserting and relying parties for the Worklist Integration application

configureWorklistDetail.py

Executable script to configure asserting and relying parties for the Worklist Community Detail application

configureWorklistSDP.py

Executable script to configure asserting and relying parties for the Worklist SDP application

26.3.2.2.2 Using the Scripts

Follow the steps below to use the scripts to configure SAML-based single sign-on:

1. Download the ZIP file (`saml_scripts.zip`) from OTN at:

   ```
   http://www.oracle.com/technology/products/webcenter/files/sam
   l_scripts.zip
   ```

2. Unzip the contents of the zip file into `$ORACLE_HOME`. This extracts the contents into `$ORACLE_HOME/wlserver_10.3/common/bin` and `$ORACLE_HOME/wlserver_10.3/common/wlst`.

3. Ensure that the Administration server for all the domains used in this configuration are up and running.

4. Generate the config and key files containing the connection information for the various domains using the `storeUserConfig` WLST command. Use the command-line help (`help('storeUserConfig'))` for usage and syntax details.

   The `wcsamlsso.properties` file assumes that the config and key files exist in the same directory. You can change this when you edit the properties file in step 6 to specify the absolute paths of the config and key files if you choose different locations.

   a. Connect using WLST to the WebCenter 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 **4a** after connecting to the services domain using the admin username and password. Even if Wiki and Discussions are installed on the same domain as WebCenter Spaces (`wc_domain`), you must connect to the WebCenter domain and run this command:

      ```
      storeUserConfig('servicesconfig.secure',
      'serviceskey.secure')
      ```

   c. Repeat step **4a** after connecting to the SOA domain using the Admin username and password. Even if SOA is installed on the same domain as WebCenter Spaces, you must connect to the WebCenter domain and run this command:

      ```
      storeUserConfig('soaconfig.secure', 'soakey.secure')
      ```

5. 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 `wcsamlsso.properties` mentioned in the next step. Since this password will be set onto the credential mapper and source site federation services in the WebCenter domain, ensure that you run the encryption utility from the WebCenter domain.

6. Edit `$ORACLE_HOME/wlserver_10.3/common/bin/wcsamlsso.properties` and complete the sections applicable to your setup. Refer to Section 26.3.2.2.1, "The Single Sign-on Script" for a detailed description of the sections in this properties file.

7. Launch WLST from `$ORACLE_HOME/wlserver_10.3/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('configureSpaces.py')`

      Restart the Administration server and the `WLS_Spaces` Managed Server in the WebCenter domain.

   b. If you have a Wiki or Discussions setup, execute the `configureServices.py` script:

      ```
      execfile('configureServices.py')
      ```

      If Wiki and Discussions belong to the same domain as WebCenter Spaces, then only restart the `WLS_Services` Managed Server. Otherwise, restart the Administration server and the `WLS_Services` Managed Server in the Services domain.

   c. If you have Worklist configured for WebCenter Spaces, execute the `configureSOA.py` script:

      ```
      execfile('configureSOA.py')
      ```

      Restart the Administration server and the SOA server in the SOA domain.

8. Follow either step **a** or **b** below depending on whether you have installed all related applications along with WebCenter Spaces, or have only selected some applications in your setup.

   a. If you have all applications installed (that is, RSS, Wiki, Discussions, Worklist Integration, Detail and SDP), then you can run this single command to configure asserting and relying parties for all applications:

      ```
      execfile('configureSSO.py')
      ```

      No restart is required after executing this script.

   b. If you do not have all applications installed, run the individual commands below as required.

`execfile('configureRSS.py')` - No restart is required.

`execfile('configureWiki.py')` - Do this if you have Wiki installed in your setup. No restart is required.

`execfile('configureForum.py')` - Do this if you have Discussions installed in your setup. No restart is required.

`execfile('configureWorklistIntegration.py')` - Do this if you have Worklist installed in your setup. No restart is required.

`execfile('configureWorklistDetail.py')` - Do this if you have Worklist installed in your setup. No restart is required.

`execfile('configureWorklistSDP.py')` - Do this if you have Worklist installed in your setup. No restart is required.

9. Check your installation using the steps provided in Section 26.3.2.4, "Checking Your Configuration."

IMPORTANT: Since the properties file contains sensitive information, delete it after you have configured and verified the SAML SSO setup. Also delete the config and key files you generated in **step 4** 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.

To remove asserting and relying parties:

- Go to the Relying Parties Management Settings Pane (Figure 26–48) as described in Section 26.3.2.3.2, "Configuring a Relying Party," and delete the appropriate relying parties.
- Go to the Asserting Parties Settings Pane (Figure 26–65) as described in Section 26.3.2.3.4, "Configuring the SAML Identity Assertion Provider," under Section , "To Configure an Asserting Party," and delete the appropriate asserting parties.

Continue by fixing the issue reported and re-running the scripts.

26.3.2.3 Configuring SAML-based SSO Manually

This section describes the equivalent manual steps to set up SAML-based single sign-on in a WebLogic environment to those performed by the scripts described in Section 26.3.2.2, "Configuring SAML-based SSO Using Scripts." These steps are not required if the scripts successfully configured single sing-on for your environment.

The manual steps consist of configuring:

- SAML Credential Mapping Provider
- Necessary relying parties
- Source Site Federation Services
- SAML Identity Asserter
- Necessary asserting parties
- Destination Site Federation Services

These steps are described in the following sub-sections:

- Section 26.3.2.3.1, "Creating the SAML Credential Mapping Provider Instance"
- Section 26.3.2.3.2, "Configuring a Relying Party"
- Section 26.3.2.3.3, "Configuring Source Site Federation Services"
- Section 26.3.2.3.4, "Configuring the SAML Identity Assertion Provider"
- Section 26.3.2.3.5, "Configuring Destination Site Federation Services"

26.3.2.3.1 Creating the SAML Credential Mapping Provider Instance

This section describes how to create a SAML Credential Mapping Provider V2 instance. Note that the SAML Credential Mapping provider is not part of the default security realm and must be created.

Creating the SAML Credential Mapping Provider instance is the first of two steps required to configure the credential mapping provider:

- Creating the SAML Credential Mapping Provider instance
- Configuring a Relying Party for each of the participating service applications (which can include OWC Wiki, OWC Discussions, RSS, Worklist Community Detail, Worklist SDP, and Worklist Integration)

To create a SAML Credential Mapping Provider instance:

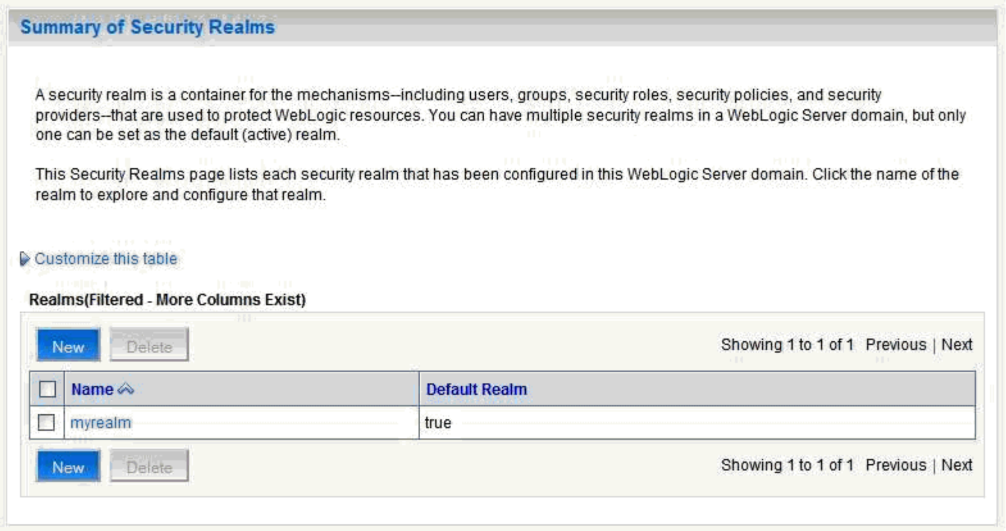
1. Log in to the WebLogic Server Administration Console.

   For information on logging in to the WebLogic Server Administration Console, see Section 1.12.2, "Oracle WebLogic Server Administration Console."

2. From the Domain Structure pane, click **Security Realms**.

   The Summary of Security Realms pane displays (see Figure 26–40).

Figure 26–40 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.

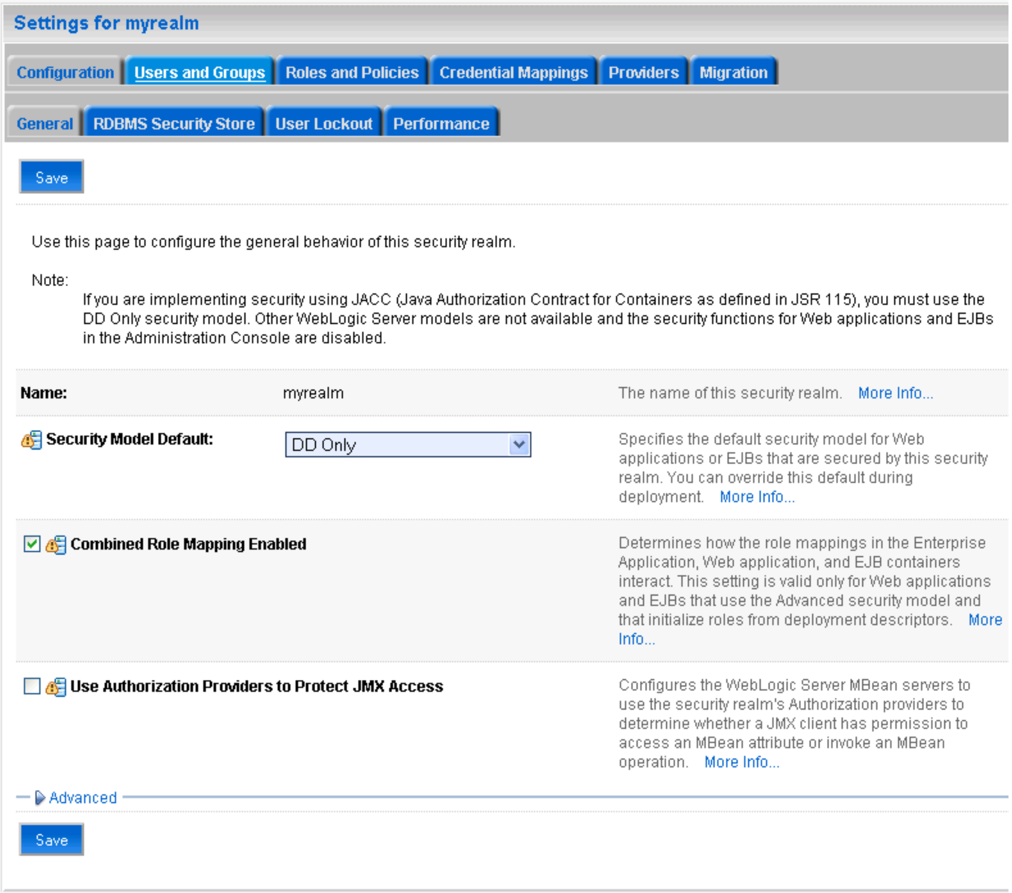
Realms(Filtered - More Columns Exist)

□	Name	Default Realm
□	myrealm	true

3. Click your security realm.

   The Settings page for the security realm displays (see Figure 26–41).

Figure 26–41 Security Realm Settings Page



Use this page to configure the general behavior of this security realm.

Note:

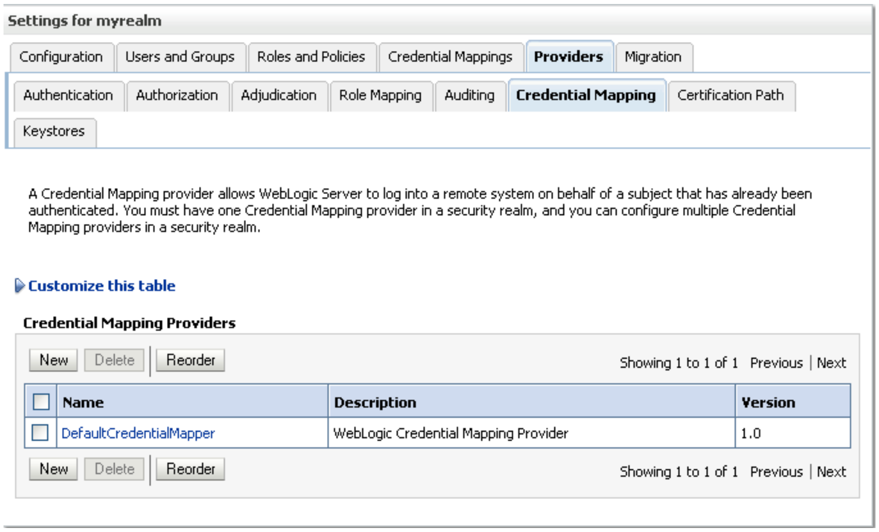
If you are implementing security using JACC (Java Authorization Contract for Containers as defined in JSR 115), you must use the DD Only security model. Other WebLogic Server models are not available and the security functions for Web applications and EJBs in the Administration Console are disabled.

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...

4. Open the Providers tab and select the Credential Mapping subtab.

   The Credential Mapping pane displays (see Figure 26–42).

Figure 26–42 Credential Mapping Pane



A Credential Mapping provider allows WebLogic Server to log into a remote system on behalf of a subject that has already been authenticated. You must have one Credential Mapping provider in a security realm, and you can configure multiple Credential Mapping providers in a security realm.

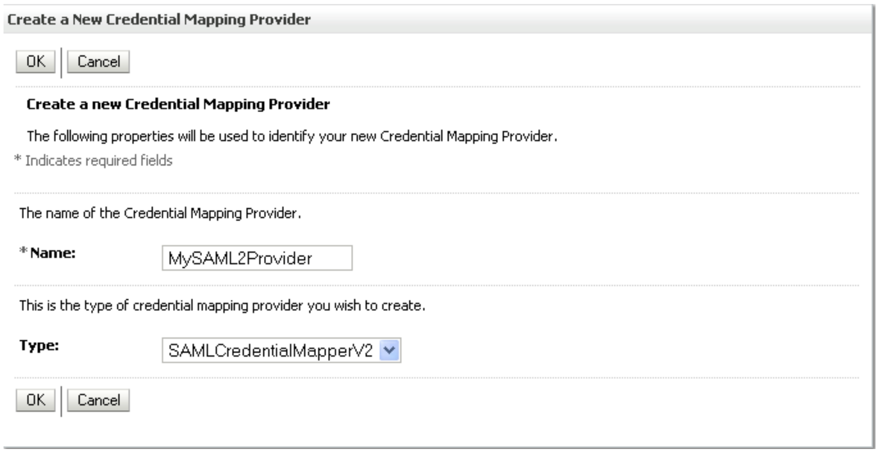
Credential Mapping Providers

□	Name	Description	Version
□	DefaultCredentialMapper	WebLogic Credential Mapping Provider	1.0

5. Click **New**.

The Create a New Credential Mapping Provider pane displays (see Figure 26–43).

Figure 26–43 Create a New Credential Provider Pane



Create a New Credential Mapping Provider

Create a new Credential Mapping Provider

The following properties will be used to identify your new Credential Mapping Provider.

* Indicates required fields

The name of the Credential Mapping Provider.

* **Name:** MySAML2Provider

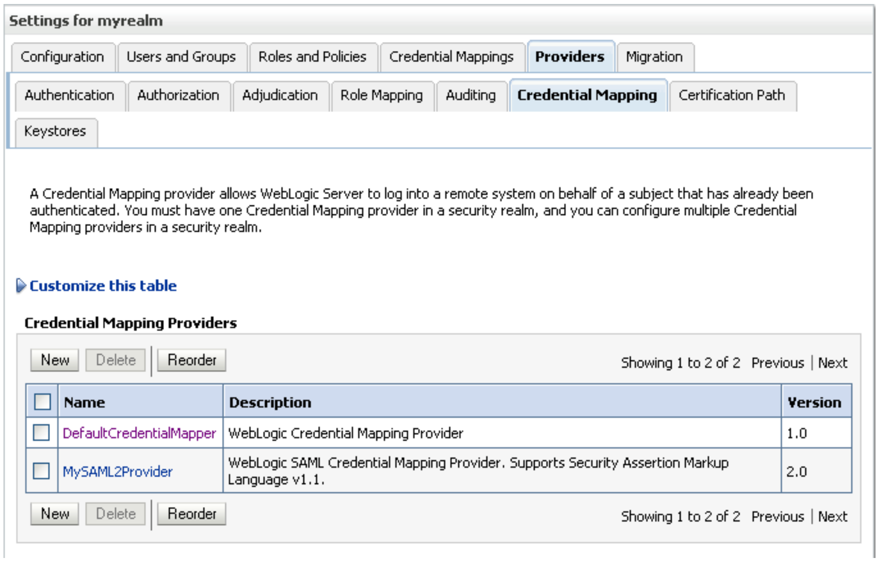
This is the type of credential mapping provider you wish to create.

Type: SAMLCredentialMapperV2

6. Enter a **Name** for the provider, select the **Type** as `SAMLCredentialMapperV2`, and click **OK**.
7. On the Security Realm Settings page, click the provider you just created.

   The Settings page for the new provider displays (see Figure 26–44).

Figure 26–44 Provider Settings Pane



Settings for myrealm

A Credential Mapping provider allows WebLogic Server to log into a remote system on behalf of a subject that has already been authenticated. You must have one Credential Mapping provider in a security realm, and you can configure multiple Credential Mapping providers in a security realm.

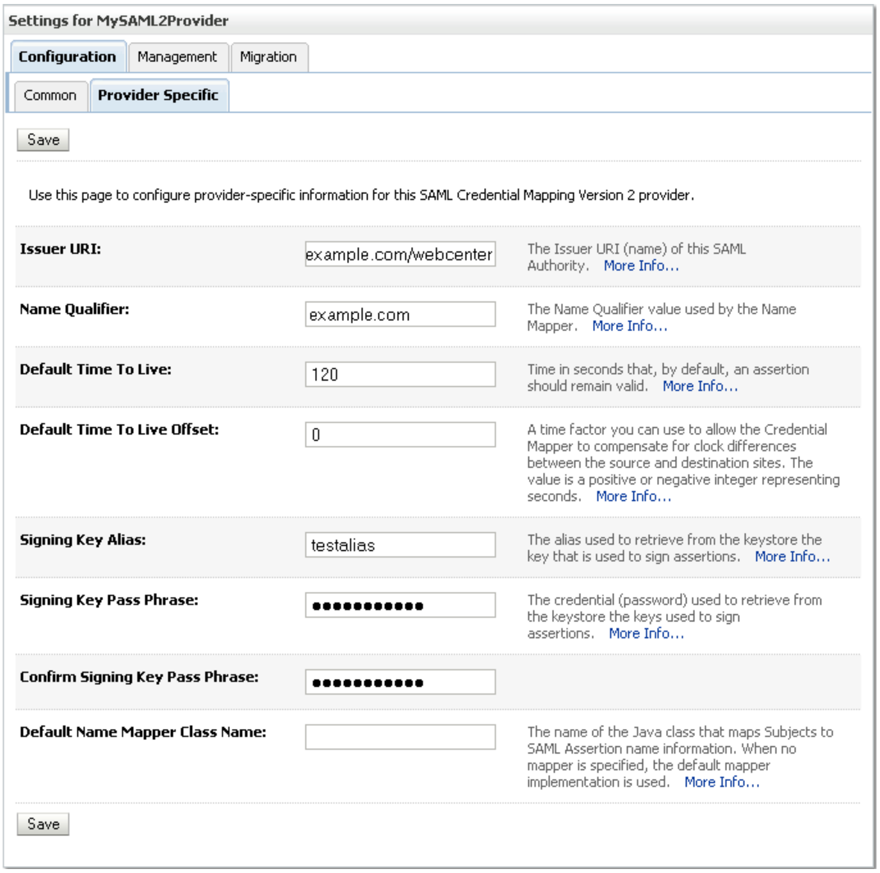
Credential Mapping Providers

□	Name	Description	Version
□	DefaultCredentialMapper	WebLogic Credential Mapping Provider	1.0
□	MySAML2Provider	WebLogic SAML Credential Mapping Provider. Supports Security Assertion Markup Language v1.1.	2.0

8. Open the Provider Specific tab.

   The Provider Specific Settings Pane displays (see Figure 26–45).

Figure 26–45 Provider Specific Settings Pane



Settings for MySAML2Provider

Use this page to configure provider-specific information for this SAML Credential Mapping Version 2 provider.

Issuer URI:	example.com/webcenter	The Issuer URI (name) of this SAML Authority. More Info...
Name Qualifier:	example.com	The Name Qualifier value used by the Name Mapper. More Info...
Default Time To Live:	120	Time in seconds that, by default, an assertion should remain valid. More Info...
Default Time To Live Offset:	0	A time factor you can use to allow the Credential Mapper to compensate for clock differences between the source and destination sites. The value is a positive or negative integer representing seconds. More Info...
Signing Key Alias:	testalias	The alias used to retrieve from the keystore the key that is used to sign assertions. More Info...
Signing Key Pass Phrase:	●●●●●●●●●●●●	The credential (password) used to retrieve from the keystore the keys used to sign assertions. More Info...
Confirm Signing Key Pass Phrase:	●●●●●●●●●●●●	
Default Name Mapper Class Name:		The name of the Java class that maps Subjects to SAML Assertion name information. When no mapper is specified, the default mapper implementation is used. More Info...

9. Configure the SAML Credential Mapping provider as a SAML authority, using the **Issuer URI**, **Name Qualifier**, and other attributes as shown below in Table 26–2. Leave the remaining parameters set to their default values.

Table 26–2 SAML Credential Mapping Provider Security Realm Settings

Parameter	Value	Description
Issuer URI	`http://www.example.com/webcenter`	The Issuer URI (name) of this SAML Authority. This unique URI tells the destination site (Wiki service) the origin of the SAML message and allows it to match with the key. Typically, the URI is used to guarantee uniqueness.
Name Qualifier	`example.com`	The Name Qualifier value used by the Name Mapper. The value of the Name Qualifier is the security or administrative domain that qualifies the name of the subject. This provides a means to federate names from disparate user stores while avoiding the possibility of subject name collision.
Web Service Assertion Signing Key Alias		The alias used to retrieve from the keystore the key that is used to sign assertions (for example, testalias).

Table 26–2 (Cont.) SAML Credential Mapping Provider Security Realm Settings

Parameter	Value	Description
Web Service Assertion Signing Key Passphrase		The credential (password) used to retrieve from the keystore the keys used to sign assertions (for example, testkeypass).
Please type again to confirm		Reenter the credential password.

10. Click **Save** to save your settings.
11. Restart the WebLogic Administration server.

26.3.2.3.2 Configuring a Relying Party

Configuring a relying party is the second of two steps required to configure the credential mapping provider:

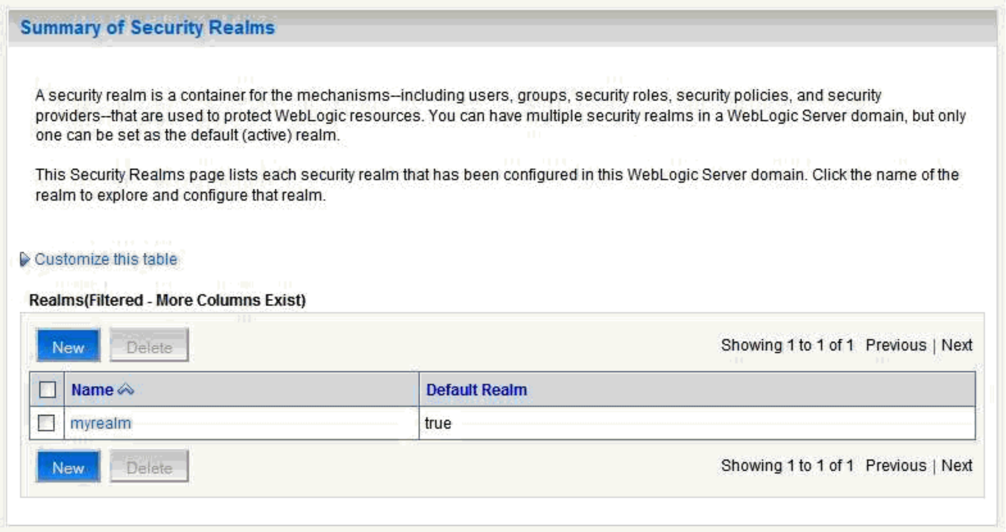
- Creating the SAML Credential Mapping Provider instance
- Configuring a relying party for each of the participating service applications (which can include OWC Wiki, OWC Discussions, RSS, Worklist Community Detail, Worklist SDP, and Worklist Integration)

To configure a relying party:

1. From the Domain Structure pane, click **Security Realms**.

   The Summary of Security Realms pane displays (see Figure 26–46).

Figure 26–46 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.

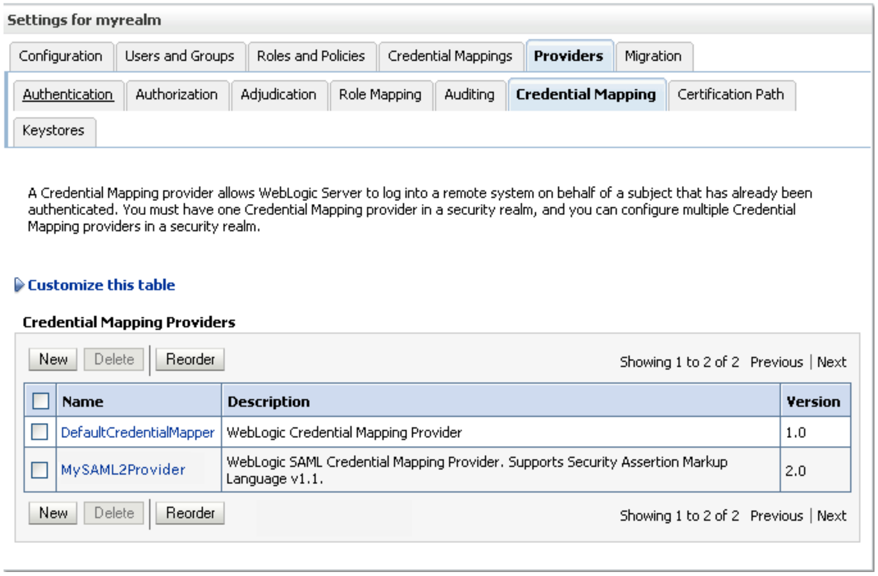
Realms(Filtered - More Columns Exist)

□	Name	Default Realm
□	myrealm	true

2. Click your security realm and open the Providers tab and the Credential Mapping subtab.

   The Credential Mapping Providers Settings pane displays (see Figure 26–47).

Figure 26–47 Credential Mapping Providers Settings Pane



A Credential Mapping provider allows WebLogic Server to log into a remote system on behalf of a subject that has already been authenticated. You must have one Credential Mapping provider in a security realm, and you can configure multiple Credential Mapping providers in a security realm.

Credential Mapping Providers

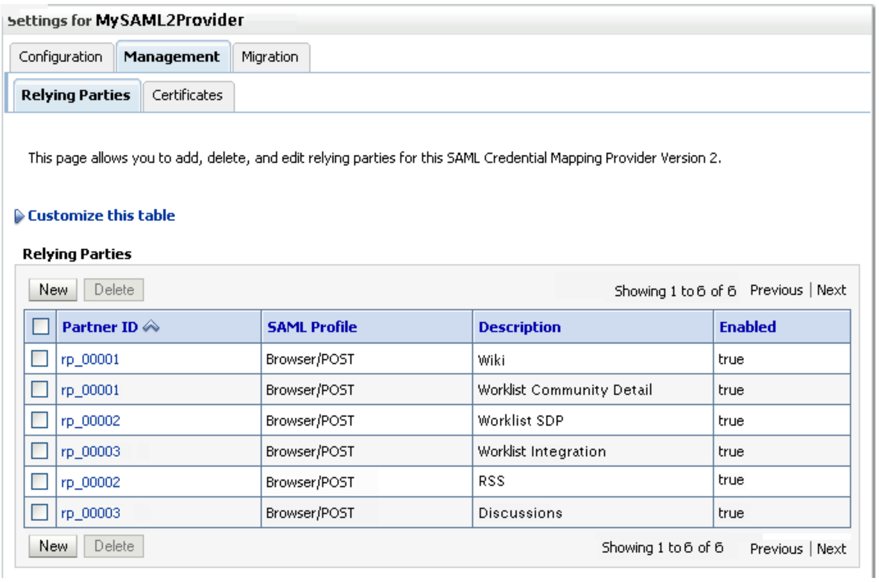
□	Name	Description	Version
□	DefaultCredentialMapper	WebLogic Credential Mapping Provider	1.0
□	MySAML2Provider	WebLogic SAML Credential Mapping Provider. Supports Security Assertion Markup Language v1.1.	2.0

3. Click the SAML Credential Mapping Provider you created.

4. Open the Management tab and the Relying Parties tab on the Settings page for the provider.

   The Relying Parties Management Settings pane displays (see Figure 26–48).

Figure 26–48 Relying Parties Management Settings Pane



This page allows you to add, delete, and edit relying parties for this SAML Credential Mapping Provider Version 2.

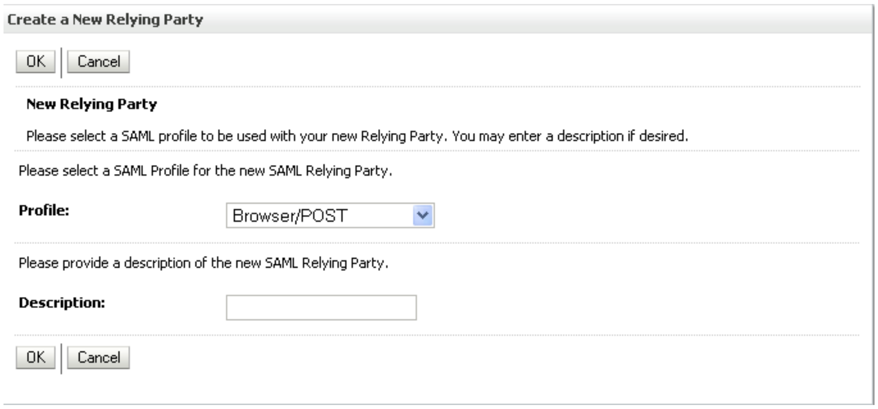
Relying Parties

□	Partner ID	SAML Profile	Description	Enabled
□	rp_00001	Browser/POST	Wiki	true
□	rp_00001	Browser/POST	Worklist Community Detail	true
□	rp_00002	Browser/POST	Worklist SDP	true
□	rp_00003	Browser/POST	Worklist Integration	true
□	rp_00002	Browser/POST	RSS	true
□	rp_00003	Browser/POST	Discussions	true

5. Click **New**.

   The Create a New Relying Parties page displays (see Figure 26–49).

Figure 26–49 Create a New Relying Party Page



Create a New Relying Party

New Relying Party

Please select a SAML profile to be used with your new Relying Party. You may enter a description if desired.

Please select a SAML Profile for the new SAML Relying Party.

Profile: Browser/POST

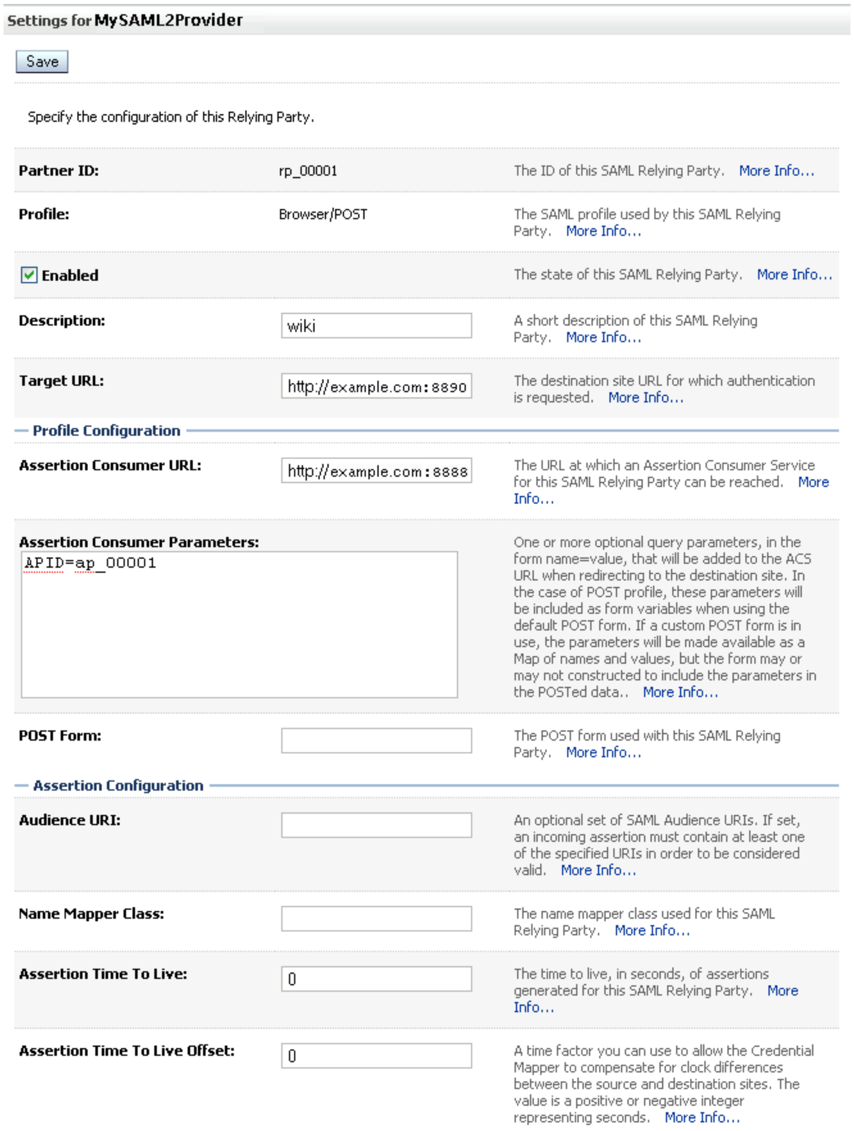
Please provide a description of the new SAML Relying Party.

Description:

6. Select `Browser/POST` as the SAML **Profile**, and provide a **Description** (for example, `Wiki`).
7. Click **OK** to save your settings.
8. On the Relying Parties Management Settings pane, click the Partner ID of the Relying Party you just created (the Partner ID is automatically generated for you).

   The Relying Party Settings page displays (see Figure 26–50).

Figure 26–50 Relying Party Settings Page



Settings for **MySAML2Provider**

Specify the configuration of this Relying Party.

Partner ID:	rp_00001	The ID of this SAML Relying Party. More Info...
Profile:	Browser/POST	The SAML profile used by this SAML Relying Party. More Info...
☑ **Enabled**		The state of this SAML Relying Party. More Info...
Description:	wiki	A short description of this SAML Relying Party. More Info...
Target URL:	http://example.com:8890	The destination site URL for which authentication is requested. More Info...
Profile Configuration		
Assertion Consumer URL:	http://example.com:8888	The URL at which an Assertion Consumer Service for this SAML Relying Party can be reached. More Info...
Assertion Consumer Parameters:	APID=ap_00001	One or more optional query parameters, in the form name=value, that will be added to the ACS URL when redirecting to the destination site. In the case of POST profile, these parameters will be included as form variables when using the default POST form. If a custom POST form is in use, the parameters will be made available as a Map of names and values, but the form may or may not constructed to include the parameters in the POSTed data.. More Info...
POST Form:		The POST form used with this SAML Relying Party. More Info...
Assertion Configuration		
Audience URI:		An optional set of SAML Audience URIs. If set, an incoming assertion must contain at least one of the specified URIs in order to be considered valid. More Info...
Name Mapper Class:		The name mapper class used for this SAML Relying Party. More Info...
Assertion Time To Live:	0	The time to live, in seconds, of assertions generated for this SAML Relying Party. More Info...
Assertion Time To Live Offset:	0	A time factor you can use to allow the Credential Mapper to compensate for clock differences between the source and destination sites. The value is a positive or negative integer representing seconds. More Info...

9. On the Relying Parties page, use the settings shown in Table 26–3 to configure a relying party for the Wiki service. Leave the remaining parameters set to their default values. Click **Save** when finished.

Table 26–3 Relying Party Settings for Wiki Service

Parameter	Value	Description
Enabled	Checked	The state of this SAML Relying Party.
Description	OWC Wiki	A short description of this Relying Party
Target URL		The destination site URL for which authentication is requested (for example: `http://example.com:8890/owc_wiki/user/login.jz`).

Table 26–3 (Cont.) Relying Party Settings for Wiki Service

Parameter	Value	Description
Assertion Consumer URL		The URL at which an Assertion Consumer Service for this SAML Relying Party can be reached (for example, `http://exmple.com:8890/owc_wiki/samlacs/acs`). 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 `WLS_Services` managed server.
Assertion Consumer Properties	`APID=ap_00001`	One or more optional query parameters, in the form `name=value`, that will be added to the ACS URL when redirecting to the destination site. In the case of POST profile, these parameters are included as form variables when using the default POST form. In this case, `ap_00001` indicates the ID of the asserting party for the Wiki application configured in the SAML Identity Asserter of the WebCenter domain which provides the source site (WebCenter Spaces) and ITS details.
Sign Assertions	Checked	Specifies whether generated assertions for this SAML Relying Party are signed.
Include KeyInfo	Checked	Indicates whether a `<ds:keyinfo>` element containing the signing certificate should be included when signing assertions. The default value is `true`. This value is ignored if **Sign Assertions** is false.

10. Repeat steps 1 - 8 to configure a relying party for the Worklist Community Detail service using the settings shown in Table 26–4. Leave the remaining parameters on the Relying Parties page set to their default values. Click **Save** when finished.

Table 26–4 Relying Party Settings for Worklist Community Detail

Parameter	Value	Description
Enabled	Checked	The state of this SAML Relying Party.
Description	Worklist Detail	A short description of this Relying Party
Target URL		The destination site URL for which authentication is requested (for example: `http://example.com:8001/workflow/WebCenterWorklistDetail/faces/adf.task-flow`).

Table 26–4 (Cont.) Relying Party Settings for Worklist Community Detail

Parameter	Value	Description
Assertion Consumer URL		The URL at which an Assertion Consumer Service for this SAML Relying Party can be reached (for example, `http://example.com:8001/workflow/WebCenterWorklistDetail/samlacs/acs`). 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 SOA managed server.
Assertion Consumer Properties	`APID=ap_00001`	One or more optional query parameters, in the form `name=value`, that will be added to the ACS URL when redirecting to the destination site. In the case of POST profile, these parameters are included as form variables when using the default POST form. In this case `ap_00001` indicates the ID of the asserting party configured for Worklist Detail in the SAML Identity Asserter of the SOA domain, which provides the source site (WebCenter Spaces) and ITS details.
Sign Assertions	Checked	Specifies whether generated assertions for this SAML Relying Party are signed.
Include KeyInfo	Checked	Indicates whether a `<ds:keyinfo>` element containing the signing certificate should be included when signing assertions. The default value is `true`. This value is ignored if **Sign Assertions** is false.

11. Repeat steps 1 - 8 to configure a relying party for the Worklist SDP service using the settings shown in Table 26–5. Leave the remaining parameters on the Relying Parties pages set to their default values. Click **Save** when finished.

Table 26–5 Relying Party Settings for Worklist SDP

Parameter	Value	Description
Enabled	Checked	The state of this SAML Relying Party.
Description	WebCenter SDP	A short description of this Relying Party
Target URL		The destination site URL for which authentication is requested (for example: `http://example.com:8001/workflow/sdpmessagingsca-ui-worklist/faces/adf.task-flow`).

Table 26–5 (Cont.) Relying Party Settings for Worklist SDP

Parameter	Value	Description
Assertion Consumer URL		The URL at which an Assertion Consumer Service for this SAML Relying Party can be reached (for example, `http://exmple.com:8001/workflow/sdpmessagingsca-ui-worklist/samlacs/acs`). 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 SOA managed server.
Assertion Consumer Properties	`APID=ap_00002`	One or more optional query parameters, in the form `name=value`, that will be added to the ACS URL when redirecting to the destination site. In the case of POST profile, these parameters are included as form variables when using the default POST form. In this case `ap_00002` indicates the ID of the asserting party configured for the Worklist SDP application in the SAML Identity Asserter of the SOA domain, which provides the source site (WebCenter Spaces) and ITS details.
Sign Assertions	Checked	Specifies whether generated assertions for this SAML Relying Party are signed.
Include KeyInfo	Checked	Indicates whether a `<ds:keyinfo>` element containing the signing certificate should be included when signing assertions. The default value is `true`. This value is ignored if Sign Assertions is false.

12. Repeat steps 1 - 8 to configure a relying party for the Worklist Integration service using the settings shown in Table 26–6. Leave the remaining parameters on the Relying Parties pages set to their default values. Click **Save** when finished.

Table 26–6 Relying Party Settings for Worklist Integration

Parameter	Value	Description
Enabled	Checked	The state of this SAML Relying Party.
Description	WebCenter SDP	A short description of this Worklist Integration
Target URL		The destination site URL for which authentication is requested (for example: `http://example.com:8001/integration/worklistapp`).

Table 26–6 (Cont.) Relying Party Settings for Worklist Integration

Parameter	Value	Description
Assertion Consumer URL		The URL at which an Assertion Consumer Service for this SAML Relying Party can be reached (for example, `http://exmple.com:8001/workflow/sdpmessagingsca-ui-worklist/samlacs/acs`). 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 SOA managed server.
Assertion Consumer Properties	`APID=ap_00003`	One or more optional query parameters, in the form `name=value`, that will be added to the ACS URL when redirecting to the destination site. In the case of POST profile, these parameters are included as form variables when using the default POST form. In this case `ap_00003` indicates the ID of the asserting party configured the for Worklist Integration application in the SAML Identity Asserter of the SOA domain, which provides the source site (WebCenter Spaces) and ITS details.
Sign Assertions	Checked	Specifies whether generated assertions for this SAML Relying Party are signed.
Include KeyInfo	Checked	Indicates whether a `<ds:keyinfo>` element containing the signing certificate should be included when signing assertions. The default value is `true`. This value is ignored if **Sign Assertions** is false.

13. Repeat steps 1 - 8 to configure a relying party for the RSS application using the settings shown in Table 26–7. Leave the remaining parameters on the Relying Parties pages set to their default values. Click **Save** when finished.

Table 26–7 Relying Party Settings for RSS

Parameter	Value	Description
Enabled	Checked	The state of this SAML Relying Party.
Description	RSS	A short description of this Relying Party
Target URL		The destination site URL for which authentication is requested (for example: `http://example.com:8888/rss/rssservlet`).

Table 26–7 (Cont.) Relying Party Settings for RSS

Parameter	Value	Description
Assertion Consumer URL		The URL at which an Assertion Consumer Service for this SAML Relying Party can be reached (for example, `http://exmple.com:8888/rss/samlacs/acs`). 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 `WLS_Spaces` managed server.
Assertion Consumer Properties	`APID=ap_00002`	One or more optional query parameters, in the form `name=value`, that will be added to the ACS URL when redirecting to the destination site. In the case of POST profile, these parameters are included as form variables when using the default POST form. In this case `ap_00002` indicates the ID of the asserting party configured for RSS in the SAML Identity Asserter of the WebCenter domain, which provides the source site (WebCenter Spaces) and ITS details.
Sign Assertions	Checked	Specifies whether generated assertions for this SAML Relying Party are signed.
Include KeyInfo	Checked	Indicates whether a <ds:keyinfo> element containing the signing certificate should be included when signing assertions. The default value is `true`. This value is ignored if **Sign Assertions** is false.

14. Repeat steps 1 - 8 to configure a relying party for the Discussions application using the settings shown in Table 26–8. Leave the remaining parameters on the Relying Parties pages set to their default values. Click **Save** when finished.

Table 26–8 Relying Party Settings for Discussions

Parameter	Value	Description
Enabled	Checked	The state of this SAML Relying Party.
Description	Discussions	A short description of this Relying Party
Target URL		The destination site URL for which authentication is requested (for example: `http://example.com:8890/owc_discussions/admin/content-main.jsp`).
Assertion Consumer URL		The URL at which an Assertion Consumer Service for this SAML Relying Party can be reached (for example, `http://exmple.com:8890/owc_discussions/samlacs/acs`). 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.

Table 26–8 (Cont.) Relying Party Settings for Discussions

Parameter	Value	Description
Assertion Consumer Properties	`APID=ap_00003`	One or more optional query parameters, in the form name=value, that will be added to the ACS URL when redirecting to the destination site. In the case of POST profile, these parameters are included as form variables when using the default POST form. In this case `ap_00003` indicates the ID of the asserting party configured for the Discussions application in the SAML Identity Asserter of the WebCenter domain, which provides the source site (WebCenter Spaces) and ITS details.
Sign Assertions	Checked	Specifies whether generated assertions for this SAML Relying Party are signed.
Include KeyInfo	Checked	Indicates whether a <ds:keyinfo> element containing the signing certificate should be included when signing assertions. The default value is `true`. This value is ignored if **Sign Assertions** is false.

26.3.2.3.3 Configuring Source Site Federation Services

This section describes how to create and configure source site Federation services.

To configure Source Site Federation Services:

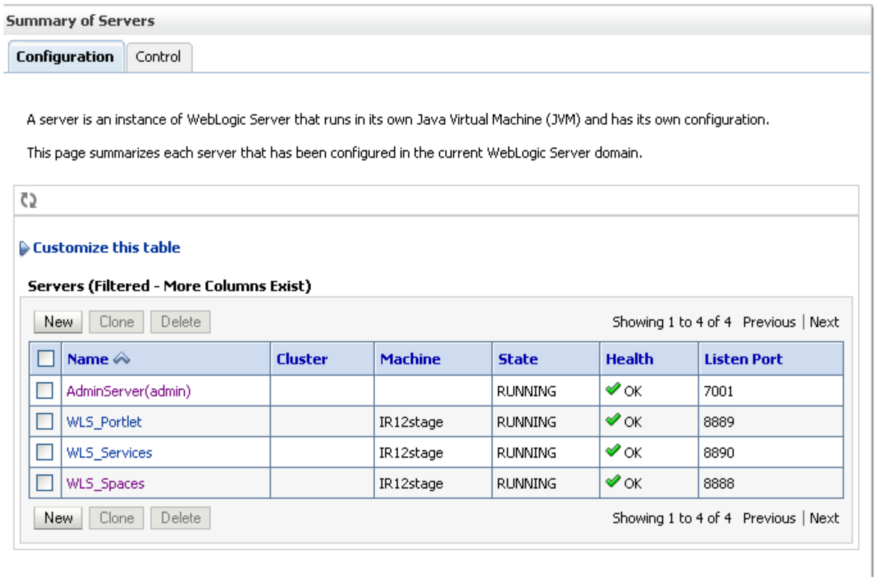
1. Log in to the WebLogic Server Administration Console.

   For information on logging in to the WebLogic Server Administration Console, see Section 1.12.2, "Oracle WebLogic Server Administration Console."

2. On the Domain Structure pane, expand the **Environment** node and click **Servers**.

   The Summary of Servers page displays (see Figure 26–51).

Figure 26–51 Summary of Servers Page



Summary of Servers

Configuration | Control

A server is an instance of WebLogic Server that runs in its own Java Virtual Machine (JVM) and has its own configuration.

This page summarizes each server that has been configured in the current WebLogic Server domain.

Customize this table

Servers (Filtered - More Columns Exist)

New | Clone | Delete — Showing 1 to 4 of 4 Previous | Next

□	Name	Cluster	Machine	State	Health	Listen Port
□	AdminServer(admin)			RUNNING	✓ OK	7001
□	WLS_Portlet		IR12stage	RUNNING	✓ OK	8889
□	WLS_Services		IR12stage	RUNNING	✓ OK	8890
□	WLS_Spaces		IR12stage	RUNNING	✓ OK	8888

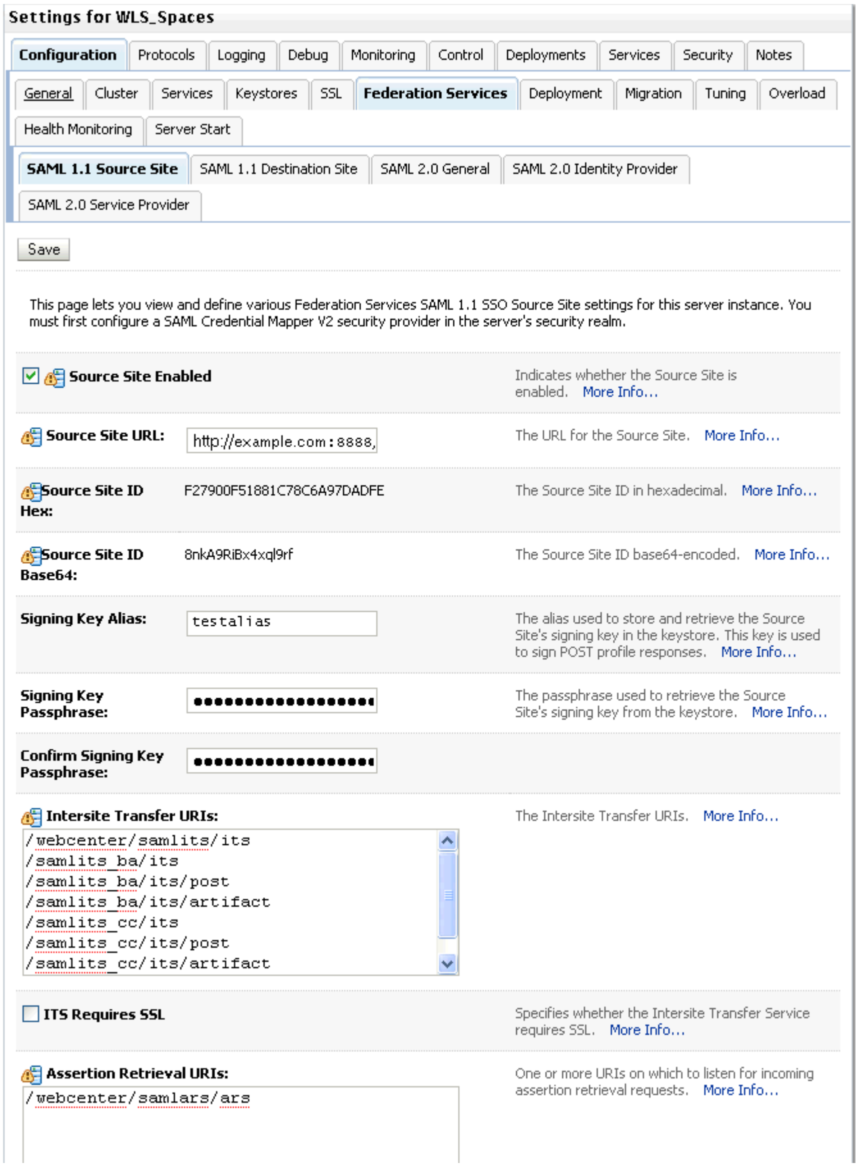
New | Clone | Delete — Showing 1 to 4 of 4 Previous | Next

3. Click **WLS_Spaces** and open the Configuration tab.

4. Open the Federation Services subtab and the SAML 1.1 Source Site subtab.

   The Federation Services Configuration SAML 1.1 Source Site Settings page for the WLS_Spaces server displays (see Figure 26–52).

Figure 26–52 Federation Services Configuration SAML 1.1 Source Site Settings Page



Settings for WLS_Spaces

This page lets you view and define various Federation Services SAML 1.1 SSO Source Site settings for this server instance. You must first configure a SAML Credential Mapper V2 security provider in the server's security realm.

☑ Source Site Enabled — Indicates whether the Source Site is enabled. More Info...

Source Site URL: http://example.com:8888, — The URL for the Source Site. More Info...

Source Site ID Hex: F27900F51881C78C6A97DADFE — The Source Site ID in hexadecimal. More Info...

Source Site ID Base64: 8nkA9RiBx4xql9rf — The Source Site ID base64-encoded. More Info...

Signing Key Alias: testalias — The alias used to store and retrieve the Source Site's signing key in the keystore. This key is used to sign POST profile responses. More Info...

Signing Key Passphrase: ●●●●●●●●●●●●●●●●●● — The passphrase used to retrieve the Source Site's signing key from the keystore. More Info...

Confirm Signing Key Passphrase: ●●●●●●●●●●●●●●●●●●

Intersite Transfer URIs: — The Intersite Transfer URIs. More Info...

```
/webcenter/samlits/its
/samlits_ba/its
/samlits_ba/its/post
/samlits_ba/its/artifact
/samlits_cc/its
/samlits_cc/its/post
/samlits_cc/its/artifact
```

☐ ITS Requires SSL — Specifies whether the Intersite Transfer Service requires SSL. More Info...

Assertion Retrieval URIs: — One or more URIs on which to listen for incoming assertion retrieval requests. More Info...

```
/webcenter/samlars/ars
```

5. Configure the SAML source site attributes as shown in Figure 26–9. Leave the remaining parameters set to their default values.

Table 26–9 Source Site Federation Services Parameters

Parameter	Value	Description
Source Site Enabled	Checked	Allow the WebLogic server instance to serve as a SAML source site by setting Source Site Enabled to true.

Table 26–9 (Cont.) Source Site Federation Services Parameters

Parameter	Value	Description
Source Site URL		Set the URL for the SAML source site (for example, `http://example.com:8888/webcenter`). 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 hexadecimal and Base64.
Signing Key Alias		The SAML source site requires a trusted certificate with which to sign assertions. Add this certificate to the keystore and enter the alias (for example, `testalias`) to be used to access the certificate. The server's SSL identity key/certificates are used by default if a signing alias and passphrase are not supplied.
Signing Key Passphrase		The SAML source site requires a trusted certificate with which to sign assertions. Add this certificate to the keystore and enter the passphrase (for example, `testkeypass`) to be used to access the certificate. The server's SSL identity key/certificates are used by default if a signing alias and passphrase are not supplied.
Intersite Transfer URIs	`/webcenter/samlits/its` [add on top, leave the rest]	Specify the URIs for the Intersite Transfer Service. These URIs are also specified in the configuration of an Asserting Party.
Assertion Retrieval URIs	`/webcenter/samlars/ars` [add on top, leave the rest]	N/A - URI for Assertion Retrieval Service used when artifact profile is used.
ITS Requires SSL	Unchecked	**Note:** If you check this, then you must change the Source Site ITS URL specified in the SAML Asserting Party configuration in the SAML Identity provider as HTTPS and the server's SSL port.
ARS Requires SSL	Unchecked	Applicable only when Artifact profile is used

6. Click **Save** to save your settings when done.
7. Restart the `WLS_Spaces` managed server.

26.3.2.3.4 Configuring the SAML Identity Assertion Provider

This section describes how to create and configure a SAML Identity Assertion Provider V2 instance (the SAML Identity Assertion provider is not part of the default security realm). This section also describes how to establish trust by registering the source site's SSL certificate in the certificate registry maintained by the SAML Identity Assertion provider.

To create a SAML Identity Assertion Provider

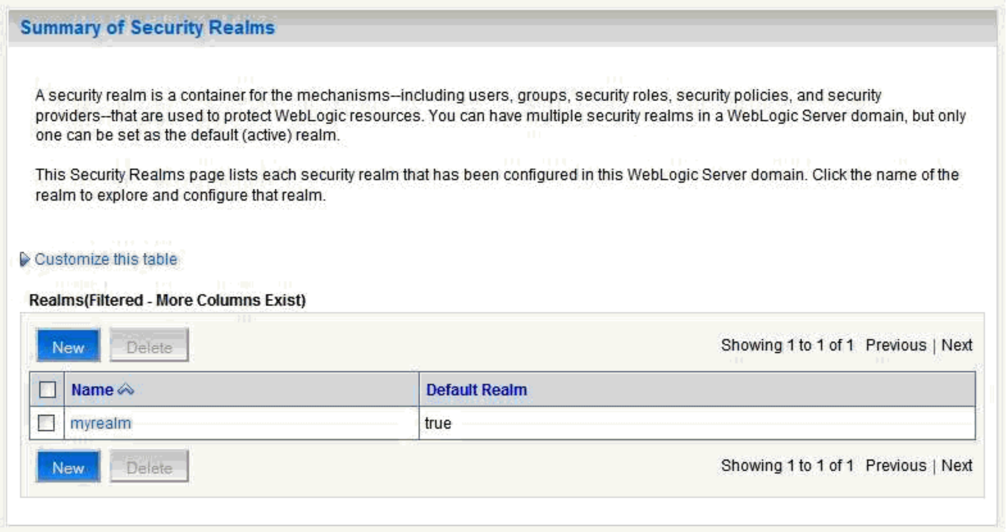
1. Log in to the WebLogic Server Administration Console.

   For information on logging in to the WebLogic Server Administration Console, see Section 1.12.2, "Oracle WebLogic Server Administration Console."

2. From the Domain Structure pane, click **Security Realms**.

The Summary of Security Realms pane displays (see Figure 26–53).

Figure 26–53 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.

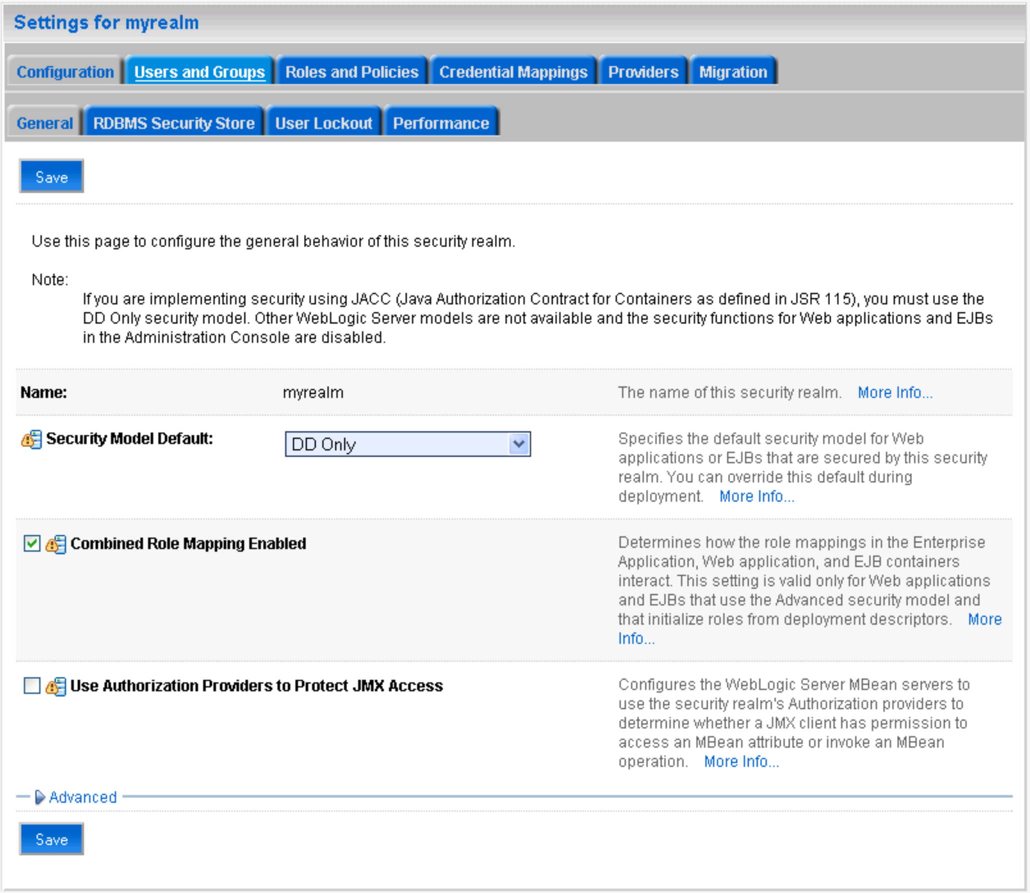
Realms(Filtered - More Columns Exist)

□	Name	Default Realm
□	myrealm	true

3. Click your security realm.

   The Settings page for the security realm displays (see Figure 26–54).

Figure 26–54 Security Realm Settings Page



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...

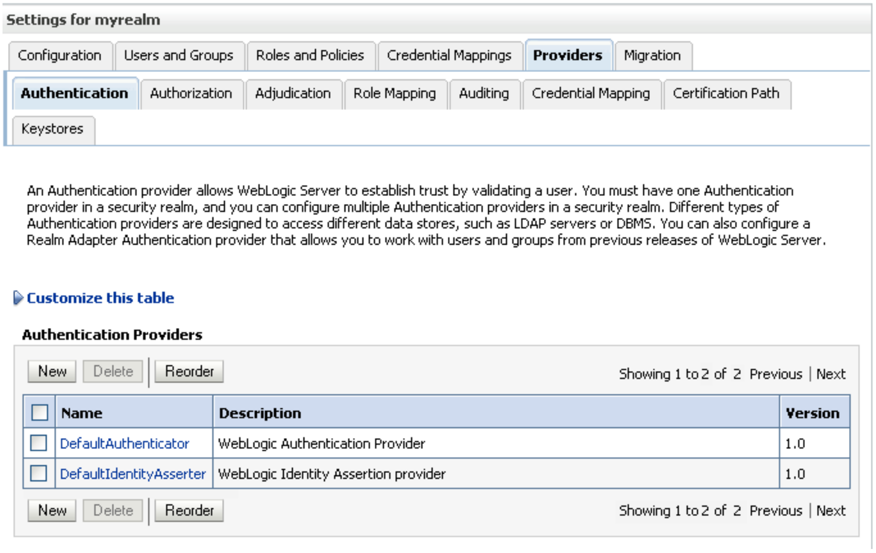
☑ **Combined Role Mapping Enabled** — Determines how the role mappings in the Enterprise Application, Web application, and EJB containers interact. This setting is valid only for Web applications and EJBs that use the Advanced security model and that initialize roles from deployment descriptors. More 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...

4. Open the Providers tab and select the Authentication subtab.

   The Authentication Settings pane displays (see Figure 26–55).

Figure 26–55 Authentication Settings Pane



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.

Authentication Providers

Showing 1 to 2 of 2

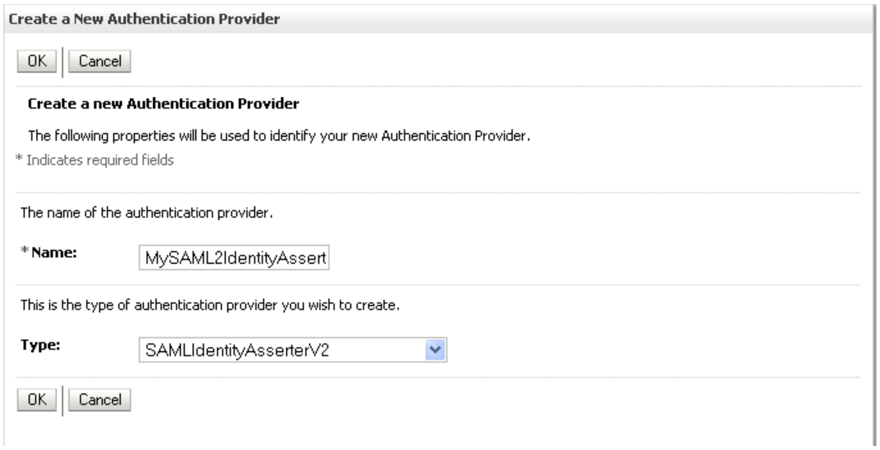
☐	Name	Description	Version
☐	DefaultAuthenticator	WebLogic Authentication Provider	1.0
☐	DefaultIdentityAsserter	WebLogic Identity Assertion provider	1.0

Showing 1 to 2 of 2

5. Click **New**.

The Create a New Authentication Provider page displays (see Figure 26–56).

Figure 26–56   Create a New Authentication Provider Page



Create a New Authentication Provider

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:** MySAML2IdentityAssert

This is the type of authentication provider you wish to create.

Type: SAMLIdentityAsserterV2

6. Enter a **Name** for the new SAML Identity Asserter, and select the **Type** as `SAMLIdentityAsserterV2`.
7. Click **OK** to save your settings.
8. Restart the WebLogic Administration server if indicated in the Messages area.
9. Go to the SOA domain and create a SAML Identity Asserter provider there as well using the steps above.

To configure a certificate for the SAML ID Asserter

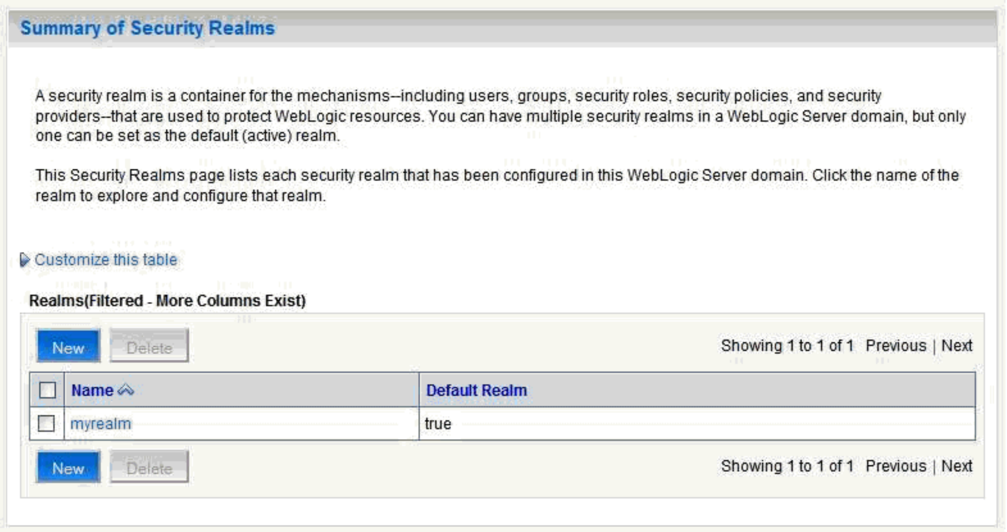
1. Log in to the WebLogic Server Administration Console.

   For information on logging in to the WebLogic Server Administration Console, see Section 1.12.2, "Oracle WebLogic Server Administration Console."

2. From the Domain Structure pane, click **Security Realms**.

   The Summary of Security Realms pane displays (see Figure 26–57).

Figure 26–57 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

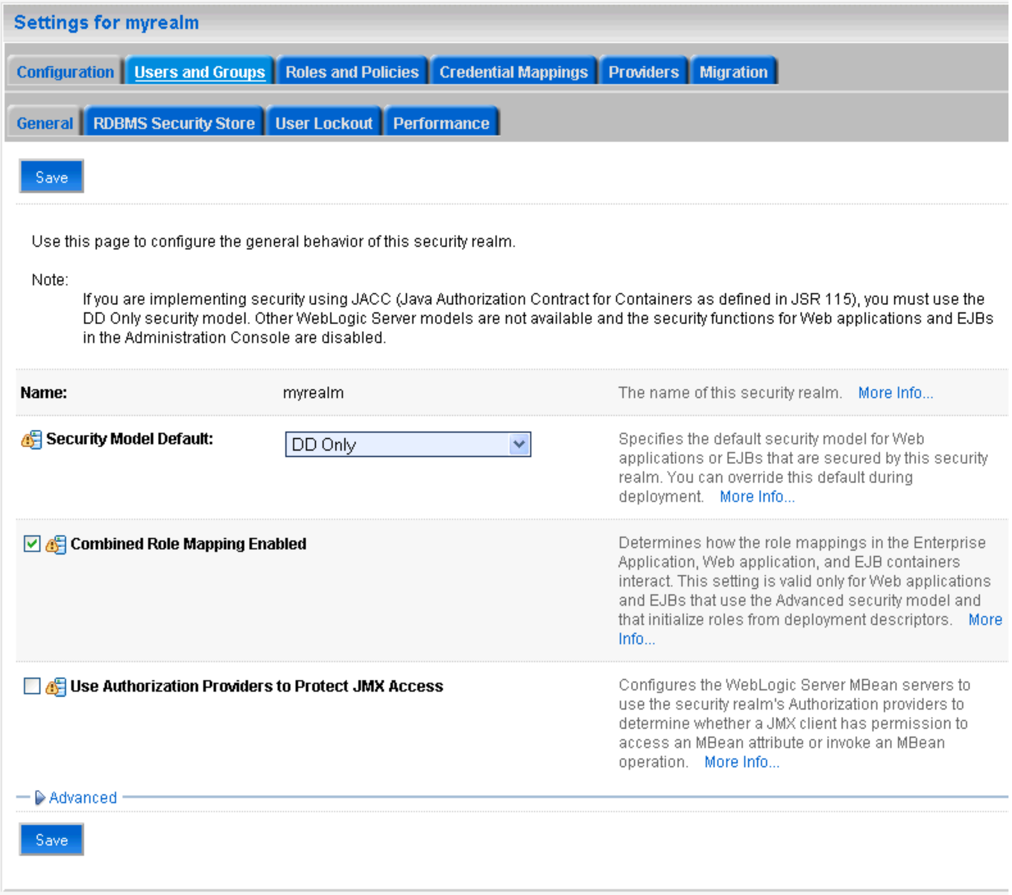
□	Name	Default Realm
□	myrealm	true

New Delete — Showing 1 to 1 of 1 Previous | Next

3. Click your security realm.

The Settings page for the security realm displays (see Figure 26–58).

Figure 26–58 Security Realm Settings Page



Settings for myrealm

Use this page to configure the general behavior of this security realm.

Note:

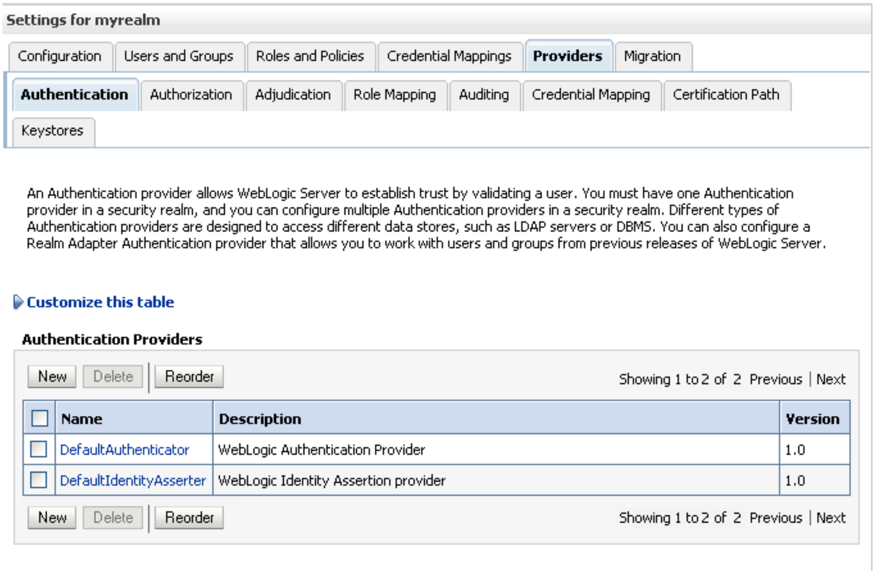
If you are implementing security using JACC (Java Authorization Contract for Containers as defined in JSR 115), you must use the DD Only security model. Other WebLogic Server models are not available and the security functions for Web applications and EJBs in the Administration Console are disabled.

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...

4. Open the Providers tab and select the Authentication subtab.

   The Authentication Settings pane displays (see Figure 26–59).

Figure 26–59 Authentication Settings Pane



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.

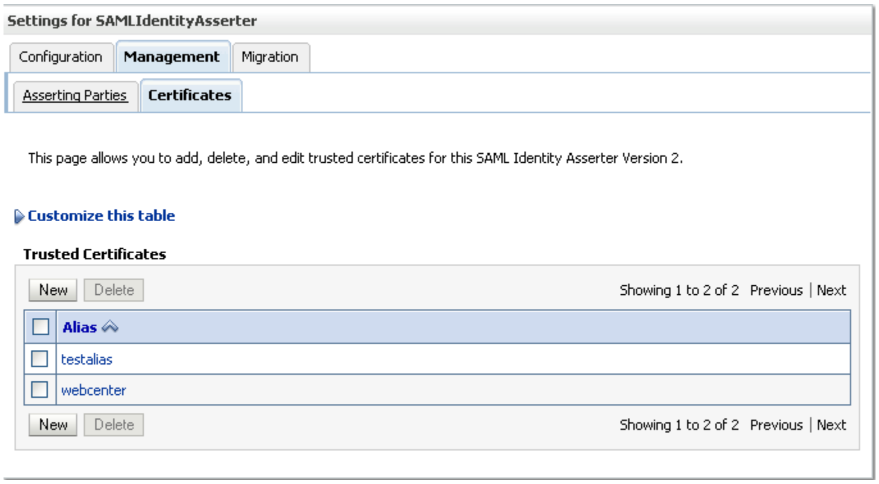
Authentication Providers

□	Name	Description	Version
□	DefaultAuthenticator	WebLogic Authentication Provider	1.0
□	DefaultIdentityAsserter	WebLogic Identity Assertion provider	1.0

5. Click the SAML Identity Asserter you created and open the Management tab and the Certificates subtab.

   The Certificate Settings pane displays (see Figure 26–60).

Figure 26–60 Certificate Settings Pane



This page allows you to add, delete, and edit trusted certificates for this SAML Identity Asserter Version 2.

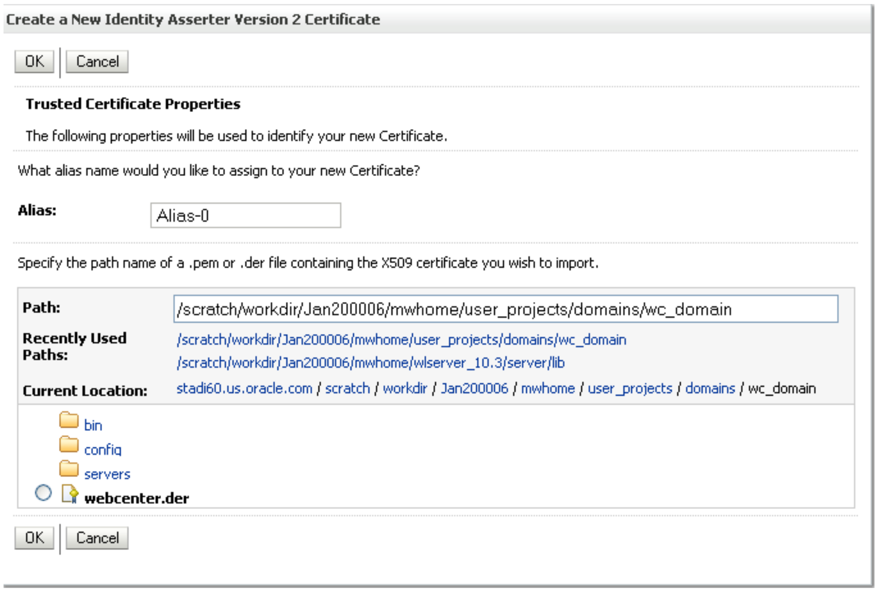
Trusted Certificates

□	Alias
□	testalias
□	webcenter

6. Click **New**.

   The Create a New Identity Asserter Certificate page displays (see Figure 26–61).

Figure 26–61 Create a New Identity Asserter Certificate Page



Create a New Identity Asserter Version 2 Certificate

Trusted Certificate Properties

The following properties will be used to identify your new Certificate.

What alias name would you like to assign to your new Certificate?

Alias: Alias-0

Specify the path name of a .pem or .der file containing the X509 certificate you wish to import.

Path: /scratch/workdir/Jan200006/mwhome/user_projects/domains/wc_domain

Recently Used Paths: /scratch/workdir/Jan200006/mwhome/user_projects/domains/wc_domain
/scratch/workdir/Jan200006/mwhome/wlserver_10.3/server/lib

Current Location: stadi60.us.oracle.com / scratch / workdir / Jan200006 / mwhome / user_projects / domains / wc_domain

bin

config

servers

○ **webcenter.der**

7. Configure the certificate as shown in Table 26–10.

Table 26–10 Certificates Page Parameters

Parameter	Value	Description
alias		The name to assign to your new Certificate This is the alias of the keystore you created in Section 26.3.2.1.2, "Generating and Registering Certificates."
Path		Specify the path name of the .der file containing the X.509 certificate you want to import. This is the file you created in Section 26.3.2.1.2, "Generating and Registering Certificates."

8. Click **OK** to save your settings.

9. Repeat the previous step for the SAML ID Asserter created in the SOA domain. Ensure that you copy over `testalias.der` (if this was the name given to your `.DER` file) from your WebLogic Home to the machine hosting the SOA domain.

To Configure an Asserting Party

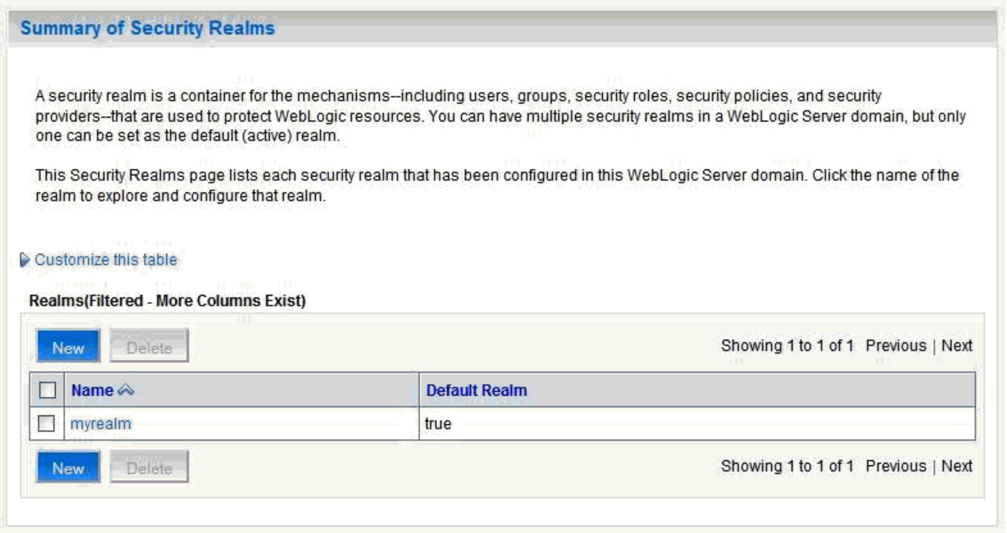
1. Log in to the WebLogic Server Administration Console.

   For information on logging in to the WebLogic Server Administration Console, see Section 1.12.2, "Oracle WebLogic Server Administration Console."

2. From the Domain Structure pane, click **Security Realms**.

   The Summary of Security Realms pane displays (see Figure 26–62).

Figure 26–62 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.

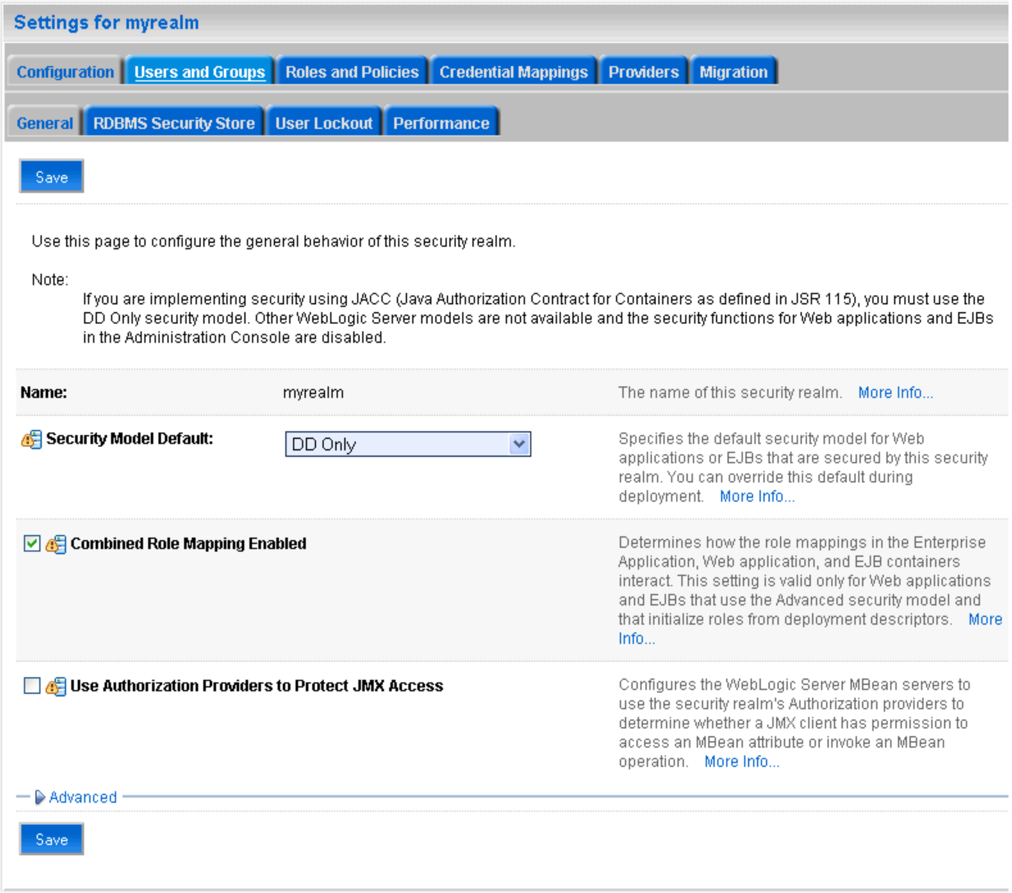
Realms(Filtered - More Columns Exist)

□	Name	Default Realm
□	myrealm	true

3. Click your security realm.

   The Settings page for the security realm displays (see Figure 26–63).

Figure 26–63 Security Realm Settings Page



Settings for myrealm

Use this page to configure the general behavior of this security realm.

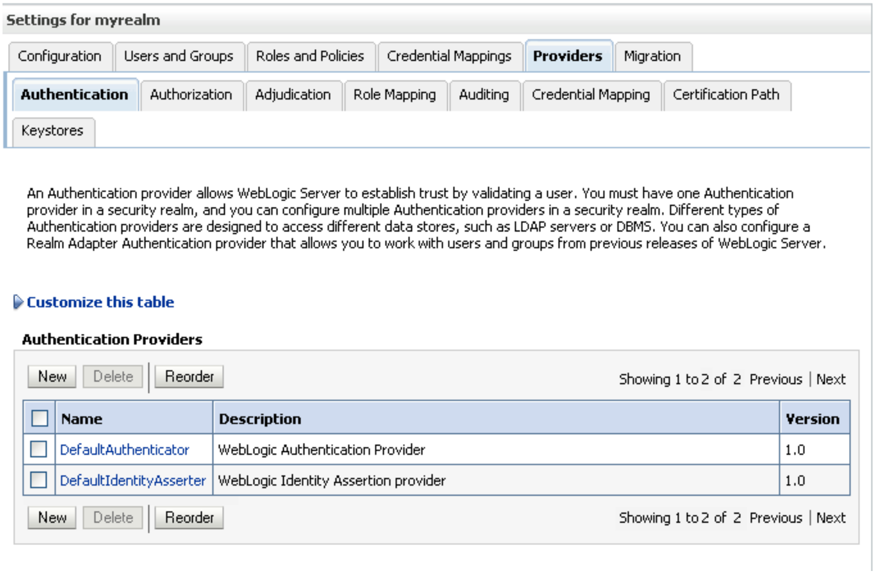
Note:
If you are implementing security using JACC (Java Authorization Contract for Containers as defined in JSR 115), you must use the DD Only security model. Other WebLogic Server models are not available and the security functions for Web applications and EJBs in the Administration Console are disabled.

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...

4. Open the Providers tab and select the Authentication subtab.

   The Authentication Settings pane displays (see Figure 26–64).

Figure 26–64 Authentication Settings Pane



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.

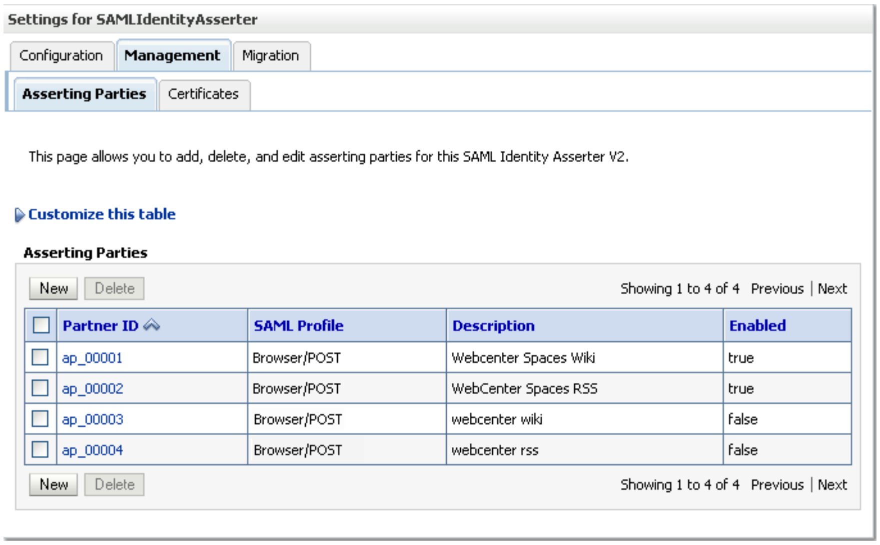
Authentication Providers

□	Name	Description	Version
□	DefaultAuthenticator	WebLogic Authentication Provider	1.0
□	DefaultIdentityAsserter	WebLogic Identity Assertion provider	1.0

5. Click the SAML Identity Asserter you created and open the Management tab and the Asserting Parties subtab.

   The Asserting Parties Settings pane displays (see Figure 26–65).

Figure 26–65 Asserting Parties Settings Pane



This page allows you to add, delete, and edit asserting parties for this SAML Identity Asserter V2.

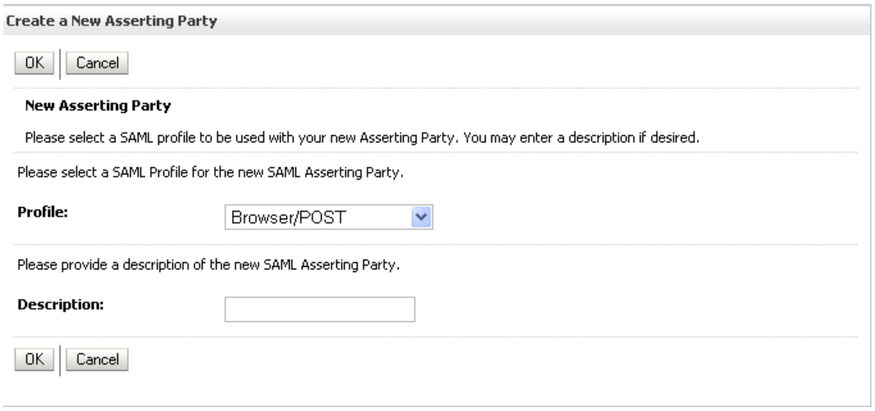
Asserting Parties

□	Partner ID	SAML Profile	Description	Enabled
□	ap_00001	Browser/POST	Webcenter Spaces Wiki	true
□	ap_00002	Browser/POST	WebCenter Spaces RSS	true
□	ap_00003	Browser/POST	webcenter wiki	false
□	ap_00004	Browser/POST	webcenter rss	false

6. Click **New**.

   The Create a New Asserting Party page displays (see Figure 26–66).

Figure 26–66 Create a New Asserting Party Page



Create a New Asserting Party

New Asserting Party

Please select a SAML profile to be used with your new Asserting Party. You may enter a description if desired.

Please select a SAML Profile for the new SAML Asserting Party.

Profile: Browser/POST

Please provide a description of the new SAML Asserting Party.

Description:

7. Select the **Profile** and provide a **Description** for the Asserting Party.

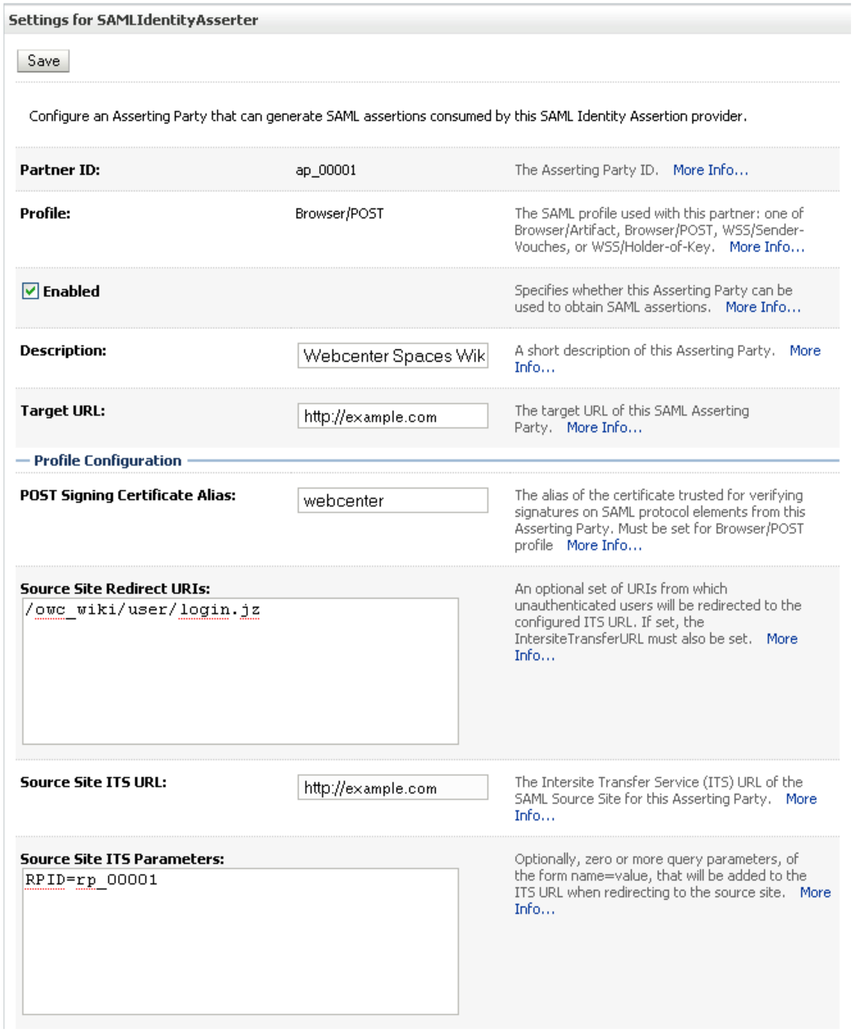
   Use the same SAML profile you chose for the corresponding relying party (for example, `Browser/POST`).

8. Click **OK** to save your settings.

9. From the Asserting Parties Settings pane, click the Partner ID of the Asserting Party you just created (the Partner ID is assigned automatically).

   The Settings page for the new Asserting Party displays (see Figure 26–67).

Figure 26–67 Asserting Party Settings Page



Settings for SAMLIdentityAsserter

Save

Configure an Asserting Party that can generate SAML assertions consumed by this SAML Identity Assertion provider.

Partner ID:	ap_00001	The Asserting Party ID. More Info...
Profile:	Browser/POST	The SAML profile used with this partner: one of Browser/Artifact, Browser/POST, WSS/Sender-Vouches, or WSS/Holder-of-Key. More Info...
☑ **Enabled**		Specifies whether this Asserting Party can be used to obtain SAML assertions. More Info...
Description:	Webcenter Spaces Wik	A short description of this Asserting Party. More Info...
Target URL:	http://example.com	The target URL of this SAML Asserting Party. More Info...

Profile Configuration

POST Signing Certificate Alias:	webcenter	The alias of the certificate trusted for verifying signatures on SAML protocol elements from this Asserting Party. Must be set for Browser/POST profile More Info...
Source Site Redirect URIs:	/owc_wiki/user/login.jz	An optional set of URIs from which unauthenticated users will be redirected to the configured ITS URL. If set, the IntersiteTransferURL must also be set. More Info...
Source Site ITS URL:	http://example.com	The Intersite Transfer Service (ITS) URL of the SAML Source Site for this Asserting Party. More Info...
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. More Info...

10. Configure the Asserting Party for the WebCenter domain Wiki service as shown in Table 26–11. For more information, see Table 26–3, " Relying Party Settings for Wiki Service".

Table 26–11 WebCenter Domain - Asserting Party for Wiki

Parameter	Value	Description
Enabled	Checked	Specifies whether this Asserting Party can be used to obtain SAML assertions
Description		A short description of this Asserting Party (for example, `WebCenter Spaces for Wiki`)
Target URL		The target URL of this SAML Asserting Party (for example, `http://example.com:8888/webcenter`)
POST Signing Certificate alias		The alias of the certificate trusted for verifying signatures on SAML protocol elements from this Asserting Party (for example, `testalias`). Must be set when using the Browser/POST profile.

Table 26–11 (Cont.) WebCenter Domain - Asserting Party for Wiki

Parameter	Value	Description
Source Site Redirect URIs	`/owc_wiki/user/login.jz`	An optional set of URIs from which unauthenticated users are redirected to the configured ITS URL. If set, the IntersiteTransferURL must also be set. **Note:** Based on this setting, when you first access the destination site, you are redirected to the configured ITS URL (which in this case is within the source application), your session is established with the source application and then redirected to the destination site.
Source Site ITS URL		The Intersite Transfer Service (ITS) URL of the SAML Source Site for this Asserting Party (for example, `http://example.com:8888/webcenter/samlits/its`). Used with SSO profiles only, to support the destination site first scenario, whereby a user tries to access a destination site URL before being authenticated and is redirected to the source site to be authenticated and obtain a SAML assertion. The Redirect URIs attribute must also be configured for source-site redirection to work. **Note:** If you check **ITS requires SSL** in Source Site Federation Services, you must also change the Source Site ITS URL to use HTTPS and the server's SSL port.
Source Site ITS parameters	`RPID=rp_00001`	Optionally, zero or more query parameters, of the form `name=value`, that will be added to the ITS URL when redirecting to the source site. In this case, `rp_00001` is the relying party ID for the OWC Wiki application specified in the SAML Credential Mapping Provider of the WebCenter domain which provides the destination site details. For more information, see Table 26–3, " Relying Party Settings for Wiki Service".
Issuer URI		The issuer URI of the SAML Authority issuing assertions for this SAML Asserting Party (for example, `http://www.example.com/webcenter`). This URI should be the same as the Issuer URI for the SAML Credential Mapping provider as specified in Table 26–2, " SAML Credential Mapping Provider Security Realm Settings".
Signature Required	Checked	If true, assertions must be signed. If false, signature elements are not required, but will be verified if present.
Assertion Signing Certificate alias		The alias of the certificate trusted for verifying signatures on assertions from this Asserting Party (for example, testalias). This must be set if **Signature Required** is checked. The certificate must also be registered in the SAML Identity Asserter's certificate registry.

11. Click **Save** to save your settings.

12. Repeat steps 1 - 11 using the settings shown in Table 26–12 to configure the Asserting party for the WebCenter domain RSS application.

Table 26–12 WE Domain - Asserting Party for RSS

Parameter	Value	Description
Enabled	Checked	Specifies whether this Asserting Party can be used to obtain SAML assertions.
Description		A short description of this Asserting Party (for example, `WebCenter Spaces for RSS`)
Target URL		The target URL of this SAML Asserting Party (for example, `http://example.com:8888/webcenter`)
POST Signing Certificate alias		The alias of the certificate trusted for verifying signatures on SAML protocol elements from this Asserting Party (for example, `testalias`). Must be set when using the Browser/POST profile.
Source Site Redirect URIs	`/rss/rssservlet`	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:** Based on this setting, when you first access the destination site, you are redirected to the configured ITS URL (which in this case is within the source application), your session is established with the source application and then redirected to the destination site.
Source Site ITS URL		The Intersite Transfer Service (ITS) URL of the SAML Source Site for this Asserting Party (for example, `http://example.com:8888/webcenter/samlits/its`). Used with SSO profiles only, to support the destination site first scenario, whereby a user tries to access a destination site URL before being authenticated and is redirected to the source site to be authenticated and obtain a SAML assertion. The Redirect URIs attribute must also be configured for source-site redirection to work. **Note:** If you check **ITS requires SSL** in Source Site Federation Services, you must also change the Source Site ITS URL to use HTTPS and the server's SSL port.
Source Site ITS parameters	`RPID=rp_00002`	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_00002` is the relying party ID for RSS specified in the SAML Credential Mapping provider of the WebCenter domain which provides the destination site details. See Table 26–7, " Relying Party Settings for RSS" for more information about RSS settings.

Table 26–12 (Cont.) WE Domain - Asserting Party for RSS

Parameter	Value	Description
Issuer URI		The issuer URI of the SAML Authority issuing assertions for this SAML Asserting Party (for example, `http://www.example.com/webcenter`). This URI should be the same as the Issuer URI for the SAML Credential Mapping provider as specified in Table 26–2, " SAML Credential Mapping Provider Security Realm Settings".
Signature Required	Checked	If true, assertions must be signed. If false, signature elements are not required, but will be verified if present.
Assertion Signing Certificate alias		The alias of the certificate trusted for verifying signatures on assertions from this Asserting Party (for example, `testalias`). This must be set if **Signature Required** is checked. The certificate must also be registered in the SAML Identity Asserter's certificate registry.

13. Repeat steps 1 - 11 using the settings shown in Table 26–13 to configure the Asserting party for the WebCenter domain Discussions application.

Table 26–13 WebCenter Domain - Asserting Party for Discussions

Parameter	Value	Description
Enabled	Checked	Specifies whether this Asserting Party can be used to obtain SAML assertions.
Description		A short description of this Asserting Party (for example, `WebCenter Spaces for Discussions`)
Target URL		The target URL of this SAML Asserting Party (for example, `http://example.com:8888/webcenter`)
POST Signing Certificate alias		The alias of the certificate trusted for verifying signatures on SAML protocol elements from this Asserting Party (for example, `testalias`). This must be set when using the Browser/POST profile.

Source Site Redirect URIs	`/owc_discussions/admin/content-main.jsp`
	`/owc_discussions/login!withRedirect.jspa`
	`/owc_discussions/login!default.jspa`
	`/owc_discussions/login.jspa`
		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: Based on this setting, when you first access the destination site, you are redirected to the configured ITS URL (which in this case is within the source application), your session is established with the source application and then redirected to the destination site.

Table 26–13 (Cont.) WebCenter Domain - Asserting Party for Discussions

Parameter	Value	Description
Source Site ITS URL		The Intersite Transfer Service (ITS) URL of the SAML Source Site for this Asserting Party (for example, `http://example.com:8888/webcenter/samlits/its`). Used with SSO profiles only, to support the destination site first scenario, whereby a user tries to access a destination site URL before being authenticated and is redirected to the source site to be authenticated and obtain a SAML assertion. The Redirect URIs attribute must also be configured for source-site redirection to work. **Note:** If you check **ITS requires SSL** in Source Site Federation Services, you must also change the Source Site ITS URL to use HTTPS and the server's SSL port.
Source Site ITS parameters	`RPID=rp_00006`	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_00006` is the relying party ID for OWC Discussions specified in the SAML Credential Mapping provider of the WebCenter domain which provides the destination site details. See Table 26–8, " Relying Party Settings for Discussions" for more information about Discussions settings.
Issuer URI		The issuer URI of the SAML Authority issuing assertions for this SAML Asserting Party (for example, `http://www.example.com/webcenter`). This URI should be the same as the Issuer URI for the SAML Credential Mapping provider as specified in Table 26–2, " SAML Credential Mapping Provider Security Realm Settings".
Signature Required	Checked	If true, assertions must be signed. If false, signature elements are not required, but will be verified if present.
Assertion Signing Certificate alias		The alias of the certificate trusted for verifying signatures on assertions from this Asserting Party (for example, `testalias`). This must be set if **Signature Required** is checked. The certificate must also be registered in the SAML Identity Asserter's certificate registry.

14. Change domains to the SOA domain and repeat steps 1 - 11 using the settings shown in Table 26–14 to configure the Asserting Party for the SOA domain Worklist Community Detail service.

Table 26–14 SOA Domain - Asserting Party for Worklist Community Detail

Parameter	Value	Description
Enabled	Checked	Specifies whether this Asserting Party can be used to obtain SAML assertions

Table 26–14 (Cont.) SOA Domain - Asserting Party for Worklist Community Detail

Parameter	Value	Description
Description		A short description of this Asserting Party (for example, `WebCenter Spaces for Worklist Detail`)
Target URL		The target URL of this SAML Asserting Party (for example, `http://example.com:8888/webcenter`)
POST Signing Certificate alias		The alias of the certificate trusted for verifying signatures on SAML protocol elements from this Asserting Party (for example, `testalias`). Must be set when using Browser/POST profile.
Source Site Redirect URIs	`/workflow/WebCenterWorklistDetail/faces/adf.task-flow`	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:** Based on this setting, when you first access the destination site, you are redirected to the configured ITS URL (which in this case is within the source application), your session is established with the source application and then redirected to the destination site.
Source Site ITS URL		The Intersite Transfer Service (ITS) URL of the SAML Source Site for this Asserting Party (for example, `http://example.com:8888/webcenter/samlits/its`). Used with SSO profiles only, to support the destination site first scenario, whereby a user tries to access a destination site URL before being authenticated and is redirected to the source site to be authenticated and obtain a SAML assertion. The Redirect URIs attribute must also be configured for source-site redirection to work. **Note:** If you check **ITS requires SSL** in Source Site Federation Services, you must also change the Source Site ITS URL to use HTTPS and the server's SSL port.
Source Site ITS parameters	`RPID=rp_00002`	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_00002` is the relying party ID for the Worklist Detail application specified in the SAML Credential Mapping provider for the WebCenter domain, which provides the destination site details. For more information, see Table 26–4, " Relying Party Settings for Worklist Community Detail".
Issuer URI		The issuer URI of the SAML Authority issuing assertions for this SAML Asserting Party (for example, `http://www.example.com/webcenter`). This URI should be the same as the Issuer URI for the SAML Credential Mapping provider as specified in Table 26–2, " SAML Credential Mapping Provider Security Realm Settings".

Table 26–14 (Cont.) SOA Domain - Asserting Party for Worklist Community Detail

Parameter	Value	Description
Signature Required	Checked	If checked, assertions must be signed. If unchecked, signature elements are not required, but will be verified if present.
Assertion Signing Certificate alias		The alias of the certificate trusted for verifying signatures on assertions from this Asserting Party (for example, `testalias`). This must be set if **Signature Required** is checked. The certificate must also be registered in the SAML Identity Asserter's certificate registry.

15. Change domains to the SOA domain and repeat steps 1 - 11 using the settings shown in Table 26–15 to configure the Asserting Party for the SOA domain Worklist SDP service. For more information see Table 26–5, " Relying Party Settings for Worklist SDP" and Table 26–6, " Relying Party Settings for Worklist Integration".

Table 26–15 SOA Domain - Asserting Party for Worklist SDP

Parameter	Value	Description
Enabled	Checked	Specifies whether this Asserting Party can be used to obtain SAML assertions.
Description		A short description of this Asserting Party (for example, `WebCenter Spaces for Worklist SDP`)
Target URL		The target URL of this SAML Asserting Party (for example, `http://example.com:8888/webcenter`)
POST Signing Certificate alias		The alias of the certificate trusted for verifying signatures on SAML protocol elements from this Asserting Party (for example, `testalias`). Must be set when using Browser/POST profile.
Source Site Redirect URIs	`/workflow/sdpmessagingsca-ui-worklist/faces/adf.task-flow`	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:** Based on this setting, when you first access the destination site, you are redirected to the configured ITS URL (which in this case is within the source application), your session is established with the source application and then redirected to the destination site.

Table 26–15 (Cont.) SOA Domain - Asserting Party for Worklist SDP

Parameter	Value	Description
Source Site ITS URL		The Intersite Transfer Service (ITS) URL of the SAML Source Site for this Asserting Party (for example, `http://example.com:8888/webcenter/samlits/its`). Used with SSO profiles only, to support the destination site first scenario, whereby a user tries to access a destination site URL before being authenticated and is redirected to the source site to be authenticated and obtain a SAML assertion. The Redirect URIs attribute must also be configured for source-site redirection to work. **Note:** If you check **ITS requires SSL** in Source Site Federation Services, you must also change the Source Site ITS URL to use HTTPS and the server's SSL port.
Source Site ITS parameters	`RPID=rp_00003`	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_00003` is the relying party ID for the Worklist SDP application specified in the SAML Credential Mapping provider of the WebCenter domain, which provides the destination site details. For more information, see Table 26–5, " Relying Party Settings for Worklist SDP".
Issuer URI		The issuer URI of the SAML Authority issuing assertions for this SAML Asserting Party (for example, `http://www.example.com/webcenter`). This URI should be the same as the Issuer URI for the SAML Credential Mapping provider as specified in Table 26–2, " SAML Credential Mapping Provider Security Realm Settings".
Signature Required	Checked	If true, assertions must be signed. If false, signature elements are not required, but will be verified if present.
Assertion Signing Certificate alias		The alias of the certificate trusted for verifying signatures on assertions from this Asserting Party (for example, `testalias`). This must be set if **Signature Required** is checked. The certificate must also be registered in the SAML Identity Asserter's certificate registry.

16. Change domains to the SOA domain and repeat steps 1 - 11 using the settings shown in Table 26–16 to configure the Asserting Party for the SOA domain Worklist Community Integration service.

Table 26–16 In SOA Domain, Asserting party For Worklist Integration

Parameter	Value	Description
Enabled	Checked	Specifies whether this Asserting Party can be used to obtain SAML assertions

Table 26–16 (Cont.) In SOA Domain, Asserting party For Worklist Integration

Parameter	Value	Description
Description	WebCenter Spaces for Worklist SDP	A short description of this Asserting Party (for example, `WebCenter Spaces for Worklist SDP`)
Target URL		The target URL of this SAML Asserting Party (for example, `http://example.com:8888/webcenter`)
POST Signing Certificate alias		The alias of the certificate trusted for verifying signatures on SAML protocol elements from this Asserting Party (for example, `testalias`). Must be set when using Browser/POST profile.
Source Site Redirect URIs	`/integration/worklistapp/ssologin` `/integration/worklistapp/faces/home.jspx`	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:** Based on this setting, when you first access the destination site, you are redirected to the configured ITS URL (which in this case is within the source application), your session is established with the source application and then redirected to the destination site.
Source Site ITS URL		The Intersite Transfer Service (ITS) URL of the SAML Source Site for this Asserting Party (for example, `http://example.com:8888/webcenter/samlits/its`). Used with SSO profiles only, to support the destination site first scenario, whereby a user tries to access a destination site URL before being authenticated and is redirected to the source site to be authenticated and obtain a SAML assertion. The Redirect URIs attribute must also be configured for source-site redirection to work. **Note:** If you check **ITS requires SSL** in Source Site Federation Services, you must also change the Source Site ITS URL to use HTTPS and the server's SSL port.
Source Site ITS parameters	`RPID=rp_00004`	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_00004` is the relying party ID for the Worklist Integration application specified in the SAML Credential Mapping provider of the WebCenter domain, which provides the destination site details. For more information, see Table 26–6, " Relying Party Settings for Worklist Integration".
Issuer URI		The issuer URI of the SAML Authority issuing assertions for this SAML Asserting Party (for example, `http://www.example.com/webcenter`). This URI should be the same as the Issuer URI for the SAML Credential Mapping provider as specified in Table 26–2, " SAML Credential Mapping Provider Security Realm Settings".

Table 26–16 (Cont.) In SOA Domain, Asserting party For Worklist Integration

Parameter	Value	Description
Signature Required	Checked	If true, assertions must be signed. If false, signature elements are not required, but will be verified if present.
Assertion Signing Certificate alias		The alias of the certificate trusted for verifying signatures on assertions from this Asserting Party (for example, `testalias`). This must be set if **Signature Required** is checked. The certificate must also be registered in the SAML Identity Asserter's certificate registry.

26.3.2.3.5 Configuring Destination Site Federation Services

This section describes how to configure the Destination Site Federation Services for the Wiki service, RSS, and the Worklist service on the WebCenter domain.

To configure the Destination Site Federation Services:

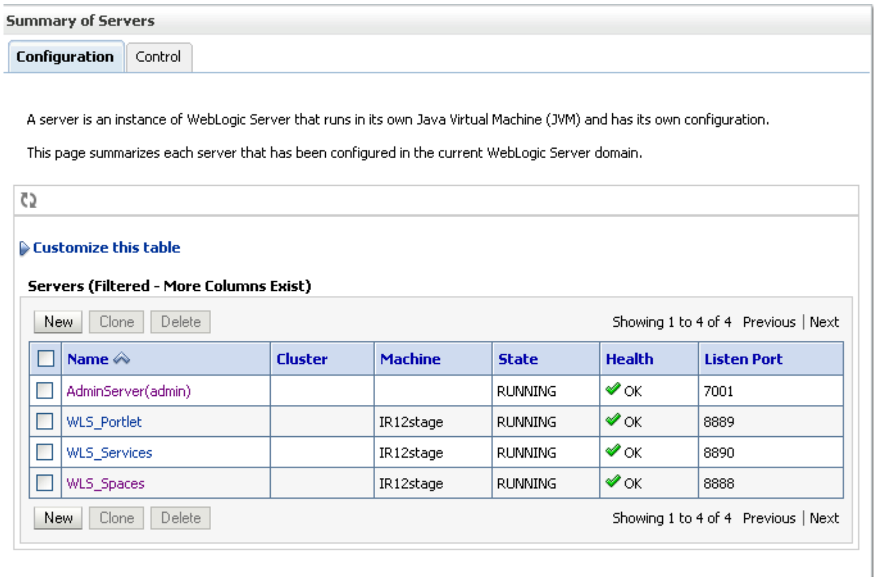
1. Log in to the WebLogic Server Administration Console.

   For information on logging in to the WebLogic Server Administration Console, see Section 1.12.2, "Oracle WebLogic Server Administration Console."

2. On the Domain Structure pane, expand the **Environment** node and click **Servers**.

   The Summary of Servers page displays (see Figure 26–68).

Figure 26–68 Summary of Servers Page



Summary of Servers

Configuration | Control

A server is an instance of WebLogic Server that runs in its own Java Virtual Machine (JVM) and has its own configuration.

This page summarizes each server that has been configured in the current WebLogic Server domain.

Customize this table

Servers (Filtered - More Columns Exist)

New | Clone | Delete — Showing 1 to 4 of 4 Previous | Next

□	Name	Cluster	Machine	State	Health	Listen Port
□	AdminServer(admin)			RUNNING	✓ OK	7001
□	WLS_Portlet		IR12stage	RUNNING	✓ OK	8889
□	WLS_Services		IR12stage	RUNNING	✓ OK	8890
□	WLS_Spaces		IR12stage	RUNNING	✓ OK	8888

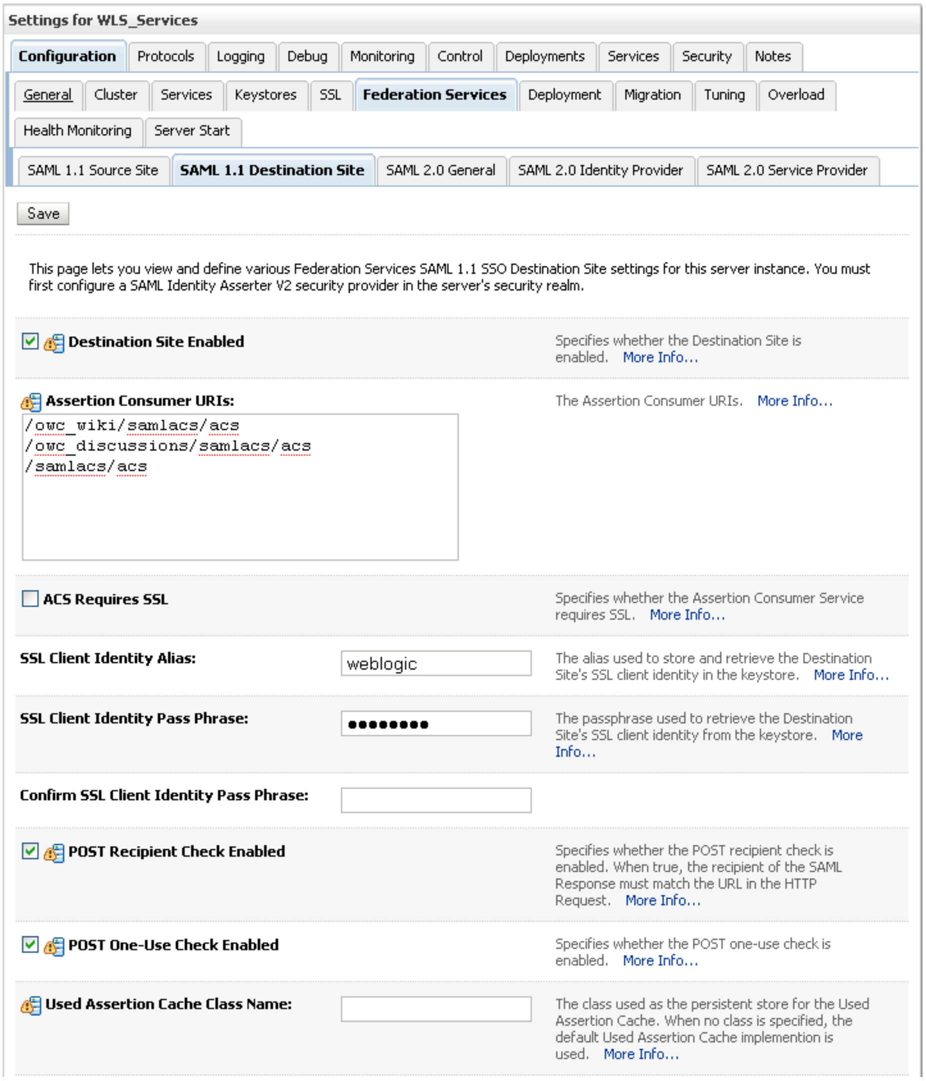
New | Clone | Delete — Showing 1 to 4 of 4 Previous | Next

3. Click `WLS_Services` (the managed server where the Wiki service and Discussions service are deployed) and open the Configuration tab.

4. Open the Federation Services tab and the SAML 1.1 Destination Site subtab.

   The SAML 1.1 Destination Site Settings pane displays (see Figure 26–69).

Figure 26–69 SAML 1.1 Destination Site Settings Pane (Wiki and Discussions)



This page lets you view and define various Federation Services SAML 1.1 SSO Destination Site settings for this server instance. You must first configure a SAML Identity Asserter V2 security provider in the server's security realm.

☑ Destination Site Enabled — Specifies whether the Destination Site is enabled. More Info...

Assertion Consumer URIs: — The Assertion Consumer URIs. More Info...

```
/owc_wiki/samlacs/acs
/owc_discussions/samlacs/acs
/samlacs/acs
```

☐ ACS Requires SSL — Specifies whether the Assertion Consumer Service requires SSL. More Info...

SSL Client Identity Alias: weblogic — The alias used to store and retrieve the Destination Site's SSL client identity in the keystore. More Info...

SSL Client Identity Pass Phrase: ●●●●●●●●● — The passphrase used to retrieve the Destination Site's SSL client identity from the keystore. More Info...

Confirm SSL Client Identity Pass Phrase:

☑ POST Recipient Check Enabled — Specifies whether the POST recipient check is enabled. When true, the recipient of the SAML Response must match the URL in the HTTP Request. More Info...

☑ POST One-Use Check Enabled — Specifies whether the POST one-use check is enabled. More Info...

Used Assertion Cache Class Name: — The class used as the persistent store for the Used Assertion Cache. When no class is specified, the default Used Assertion Cache implemention is used. More Info...

5. Configure the SAML destination site attributes for the Wiki and Discussions applications as shown in Table 26–17.

Table 26–17 SAML Destination Site Attributes (Wiki and Discussions)

Parameter	Value	Description
Destination Site Enabled	Checked	Specifies whether the Destination Site is enabled.
ACS Requires SSL	Unchecked	Specifies whether the Assertion Consumer Service requires SSL. If checked, then ensure that the ACS URL specified in the Credential Mapper's relying party uses HTTPS and target server's SSL port.

Table 26–17 (Cont.) SAML Destination Site Attributes (Wiki and Discussions)

Parameter	Value	Description

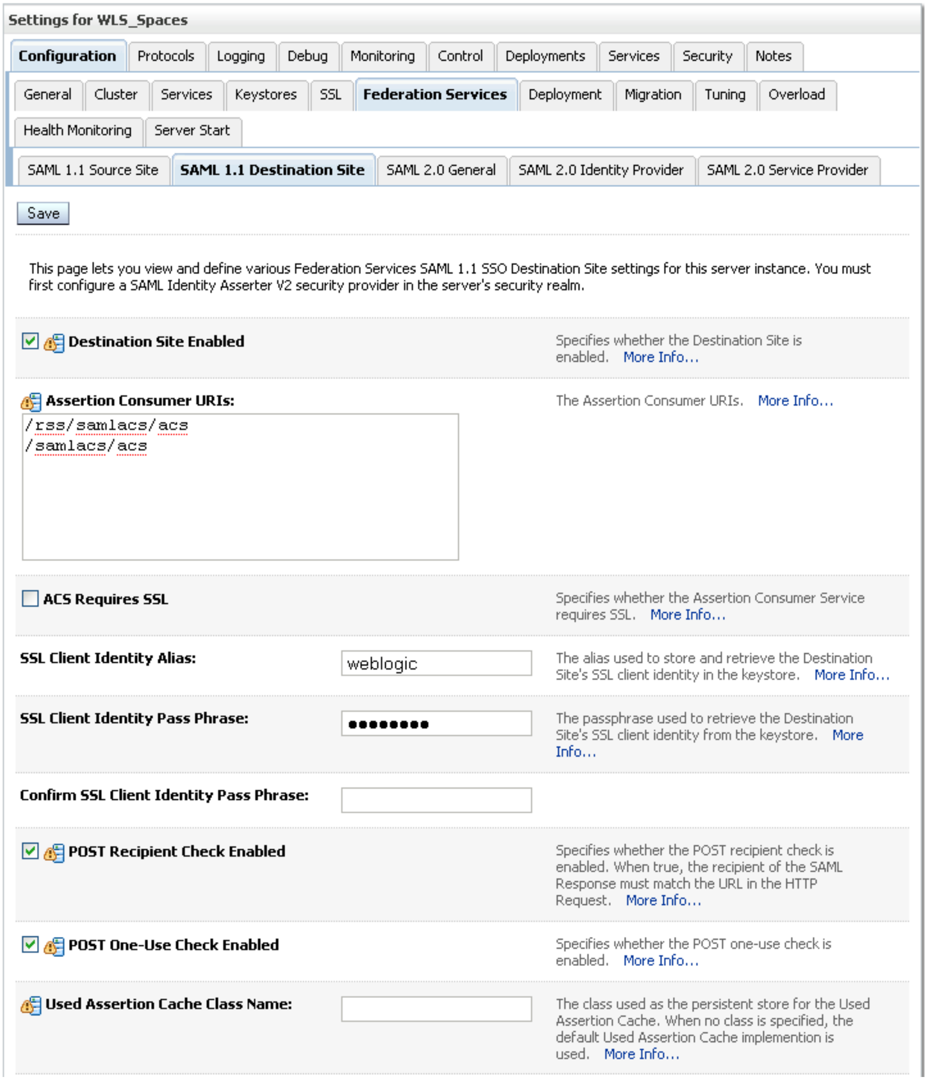
Assertion Consumer URIs	`/owc_wiki/samlacs/acs`
	`/owc_discussions/samlacs/acs`
	[add on top, leave rest as is]
		The Assertion Consumer URIs. In this case, we have chosen for the ACS to reside within the target app so that it uses the same login cookie.

POST Recipient Check Enabled	Checked	Specifies whether the POST recipient check is enabled. When checked, the recipient of the SAML Response must match the URL in the HTTP Request.
POST One use Check Enabled	Checked	Specifies whether the POST one-use check is enabled.

6. Click **Save** to save your settings, and restart the `WLS_Services` server so that they take effect.
7. From the Domain Structure pane, expand the **Environment** node and click **Servers**.
8. Click `WLS_Spaces` (the managed server where RSS is deployed) and open the Configuration tab.
9. Open the Federation Services tab and the SAML 1.1 Destination Site subtab.

   The SAML 1.1 Destination Site Settings pane displays (see Figure 26–70).

Figure 26–70 SAML 1.1 Destination Site Settings Pane (RSS)



This page lets you view and define various Federation Services SAML 1.1 SSO Destination Site settings for this server instance. You must first configure a SAML Identity Asserter V2 security provider in the server's security realm.

☑ **Destination Site Enabled** — Specifies whether the Destination Site is enabled. More Info...

Assertion Consumer URIs: — The Assertion Consumer URIs. More Info...

```
/rss/samlacs/acs
/samlacs/acs
```

☐ **ACS Requires SSL** — Specifies whether the Assertion Consumer Service requires SSL. More Info...

SSL Client Identity Alias: weblogic — The alias used to store and retrieve the Destination Site's SSL client identity in the keystore. More Info...

SSL Client Identity Pass Phrase: ●●●●●●●● — The passphrase used to retrieve the Destination Site's SSL client identity from the keystore. More Info...

Confirm SSL Client Identity Pass Phrase:

☑ **POST Recipient Check Enabled** — Specifies whether the POST recipient check is enabled. When true, the recipient of the SAML Response must match the URL in the HTTP Request. More Info...

☑ **POST One-Use Check Enabled** — Specifies whether the POST one-use check is enabled. More Info...

Used Assertion Cache Class Name: — The class used as the persistent store for the Used Assertion Cache. When no class is specified, the default Used Assertion Cache implemention is used. More Info...

10. Configure the SAML destination site attributes for RSS as shown in Table 26–18.

Table 26–18 SAML Destination Site Attributes (RSS)

Parameter	Value	Description
Destination Site Enabled	Checked	Specifies whether the Destination Site is enabled.
ACS Requires SSL	Unchecked	Specifies whether the Assertion Consumer Service requires SSL. If checked, then ensure that ACS URL specified in Credential Mapper's relying party uses https and target server's SSL port.
Assertion Consumer URIs	`/rss/samlacs/acs` (add on top, leave rest as is)	The Assertion Consumer URIs. In this case, we have chosen for the ACS to reside within the target app so that it uses the same login cookie.

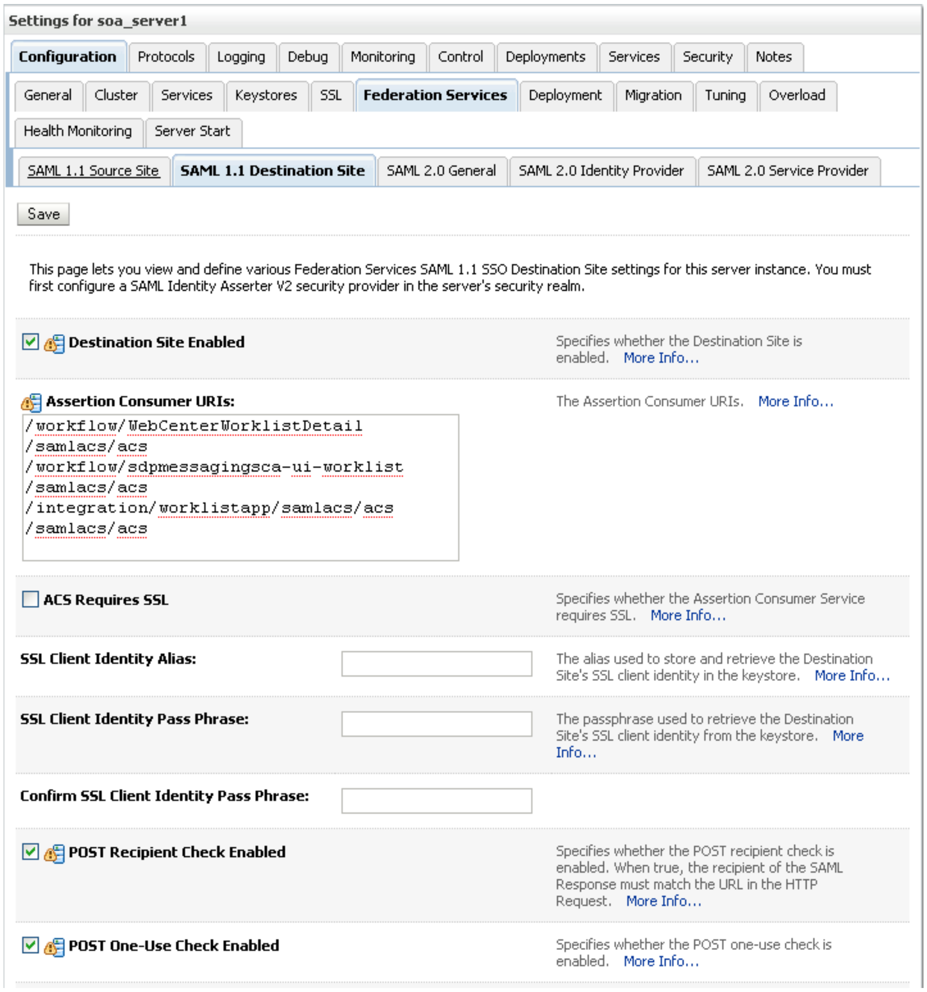
Table 26–18 (Cont.) SAML Destination Site Attributes (RSS)

Parameter	Value	Description
POST Recipient Check Enabled	Checked	Specifies whether the POST recipient check is enabled. When true, the recipient of the SAML Response must match the URL in the HTTP Request.
POST One use Check Enabled	Checked	Specifies whether the POST one-use check is enabled.

11. Click **Save** to save your settings, and restart the `WSL_Spaces` server so that they take effect.
12. Navigate to the SOA domain and then to `soa_server1`, or the managed server where the Worklist applications are deployed.
13. Follow the same steps as above to open the SAML 1.1 Destination Site subtab.

    The SAML 1.1 Destination Site Settings pane displays (see Figure 26–71).

Figure 26–71 SAML 1.1 Destination Site Settings Pane (Worklist Detail and SDP)



This page lets you view and define various Federation Services SAML 1.1 SSO Destination Site settings for this server instance. You must first configure a SAML Identity Asserter V2 security provider in the server's security realm.

☑ Destination Site Enabled — Specifies whether the Destination Site is enabled. More Info...

Assertion Consumer URIs: — The Assertion Consumer URIs. More Info...

```
/workflow/WebCenterWorklistDetail
/samlacs/acs
/workflow/sdpmessagingsca-ui-worklist
/samlacs/acs
/integration/worklistapp/samlacs/acs
/samlacs/acs
```

☐ ACS Requires SSL — Specifies whether the Assertion Consumer Service requires SSL. More Info...

SSL Client Identity Alias: — The alias used to store and retrieve the Destination Site's SSL client identity in the keystore. More Info...

SSL Client Identity Pass Phrase: — The passphrase used to retrieve the Destination Site's SSL client identity from the keystore. More Info...

Confirm SSL Client Identity Pass Phrase:

☑ POST Recipient Check Enabled — Specifies whether the POST recipient check is enabled. When true, the recipient of the SAML Response must match the URL in the HTTP Request. More Info...

☑ POST One-Use Check Enabled — Specifies whether the POST one-use check is enabled. More Info...

14. Configure the SAML 1.1 Destination Site attributes for Worklist Detail and SDP as shown in Table 26–19.

Table 26–19 SOA Domain - SAML Destination Site Attributes (Worklist Detail and SDP)

Parameter	Value	Description
Destination Site Enabled	Checked	Specifies whether the Destination Site is enabled.
ACS Requires SSL	Unchecked	Specifies whether the Assertion Consumer Service requires SSL. If checked, then ensure that ACS URL specified in Credential Mapper's relying party uses HTTPS and the target server's SSL port.

Assertion Consumer URIs	`/workflow/WebCenterWorklistDetail/samlacs/acs`
	`/workflow/sdpmessagingsca-ui-worklist/samlacs/acs`
	`/integration/worklistapp/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 app so that it uses the same login cookie.

POST Recipient Check Enabled	Checked	Specifies whether the POST recipient check is enabled. When checked, the recipient of the SAML Response must match the URL in the HTTP Request.
POST One use Check Enabled	Checked	Specifies whether the POST one-use check is enabled.

15. Click **Save** to save your settings.
16. Restart the SOA managed server.
17. Check your configuration as described in Section 26.3.2.4, "Checking Your Configuration."

26.3.2.4 Checking Your Configuration

The last step in the process is to check that your single sign-on configuration is working. To do that:

1. Check that when you try to access wiki and RSS applications independently, you are taken to the WebCenter Spaces login page (source site) and then directed to the URL you were trying to access.
2. Using a new browser, log in to WebCenter Spaces and check that you're not challenged for credentials when:
   - You access a wiki from a group space
   - You access RSS from a list task flow
   - You click **Forum Administration** from **Group Space Settings > Services > Discussions** (assuming this service is provisioned for the group space)
3. If you see that you are still challenged to log in, or see a 401 or 403 error code, check the configuration in the Administration Console and compare it with the documented configuration in Section 26.3.2.3, "Configuring SAML-based SSO Manually."

26.4 Configuring SSO with Microsoft Clients

This section describes how to set up single sign-on (SSO) with Microsoft clients, using Windows authentication based on the Simple and Protected Negotiate (SPNEGO) mechanism and the Kerberos protocol, together with the WebLogic Negotiate Identity Assertion provider for the WebCenter Spaces application. This SSO approach enables Microsoft clients (such as browsers), authenticated in a Windows domain using Kerberos, to be transparently authenticated to web applications (such as WebCenter Spaces) in a WebLogic domain based on the same credentials, and without the need to type in their password again.

Cross-platform authentication is achieved by emulating the negotiate behavior of native Windows-to-Windows authentication services that use the Kerberos protocol. In order for cross-platform authentication to work, non-Windows servers (in this case, WebLogic Server) must parse SPNEGO tokens in order to extract Kerberos tokens, which are then used for authentication.

This section contains the following sub-sections:

- Section 26.4.1, "Microsoft Client SSO Concepts"
- Section 26.4.2, "System Requirements"
- Section 26.4.3, "Configuring SSO with Microsoft Clients"

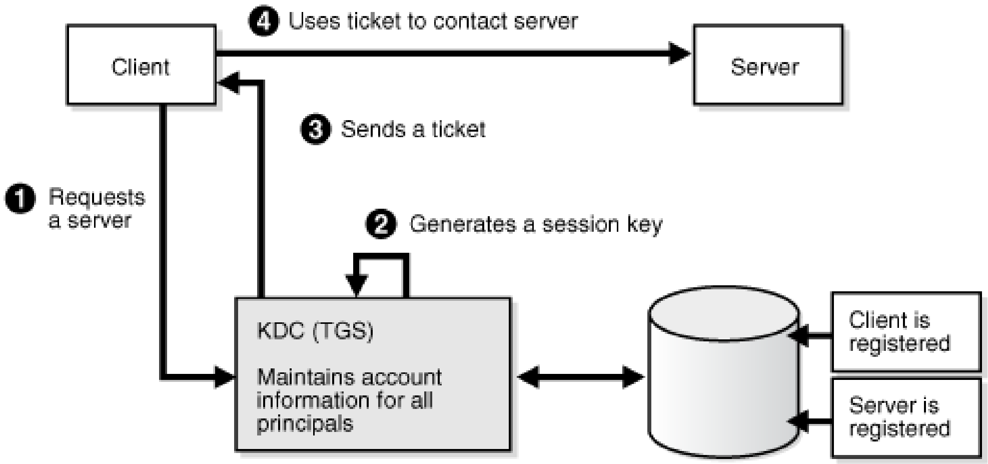
26.4.1 Microsoft Client SSO Concepts

Understanding Kerberos

Kerberos is a secure method for authenticating a request for a service in a network. The Kerberos protocol comprises three parties: a client, a server and a trusted third party to mediate between them, known as the KDC (Key Distribution Center). Under Kerberos, a server allows a user to access its service if the user can provide the server a Kerberos ticket that proves its identity. Both the user and the service are required to have keys registered with the KDC.

The diagram below describes the basic exchanges that must take place before a client connects to a server.

Figure 26–72 Connecting to a Server Through a Key Distribution Center


4 Uses ticket to contact server
Client
Server
3 Sends a ticket
1 Requests a server
2 Generates a session key
KDC (TGS)
Maintains account information for all principals
Client is registered
Server is registered

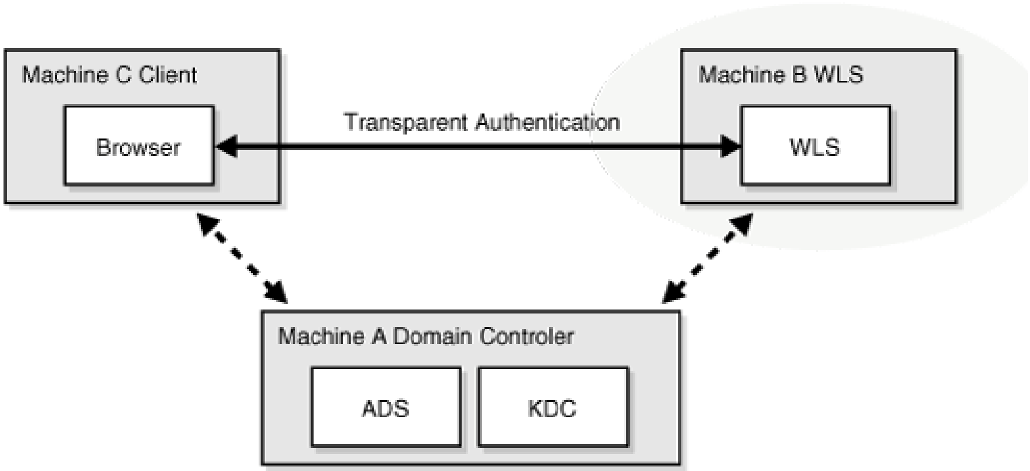
Understanding SPNEGO

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 26–73 SPNEGO-based Authentication



26.4.2 System Requirements

To use SSO with Microsoft clients you need:

A host computer with:

- Windows 2000 or later installed
- Fully-configured Active Directory authentication service. Specific Active Directory requirements include:
  - User accounts for mapping Kerberos services
  - Service Principal Names (SPNs) for those accounts
  - Key tab files created and copied to the start-up directory in the WebLogic Server domain
- WebLogic Server installed and configured properly to authenticate through Kerberos, as described in this section

Client systems with:

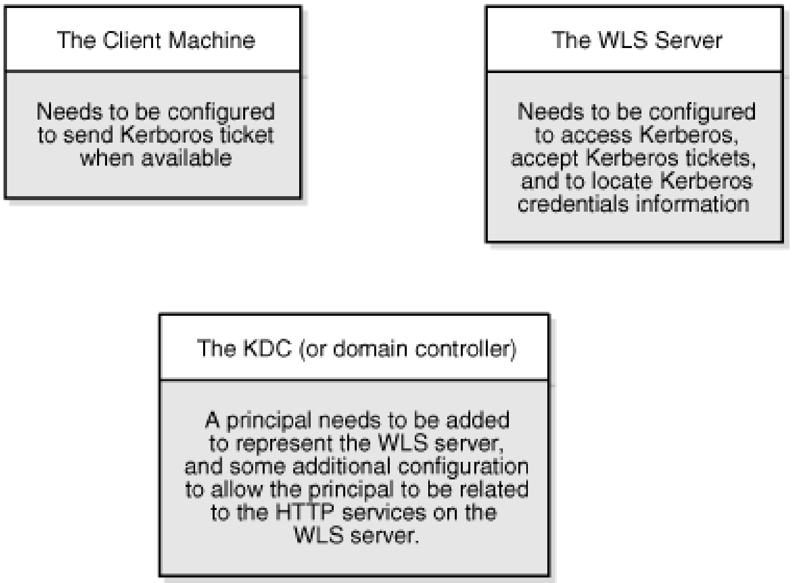
- Windows 2000 Professional SP2 or later installed
- One of the following types of clients:
  - A properly configured Internet Explorer browser. Internet Explorer 6.01 or later is supported.
  - .NET Framework 1.1 and a properly configured Web Service client.

> **Note:** Clients must be logged on to a Windows 2000 domain and have Kerberos credentials acquired from the Active Directory server in the domain. Local logons will not work.

26.4.3 Configuring SSO with Microsoft Clients

Configuring SSO with Microsoft clients requires configuring the Microsoft Active Directory, the client, and the WebLogic Server domain shown in Figure 26–74. For detailed configuration steps and troubleshooting, see "Configuring Single Sign-On with Microsoft Clients" in *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

Figure 26–74 Configuring SSO with Microsoft Clients


The Client Machine
Needs to be configured to send Kerboros ticket when available
The WLS Server
Needs to be configured to access Kerberos, accept Kerberos tickets, and to locate Kerberos credentials information
The KDC (or domain controller)
A principal needs to be added to represent the WLS server, and some additional configuration to allow the principal to be related to the HTTP services on the WLS server.

To configure Microsoft clients for SSO:

1. Configure your network domain to use Kerberos.
2. Create a Kerberos identification for WebLogic Server.
   a. Create a user account in the Active Directory for the host on which WebLogic Server is running.
   b. Create a Service Principal Name for this account.
   c. Create a user mapping and keytab file for this account.
3. Choose a Microsoft client (in this case Internet Explorer) and configure it to use Windows Integrated authentication.

4. Set up the WebLogic Server domain (`wc_domain` in this case) to use Kerberos authentication.

   a. Create a JAAS login file that points to the Active Directory server in the Microsoft domain and the keytab file created in Step 2.

   b. Configure a Negotiate Identity Assertion provider in the WebLogic Server security realm (see Section 26.4.3.1, "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 26.4.3.2, "Configuring an Active Directory Authentication Provider").

   Caution: Ensure that only the identity store is configured for Active Directory. The policy and credential stores are not certified for Active Directory.

5. Start the WebLogic Servers (Administration Server and managed servers) using specific start-up arguments. Repeat steps 4 and 5 for the SOA Domain to enable single sign-on for SOA applications.

6. Configure WebCenter Spaces (see Section 26.4.3.3, "Configuring WebCenter Spaces").

7. Configure the discussions server (see Section 26.4.3.4, "Configuring the Discussions Server for SSO").

26.4.3.1 Configuring the Negotiate Identity Assertion Provider

This section provides instructions for creating and configuring a Negotiate Identity Assertion provider. The Negotiate Identity Assertion provider enables single sign-on (SSO) with Microsoft clients. The identity assertion provider decodes Simple and Protected Negotiate (SPNEGO) tokens to obtain Kerberos tokens, validates the Kerberos tokens, and maps them to WebLogic users. The Negotiate Identity Assertion provider uses the Java Generic Security Service (GSS) Application Programming Interface (API) to accept the GSS security context through Kerberos.

To configure the Negotiate Identity Assertion provider:

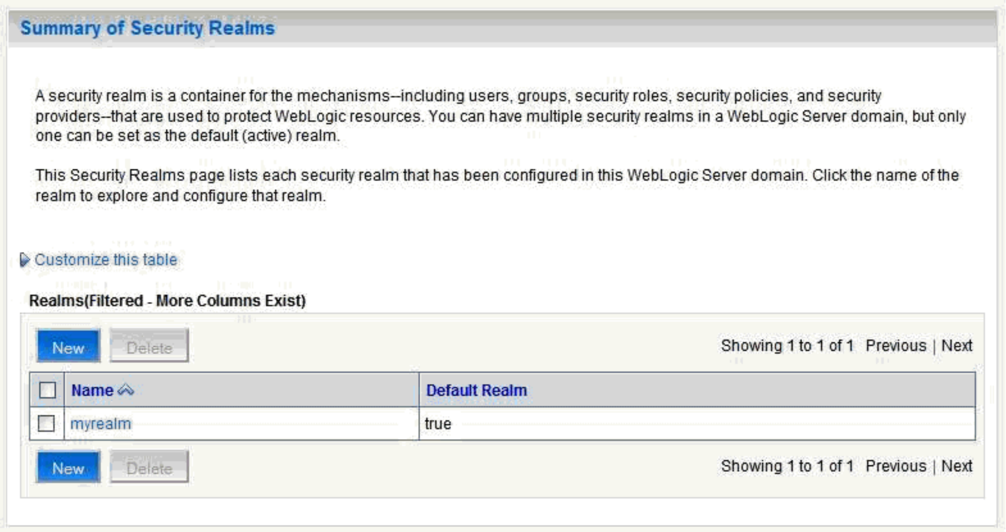
1. Log in to the WebLogic Server Administration Console.

   For information on logging in to the WebLogic Server Administration Console, see Section 1.12.2, "Oracle WebLogic Server Administration Console."

2. From the Domain Structure pane, click **Security Realms**.

   The Summary of Security Realms pane displays (see Figure 26–75).

Figure 26–75 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.

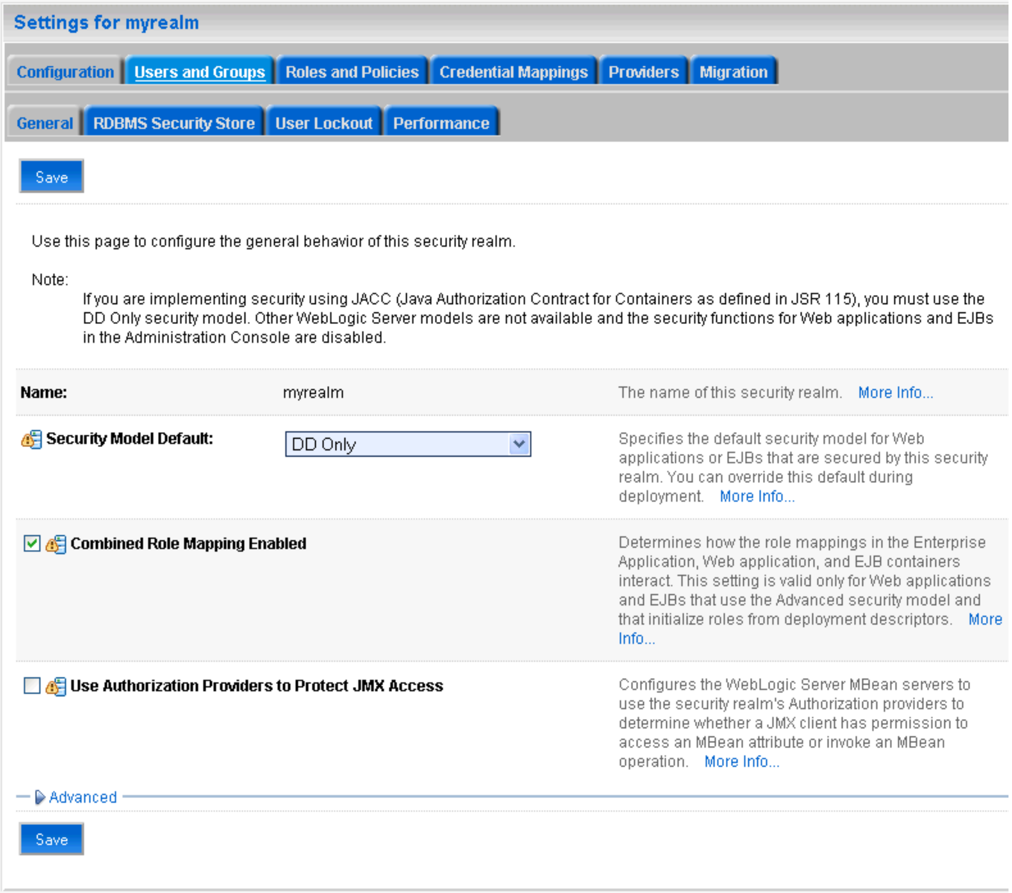
Realms(Filtered - More Columns Exist)

□	Name	Default Realm
□	myrealm	true

3. Click your security realm.

   The Settings page for the security realm displays (see Figure 26–76).

Figure 26–76 Security Realm Settings Page



Settings for myrealm

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...

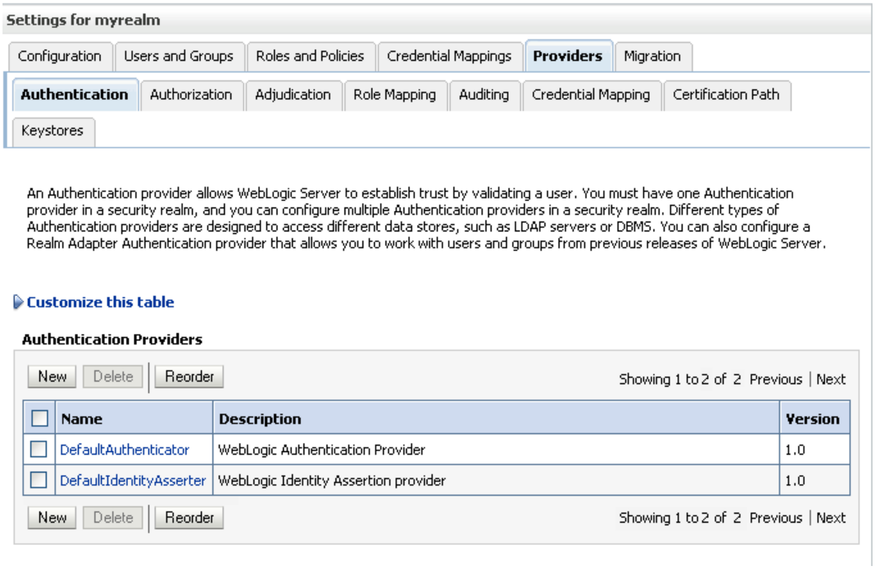
☑ Combined Role Mapping Enabled — Determines how the role mappings in the Enterprise Application, Web application, and EJB containers interact. This setting is valid only for Web applications and EJBs that use the Advanced security model and that initialize roles from deployment descriptors. More Info...

□ 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...

4. Open the Providers tab and select the Authentication subtab.

   The Authentication Settings pane displays (see Figure 26–77).

Figure 26–77 Authentication Settings Pane



Settings for myrealm

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.

Authentication Providers

Showing 1 to 2 of 2 Previous | Next

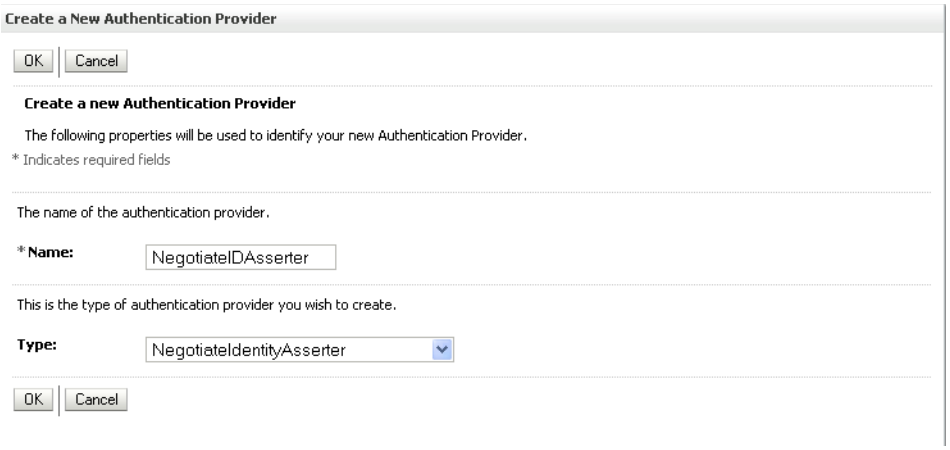
□	Name	Description	Version
□	DefaultAuthenticator	WebLogic Authentication Provider	1.0
□	DefaultIdentityAsserter	WebLogic Identity Assertion provider	1.0

Showing 1 to 2 of 2 Previous | Next

5. Click **New**.

   The Create a New Authentication Provider pane displays (see Figure 26–78).

Figure 26–78 Create a New Authentication Provider Pane



Create a New Authentication Provider

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: NegotiateIDAsserter

This is the type of authentication provider you wish to create.

Type: NegotiateIdentityAsserter

6. Enter a **Name** for the identity asserter, and select `NegotiateIdentityAsserter` as the **Type**.
7. Click **OK**.

26.4.3.2 Configuring an Active Directory Authentication Provider

Follow the steps below to configure an Active Directory authentication provider using the WebLogic Administration Console.

To configure an Active Directory Authentication provider:

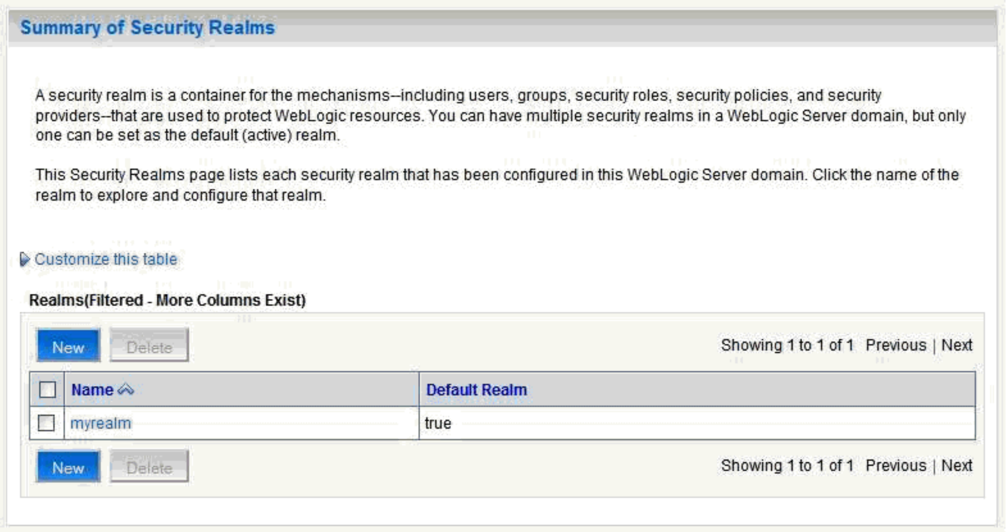
1. Log in to the WebLogic Server Administration Console.

   For information on logging in to the WebLogic Server Administration Console, see Section 1.12.2, "Oracle WebLogic Server Administration Console."

2. From the Domain Structure pane, click **Security Realms**.

   The Summary of Security Realms pane displays (see Figure 26–79).

Figure 26–79 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.

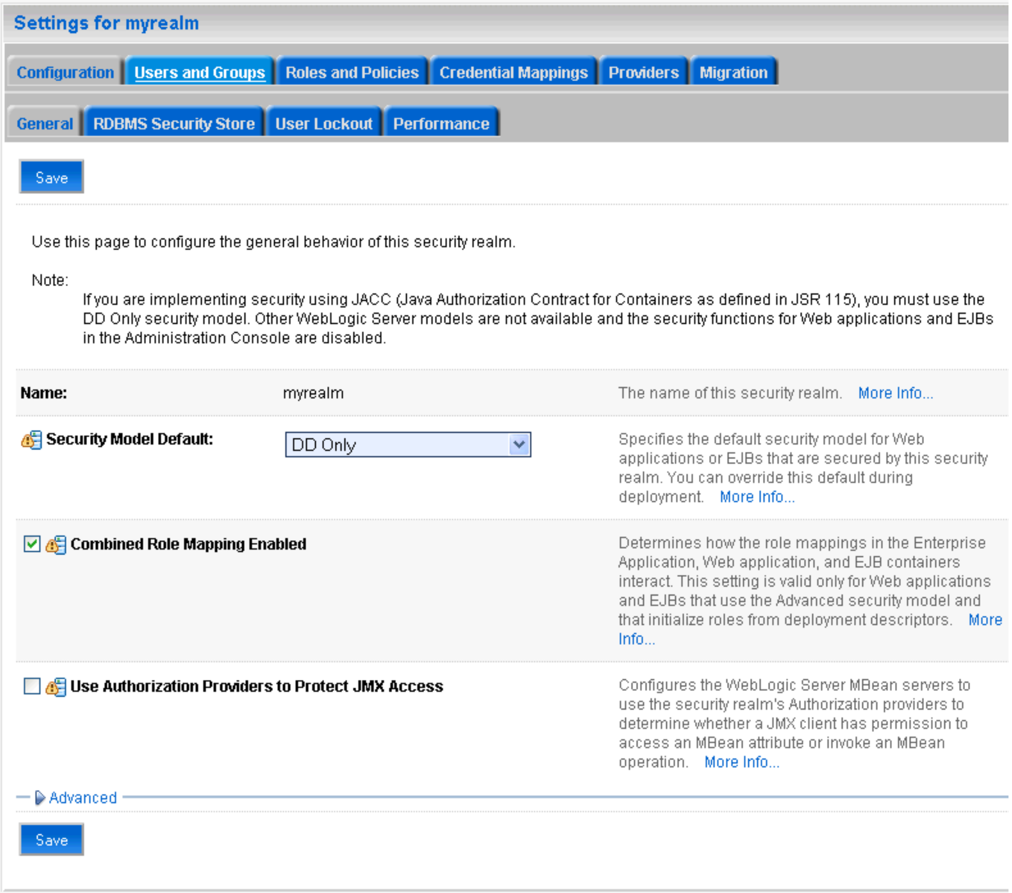
Realms(Filtered - More Columns Exist)

□	Name	Default Realm
□	myrealm	true

3. Click your security realm.

   The Settings page for the security realm displays (see Figure 26–80).

Figure 26–80 Security Realm Settings Page



Use this page to configure the general behavior of this security realm.

Note:

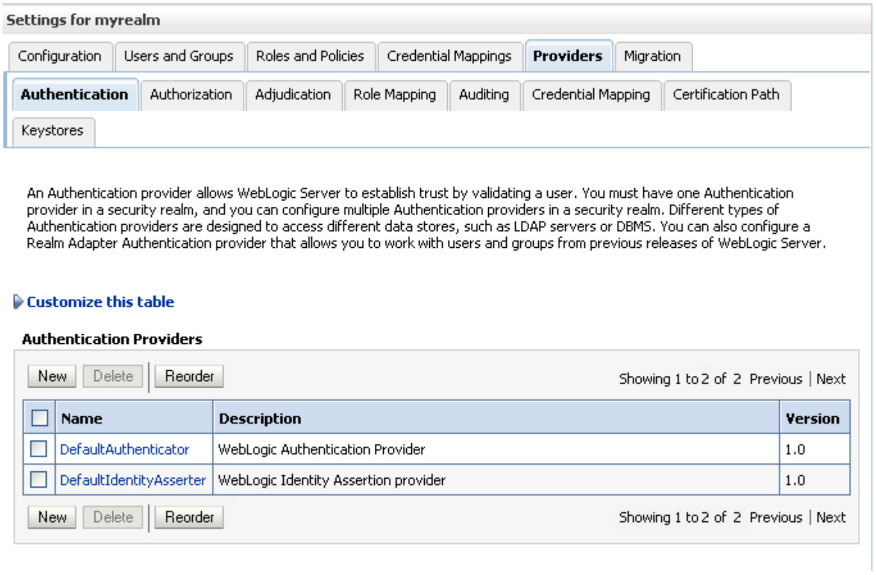
If you are implementing security using JACC (Java Authorization Contract for Containers as defined in JSR 115), you must use the DD Only security model. Other WebLogic Server models are not available and the security functions for Web applications and EJBs in the Administration Console are disabled.

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...

4. Open the Providers tab and select the Authentication subtab.

   The Authentication Settings pane displays (see Figure 26–81).

Figure 26–81 Authentication Settings Pane



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.

Authentication Providers

Showing 1 to 2 of 2 Previous | Next

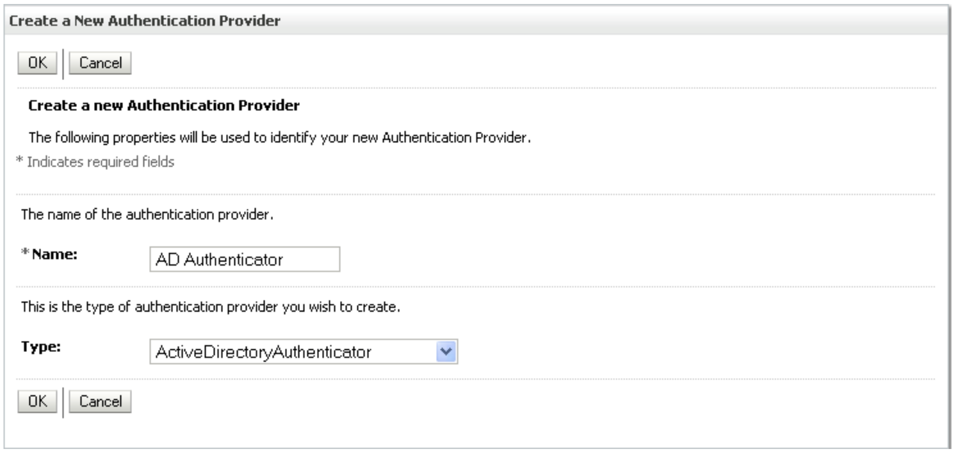
□	Name	Description	Version
□	DefaultAuthenticator	WebLogic Authentication Provider	1.0
□	DefaultIdentityAsserter	WebLogic Identity Assertion provider	1.0

Showing 1 to 2 of 2 Previous | Next

5. Click **New**.

   The Create a New Authentication Provider pane displays (see Figure 26–82).

Figure 26–82 Create a New Authentication Provider Pane



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:** AD Authenticator

This is the type of authentication provider you wish to create.

Type: ActiveDirectoryAuthenticator

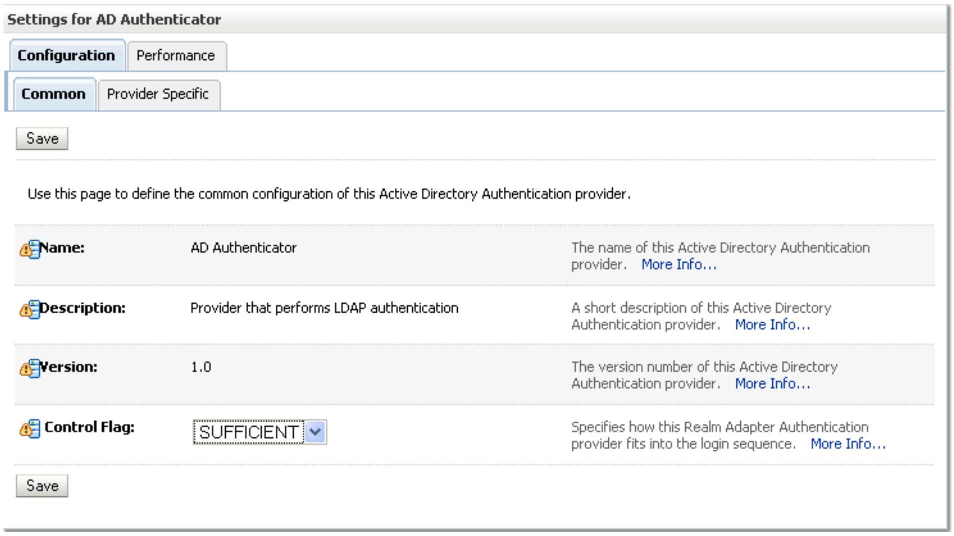
6. Enter a **Name** for the authentication provider, and select `ActiveDirectoryAuthenticator` as the **Type**.

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 26–83).

Figure 26–83 Provider Settings Page



Use this page to define the common configuration of this Active Directory Authentication provider.

Name:	AD Authenticator	The name of this Active Directory Authentication provider. More Info...
Description:	Provider that performs LDAP authentication	A short description of this Active Directory Authentication provider. More Info...
Version:	1.0	The version number of this Active Directory Authentication provider. More Info...
Control Flag:	SUFFICIENT	Specifies how this Realm Adapter Authentication provider fits into the login sequence. More Info...

9. Open the Configuration tab and the Common subtab.

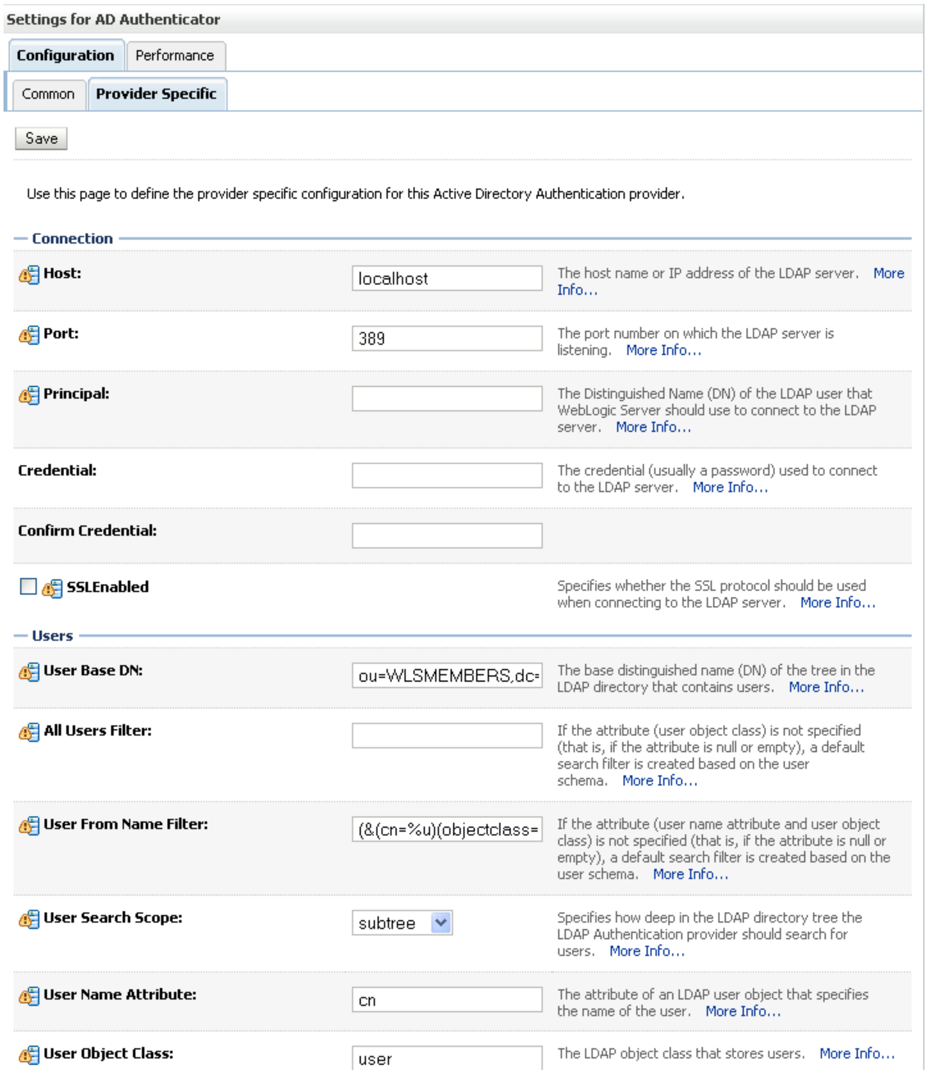
10. Set the Control Flag to `SUFFICIENT` and click **Save**.

> **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 26–84).

Figure 26–84 Provider Specific Settings Pane



Settings for AD Authenticator

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 26–20 Active Directory Authenticator Settings

Parameter	Value	Description
Host:		The host ID of the LDAP server

Table 26–20 (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 DNs 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...

26.4.3.3 Configuring WebCenter Spaces

Once you have completed the steps for configuring the Negotiate Identity Assertion Provider and Active Directory Authenticator, and all applications on your WebLogic domain are configured for single sign-on with Microsoft clients in the required domain, a final step is required to provide a seamless single-sign-on experience for your users when accessing WebCenter Spaces. There are two options for doing this:

- Turn off public access, by logging in to WebCenter 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 WebCenter Spaces only using Internet Explorer, and are confined to the domain where WNA is set up.

- If you must retain public access to WebCenter Spaces, then the recommendation is to use the `oracle.webcenter.osso.enabled` flag when starting the `WLS_Spaces` server. This flag tells WebCenter Spaces that SSO is being used and no login form should be displayed on the default landing page. A Login link is displayed instead that the user can click to invoke the SSO authentication where the user will be automatically logged in. If Firefox is used to access WebCenter Spaces within the Windows network configured for WNA, or any browser is used to access WebCenter Spaces from outside the Windows network domain, users see the login page after clicking the Login link.

26.4.3.4 Configuring the Discussions Server for SSO

This section describes how to configure Oracle WebCenter Discussions 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 WebCenter Spaces, as described in Section 24.5.1, "Migrating the WebCenter Discussions Server to Use an External LDAP."

To set up the discussions server for SSO:

1. Log in to the Oracle WebCenter Discussions Server Admin Console at:

   ```
   http://host:port/owc_discussions/admin
   ```

   Where *`host`* and *`port`* are the host ID and port number of the `WLS_Services` managed server.

2. Open the System Properties page and edit (if it already exists) or add the `owc_discussions.sso.mode` property, setting it's value to `true`.

3. Edit or add the `jiveURL` property to point to the base URL of the SSO server. For example:

   ```
   jiveURL = example.com:8890/owc_discussions
   ```

27

Securing WebCenter Applications and Components with SSL

This chapter describes how to secure Oracle WebCenter applications and components with SSL.

This chapter includes the following sections:

Note: The following can use WS-Security with message protection, and consequently have no hard requirement for SSL:

- BPEL servers - Worklist service
- WSRP Producers
- Oracle WebLogic Communication Services (OWLCS) - IMP service
- Microsoft Live Communication Server (LCS) - IMP service
- Oracle WebCenter Discussions - Discussions and Announcements

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."

27.1 Securing the Browser Connection to WebCenter Spaces with SSL

Securing the browser connection to WebCenter Spaces with SSL consists of the following steps:

- Section 27.1.1, "Creating the Custom Keystore"
- Section 27.1.2, "Configuring the Custom Identity and Java Trust Keystores"
- Section 27.1.3, "Configuring the SSL Connection"

27.1.1 Creating the Custom Keystore

The first step is to generate a custom keystore for WebCenter Spaces.

To create a custom keystore:

1. Go to *`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 WebCenter Spaces clients can import it into their trust store:

   ```
   keytool -exportcert -v -alias alias -keystore keystore
   -storepass keystore_password -rfc -file certificate_file
   ```

   Where:

   - *`alias`* is the WebCenter Spaces alias (for example, `webcenter_wls`)
   - *`keystore`* is the keystore name, (for example, `webcenter_wls.jks`)
   - *`keystore_password`* is the keystore password, (for example, `welcome1`)
   - *`certificate_file`* is the file name for the certificate to export the key to (for example, `webcenter_wls.cer`)

4. Determine the trust store to use:

   Since you are using a self-signed certificate, you must update it as a trusted certificate in the server trust store. To do this, you must determine your trust store by going to the server:

   a. Log into the WebLogic Server Administration Console.

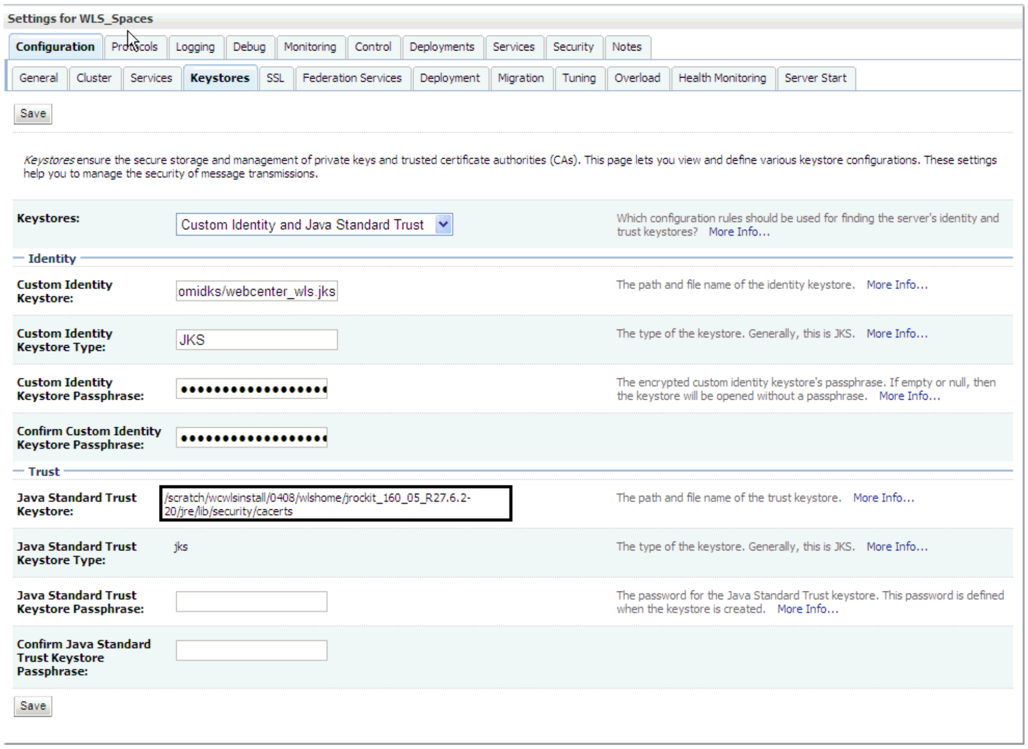
   b. In the Domain Structure pane, expand Environments and click `Servers`.

   c. In the list of servers, click `WLS_Spaces`.

   d. Open the Configuration tab, and the Keystores subtab.

      The Keystores Settings pane displays (see Figure 27–1).

Figure 27–1 Keystores Settings Pane



Settings for WLS_Spaces

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:	omidks/webcenter_wls.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:	/scratch/wcwlsinstall/0408/wlshome/jrockit_160_05_R27.6.2-20/jre/lib/security/cacerts	The path and file name of the trust keystore. More Info...
Java Standard Trust Keystore Type:	jks	The type of the keystore. Generally, this is JKS. More Info...
Java Standard Trust Keystore Passphrase:		The password for the Java Standard Trust keystore. This password is defined when the keystore is created. More Info...
Confirm Java Standard Trust Keystore Passphrase:		

e. Note down the location of the server in the **Java Standard Trust Keystore** field (shown in Figure 27–1).

   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 WebCenter Spaces alias (for example, `webcenter_wls`)
   - *`certificate_file`* is the file name for the certificate to export the key to (for example, `webcenter_wls.cer`)

   When prompted whether to trust the self-signed certificate, answer `yes`.

27.1.2 Configuring the Custom Identity and Java Trust Keystores

The next step is to configure the Custom Identity and Java Trust keystores on the WebCenter Spaces server.

To configure the identity and trust keystores:

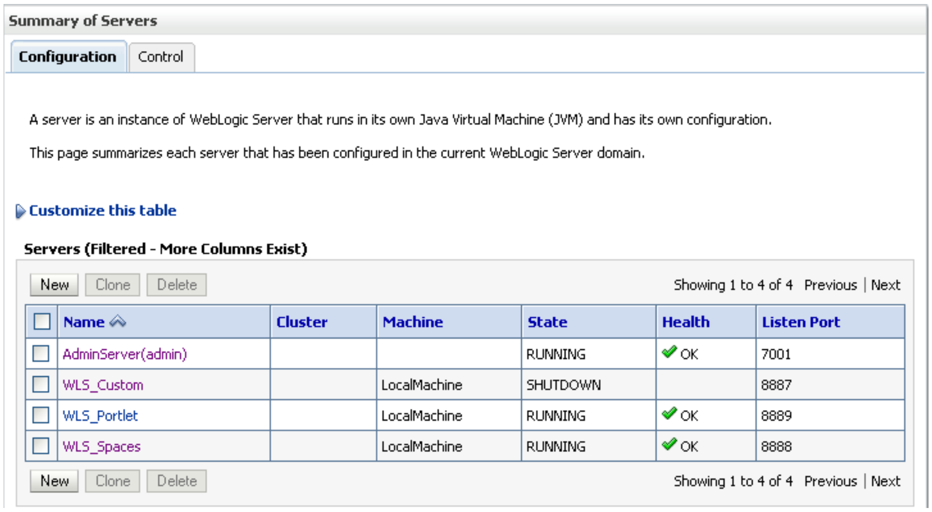
1. Log in to the WebLogic Server Administration Console.

   For information on logging into the WebLogic Server Administration Console, see Section 1.12.2, "Oracle WebLogic Server Administration Console."

2. In the Domain Structure pane, expand **Environment** and click **Servers**.

   The Summary of Servers pane displays (see Figure 27–2).

Figure 27–2 Summary of Servers Pane



Summary of Servers

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.

Servers (Filtered - More Columns Exist)

Showing 1 to 4 of 4 Previous | Next

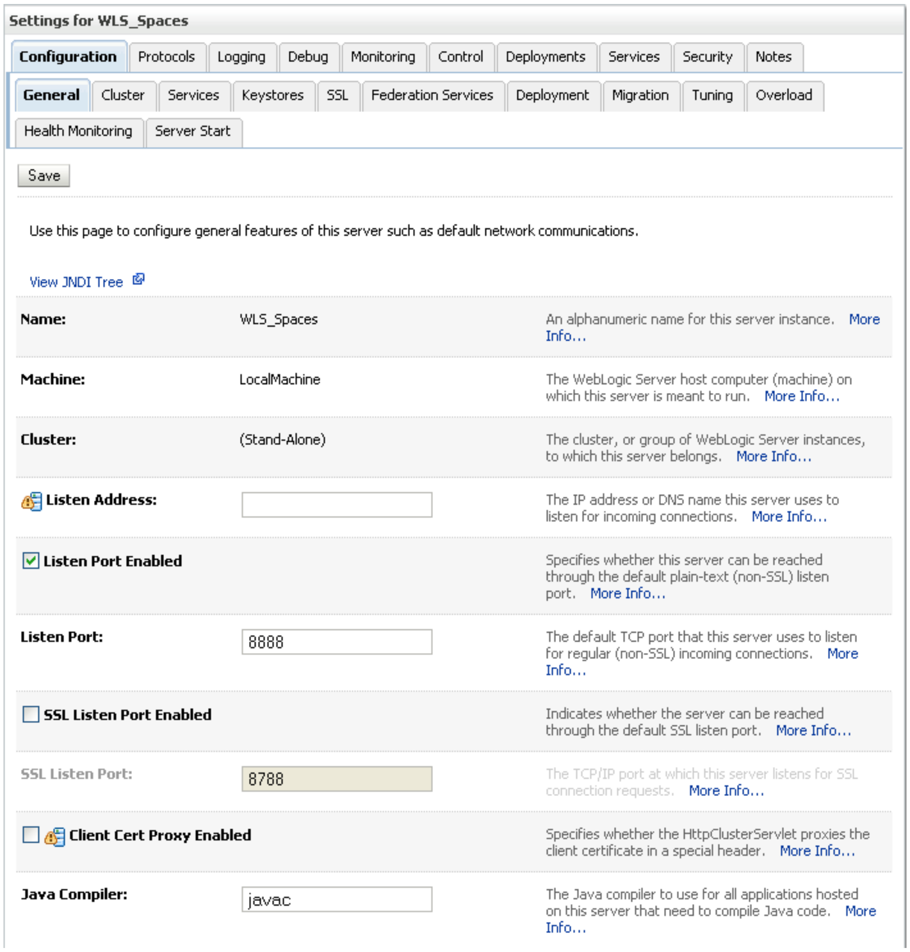
□	Name	Cluster	Machine	State	Health	Listen Port
□	AdminServer(admin)			RUNNING	✓ OK	7001
□	WLS_Custom		LocalMachine	SHUTDOWN		8887
□	WLS_Portlet		LocalMachine	RUNNING	✓ OK	8889
□	WLS_Spaces		LocalMachine	RUNNING	✓ OK	8888

Showing 1 to 4 of 4 Previous | Next

3. Click the WebCenter Spaces server (`WLS_Spaces`) to configure the identity and trust keystores.

   The Settings pane for the WebCenter Spaces server displays (see Figure 27–3).

Figure 27–3 Settings Pane for WebCenter Spaces Server



Settings for WLS_Spaces

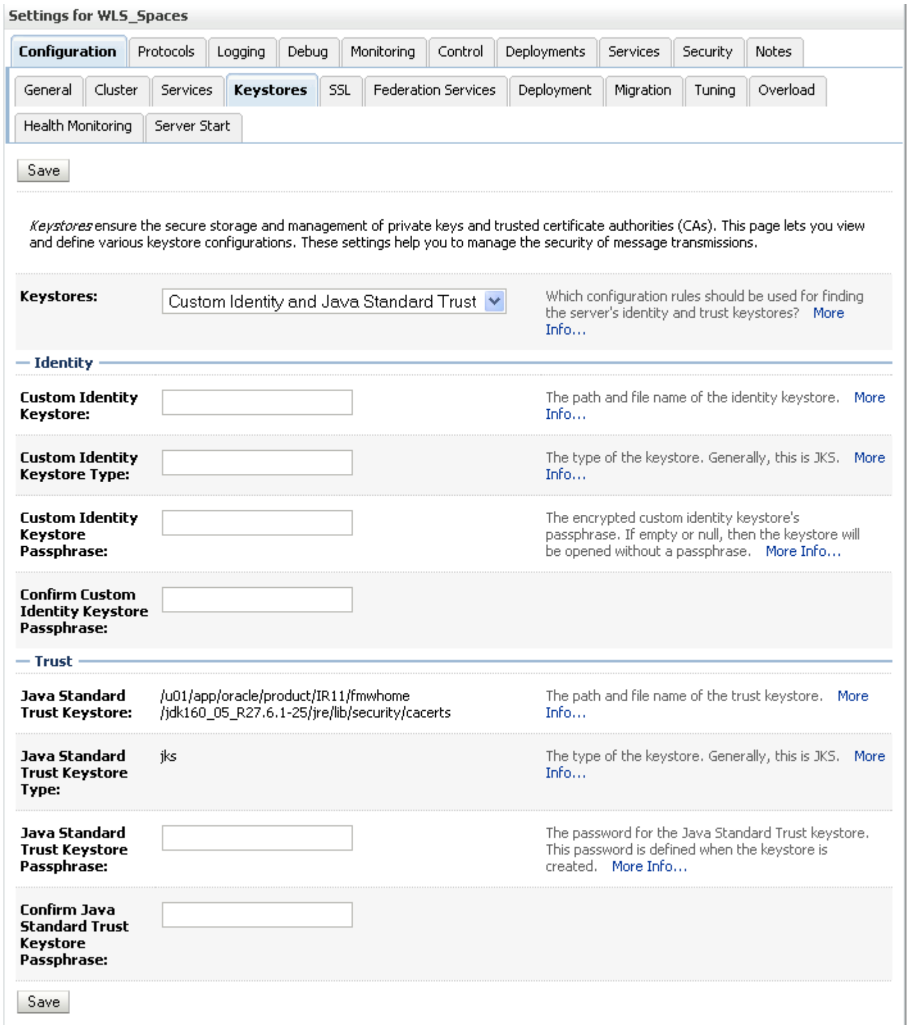
Use this page to configure general features of this server such as default network communications.

Name:	WLS_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:		The IP address or DNS name this server uses to listen for incoming connections. More Info...
☑ **Listen Port Enabled**		Specifies whether this server can be reached through the default plain-text (non-SSL) listen port. More Info...
Listen Port:	8888	The default TCP port that this server uses to listen for regular (non-SSL) incoming connections. More Info...
☐ **SSL Listen Port Enabled**		Indicates whether the server can be reached through the default SSL listen port. More Info...
SSL Listen Port:	8788	The TCP/IP port at which this server listens for SSL connection requests. More Info...
☐ **Client Cert Proxy Enabled**		Specifies whether the HttpClusterServlet proxies the client certificate in a special header. More Info...
Java Compiler:	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 27–4).

Figure 27–4 Keystores Pane



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:

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 27.1.1, "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.

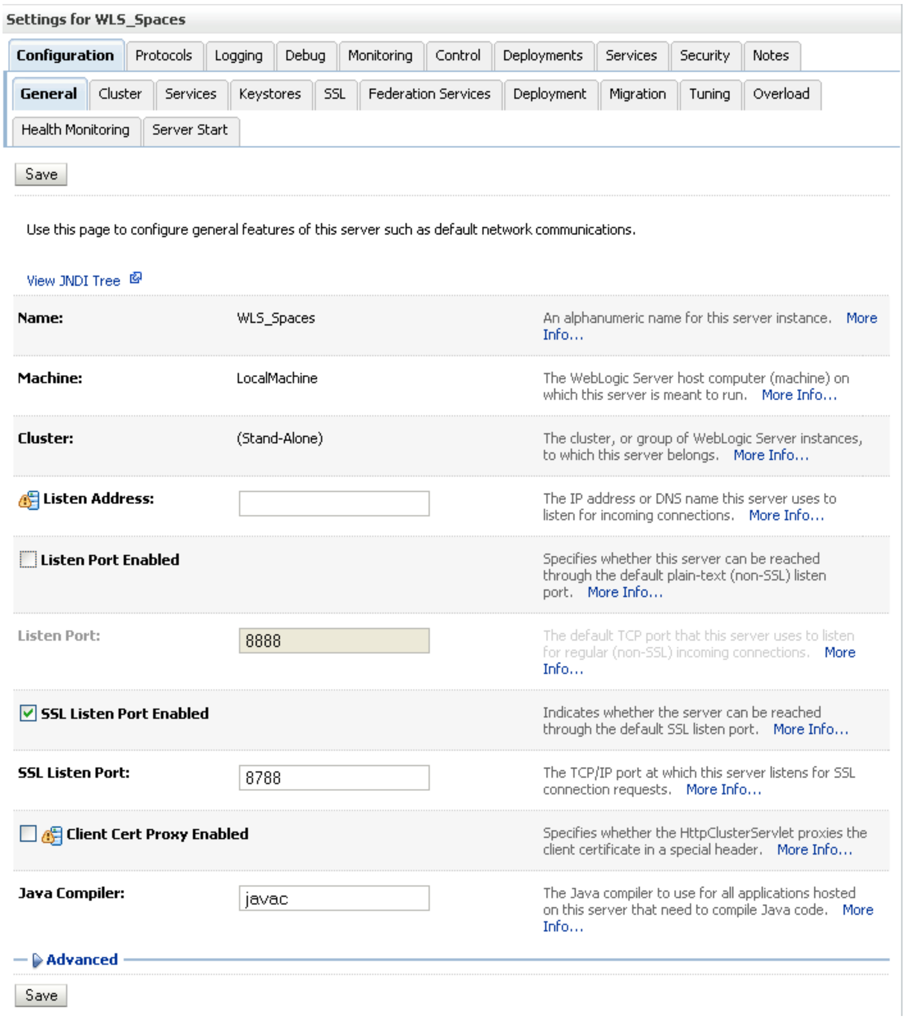
27.1.3 Configuring the SSL Connection

To configure the SSL connection:

1. On the Settings pane for the WebCenter Spaces server, open the Configuration tab and then the General subtab.

   The General Configuration pane displays (see Figure 27–5).

Figure 27–5 General Configuration Pane



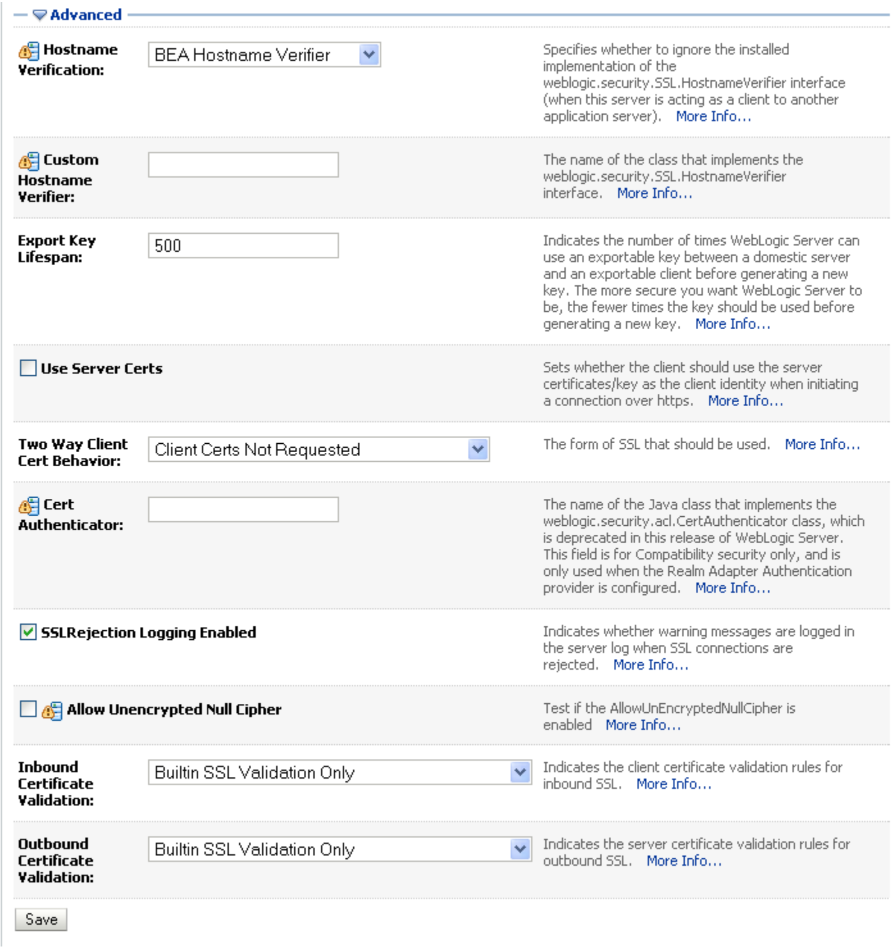
Use this page to configure general features of this server such as default network communications.

Name:	WLS_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:		The IP address or DNS name this server uses to listen for incoming connections. More Info...
□ **Listen Port Enabled**		Specifies whether this server can be reached through the default plain-text (non-SSL) listen port. More Info...
Listen Port:	8888	The default TCP port that this server uses to listen for regular (non-SSL) incoming connections. More Info...
☑ **SSL Listen Port Enabled**		Indicates whether the server can be reached through the default SSL listen port. More Info...
SSL Listen Port:	8788	The TCP/IP port at which this server listens for SSL connection requests. More Info...
□ **Client Cert Proxy Enabled**		Specifies whether the HttpClusterServlet proxies the client certificate in a special header. More Info...
Java Compiler:	javac	The Java compiler to use for all applications hosted on this server that need to compile Java code. More Info...

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 27–6).

Figure 27–6 Advanced SSL Configuration Settings



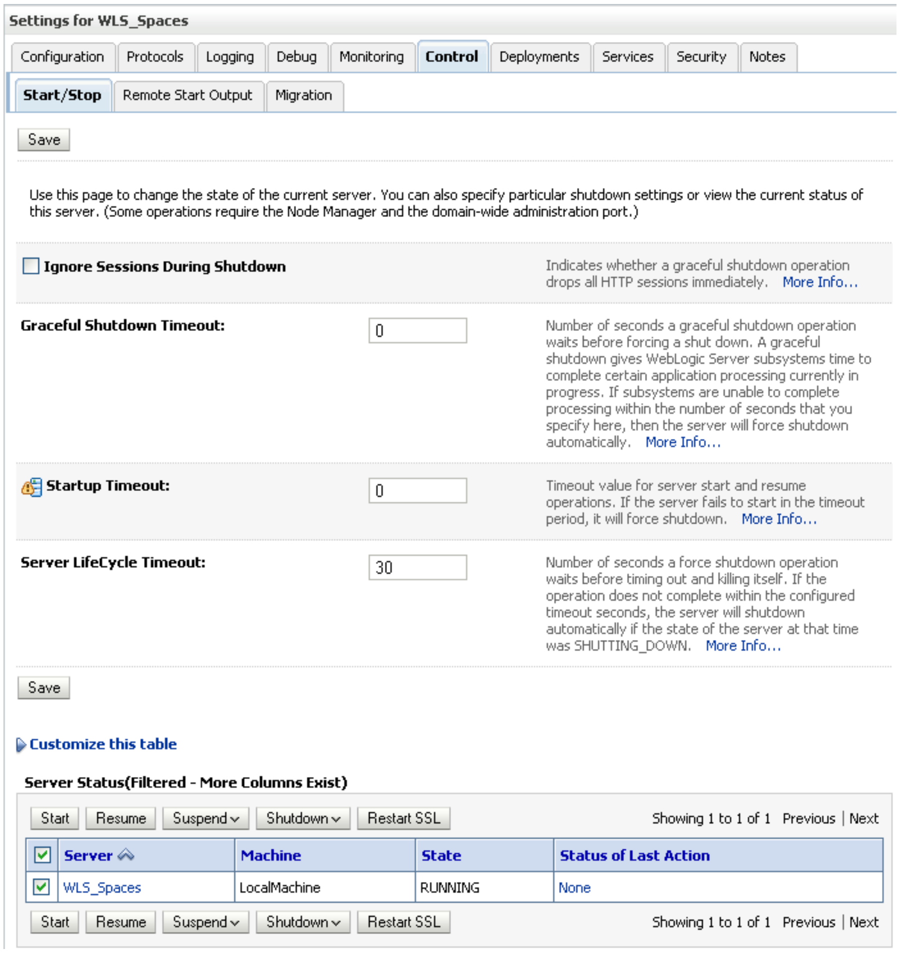
Hostname Verification:	BEA Hostname Verifier	Specifies whether to ignore the installed implementation of the weblogic.security.SSL.HostnameVerifier interface (when this server is acting as a client to another application server). More Info...
Custom Hostname Verifier:		The name of the class that implements the weblogic.security.SSL.HostnameVerifier 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...
☐ **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 weblogic.security.acl.CertAuthenticator class, which is deprecated in this release of WebLogic Server. This field is for Compatibility security only, and is only used when the Realm Adapter Authentication provider is configured. More Info...
☑ **SSLRejection Logging Enabled**		Indicates whether warning messages are logged in the server log when SSL connections are rejected. More Info...
☐ **Allow Unencrypted Null Cipher**		Test if the AllowUnEncryptedNullCipher 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...

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 27–7).

Figure 27–7 Control Settings Pane



Settings for WLS_Spaces

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: 0 — 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: 0 — 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: 30 — Number of seconds a force shutdown operation waits before timing out and killing itself. If the 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...

Server Status(Filtered - More Columns Exist)

☑	Server	Machine	State	Status of Last Action
☑	WLS_Spaces	LocalMachine	RUNNING	None

7. Click **Restart SSL**.

8. Restart the WebLogic Server and open the SSL WebCenter 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.

27.2 Securing the Browser Connection to a Custom WebCenter Application with SSL

Securing the browser connection to a custom WebCenter application uses the same configuration steps as for securing the browser connection to WebCenter Spaces. The only difference is that the configuration occurs on the managed server that is hosting the custom WebCenter application deployment rather than the `WLS_Spaces` server. For more information, see Section 27.1, "Securing the Browser Connection to WebCenter Spaces with SSL."

27.3 Securing the Connection from Oracle HTTP Server to WebCenter Spaces with SSL

Securing the connection between the Oracle HTTP Server (OHS) and WebCenter Spaces is described in the following sections:

- Section 27.3.1, "Configuring the Identity and Trust Keystores"
- Section 27.3.2, "Configuring the SSL Connection"
- Section 27.3.3, "Installing the Oracle HTTP Server"
- Section 27.3.4, "Wiring the WebCenter Spaces Ports to the HTTP Server"
- Section 27.3.5, "Configuring the SSL Certificates"

27.3.1 Configuring the Identity and Trust Keystores

For instructions on how to configure the Identity and Trust keystores, see Section 27.1, "Securing the Browser Connection to WebCenter Spaces with SSL."

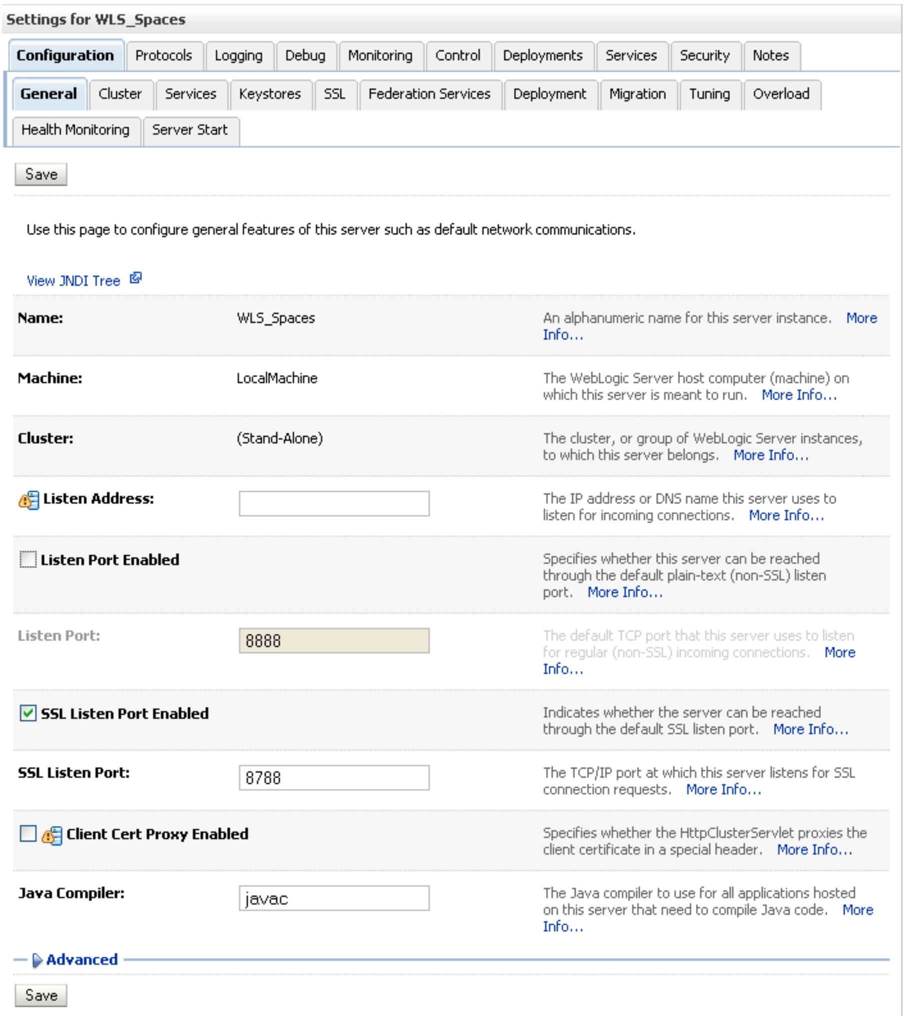
27.3.2 Configuring the SSL Connection

To configure the SSL Connection:

1. On the Settings pane for the WebCenter Spaces server, open the Configuration tab and then the General subtab.

   The General Configuration pane displays (see Figure 27–8).

Figure 27–8 General Configuration Pane



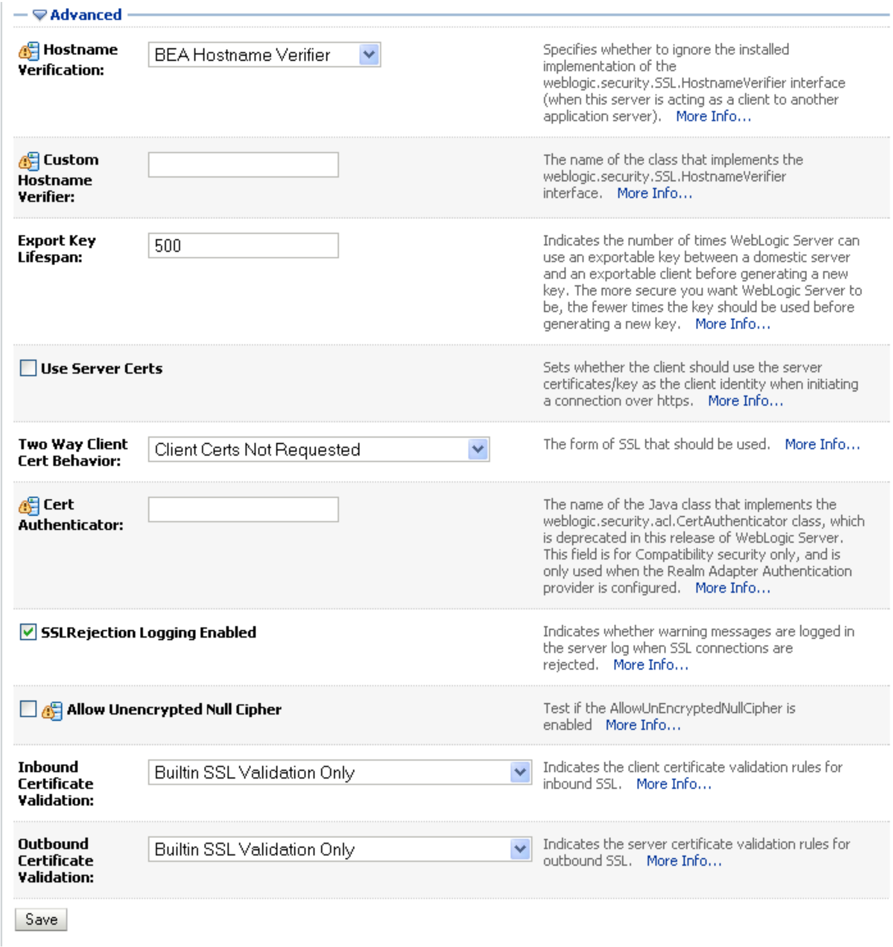
Use this page to configure general features of this server such as default network communications.

Name:	WLS_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:		The IP address or DNS name this server uses to listen for incoming connections. More Info...
□ **Listen Port Enabled**		Specifies whether this server can be reached through the default plain-text (non-SSL) listen port. More Info...
Listen Port:	8888	The default TCP port that this server uses to listen for regular (non-SSL) incoming connections. More Info...
☑ **SSL Listen Port Enabled**		Indicates whether the server can be reached through the default SSL listen port. More Info...
SSL Listen Port:	8788	The TCP/IP port at which this server listens for SSL connection requests. More Info...
□ **Client Cert Proxy Enabled**		Specifies whether the HttpClusterServlet proxies the client certificate in a special header. More Info...
Java Compiler:	javac	The Java compiler to use for all applications hosted on this server that need to compile Java code. More Info...

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 27–9).

Figure 27–9 Advanced SSL Configuration Settings



▽ Advanced

Hostname Verification:	BEA Hostname Verifier	Specifies whether to ignore the installed implementation of the weblogic.security.SSL.HostnameVerifier interface (when this server is acting as a client to another application server). More Info...
Custom Hostname Verifier:		The name of the class that implements the weblogic.security.SSL.HostnameVerifier 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...
□ **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 weblogic.security.acl.CertAuthenticator class, which is deprecated in this release of WebLogic Server. This field is for Compatibility security only, and is only used when the Realm Adapter Authentication provider is configured. More Info...
☑ **SSLRejection Logging Enabled**		Indicates whether warning messages are logged in the server log when SSL connections are rejected. More Info...
□ **Allow Unencrypted Null Cipher**		Test if the AllowUnEncryptedNullCipher 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...

5. Set the **Two Way Client Cert Behavior** option to `Client Certs Not Requested` and click **Save**.
6. Open the Control tab on the Settings pane, and select the Start/Stop subtab.
7. Click **Restart SSL**.
8. Open the SSL WebCenter Spaces URL.
9. Accept the certificate for the session and log in.
10. In the WSL Administration Console, click **View Changes and Restarts** on the Change Center pane and restart any affected servers or components.

27.3.3 Installing the Oracle HTTP Server

To install the Oracle HTTP Server:

1. Install the WebTier.
   - Do not select WebCache; only select the HTTP Server.
   - Uncheck the checkbox to associate a WebLogic server during install.
2. Navigate to the `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
   ```

27.3.4 Wiring the WebCenter Spaces Ports to the HTTP Server

To wire the WebCenter Spaces ports to the HTTP server:

1. Open the file `WT_ORACLE_HOME/instances/<your_instance>/config/OHS/ohs1/mod_wl.conf`.

2. Add the following entry to `mod_wl.conf` to make WebCenter Spaces work with OHS:

   ```
   <IfModule mod_weblogic.c>
           WebLogicHost host_id
           WebLogicPort port
           Debug OFF
           WLLogFile /tmp/ohs.log
           MatchExpression *.jsp
        </IfModule>

        <Location />
          SetHandler weblogic-handler
        </Location>
   ```

   Replacing *`host_id`* and *`port`* with the WebCenter Spaces server ID and port number.

3. Open the file `WT_ORACLE_HOME/instances/<your_instance>/config/OHS/ohs1/mod_ssl.conf`.

4. Add the following entry to `mod_ssl.conf` to make WebCenter Spaces run on the OHS SSL port:

   ```
   <IfModule mod_weblogic.c>
           WebLogicHost host_id
           WebLogicPort port
           WLLogFile /tmp/ohs_ssl.log
           Debug OFF
           DebugConfigInfo ON
           SecureProxy ON
           MatchExpression *.jsp
           WlSSLWallet SSL_wallet
         </IfModule>

        <Location />
          SetHandler weblogic-handler
        </Location>
   ```

   Replacing *`host_id`* and *`port`* with the WebCenter SSL server ID and port number, and *`SSL_wallet`* with the path to the WebLogic SSL wallet (for example, `WT_ORACLE_HOME/instances/<your_instance>/config/OHS/ohs1/keystores/default`).

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
```

27.3.5 Configuring the SSL Certificates

To configure the SSL certificates:

1. For OHS to trust WebCenter's certificate, the `WLS_Spaces` certificate must be imported into the OHS trust store. Export the certificate from the `WLS_Spaces` identity keystore:

   ```
   keytool -exportcert -v -alias webcenter_wls -keystore webcenter_wls.jks
   -storepass <password> -rfc -file webcenter_wls.cer
   ```

2. Import the certificate into the wallet on the OHS side using `orapki`:

   ```
   orapki wallet add -wallet . -trusted_cert -cert webcenter_wls.cer
   -auto_login_only
   ```

3. For WebCenter to trust OHS certificates, export the user certificate from OHS wallet and import it as a trusted certificate in the WebLogic trust store.

   ```
   orapki wallet export -wallet . -cert cert.txt  -dn 'CN=\"Self-signed
   Certificate for ohs1
   \",OU=EXAMPLEORGUNIT,O=EXAMPLEORG,L=EXAMPLELOCATION,ST=CA,C=US'
   ```

4. Import the above certificate into the `WLS_Spaces` managed server trust store available in `/scratch/wcwlsinstall/0408/wlshome/jrockit_160_05_R27.6.2-20/jre/lib/security/cacerts`:

   ```
   keytool -file cert.txt -importcert -trustcacerts -alias ohs_cert
   -keystore cacerts -storepass changeit
   ```

5. Restart OHS and the `WLS_Spaces` server.

   You should now be able to access the SSL OHS, as well as the non-SSL OHS.

27.4 Securing the Browser Connection to the Wiki Service with SSL

As with securing the browser connection to WebCenter Spaces, securing the Wiki service connection with SSL is described in the following sections:

- Section 27.4.1, "Configuring the Identity and Trust Key Stores"
- Section 27.4.2, "Configuring the SSL Connection"

27.4.1 Configuring the Identity and Trust Key Stores

To configure the identity and trust key stores:

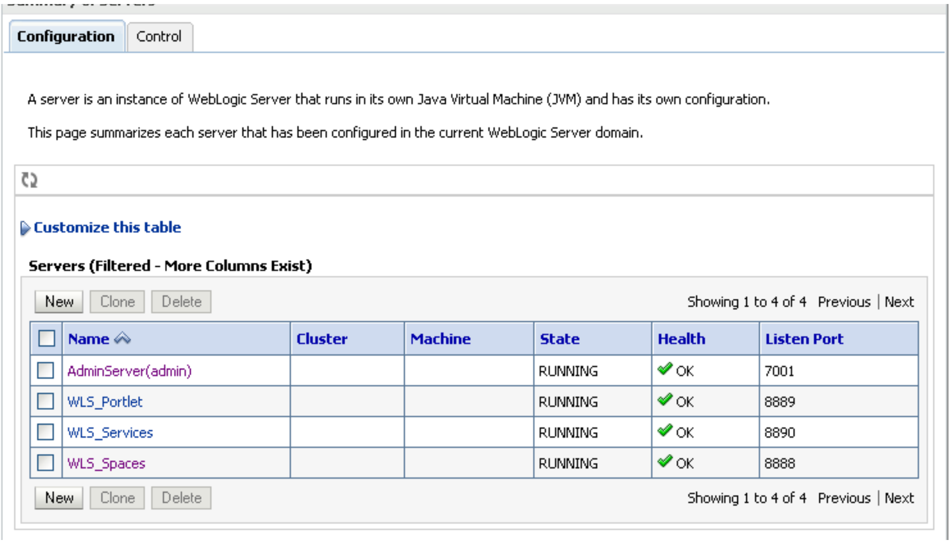
1. Log in to the WebLogic Server Administration Console.

   For information on logging into the WebLogic Server Administration Console, see Section 1.12.2, "Oracle WebLogic Server Administration Console."

2. In the Domain Structure pane, expand **Environment** and click **Servers**.

   The Summary of Servers pane displays (see Figure 27–10).

Figure 27–10 Summary of Servers Pane



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.

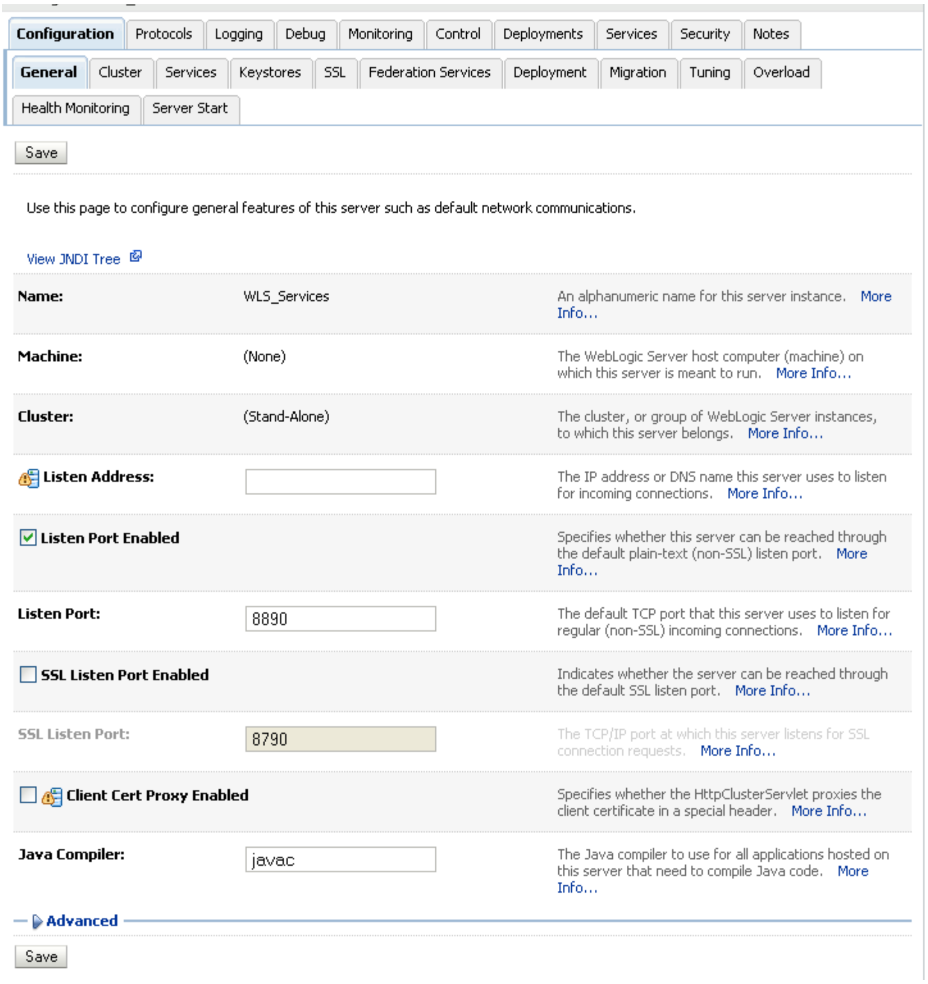
Servers (Filtered - More Columns Exist)

□	Name	Cluster	Machine	State	Health	Listen Port
□	AdminServer(admin)			RUNNING	✓ OK	7001
□	WLS_Portlet			RUNNING	✓ OK	8889
□	WLS_Services			RUNNING	✓ OK	8890
□	WLS_Spaces			RUNNING	✓ OK	8888

3. Click the Services server (`WLS_Services`) to configure the identity and trust keystores.

   The Settings pane for the services server displays (see Figure 27–11).

Figure 27–11 Settings Pane for Services Server



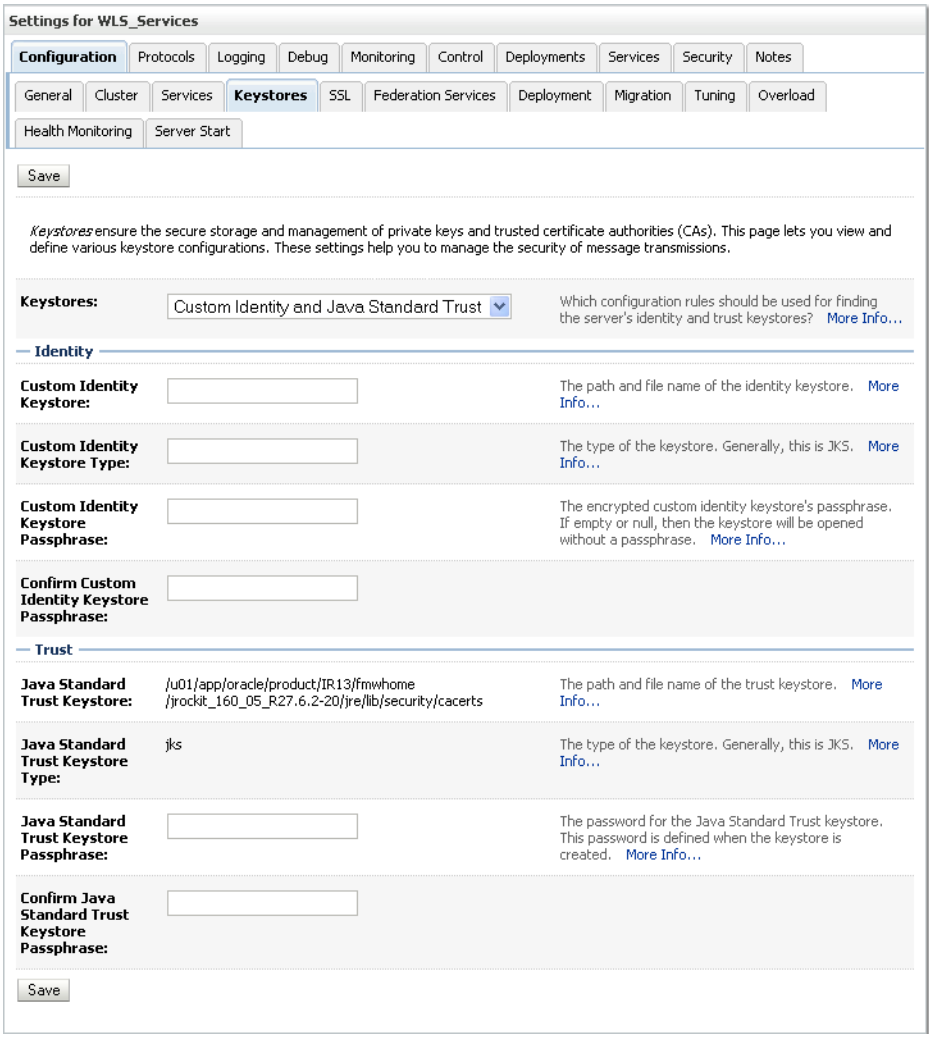
Use this page to configure general features of this server such as default network communications.

Name:	WLS_Services	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:		The IP address or DNS name this server uses to listen for incoming connections. More Info...
☑ **Listen Port Enabled**		Specifies whether this server can be reached through the default plain-text (non-SSL) listen port. More Info...
Listen Port:	8890	The default TCP port that this server uses to listen for regular (non-SSL) incoming connections. More Info...
☐ **SSL Listen Port Enabled**		Indicates whether the server can be reached through the default SSL listen port. More Info...
SSL Listen Port:	8790	The TCP/IP port at which this server listens for SSL connection requests. More Info...
☐ **Client Cert Proxy Enabled**		Specifies whether the HttpClusterServlet proxies the client certificate in a special header. More Info...
Java Compiler:	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 27–12).

Figure 27–12   Keystores Pane



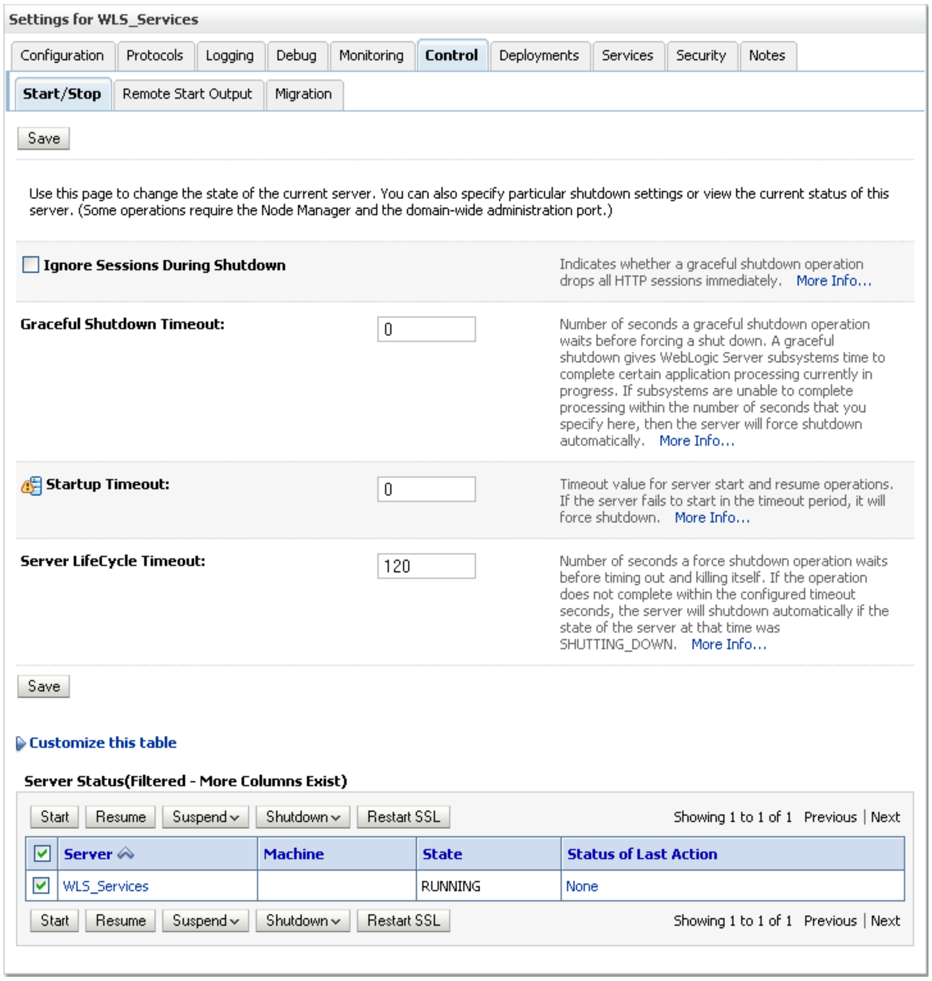
Keystores ensure the secure storage and management of private keys and trusted certificate authorities (CAs). This page lets you view and define various keystore configurations. These settings help you to manage the security of message transmissions.

Keystores:	Custom Identity and Java Standard Trust	Which configuration rules should be used for finding the server's identity and trust keystores? More Info...
Identity		
Custom Identity Keystore:		The path and file name of the identity keystore. More Info...
Custom Identity Keystore Type:		The type of the keystore. Generally, this is JKS. More Info...
Custom Identity Keystore Passphrase:		The encrypted custom identity keystore's passphrase. If empty or null, then the keystore will be opened without a passphrase. More Info...
Confirm Custom Identity Keystore Passphrase:		
Trust		
Java Standard Trust Keystore:	/u01/app/oracle/product/IR13/fmwhome /jrockit_160_05_R27.6.2-20/jre/lib/security/cacerts	The path and file name of the trust keystore. More Info...
Java Standard Trust Keystore Type:	jks	The type of the keystore. Generally, this is JKS. More Info...
Java Standard Trust Keystore Passphrase:		The password for the Java Standard Trust keystore. This password is defined when the keystore is created. More Info...
Confirm Java Standard Trust Keystore Passphrase:		

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 27–13).

Figure 27–13 Control Settings Pane



Settings for WLS_Services

Configuration | Protocols | Logging | Debug | Monitoring | Control | Deployments | Services | Security | Notes
Start/Stop | Remote Start Output | Migration
Save

Use this page to change the state of the current server. You can also specify particular shutdown settings or view the current status of this server. (Some operations require the Node Manager and the domain-wide administration port.)

□ Ignore Sessions During Shutdown		Indicates whether a graceful shutdown operation drops all HTTP sessions immediately. More Info...
Graceful Shutdown Timeout:	0	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:	0	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:	120	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...

Server Status(Filtered - More Columns Exist)

Start | Resume | Suspend | Shutdown | Restart SSL   Showing 1 to 1 of 1 Previous | Next

☑	Server	Machine	State	Status of Last Action
☑	WLS_Services		RUNNING	None

Start | Resume | Suspend | Shutdown | Restart SSL   Showing 1 to 1 of 1 Previous | Next

7. Click **Restart SSL**.

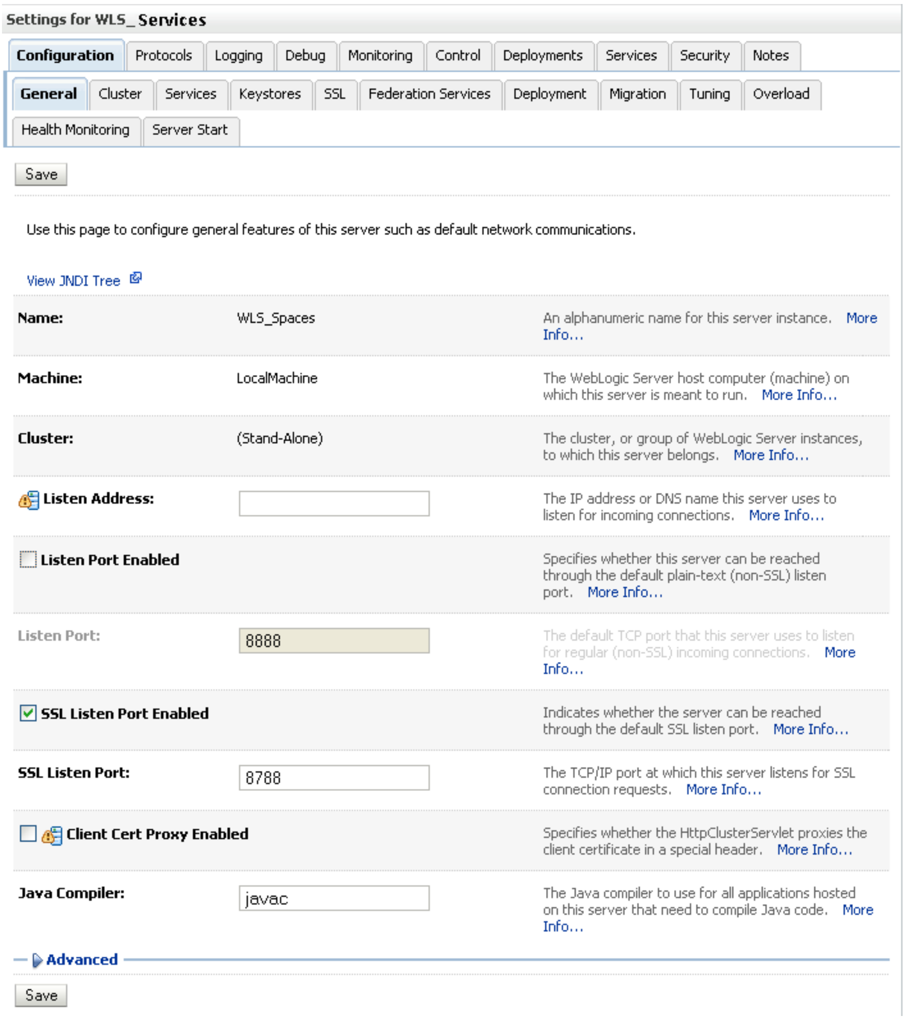
27.4.2 Configuring the SSL Connection

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 27–14).

Figure 27–14 General Configuration Pane


Settings for WLS_Services
Configuration | Protocols | Logging | Debug | Monitoring | Control | Deployments | Services | Security | Notes
General | Cluster | Services | Keystores | SSL | Federation Services | Deployment | Migration | Tuning | Overload
Health Monitoring | Server Start
Save
View JNDI Tree
Advanced
Save

Use this page to configure general features of this server such as default network communications.

Name:	WLS_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:		The IP address or DNS name this server uses to listen for incoming connections. More Info...
□ **Listen Port Enabled**		Specifies whether this server can be reached through the default plain-text (non-SSL) listen port. More Info...
Listen Port:	8888	The default TCP port that this server uses to listen for regular (non-SSL) incoming connections. More Info...
☑ **SSL Listen Port Enabled**		Indicates whether the server can be reached through the default SSL listen port. More Info...
SSL Listen Port:	8788	The TCP/IP port at which this server listens for SSL connection requests. More Info...
□ **Client Cert Proxy Enabled**		Specifies whether the HttpClusterServlet proxies the client certificate in a special header. More Info...
Java Compiler:	javac	The Java compiler to use for all applications hosted on this server that need to compile Java code. More Info...

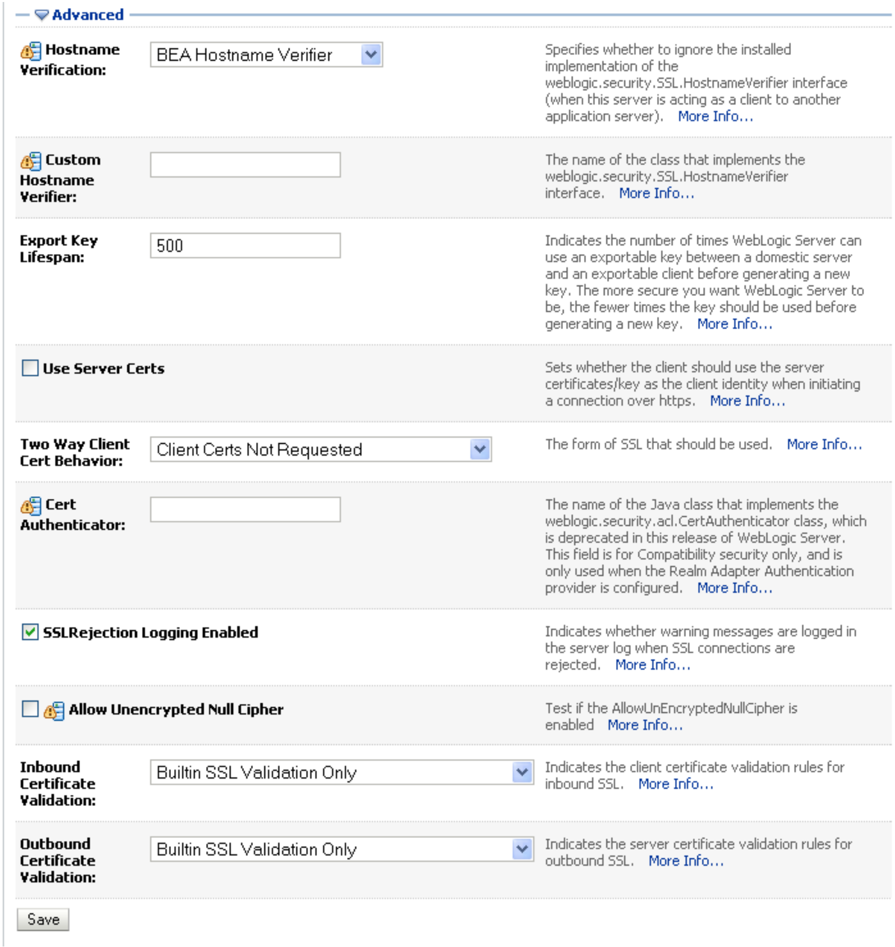
2. Check **SSL Listen Port Enabled**.

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 27–15).

Figure 27–15 Advanced SSL Configuration Settings



▽ Advanced

Hostname Verification: BEA Hostname Verifier — Specifies whether to ignore the installed implementation of the weblogic.security.SSL.HostnameVerifier interface (when this server is acting as a client to another application server). More Info...

Custom Hostname Verifier: — The name of the class that implements the weblogic.security.SSL.HostnameVerifier 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...

□ **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 weblogic.security.acl.CertAuthenticator class, which is deprecated in this release of WebLogic Server. This field is for Compatibility security only, and is only used when the Realm Adapter Authentication provider is configured. More Info...

☑ **SSLRejection Logging Enabled** — Indicates whether warning messages are logged in the server log when SSL connections are rejected. More Info...

□ **Allow Unencrypted Null Cipher** — Test if the AllowUnEncryptedNullCipher 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...

5. Make sure that the **Two Way Client Cert Behavior** option is set to `Client Certs Not Requested` and click **Save**.

6. Restart the `WLS_Services` server and open the SSL Wiki URL at `https://host:port/owc_wiki`.

7. Accept the certificate for the session and log in.

27.5 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 27.5.1, "Creating the Custom Keystore"
- Section 27.5.2, "Configuring the Identity and Trust Key Stores"
- Section 27.5.3, "Configuring the SSL Connection"

27.5.1 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.

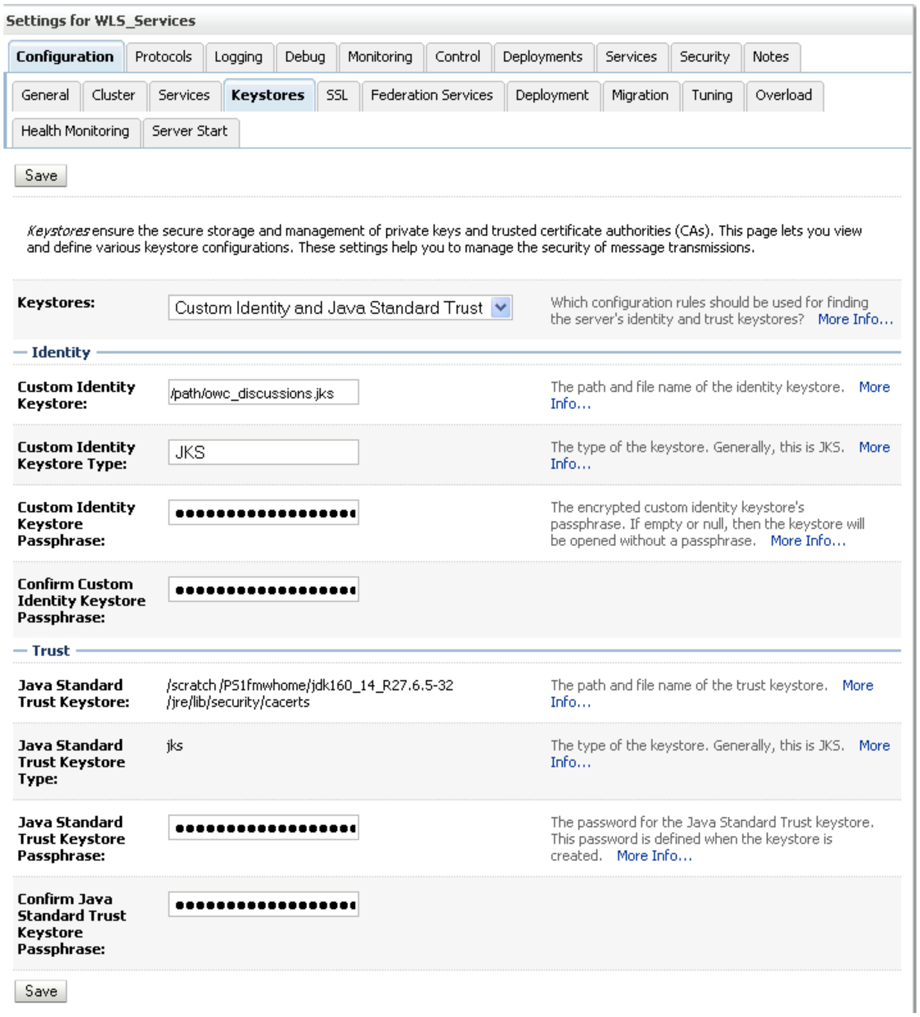
   b. In the Domain Structure pane, expand Environments and click Servers.

   c. In the list of servers, click WLS_Services.

   d. Open the Configuration tab, and the Keystores subtab.

   The Keystores Settings pane displays (see Figure 27–16).

Figure 27–16 Keystores Sub-tab for WLS_Services



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:	●●●●●●●●●●●●●●●●●●	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:	/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:	●●●●●●●●●●●●●●●●●●	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:	●●●●●●●●●●●●●●●●●●	

   e. Note down the location of the server in the **Java Standard Trust Keystore** field (shown in Figure 27–1).

   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`.

27.5.2 Configuring the Identity and Trust Key Stores

To configure the identity and trust key stores:

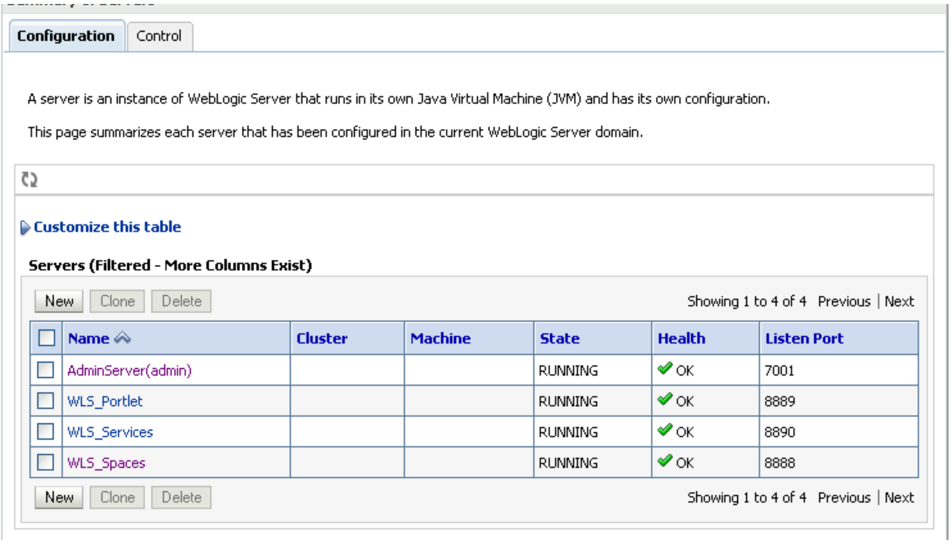
1. Log in to the WebLogic Server Administration Console.

   For information on logging into the WebLogic Server Administration Console, see Section 1.12.2, "Oracle WebLogic Server Administration Console."

2. In the Domain Structure pane, expand **Environment** and click **Servers**.

The Summary of Servers pane displays (see Figure 27–17).

Figure 27–17 Summary of Servers Pane



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.

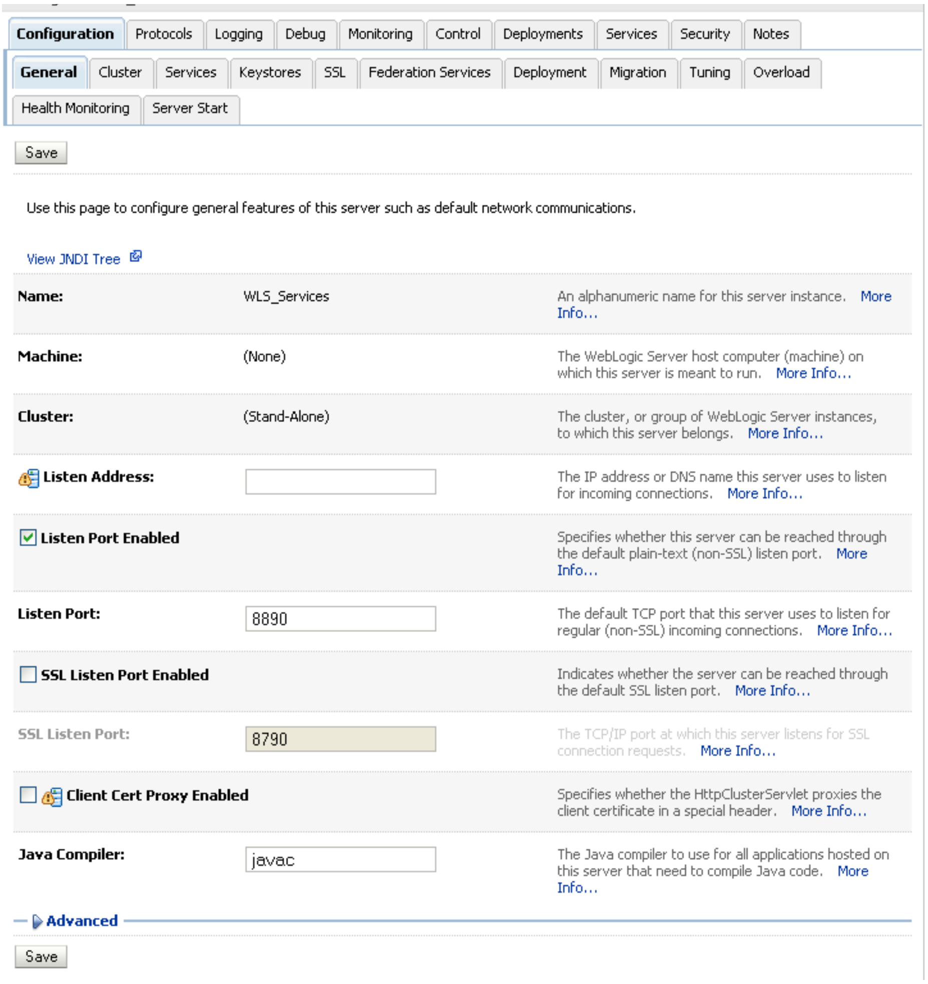
Servers (Filtered - More Columns Exist)

□	Name	Cluster	Machine	State	Health	Listen Port
□	AdminServer(admin)			RUNNING	✓ OK	7001
□	WLS_Portlet			RUNNING	✓ OK	8889
□	WLS_Services			RUNNING	✓ OK	8890
□	WLS_Spaces			RUNNING	✓ OK	8888

3. Click the Services server (`WLS_Services`) to configure the identity and trust keystores.

   The Settings pane for the services server displays (see Figure 27–18).

Figure 27–18 Settings Pane for Services Server



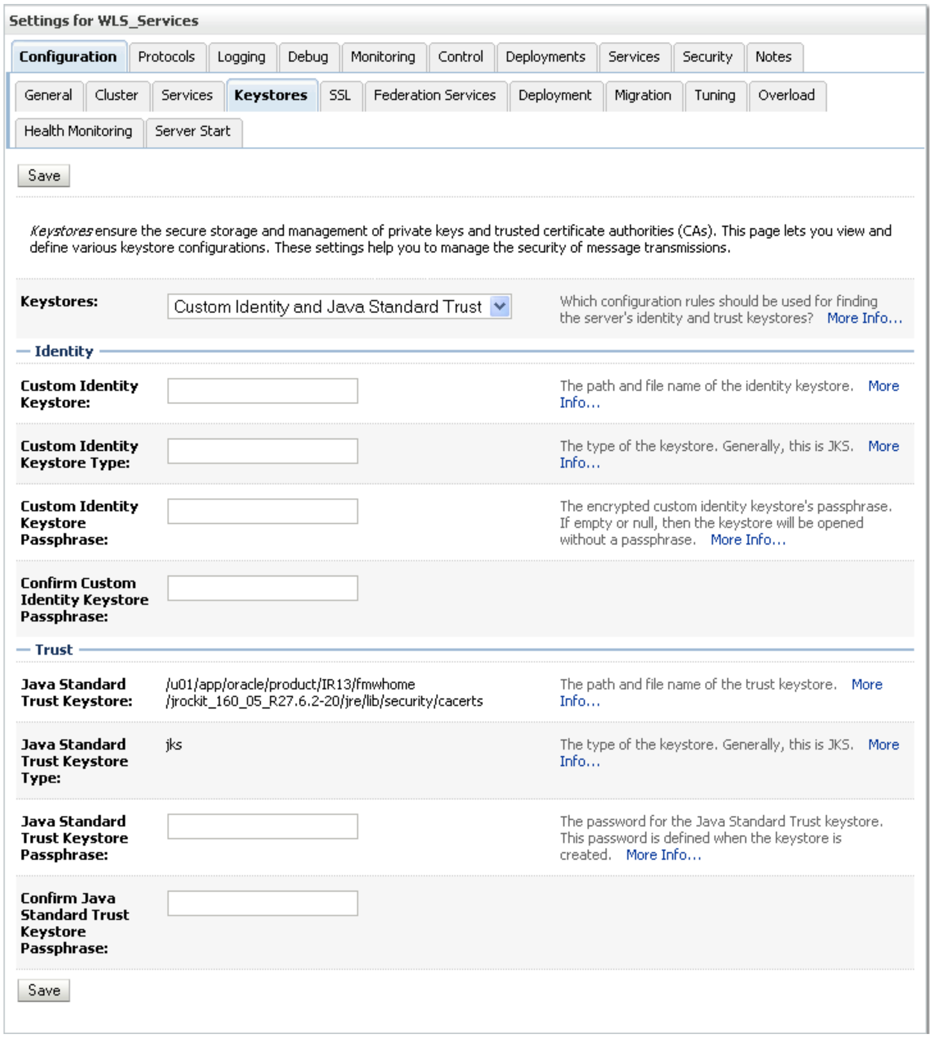
Use this page to configure general features of this server such as default network communications.

Name:	WLS_Services	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:		The IP address or DNS name this server uses to listen for incoming connections. More Info...
☑ Listen Port Enabled		Specifies whether this server can be reached through the default plain-text (non-SSL) listen port. More Info...
Listen Port:	8890	The default TCP port that this server uses to listen for regular (non-SSL) incoming connections. More Info...
☐ SSL Listen Port Enabled		Indicates whether the server can be reached through the default SSL listen port. More Info...
SSL Listen Port:	8790	The TCP/IP port at which this server listens for SSL connection requests. More Info...
☐ Client Cert Proxy Enabled		Specifies whether the HttpClusterServlet proxies the client certificate in a special header. More Info...
Java Compiler:	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 27–19).

Figure 27–19 Keystores Pane



Settings for WLS_Services

Keystores ensure the secure storage and management of private keys and trusted certificate authorities (CAs). This page lets you view and define various keystore configurations. These settings help you to manage the security of message transmissions.

Keystores: Custom Identity and Java Standard Trust — Which configuration rules should be used for finding the server's identity and trust keystores? More Info...

Identity

Custom Identity Keystore: — The path and file name of the identity keystore. More Info...

Custom Identity Keystore Type: — The type of the keystore. Generally, this is JKS. More Info...

Custom Identity Keystore Passphrase: — The encrypted custom identity keystore's passphrase. If empty or null, then the keystore will be opened without a passphrase. More Info...

Confirm Custom Identity Keystore Passphrase:

Trust

Java Standard Trust Keystore: /u01/app/oracle/product/IR13/fmwhome /jrockit_160_05_R27.6.2-20/jre/lib/security/cacerts — The path and file name of the trust keystore. More Info...

Java Standard Trust Keystore Type: jks — The type of the keystore. Generally, this is JKS. More Info...

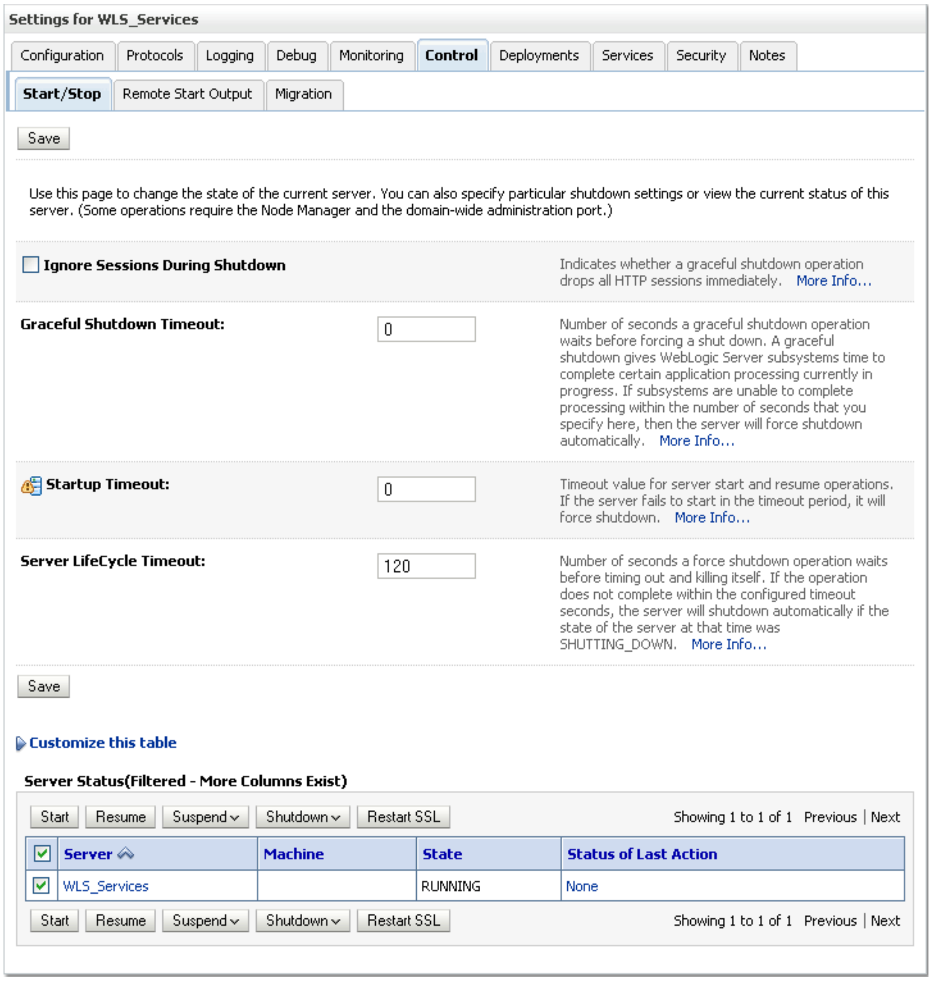
Java Standard Trust Keystore Passphrase: — The password for the Java Standard Trust keystore. This password is defined when the keystore is created. More Info...

Confirm Java Standard Trust Keystore Passphrase:

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 Trustore passphrase to `changeit` (this is fixed value) and click **Save**.
10. Go to WLS console -> servers -> WLS_Services -> Configuration tab -> General sub tab
11. Check the SSL Port enabled, specify a port that you want, and save
12. Go to WLS console -> servers -> WLS_Services -> Configuration tab -> SSL sub tab
13. Specify private key alias as owc_discussions, passwd -> welcome1
14. Open the Control tab.

    The Control Settings pane displays (see Figure 27–20).

Figure 27–20 Control Settings Pane



Settings for WLS_Services

Configuration | Protocols | Logging | Debug | Monitoring | Control | Deployments | Services | Security | Notes
Start/Stop | Remote Start Output | Migration
Save

Use this page to change the state of the current server. You can also specify particular shutdown settings or view the current status of this server. (Some operations require the Node Manager and the domain-wide administration port.)

☐ Ignore Sessions During Shutdown — Indicates whether a graceful shutdown operation drops all HTTP sessions immediately. More Info...

Graceful Shutdown Timeout: 0 — 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: 0 — 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: 120 — 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...

Server Status(Filtered - More Columns Exist)

Start | Resume | Suspend | Shutdown | Restart SSL
Showing 1 to 1 of 1 Previous | Next

☑	Server	Machine	State	Status of Last Action
☑	WLS_Services		RUNNING	None

Start | Resume | Suspend | Shutdown | Restart SSL
Showing 1 to 1 of 1 Previous | Next

15. Click **Restart SSL**.

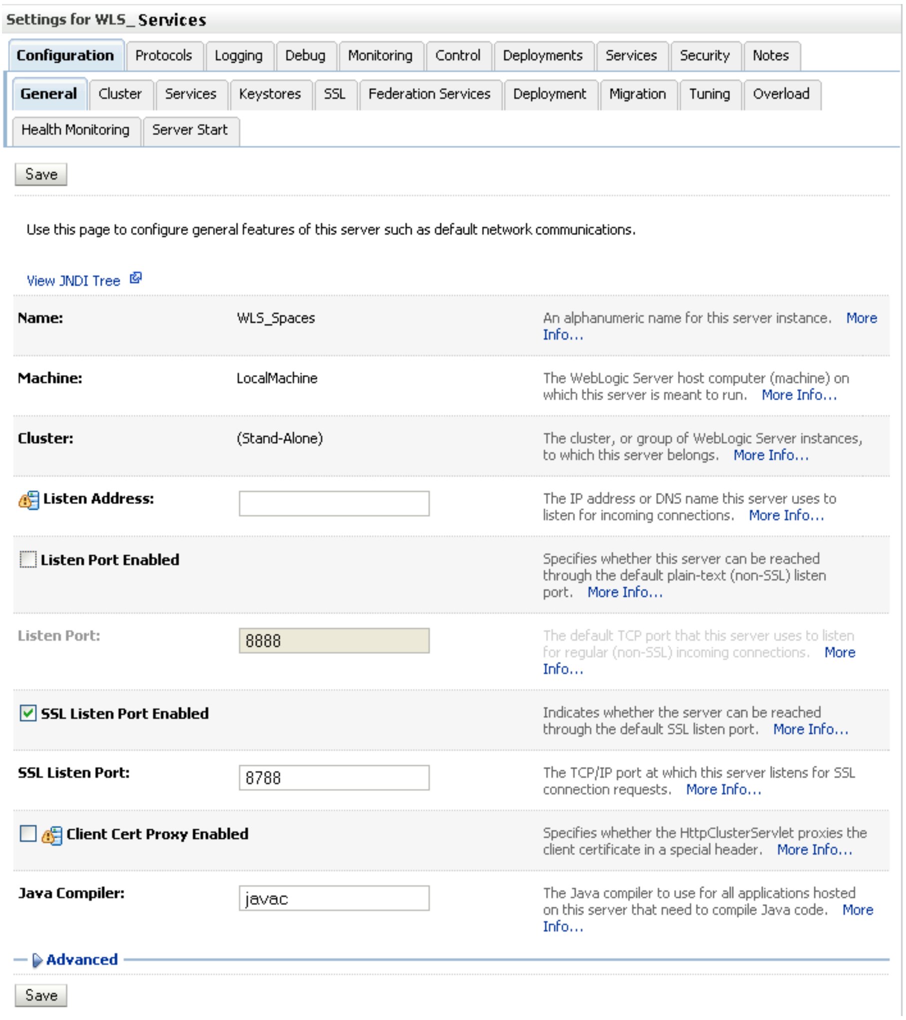
27.5.3 Configuring the SSL Connection

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 27–21).

Figure 27–21 General Configuration Pane



Use this page to configure general features of this server such as default network communications.

Name:	WLS_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:		The IP address or DNS name this server uses to listen for incoming connections. More Info...
□ **Listen Port Enabled**		Specifies whether this server can be reached through the default plain-text (non-SSL) listen port. More Info...
Listen Port:	8888	The default TCP port that this server uses to listen for regular (non-SSL) incoming connections. More Info...
☑ **SSL Listen Port Enabled**		Indicates whether the server can be reached through the default SSL listen port. More Info...
SSL Listen Port:	8788	The TCP/IP port at which this server listens for SSL connection requests. More Info...
□ **Client Cert Proxy Enabled**		Specifies whether the HttpClusterServlet proxies the client certificate in a special header. More Info...
Java Compiler:	javac	The Java compiler to use for all applications hosted on this server that need to compile Java code. More Info...

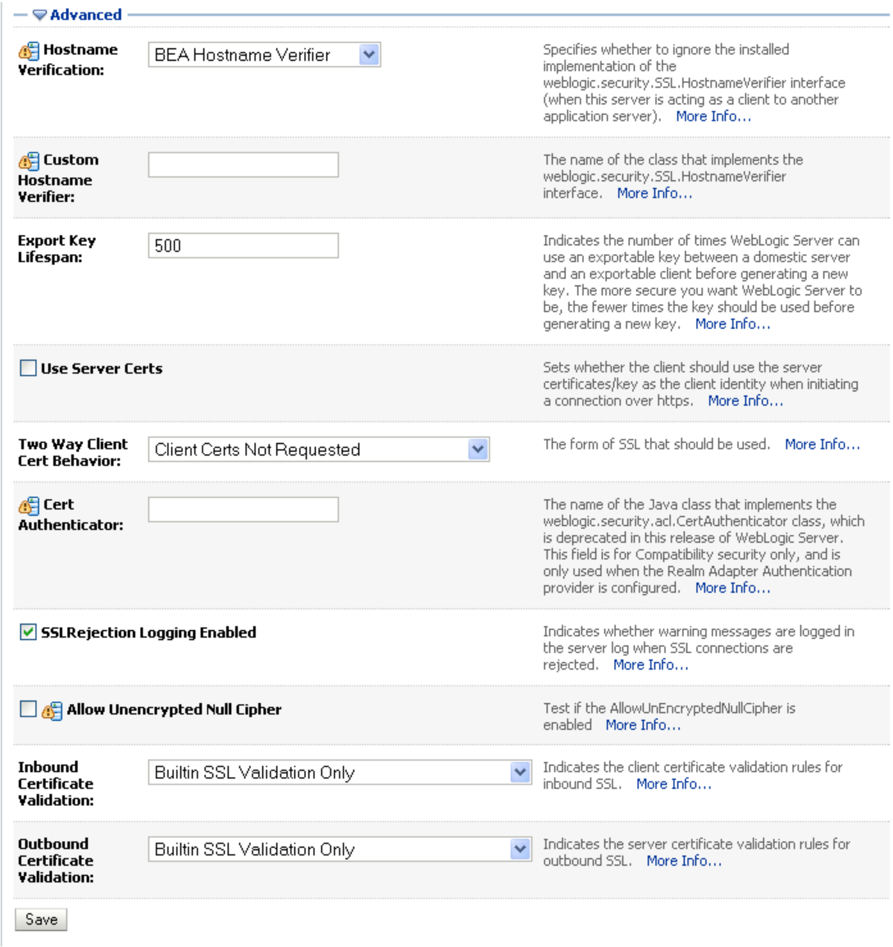
2. Check **SSL Listen Port Enabled**.

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 27–22).

Figure 27–22 Advanced SSL Configuration Settings



Hostname Verification:	BEA Hostname Verifier	Specifies whether to ignore the installed implementation of the weblogic.security.SSL.HostnameVerifier interface (when this server is acting as a client to another application server). More Info...
Custom Hostname Verifier:		The name of the class that implements the weblogic.security.SSL.HostnameVerifier 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...
☐ **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 weblogic.security.acl.CertAuthenticator class, which is deprecated in this release of WebLogic Server. This field is for Compatibility security only, and is only used when the Realm Adapter Authentication provider is configured. More Info...
☑ **SSLRejection Logging Enabled**		Indicates whether warning messages are logged in the server log when SSL connections are rejected. More Info...
☐ **Allow Unencrypted Null Cipher**		Test if the AllowUnEncryptedNullCipher 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...

5. Set the **Two Way Client Cert Behavior** option to `Client Certs Not Requested` and click **Save**.

6. Restart the `WLS_Services` server and open the SSL Discussions URL at `https://host:port/owc_discussions`.

7. Accept the certificate for the session and log in.

27.6 Securing the WebCenter 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 27.6.1, "Configuring the Identity and Trust Key Stores"
- Section 27.6.2, "Configuring the SSL Connection"
- Section 27.6.3, "Registering the SSL-enabled WSRP Producer and Running the Portlets"
- Section 27.6.4, "Registering the SSL-enabled PDK-Java Producer and Running the Portlets"

27.6.1 Configuring the Identity and Trust Key Stores

To configure the identity and trust key stores:

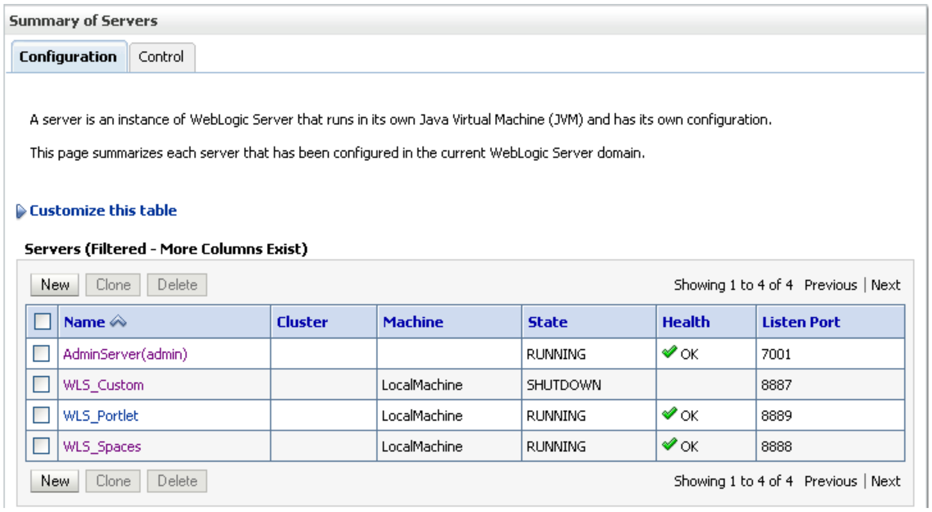
1. Log in to the WebLogic Server Administration Console.

   For information on logging into the WebLogic Server Administration Console, see Section 1.12.2, "Oracle WebLogic Server Administration Console."

2. In the Domain Structure pane, expand **Environment** and click **Servers**.

   The Summary of Servers pane displays (see Figure 27–23).

Figure 27–23 Summary of Servers Pane



Summary of Servers

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.

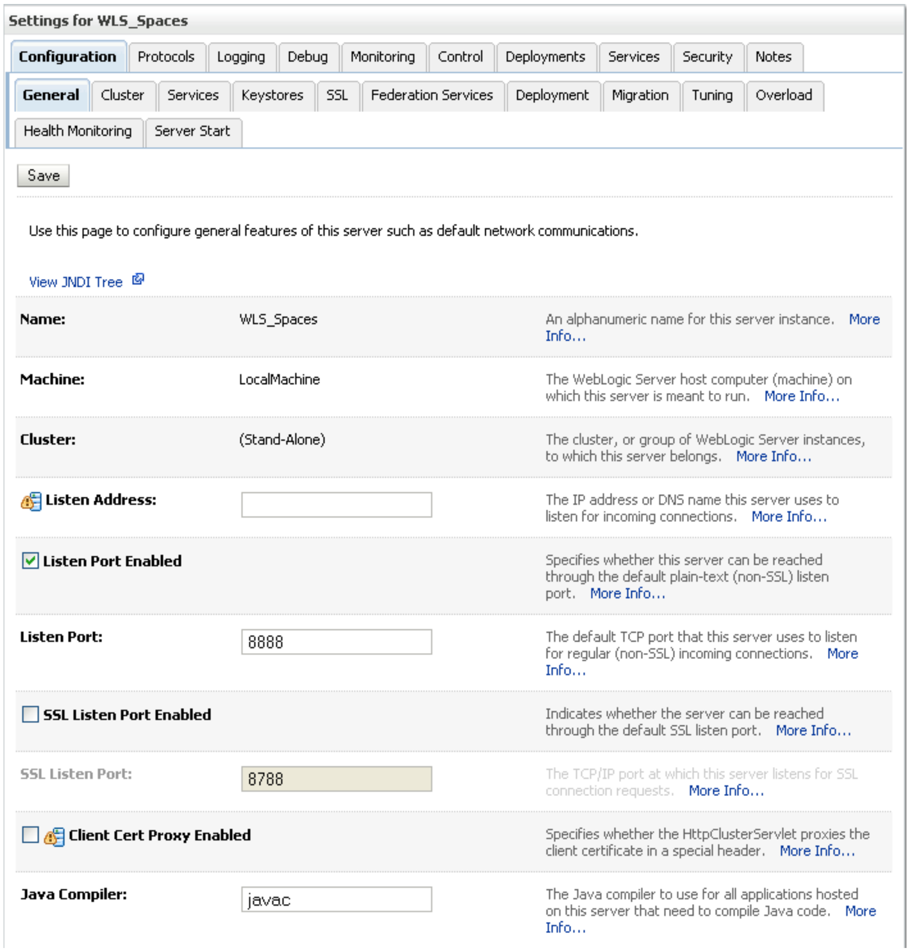
Servers (Filtered - More Columns Exist)

□	Name	Cluster	Machine	State	Health	Listen Port
□	AdminServer(admin)			RUNNING	✓ OK	7001
□	WLS_Custom		LocalMachine	SHUTDOWN		8887
□	WLS_Portlet		LocalMachine	RUNNING	✓ OK	8889
□	WLS_Spaces		LocalMachine	RUNNING	✓ OK	8888

3. Click the Portlet server (for example, `WLS_Portlet`) to configure the identity and trust keystores.

   The Settings pane for the Portlet server displays (see Figure 27–24).

Figure 27–24 Settings Pane for Portlet Server



Settings for WLS_Spaces

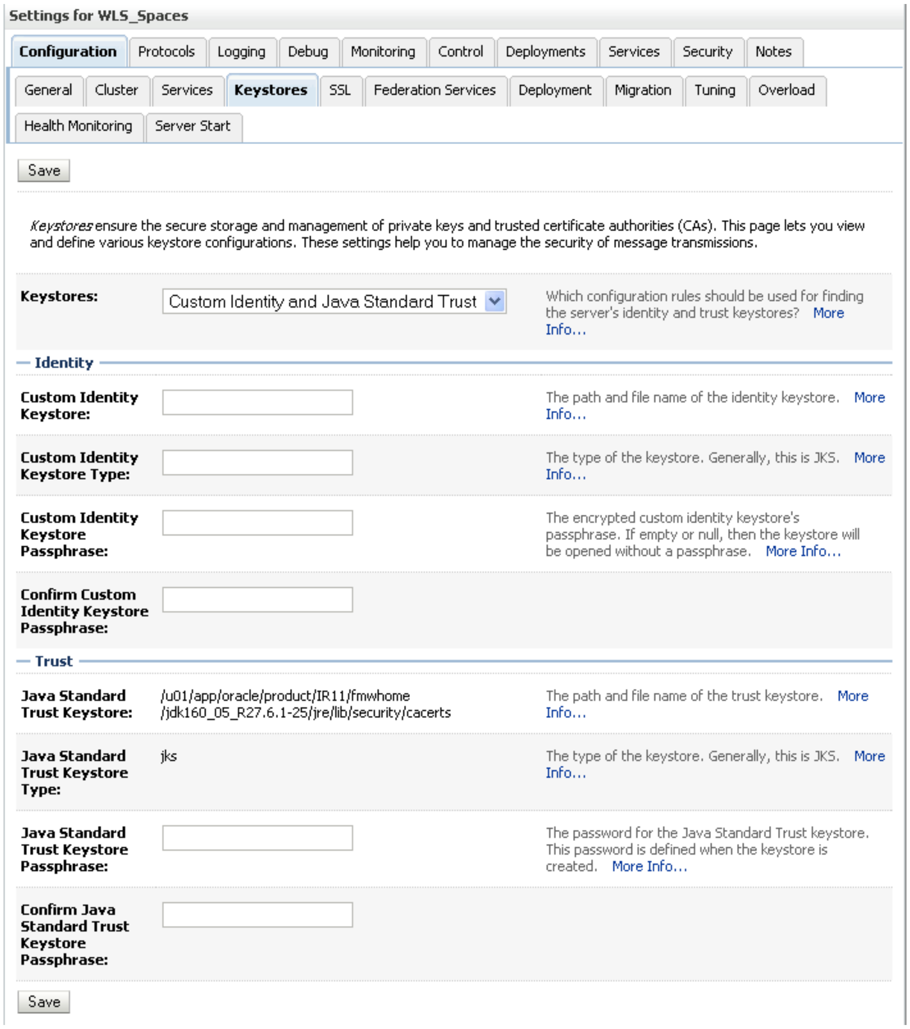
Use this page to configure general features of this server such as default network communications.

Name:	WLS_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:		The IP address or DNS name this server uses to listen for incoming connections. More Info...
☑ **Listen Port Enabled**		Specifies whether this server can be reached through the default plain-text (non-SSL) listen port. More Info...
Listen Port:	8888	The default TCP port that this server uses to listen for regular (non-SSL) incoming connections. More Info...
☐ **SSL Listen Port Enabled**		Indicates whether the server can be reached through the default SSL listen port. More Info...
SSL Listen Port:	8788	The TCP/IP port at which this server listens for SSL connection requests. More Info...
☐ **Client Cert Proxy Enabled**		Specifies whether the HttpClusterServlet proxies the client certificate in a special header. More Info...
Java Compiler:	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 27–25).

Figure 27–25 Keystores Pane



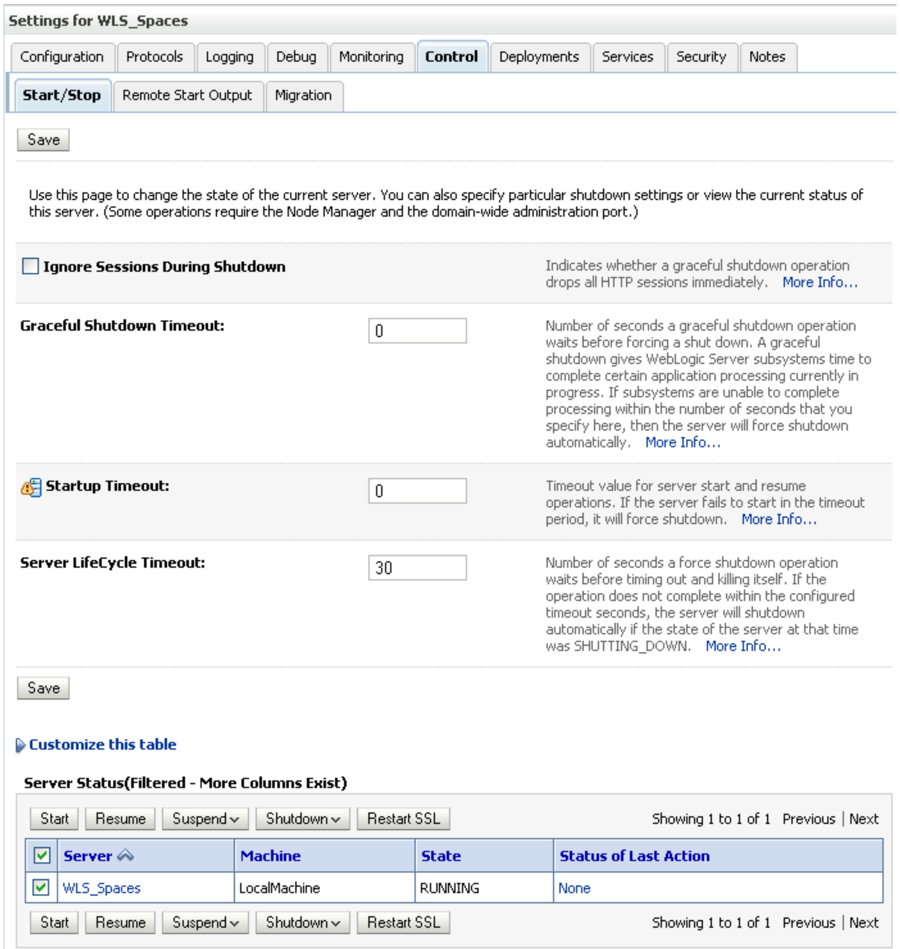
Keystores ensure the secure storage and management of private keys and trusted certificate authorities (CAs). This page lets you view and define various keystore configurations. These settings help you to manage the security of message transmissions.

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:		

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 27–26).

Figure 27–26 Control Settings Pane



Settings for WLS_Spaces

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: 0 — 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: 0 — 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: 30 — 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...

Server Status(Filtered - More Columns Exist)

☑	Server	Machine	State	Status of Last Action
☑	WLS_Spaces	LocalMachine	RUNNING	None

7. Click **Restart SSL**.

27.6.2 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, `WLS_Portlet`) for which you want to configure SSL.
3. Select **Configuration**.
4. Check **SSL Listen Port Enable**.
5. Enter a listen port number.
6. Select **Configuration** > **SSL**, and then open the Advanced options at the bottom of the page.
7. Select the **Two Way Client Cert Behavior** attribute and choose the **Client Certs Not Requested** option.
8. Click **Save**.
9. Restart the WebLogic Server and open the SSL URL.

10. Accept the certificate for the session and log in.

27.6.3 Registering the SSL-enabled WSRP Producer and Running the Portlets

To register the SSL-enabled WSRP producer and run the portlets:

1. Configure the WebCenter 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 `WLS_Spaces`.
5. Start WLST as described in Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool (WLST) Commands."
6. Connect to the Administration Server for the target domain with the following command:

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

   Where:

   - *`user_name`* is the name of the user account with which to access the `WLS_Spaces` server (for example, weblogic)
   - *`password`* is the password with which to access the `WLS_Spaces` server
   - *`host_id`* is the host ID of the Administration Server
   - *`port`* is the port number of the Administration Server (for example, `7001`).
7. Run the `registerWSRPProducer` WLST command to register the producer:

   ```
   registerWSRPProducer('webcenter', 'sslwsrpprod','producer_wsdl)
   ```

   Where:

   - *`sslwsrpprod`* is the name of the SSL-enabled WSRP producer
   - *`producer_wsdl`* is the WSDL URL of the SSL-enabled WSRP producer

   For example:

   ```
   registerWSRPProducer('webcenter',
   ```

```
'sslwsrpprod','https://example.oracle.com:7004/richtextportlet/portlets/wsrp2?W
SDL')
```

8. Navigate to the HTTP or HTTPS WebCenter URL.
9. Create a page and go to the Portlets link.
10. Go to the registered WSRP producer.
11. Add the portlet to the page.
12. Go to the view mode of the page and check that the WSRP portlet renders correctly.

27.6.4 Registering the SSL-enabled PDK-Java Producer and Running the Portlets

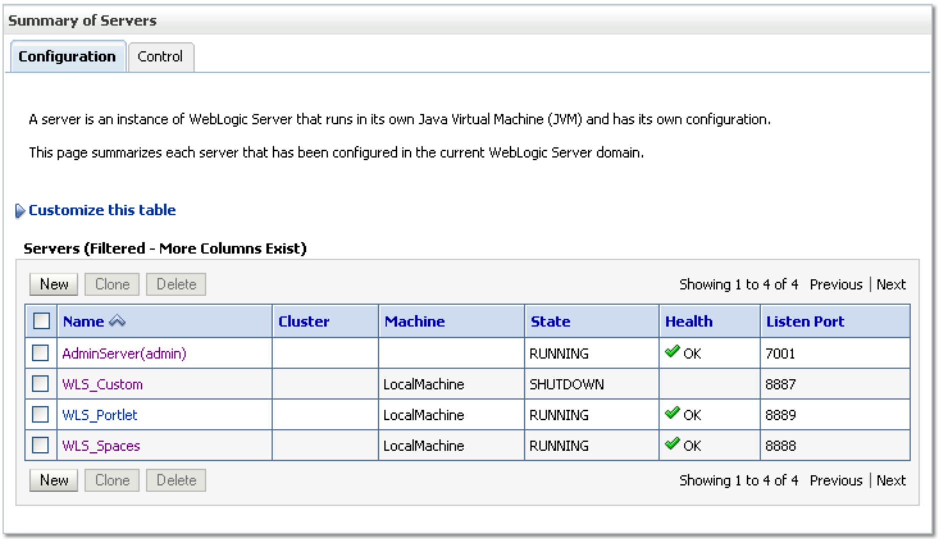
To register the SSL-enabled PDK-Java Producer and run the portlets:

1. Configure the WebCenter 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 1.12.2, "Oracle WebLogic Server Administration Console."
3. On the Domain Structure pane, expand **Environment** and click **Servers**.

   The Summary of Servers pane displays (see Figure 27–27).

Figure 27–27 Summary of Servers Pane



Summary of Servers

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.

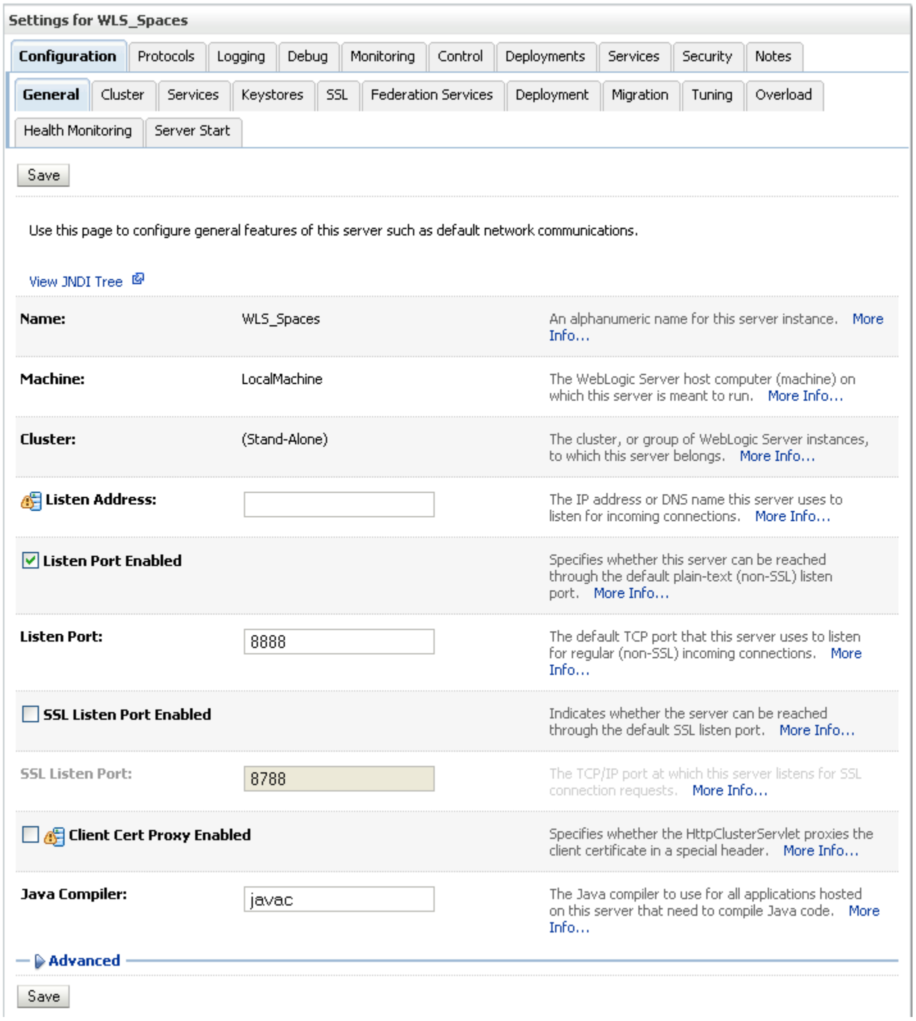
Servers (Filtered - More Columns Exist)

□	Name	Cluster	Machine	State	Health	Listen Port
□	AdminServer(admin)			RUNNING	✓ OK	7001
□	WLS_Custom		LocalMachine	SHUTDOWN		8887
□	WLS_Portlet		LocalMachine	RUNNING	✓ OK	8889
□	WLS_Spaces		LocalMachine	RUNNING	✓ OK	8888

4. Click `WLS_Spaces` in the servers list.

   The Settings pane displays (see Figure 27–28).

Figure 27–28 Settings Pane (WLS_Spaces Server)



Settings for WLS_Spaces

Use this page to configure general features of this server such as default network communications.

Name: WLS_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: — The IP address or DNS name this server uses to listen for incoming connections. More Info...

☑ **Listen Port Enabled** — Specifies whether this server can be reached through the default plain-text (non-SSL) listen port. More Info...

Listen Port: 8888 — The default TCP port that this server uses to listen for regular (non-SSL) incoming connections. More Info...

☐ **SSL Listen Port Enabled** — Indicates whether the server can be reached through the default SSL listen port. More Info...

SSL Listen Port: 8788 — The TCP/IP port at which this server listens for SSL connection requests. More Info...

☐ **Client Cert Proxy Enabled** — Specifies whether the HttpClusterServlet proxies the client certificate in a special header. More Info...

Java Compiler: javac — The Java compiler to use for all applications hosted on this server that need to compile Java code. More Info...

5. Open the Configuration tab and select the Keystores tab.
6. Make sure that the value for **Demo Identity and Demo Trust** is either `jks` or left blank.
7. Click **Save**.
8. Download the certificate of the HTTPS producer URL and save it in `.PEM` format.

   Use Firefox 3.0 or later to download the certificate directly to `.PEM` format, or for other browsers use the 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 WLS_Spaces.
11. Start WLST as described in Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool (WLST) Commands."

12. Connect to the Administration Server for the target domain with the following command:

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

    where:

    - *user_name* is the name of the user account with which to access the WLS_Spaces server (for example, weblogic)
    - *password* is the password with which to access the WLS_Spaces server
    - *host_id* is the host ID of the Administration Server
    - *port* is the port number of the Administration Server (for example, 7001).

13. Run the registerPDKJavaProducer command:

    ```
    registerPDKJavaProducer('webcenter', 'ssljpdkprod', 'producer_wsdl')
    ```

    Where:

    - *ssljpdkprod* is the name of the SSL-enabled PDK-Java producer
    - *producer_wsdl* 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 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.

27.7 Securing the WebCenter Spaces Connection to the LDAP Identity Store

To configure the LDAP server port for SSL, refer to the appropriate administration documentation for the LDAP server. For Oracle Internet Directory (OID), an SSL port is installed by default. To use this port for LDAP communication from WebCenter, the identity store should be configured for authentication with the appropriate authenticator. See Chapter 24, "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 27.7.1, "Exporting the OID Certificate Authority (CA)"
- Section 27.7.2, "Setting Up the WebLogic Server"

For more information, see "Setting Up a One- Way SSL Connection" in the *Oracle Fusion Middleware Security Guide*.

27.7.1 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
```

27.7.2 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
```

27.8 Securing the WebCenter Spaces Connection to Oracle Content Server with SSL

For instructions on how to configure Oracle Content Server (OCS) for SSL, see Section 11.2.1.2.3, "Configuring Secure Sockets Layer (SSL)." For instructions on adding a trusted certificate to the WebCenter Spaces trust store, see the section on importing the certificate into the trust store in Section 27.1.2, "Configuring the Custom Identity and Java Trust Keystores."

27.9 Securing the WebCenter 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 WebCenter Spaces to use the trust store.

To secure the WebCenter Spaces connection to IMAP and SMTP with SSL:

1. Open a browser and connect to your IMAP server with the following command:

   ```
   https://imapserver:ssl_port
   ```

   For example:

   ```
   https:mailserver.example:993
   ```

2. Place your cursor on the page, right-click, and select **Properties**.
3. Click **Certificate**.
4. In the popup window, click the **Details** tab and click **Copy to File...**

   Be sure to use the DER encoded binary(X.509) format and copy to a file.
5. Convert the .DER format certificate to .PEM format.

   Use Firefox 3.0 or later to download the certificate directly to .PEM format, or for other browsers use the 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 15.3, "Registering Mail Servers."

8. Restart Webcenter Spaces.

9. Log into WebCenter Spaces and provide your mail credentials.

27.10 Securing a Custom WebCenter Application's Connection to IMAP and SMTP with SSL

To secure the connection to IMAP and SMTP with SSL for a custom WebCenter application:

1. Follow the steps in Section 27.9, "Securing the WebCenter 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 custom WebCenter application.

4. Log into the application and provide your mail credentials.

27.11 Securing the WebCenter Spaces 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 18.3.1, "Registering Oracle SES Services."

8. Restart WebCenter Spaces.

27.12 Securing the WebCenter Spaces Connection to OWLCS with SSL

To secure the WebCenter Spaces connection to Oracle WebLogic Communication Services (OWLCS) with SSL, follow the steps below to import the certificate into the trust store, and point WebCenter Spaces to use the trust store. Note that securing the WebCenter Spaces connection to OWLCS with SSL is optional since OWLCS can be configured with confidentiality using WS-Security. See Section 28.4, "Securing Oracle WebLogic Communication Services (OWLCS) with WS-Security."

Before registering the OWLCS 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 OWLCS server (for example, `https://example.com:port/PresenceConsumerService/services/PresenceConsumer`)

2. Place your cursor on the page, right-click, and select **Properties**.

3. Click **Certificate**.

4. In the popup window, open the **Details** tab and click **Copy to File...**

   Use Firefox 3.0 or later to download the certificate directly to `.PEM` format, or for other browsers use the 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 owlcs_cer -file cert_file.cer -keystore cacerts
   -storepass changeit
   ```

   where *`cert_file`* is the name of the certificate file you downloaded.

6. Locate the `cacerts` file used by the OWLCS server in the OWLCS installation, and also update the OWLCS referenced `cacerts` file with this certificate:

   ```
   keytool -import -alias owlcs_cer -file cert_file.cer -keystore cacerts
   ```

```
-storepass changeit
```

7. Register the Oracle WebLogic Communication Services connection as described in Section 14.3, "Registering Instant Messaging and Presence Servers."
8. Restart the WebCenter Spaces server.

27.13 Securing the WebCenter Spaces Connection to Microsoft Live Communication Server and Office Communication Server with SSL

To secure the WebCenter 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 WebCenter Spaces to use the trust store. Note that securing the WebCenter 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 14.3, "Registering Instant Messaging and Presence Servers."
8. Restart the WebCenter Spaces server.

27.14 Securing the WebCenter Spaces Connection to an External BPEL Server with SSL

This section describes how to secure the WebCenter 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. For more information on configuring the Identity Asserter and Authenticator for an external LDAP identity store, see Section 24.1, "Reassociating the Identity Store with an External LDAP."

To secure the WebCenter Spaces connection to an external BPEL server with SSL:

1. Copy the public certificate (`webcenter_wls.cer`) from WebCenter 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_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
   ```

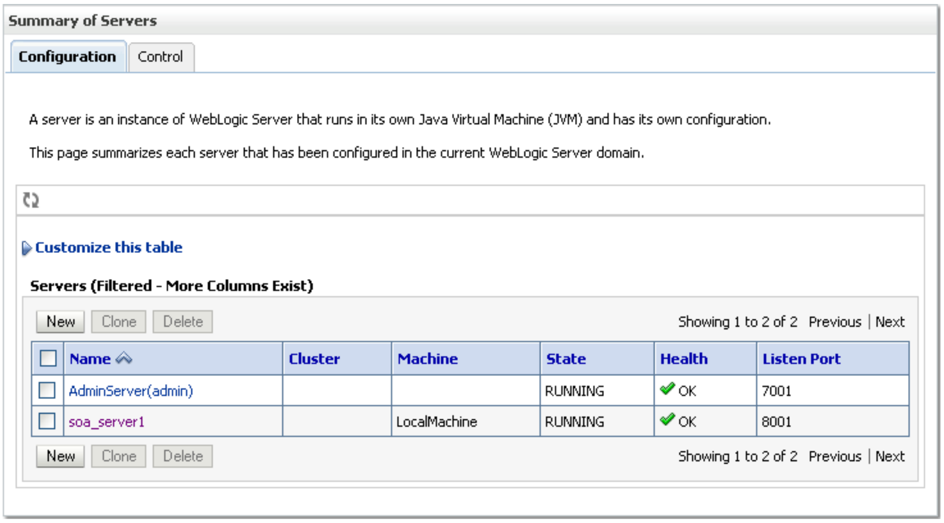
   Where:

   - *`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 1.12.2, "Oracle WebLogic Server Administration Console."
6. In the Navigation pane, expand **Environment** and click **Servers**.

   The Summary of Servers pane displays (see Figure 27–29).

Figure 27–29 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

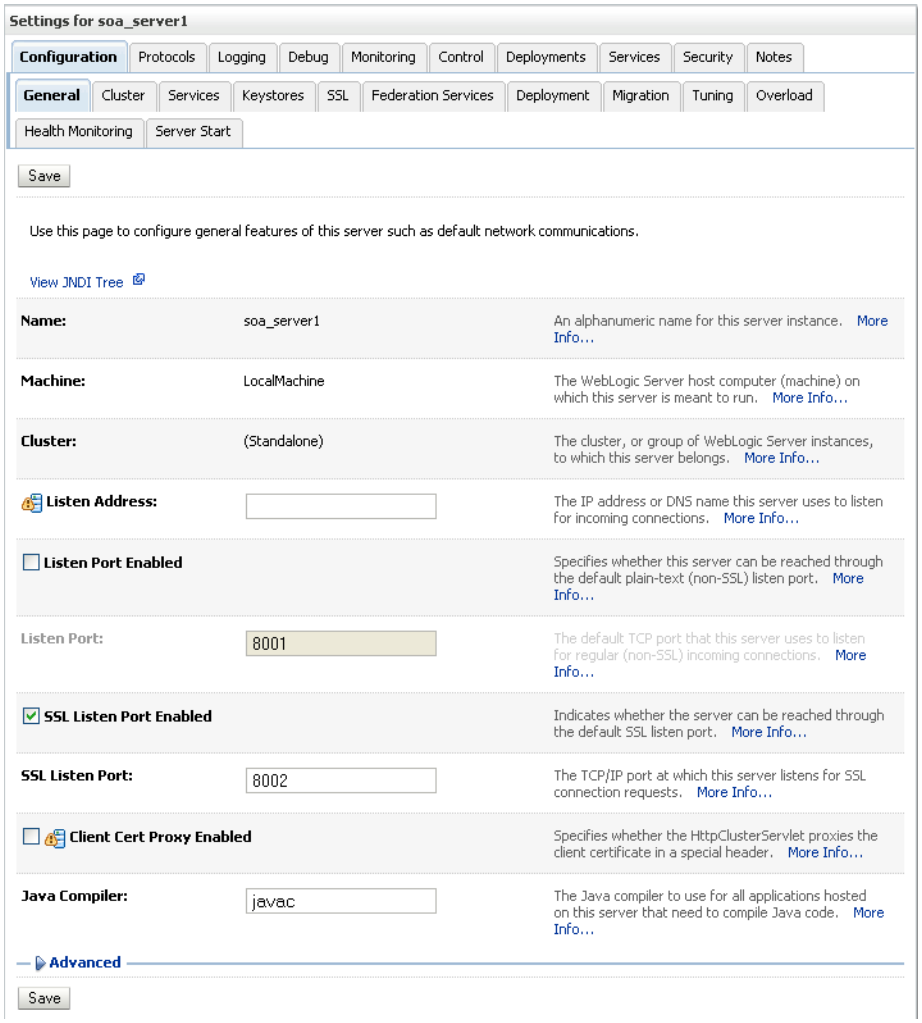
☐	Name	Cluster	Machine	State	Health	Listen Port
☐	AdminServer(admin)			RUNNING	✓ OK	7001
☐	soa_server1		LocalMachine	RUNNING	✓ OK	8001

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 27–30).

Figure 27–30 Settings Page for soa_server1



Settings for soa_server1

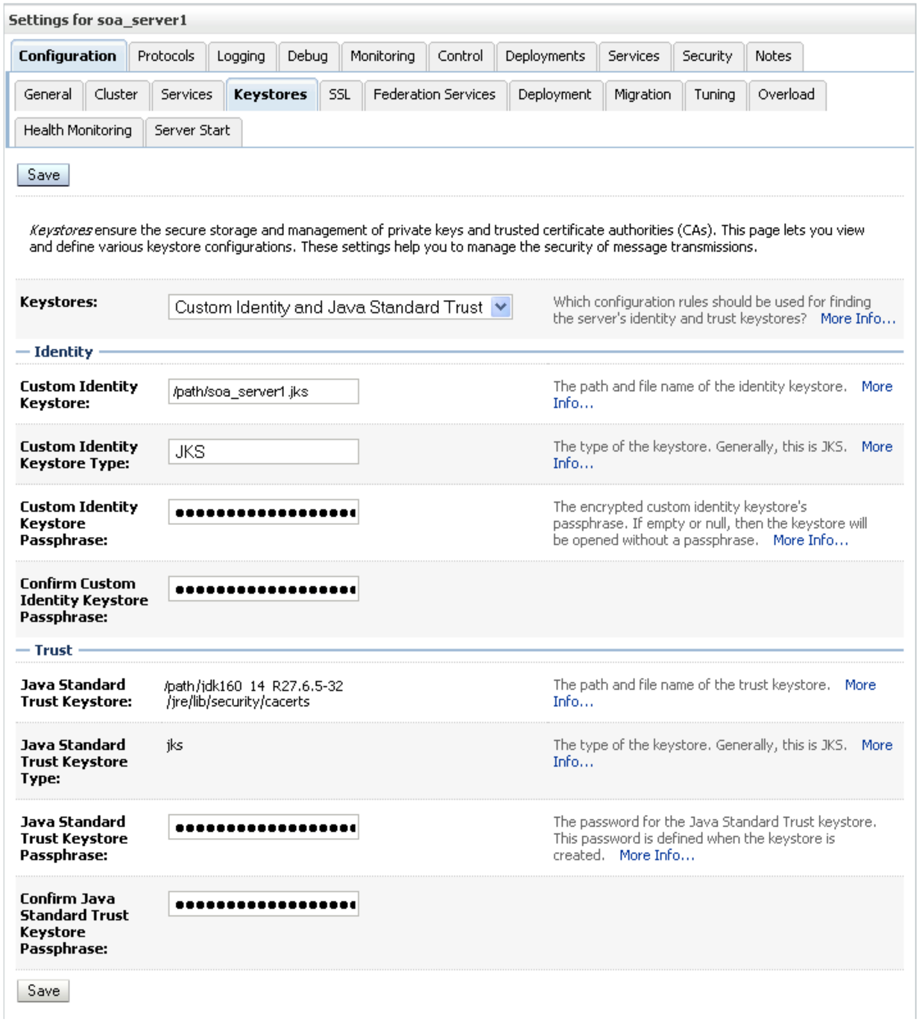
Use this page to configure general features of this server such as default network communications.

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:		The IP address or DNS name this server uses to listen for incoming connections. More Info...
□ **Listen Port Enabled**		Specifies whether this server can be reached through the default plain-text (non-SSL) listen port. More Info...
Listen Port:	8001	The default TCP port that this server uses to listen for regular (non-SSL) incoming connections. More Info...
☑ **SSL Listen Port Enabled**		Indicates whether the server can be reached through the default SSL listen port. More Info...
SSL Listen Port:	8002	The TCP/IP port at which this server listens for SSL connection requests. More Info...
□ **Client Cert Proxy Enabled**		Specifies whether the HttpClusterServlet proxies the client certificate in a special header. More Info...
Java Compiler:	javac	The Java compiler to use for all applications hosted on this server that need to compile Java code. More Info...

8. Open the Keystores tab.

   The Keystore settings for `soa_server1` displays (see Figure 27–31).

Figure 27–31 Keystore Settings for soa_server1



Settings for soa_server1

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: ●●●●●●●●●●●●●●●●●●

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 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
    ```

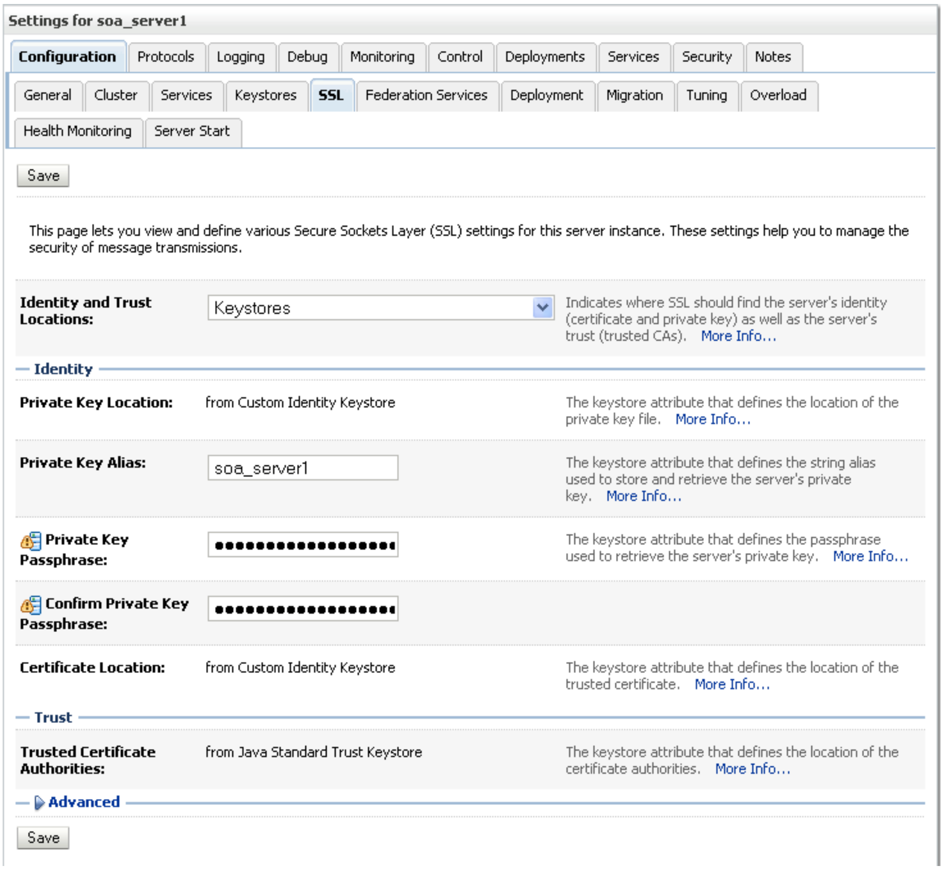
    Where:

    - *`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 27–32).

Figure 27–32 SSL Settings for soa_server1



Settings for soa_server1

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: Keystores — 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 — The keystore attribute that defines the location of the private key file. More Info...

Private Key Alias: soa_server1 — The keystore attribute that defines the string alias used to store and retrieve the server's private key. More Info...

Private Key Passphrase: ••••••••••••••••••• — The keystore attribute that defines the passphrase used to retrieve the server's private key. More Info...

Confirm Private Key Passphrase: •••••••••••••••••••

Certificate Location: from Custom Identity Keystore — The keystore attribute that defines the location of the trusted certificate. More Info...

Trusted Certificate Authorities: from Java Standard Trust Keystore — The keystore attribute that defines the location of the certificate authorities. More Info...

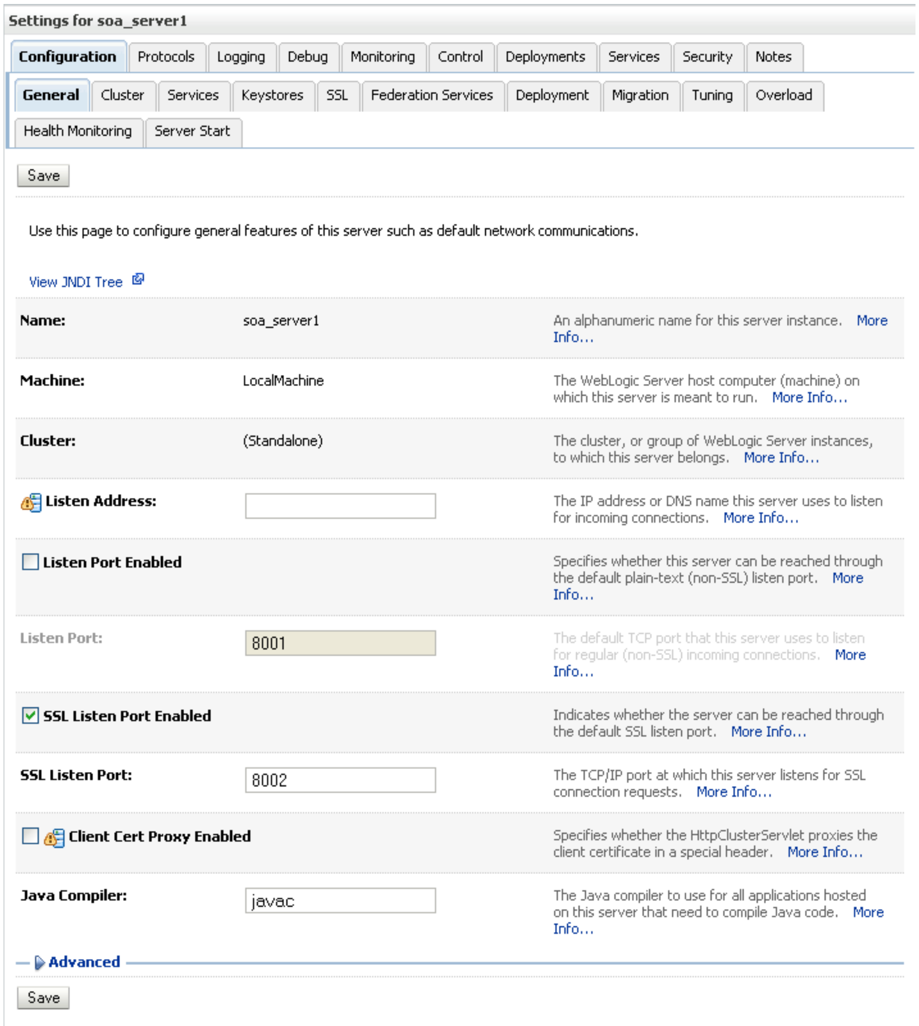
13. Specify soa_server1 as the **Private Key Alias**.

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 27–33).

Figure 27–33 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
View JNDI Tree
Advanced
Save

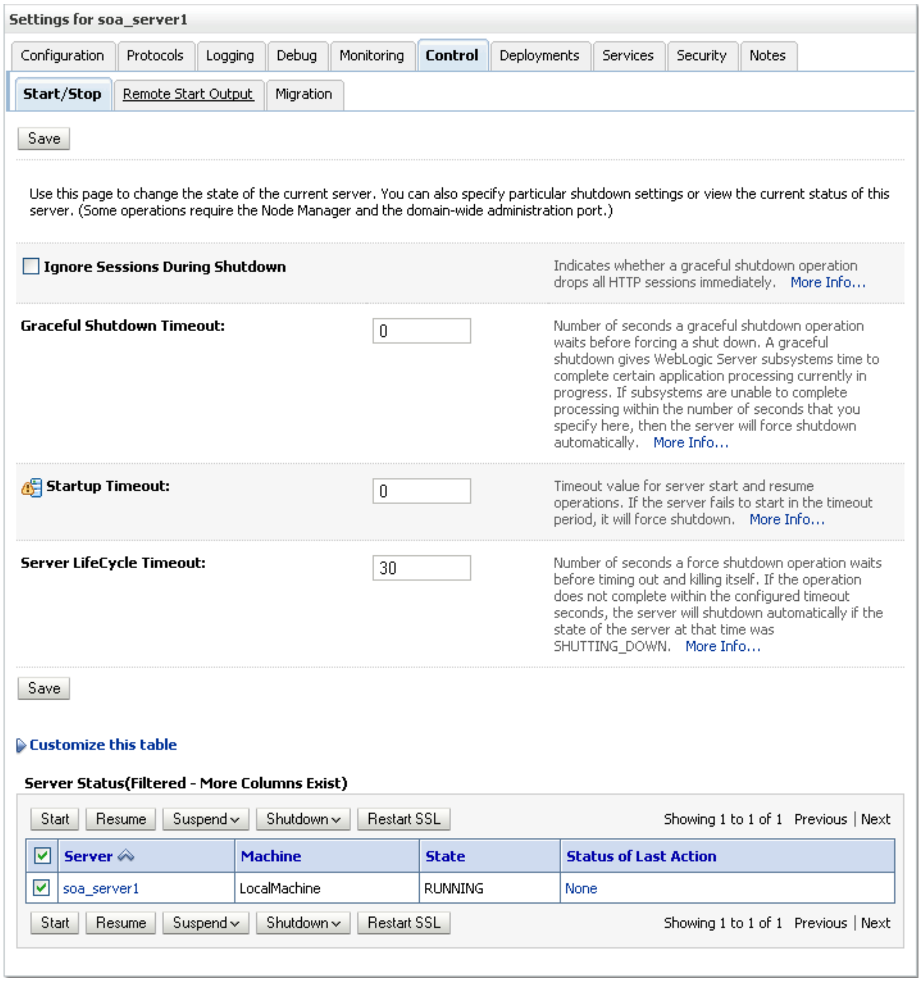
Use this page to configure general features of this server such as default network communications.

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:		The IP address or DNS name this server uses to listen for incoming connections. More Info...
□ **Listen Port Enabled**		Specifies whether this server can be reached through the default plain-text (non-SSL) listen port. More Info...
Listen Port:	8001	The default TCP port that this server uses to listen for regular (non-SSL) incoming connections. More Info...
☑ **SSL Listen Port Enabled**		Indicates whether the server can be reached through the default SSL listen port. More Info...
SSL Listen Port:	8002	The TCP/IP port at which this server listens for SSL connection requests. More Info...
□ **Client Cert Proxy Enabled**		Specifies whether the HttpClusterServlet proxies the client certificate in a special header. More Info...
Java Compiler:	javac	The Java compiler to use for all applications hosted on this server that need to compile Java code. More Info...

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 27–34).

Figure 27–34 Start/Stop Settings for soa_server1



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: 0 — 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: 0 — 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: 30 — 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...

Server Status(Filtered - More Columns Exist)

☑	Server	Machine	State	Status of Last Action
☑	soa_server1	LocalMachine	RUNNING	None

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 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 domain as described in Section 20.3.2, "Registering Worklist Connections" specifying the host:ssl_port settings for `soa_server1` when defining the BPEL URL.
23. Restart the `WLS_Spaces` Managed Server.

28

Configuring WS-Security for WebCenter Applications and Components

This chapter describes how to set up WS-Security for WebCenter applications (including WebCenter Spaces and custom WebCenter applications) and related services and components based on your topology. This section covers the following configurations:

- a simple topology, with the WebCenter application and all components sharing the same domain,
- a typical topology, with the WebCenter application and components divided across two domains, and
- a complex topology, with the WebCenter application and components divided across multiple domains.

Within these three topologies, configuration is described for the WebCenter application (WebCenter Spaces, for example), Oracle WebCenter Discussions, the Worklist service, and WSRP producers. These configurations and the steps for securing OWLCS and applications consuming WebCenter Spaces APIs are covered in the following sections:

- Section 28.1, "Configuring WS-Security for a Simple Topology"
- Section 28.2, "Configuring WS-Security for a Typical Topology"
- Section 28.3, "Configuring WS-Security for a Complex Topology"
- Section 28.4, "Securing Oracle WebLogic Communication Services (OWLCS) with WS-Security"
- Section 28.5, "Securing WebCenter Spaces for Applications Consuming Spaces Client APIs with WS-Security"

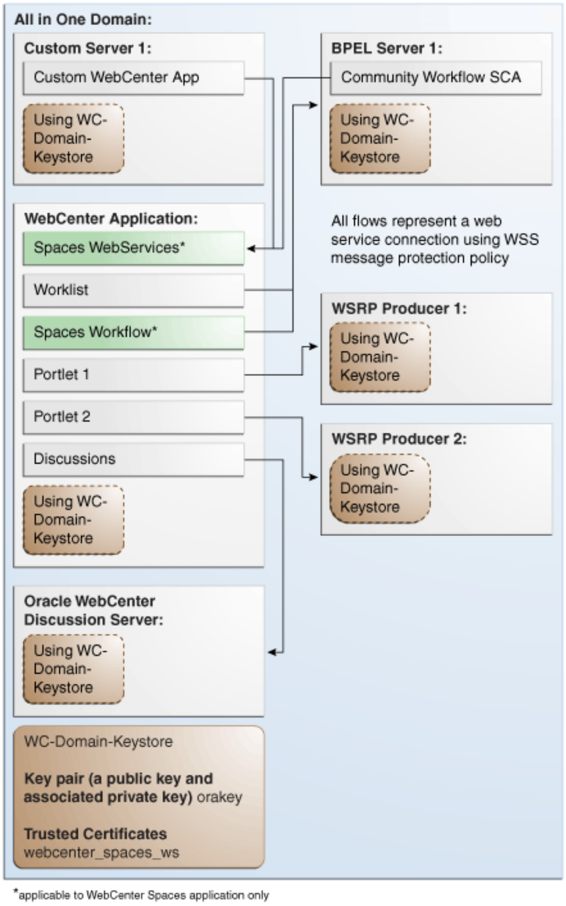
Audience

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."

28.1 Configuring WS-Security for a Simple Topology

This section describes how to configure WS-Security for a topology where the WebCenter application, the BPEL server, and WSRP producers share the same domain (Figure 28–1).

Figure 28–1 WS-Security for a Simple Configuration



The steps to configure WS-Security for a simple single-domain WebCenter topology are described in the following sections:

- Section 28.1.1, "Setting Up the WebCenter Domain Keystore"
- Section 28.1.2, "Configuring the Discussions Server for a Simple Topology"
- Section 28.1.3, "Configuring the BPEL Server for a Simple Topology"
- Section 28.1.4, "Command Summary for a Simple Topology"

28.1.1 Setting Up the WebCenter Domain Keystore

The security credentials of the WebCenter 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 28.1.1.1, "Creating the WebCenter Domain Keystore"
- Section 28.1.1.2, "Configuring the Keystore with WLST"

- Section 28.1.1.3, "Configuring the Keystore Using Fusion Middleware Control"
- Section 28.1.1.4, "Unconfiguring a Keystore Provider Using Fusion Middleware Control"

28.1.1.1 Creating the WebCenter 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 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 (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 28–1 Generating the Keypair

```
keytool -genkeypair -keyalg RSA -dname "cn=spaces,dc=example,dc=com" -alias orakey
-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 orakey -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 28–2 Exporting the Certificate Containing the Public Key

```
keytool -exportcert -v -alias orakey -keystore webcenter.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 webcenter.jks -storepass keystore_password
   ```

   Where:

   - *`keystore_password`* is the keystore password

Example 28–3 Importing the Certificate

```
keytool -importcert -alias webcenter_spaces_ws -file orakey.cer -keystore
webcenter.jks -storepass welcome1
```

5. Continue by configuring the keystore using either WLST as described in Section 28.1.1.2, "Configuring the Keystore with WLST," or using Fusion Middleware Control as described in Section 28.1.1.3, "Configuring the Keystore Using Fusion Middleware Control."

   Table 28–1 shows the keystore contents you should wind up with after creating and configuring the keystore.

Table 28–1 WebCenter Domain Keystore Contents for a Simple Topology

Key Alias	Description
`orakey`	Key pair used to sign and encrypt outbound messages from WebCenter Spaces. This key is used by both OWSM (Portlets and Worklist) and Discussions.
`webcenter_spaces_ws`	Certificate containing the public key for the `orakey` private key used in the WebCenter domain. The certificate is used to encrypt outbound WebService messages from the Workflow application on BPEL Server1 in the WebCenter domain, to the WebService APIs on WebCenter domain.

28.1.1.2 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.

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`
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:

   ```
   createCred(map="oracle.wsm.security", key="keystore-csf-key", user="owsm",
   password=keystore_password, desc="Keystore key")
   createCred(map="oracle.wsm.security", key="enc-csf-key", user="orakey",
   password=private_key_password, desc="Encryption key")
   createCred(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 28.1.1.1, "Creating the WebCenter Domain Keystore," (for example, welcome1)
- *private_key_password* is the private key password specified in step 2 of Section 28.1.1.1, "Creating the WebCenter Domain Keystore," (for example, welcome1)

Example 28–4 Updating the Credential Store

```
createCred(map="oracle.wsm.security", key="keystore-csf-key", user="owsm",
password="welcome1", desc="Keystore key")
createCred(map="oracle.wsm.security", key="enc-csf-key", user="orakey",
password="welcome1", desc="Encryption key")
createCred(map="oracle.wsm.security", key="sign-csf-key", user="orakey",
password="welcome1", desc="Signing key")
```

5. Restart all servers.

28.1.1.3 Configuring the Keystore Using Fusion Middleware Control

If a keystore provider is already configured, you must first unconfigure the existing keystore provider as described in Section 28.1.1.4, "Unconfiguring a Keystore Provider Using Fusion Middleware Control." Otherwise, continue with the steps below.

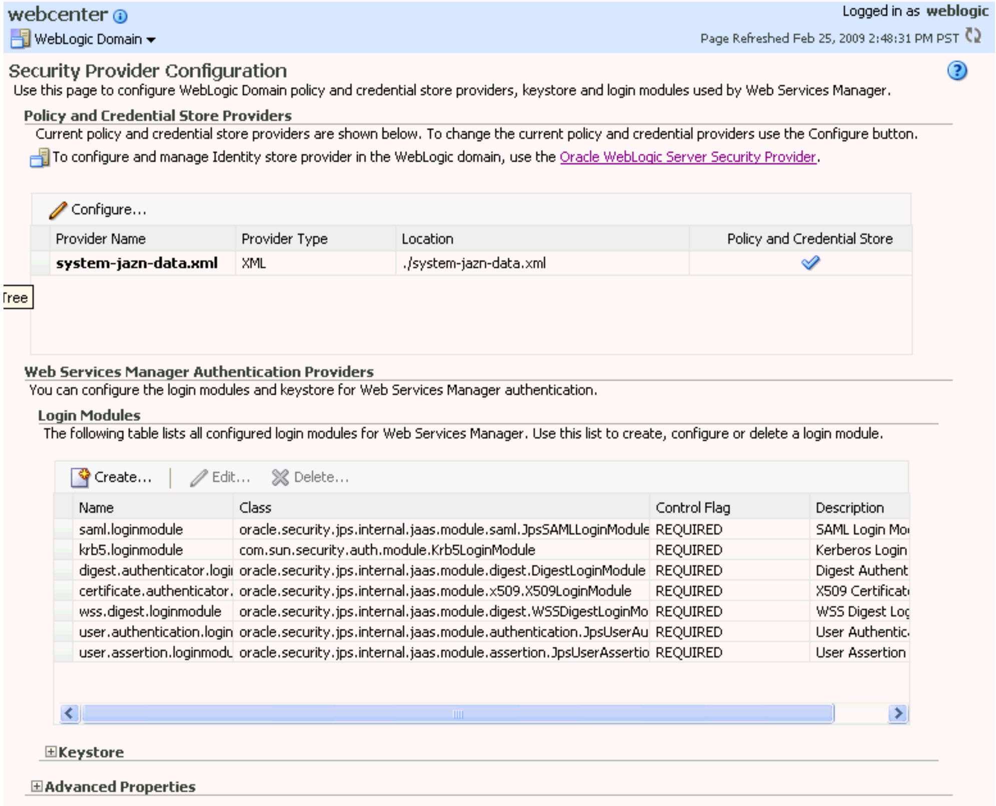
To configure the keystore provider:

1. Ensure that the `webcenter.jks` keystore file is copied to the *<DOMAIN_HOME>*`/config/fmwconfig` directory, and then specify the location as `./webcenter.jks`.
2. Open Fusion Middleware Control and log in to the WebCenter domain.

   For information on logging in to 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 WebCenter domain (`webcenter` by default).
4. From the WebLogic Domain menu, select **Security -> Security Provider Configuration**.

   The Security Provider Configuration page displays (see Figure 28–2).

Figure 28–2 Security Provider Configuration Page



webcenter ⓘ

WebLogic Domain ▾

Logged in as **weblogic**

Page Refreshed Feb 25, 2009 2:48:31 PM PST

Security Provider Configuration

Use this page to configure WebLogic Domain policy and credential store providers, keystore and login modules used by Web Services Manager.

Policy and Credential Store Providers

Current policy and credential store providers are shown below. To change the current policy and credential providers use the Configure button.

To configure and manage Identity store provider in the WebLogic domain, use the Oracle WebLogic Server Security Provider.

Provider Name	Provider Type	Location	Policy and Credential Store
system-jazn-data.xml	XML	./system-jazn-data.xml	✓

Web Services Manager Authentication Providers

You can configure the login modules and keystore for Web Services Manager authentication.

Login Modules

The following table lists all configured login modules for Web Services Manager. Use this list to create, configure or delete a login module.

Name	Class	Control Flag	Description
saml.loginmodule	oracle.security.jps.internal.jaas.module.saml.JpsSAMLLoginModule	REQUIRED	SAML Login Mo
krb5.loginmodule	com.sun.security.auth.module.Krb5LoginModule	REQUIRED	Kerberos Login
digest.authenticator.logi	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.login	oracle.security.jps.internal.jaas.module.authentication.JpsUserAu	REQUIRED	User Authentic
user.assertion.loginmodu	oracle.security.jps.internal.jaas.module.assertion.JpsUserAssertio	REQUIRED	User Assertion

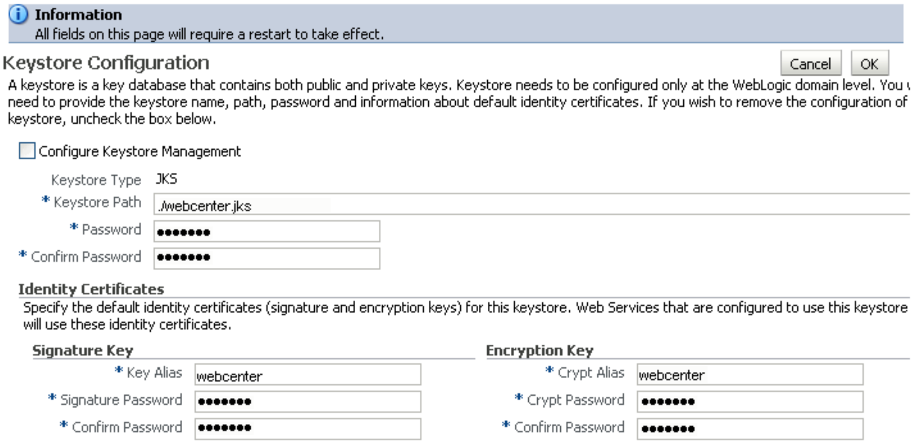
⊞ **Keystore**

⊞ **Advanced Properties**

5. Expand the Keystore section on the Security Provider Configuration page.
6. Click **Configure**.

   The Keystore Configuration page displays (see Figure 28–3).

Figure 28–3 Keystore Configuration Page



ⓘ **Information**

All fields on this page will require a restart to take effect.

Keystore Configuration

A keystore is a key database that contains both public and private keys. Keystore needs to be configured only at the WebLogic domain level. You need to provide the keystore name, path, password and information about default identity certificates. If you wish to remove the configuration of keystore, uncheck the box below.

□ Configure Keystore Management

Keystore Type	JKS
* Keystore Path	./webcenter.jks
* Password	●●●●●●●
* Confirm Password	●●●●●●●

Identity Certificates

Specify the default identity certificates (signature and encryption keys) for this keystore. Web Services that are configured to use this keystore will use these identity certificates.

Signature Key		**Encryption Key**	
* Key Alias	webcenter	* Crypt Alias	webcenter
* Signature Password	●●●●●●●	* Crypt Password	●●●●●●●
* Confirm Password	●●●●●●●	* Confirm Password	●●●●●●●

7. Check **Configure Keystore Management** and 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**: `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.

28.1.1.4 Unconfiguring a Keystore Provider Using Fusion Middleware Control

If a keystore provider is already configured, you must unconfigure the existing keystore provider before configuring a new provider. If a keystore provider is not already configured, ignore this section and continue with the steps to configure the keystore in Section 28.1.1.3, "Configuring the Keystore Using Fusion Middleware Control."

To unconfigure a keystore provider using Fusion Middleware Control:

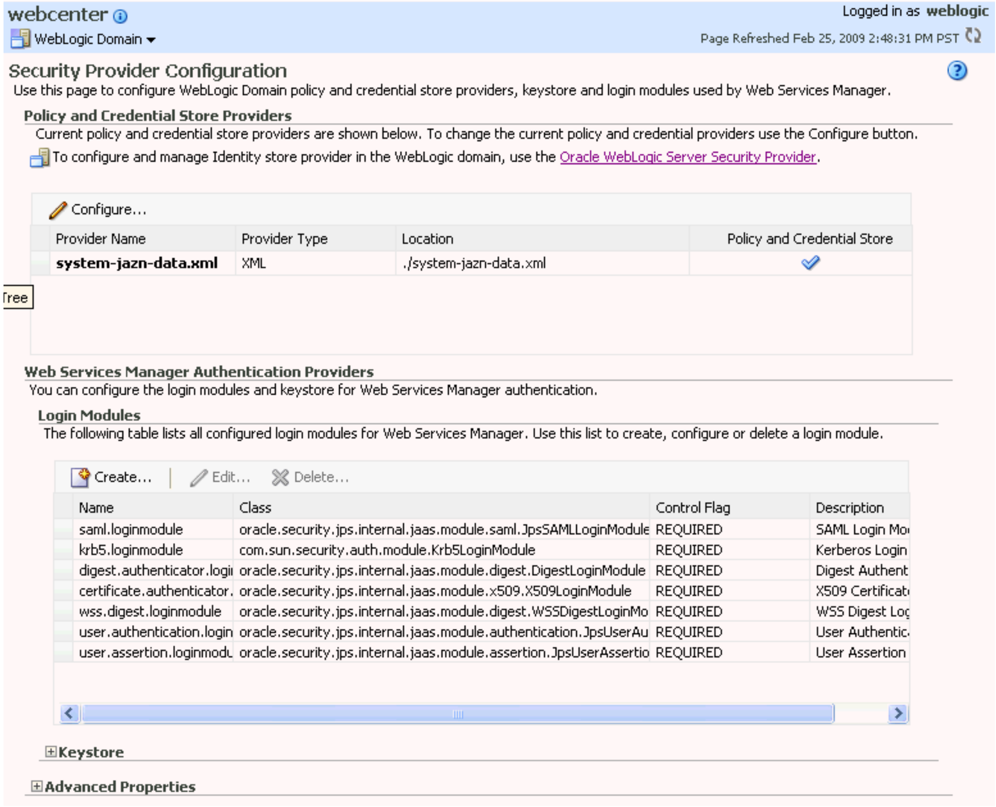
1. Open Fusion Middleware Control and log in to the target domain.

   For information on logging in to Fusion Middleware Control, see Section 6, "Starting Enterprise Manager Fusion Middleware Control."

2. From the WebLogic Domain menu, select **Security -> Security Provider Configuration**.

   The Security Provider Configuration page displays (see Figure 28–4).

Figure 28–4 Security Provider Configuration Page



Security Provider Configuration

Use this page to configure WebLogic Domain policy and credential store providers, keystore and login modules used by Web Services Manager.

Policy and Credential Store Providers

Current policy and credential store providers are shown below. To change the current policy and credential providers use the Configure button.

To configure and manage Identity store provider in the WebLogic domain, use the Oracle WebLogic Server Security Provider.

Provider Name	Provider Type	Location	Policy and Credential Store
system-jazn-data.xml	XML	./system-jazn-data.xml	✓

Web Services Manager Authentication Providers

You can configure the login modules and keystore for Web Services Manager authentication.

Login Modules

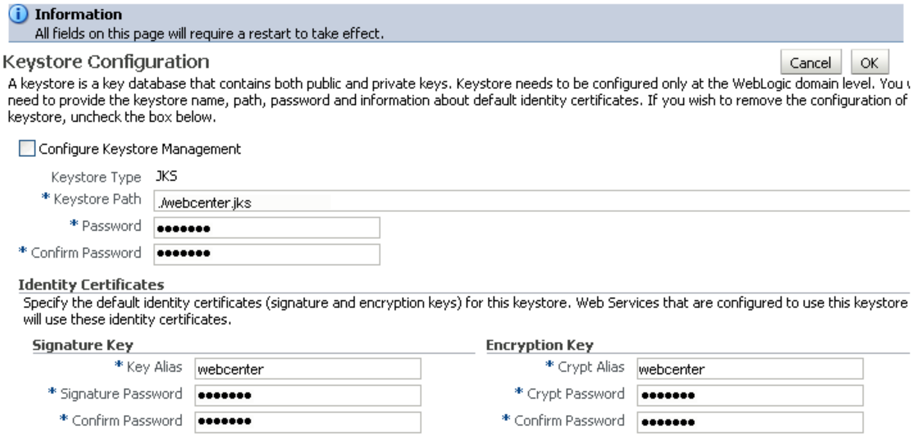
The following table lists all configured login modules for Web Services Manager. Use this list to create, configure or delete a login module.

Name	Class	Control Flag	Description
saml.loginmodule	oracle.security.jps.internal.jaas.module.saml.JpsSAMLLoginModule	REQUIRED	SAML Login Mo
krb5.loginmodule	com.sun.security.auth.module.Krb5LoginModule	REQUIRED	Kerberos Login
digest.authenticator.logi	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.login	oracle.security.jps.internal.jaas.module.authentication.JpsUserAu	REQUIRED	User Authentic
user.assertion.loginmodu	oracle.security.jps.internal.jaas.module.assertion.JpsUserAssertio	REQUIRED	User Assertion

3. Expand the Keystore section on the Security Provider Configuration page.
4. Click **Configure**.

   The Keystore Configuration page displays (see Figure 28–5).

Figure 28–5 Keystore Configuration Page



Information

All fields on this page will require a restart to take effect.

Keystore Configuration

A keystore is a key database that contains both public and private keys. Keystore needs to be configured only at the WebLogic domain level. You need to provide the keystore name, path, password and information about default identity certificates. If you wish to remove the configuration of keystore, uncheck the box below.

□ Configure Keystore Management

Keystore Type	JKS
* Keystore Path	./webcenter.jks
* Password	●●●●●●●
* Confirm Password	●●●●●●●

Identity Certificates

Specify the default identity certificates (signature and encryption keys) for this keystore. Web Services that are configured to use this keystore will use these identity certificates.

Signature Key		Encryption Key	
* Key Alias	webcenter	* Crypt Alias	webcenter
* Signature Password	●●●●●●●	* Crypt Password	●●●●●●●
* Confirm Password	●●●●●●●	* Confirm Password	●●●●●●●

5. Uncheck **Configure Keystore Management**.
6. Click **OK**.

28.1.2 Configuring the Discussions Server for a Simple Topology

To use the Oracle WebCenter Discussions with WebCenter Spaces or a custom WebCenter application, you must enable Web Services Security (WS-Security) trusted authentication. WS-Security establishes a trust relationship between your WebCenter application and Oracle WebCenter Discussions so that the application can pass the user identity information to the discussions server without knowing the user's credentials.

> **Note:** Discussions-specific Web Services messages sent by WebCenter applications to the Oracle WebCenter 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 27, "Securing WebCenter Applications and Components with SSL."

To set WS-Security-related properties on the discussions server connection that is configured for WebCenter Spaces or your custom WebCenter application, refer to Table 12–4, " Additional Discussion Connection Properties" in Section 12.3.1, "Registering Discussions Servers Using Fusion Middleware Control."

To configure WS-Security on the discussions server side, you must create a keystore certificate properties file, specify it for the ClassLoader, and modify the `webservices.soap.custom.crypto.fileName` system property. These configuration steps are described in the following sub-sections:

- Section 28.1.2.1, "Importing the WebCenter Domain Certificate"
- Section 28.1.2.2, "Creating the Keystore Certificate Properties File"
- Section 28.1.2.3, "Specifying the Properties File for ClassLoader"
- Section 28.1.2.4, "Updating the System Properties for WS-Security"

28.1.2.1 Importing the WebCenter Domain Certificate

Create a keystore by importing the certificate containing the public key of the WebCenter domain.

To import the WebCenter domain certificate:

1. Go to *`JDK_HOME`*`/jdk/bin` and open a command prompt.
2. Using keytool, import the certificate containing the public key of the WebCenter domain:

   ```
   keytool -importcert -alias df_orakey_public -file orakey.cer
    -keystore owc_discussions.jks -storepass keystore_password
   ```

   Where:

   - *`keystore_password`* is the keystore password, (for example, `welcome1`)

Example 28–5 Importing the WebCenter Domain Certificate

```
keytool -importcert -alias df_orakey_public -file orakey.cer
-keystore owc_discussions.jks -storepass welcome1
```

3. At the prompt "Trust this certificate?", choose `yes`.

28.1.2.2 Creating the Keystore Certificate Properties File

The server-side keystore certificate configuration must be stored in a properties file (keystore.properties) and specified as a system property on the discussions server. The properties file must then be loaded in the ClassLoader for the WS-Secure Handler to pick it up.

> **Note:** When you are updating the properties file, be sure to remove any spaces from the property names and values. The properties file should not contain any extraneous spaces.

To create the properties file:

1. Create a properties file with the following entries:

   ```
   org.apache.ws.security.crypto.provider= <Specify your crypto provider
   (typically org.apache.ws.security.components.crypto.Merlin)>
   org.apache.ws.security.crypto.merlin.keystore.type=jks
   org.apache.ws.security.crypto.merlin.keystore.password=<Specify the keystore
    password of your server certificate.
    Note that the password stored in this file is in clear text because of a
   limitation of the Ws-Security provider WSS4J used in Oracle Discussions
   Server.>
   org.apache.ws.security.crypto.merlin.keystore.alias=df_orakey_public
   org.apache.ws.security.crypto.merlin.file=<Absolute path of directory
    containing the certificate file created above>/owc_discussions.jks
   ```

2. Save the file as keystore.properties.

28.1.2.3 Specifying the Properties File for ClassLoader

There are two ways you can choose to specify your keystore.properties file based on your setup. Using the same file mounted across different servers is recommended when using a Clustered Discussions Server installation in Linux.

To specify the properties file for ClassLoader, do one of the following:

- Specify the properties file as the CLASSPATH in setDomainEnv.sh.

  For Linux:

  1. Place the keystore.properties file in a directory (for example, . /home/user/keystore/)
  2. Open DOMAIN_HOME/bin/setDomainEnv.sh.
  3. Towards the end of the file, add the following lines to specify this directory as the CLASSPATH.

     ```
     if [ "${CLASSPATH}" != "" ] ; then
       CLASSPATH="${CLASSPATH}${CLASSPATHSEP}/home/user/keystore/"
       export CLASSPATH
     else
       CLASSPATH="/home/user/keystore/"
       export CLASSPATH
     fi
     ```

     Note that the CLASSPATH directory name must end with "/".

  For Windows:

1. Place the keystore.properties file in a directory (for example, c:\keystore\).
2. Open DOMAIN_HOME\bin\setDomainEnv.cmd.
3. Towards the end of the file, add the following lines to specify this directory in CLASSPATH.

   ```
   if NOT "%CLASSPATH%"=="" (
     set CLASSPATH=%CLASSPATH%;c:\keystore\
   ) else (
     set CLASSPATH=c:\keystore\
   )
   ```

   Note that the CLASSPATH directory name must end with "\".

- Or, add the keystore.properties file to a .JAR file and place the .JAR file in your DOMAIN_HOME/lib directory. Be sure to also set the system property webservices.soap.custom.crypto.fileName to keystore.properties as described in Section 28.1.2.4, "Updating the System Properties for WS-Security."

28.1.2.4 Updating the System Properties for WS-Security

To update your system properties:

1. Log in to the Oracle WebCenter Discussions Administration Console at the following URL:

   http://host:port/owc_discussions/admin

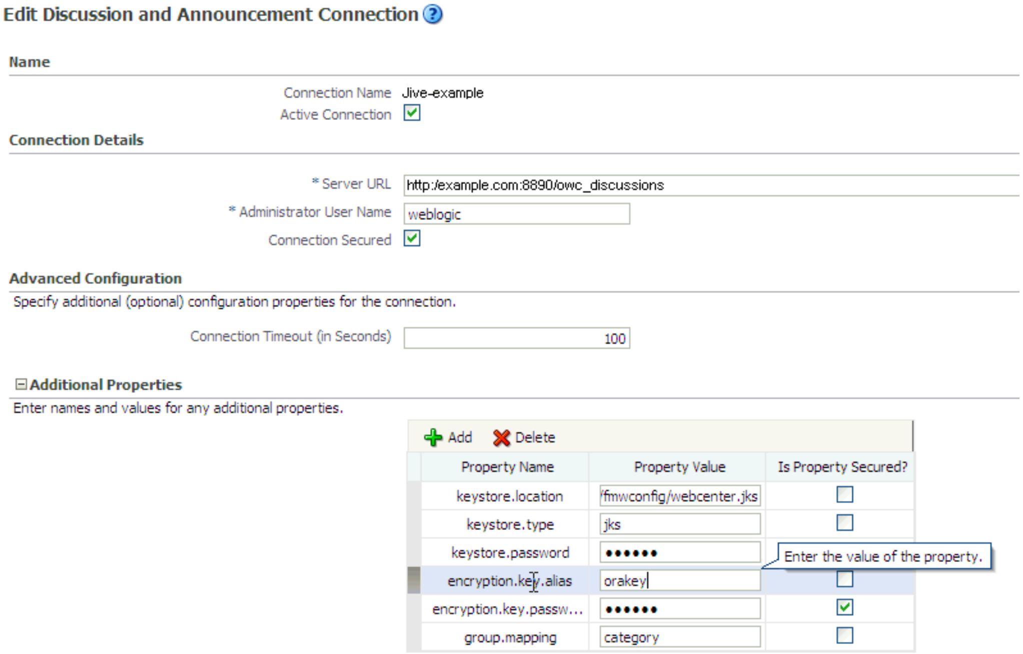
   Where host and port are the address and the port number of the server where you deployed Oracle WebCenter Discussions (for example, http://localhost:7001/owc_discussions).
2. Click **System Properties** under **Forum System** to display the Jive Properties page.
3. Modify the system property webservices.soap.custom.crypto.fileName and specify the properties file that you created (that is, keystore.properties).

   Ensure that you specify the name of the file, and not the directory or .JAR name.
4. Click **OK**.
5. Restart the WLS_Services Managed Server.

28.1.2.5 Configuring the Discussions Server Connection Settings

After setting the system properties, you must supply the WS-Security client certificate information within the discussions server connection that is configured for WebCenter Spaces or your custom WebCenter application, as described in Section 12.3, "Registering Discussions Servers." Figure 28–6 shows example settings for the Edit Discussions and Announcement Connection page.

Figure 28–6 Edit Discussions and Announcement Connection Page



Edit Discussion and Announcement Connection

Name

Connection Name	Jive-example
Active Connection	☑

Connection Details

* Server URL	http:/example.com:8890/owc_discussions
* Administrator User Name	weblogic
Connection Secured	☑

Advanced Configuration

Specify additional (optional) configuration properties for the connection.

Connection Timeout (in Seconds)	100

Additional Properties

Enter names and values for any additional properties.

Property Name	Property Value	Is Property Secured?
keystore.location	'fmwconfig/webcenter.jks	□
keystore.type	jks	□
keystore.password	••••••	
encryption.key.alias	orakey	□
encryption.key.passw...	••••••	☑
group.mapping	category	□

Enter the value of the property.

28.1.3 Configuring the BPEL Server for a Simple Topology

The BPEL server's Worklist connection must be configured to use message protected SAML service policy. The BPEL server's `oracle-webservices.xml` file must also be edited so that the server-side SAML policy matches that of the client's policy.

To configure the BPEL server:

1. To configure the Worklist connection on the BPEL server to use the SAML policy with message protection, follow the steps in Section 20.3.2, "Registering Worklist Connections" selecting `SAML Token With Message Client Policy` in Fusion Middleware Control, or entering `oracle/wss10_saml_token_with_message_protection_client_policy` as the policy value if using WLST.

2. Use `grep` to find the strings `TaskQueryServicePortSAML` and `provider-name` in all the BPEL server's `oracle-webservices.xml` files. For example:

```
cd <domain home>
find . | grep webservices.xml | xargs grep TaskQueryServicePortSAML | grep
provider-name
./servers/BPEL Server
1/tmp/_WL_user/soa-infra/ugh7wb/war/WEB-INF/oracle-webservices.xml:
<provider-name>TaskQueryServicePortSAML</provider-name>
```

3. Back up the file. For example:

```
cp
./servers/BPEL Server
1/tmp/_WL_user/soa-infra/ugh7wb/war/WEB-INF/oracle-webservices.xml
./servers/BPEL Server
1/tmp/_WL_user/soa-infra/ugh7wb/war/WEB-INF/oracle-webservices.xml.original
```

4. Edit the file, replacing:

```
<policy-reference uri="oracle/wss10_saml_token_service_policy"
category="security" enabled="true"/>
```

with:

```
<policy-reference
uri="oracle/wss10_saml_token_with_message_protection_service_policy"
category="security" enabled="true"/>
```

5. Save the file and restart the Managed Servers. The message protected SAML access is now configured. Examine the managed server diagnostic logs for exception stack information should the worklist service still not work to obtain information about configuration issues.

28.1.4 Command Summary for a Simple Topology

Use the following command summary to quickly configure the keystore and DF properties 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
```

When prompted to trust the certificate, say `yes`.

Copy the `default-keystore.jks` file to your `domain_home/config/fmwconfig` directory.

Configure the Keystore

Using WLST, connect to the WebCenter Spaces domain as an admin user and run the following commands:

```
createCred(map="oracle.wsm.security", key="keystore-csf-key", user="owsm",
password="welcome1", desc="Keystore key")
createCred(map="oracle.wsm.security", key="enc-csf-key", user="orakey",
password="welcome1", desc="Encryption key")
createCred(map="oracle.wsm.security", key="sign-csf-key", user="orakey",
password="welcome1", desc="Signing key")
```

Configure the DF Keystore Properties File

Using WLST, connect to the WebCenter Spaces domain as an admin user and run the following commands:

```
org.apache.ws.security.crypto.merlin.keystore.type=jks
org.apache.ws.security.crypto.merlin.keystore.password=welcome1
org.apache.ws.security.crypto.merlin.keystore.alias=df_orakey_public
org.apache.ws.security.crypto.merlin.file=<dir_containing_keystore>/owc_discussion
```

```
s.jks
```

Note: Be sure to trim any spaces from the line endings. If you are working in a Windows environment, also be sure to use "\\" as the file path separator.

Additional DF Connection properties are shown in Table 28–2.

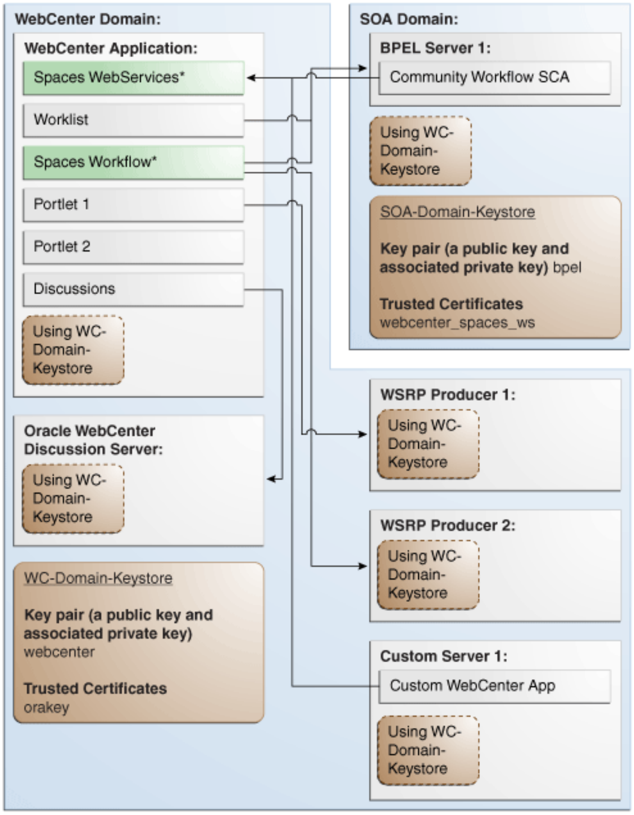
Table 28–2 Additional DF Connection Properties

Property Name	Property Value	Secured
`keystore.location`	`<doamin_home>/config/fmwconfig/default-keystore.jks`	No
`keystore.type`	`jks`	No
`keystore.password`	`welcome1`	Yes
`encryption.key.alias`	`orakey`	No
`encryption.key.password`	`welcome1`	Yes
`group.mapping`	`category`	No

28.2 Configuring WS-Security for a Typical Topology

This section describes how to configure WS-Security for a topology where the WebCenter application and the WSRP producers share the same domain, but the BPEL server is in an external domain - the SOA domain (see Figure 28–7).

Figure 28–7 Typical WS-Security Configuration



*applicable to WebCenter Spaces application only

The steps to configure WS-Security for a typical two domain WebCenter topology are described in the following sections:

- Section 28.2.1, "Setting Up the WebCenter Domain Keystore"
- Section 28.2.2, "Configuring the Discussions Server for a Typical Topology"
- Section 28.2.4, "Configuring the BPEL Server for a Typical Topology"
- Section 28.2.5, "Command Summary for a Typical Topology"

28.2.1 Setting Up the WebCenter Domain Keystore

The security credentials of a WebCenter 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 28.2.1.1, "Creating the WebCenter Domain Keystore"
- Section 28.2.1.2, "Configuring the Keystore Using WLST"
- Section 28.2.1.4, "Unconfiguring a Keystore Provider"
- Section 28.2.1.3, "Configuring the Keystore Using Fusion Middleware Control"

- Section 28.2.5, "Command Summary for a Typical Topology"

28.2.1.1 Creating the WebCenter 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 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 28–6 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 28–7 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 28.2.1.2, "Configuring the Keystore Using WLST," or Fusion Middleware Control, as described in Section 28.2.1.3, "Configuring the Keystore Using Fusion Middleware Control."

   Table 28–3 shows the keystore contents you should wind up with after creating and configuring the keystore.

Table 28–3 WebCenter Domain Keystore Contents for a Typical Topology

Key Alias	Description
`webcenter`	Key pair used to sign and encrypt outbound messages from WebCenter 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 domain, to the Worklist service to the SOA server on the SOA domain.

28.2.1.2 Configuring the Keystore Using WLST

After creating the WebCenter 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:

```
createCred(map="oracle.wsm.security", key="keystore-csf-key", user="owsm",
password=keystore_password, desc="Keystore key")
createCred(map="oracle.wsm.security", key="enc-csf-key", user="webcenter",
password=private_key_password, desc="Encryption key")
createCred(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 28.2.1.1, "Creating the WebCenter Domain Keystore," (for example, `welcome1`)
   - *`private_key_password`* is the private key password specified in step 2 of Section 28.2.1.1, "Creating the WebCenter Domain Keystore," (for example, `welcome1`)

Example 28–8 Updating the Credential Store

```
createCred(map="oracle.wsm.security", key="keystore-csf-key", user="owsm",
password="welcome1", desc="Keystore key")
createCred(map="oracle.wsm.security", key="enc-csf-key", user="webcenter",
password="welcome1", desc="Encryption key")
createCred(map="oracle.wsm.security", key="sign-csf-key", user="webcenter",
password="welcome1", desc="Signing key")
```

5. Restart all servers.

28.2.1.3 Configuring the Keystore Using Fusion Middleware Control

If a keystore provider is already configured, you must first unconfigure the existing keystore provider as described in Section 28.2.1.4, "Unconfiguring a Keystore Provider." Otherwise, continue with the steps below.

To configure the keystore provider:

1. Open Fusion Middleware Control and log in to the WebCenter domain.

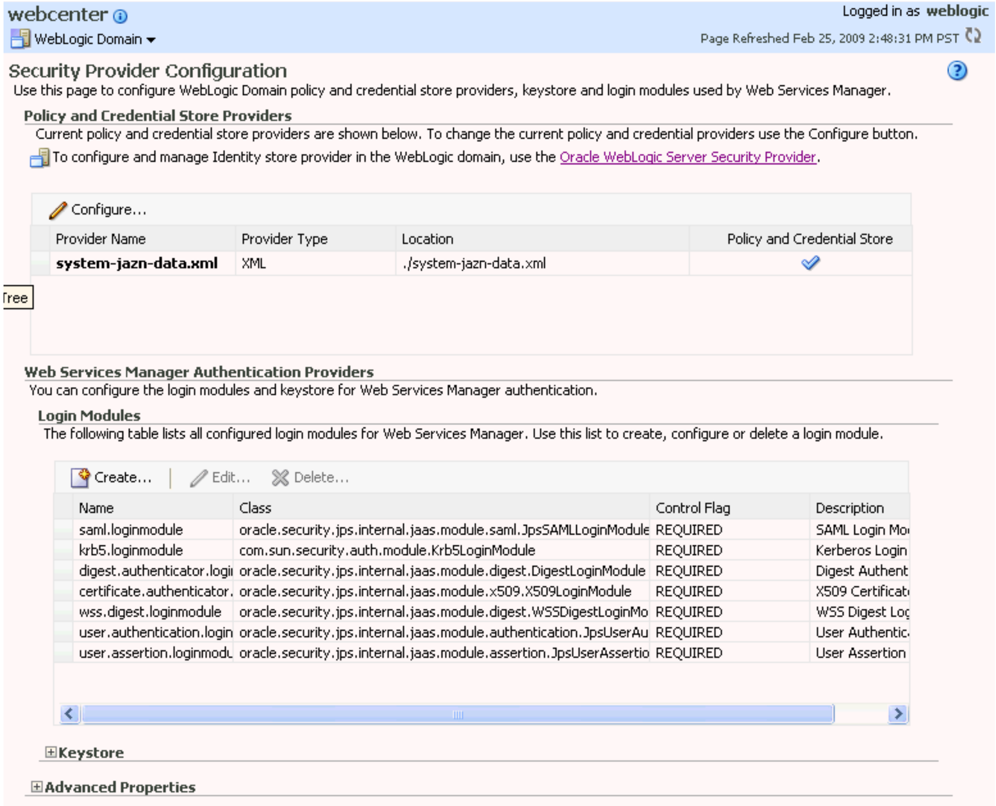
   For information on logging in to Fusion Middleware Control, see Section 6, "Starting Enterprise Manager Fusion Middleware Control."

2. In the Navigation pane, expand the WebLogic Domain node and click the WebCenter domain (`webcenter` by default).

3. From the WebLogic Domain menu, select **Security -> Security Provider Configuration**.

   The Security Provider Configuration page displays (see Figure 28–8).

Figure 28–8 Security Provider Configuration Page



Security Provider Configuration

Use this page to configure WebLogic Domain policy and credential store providers, keystore and login modules used by Web Services Manager.

Policy and Credential Store Providers

Current policy and credential store providers are shown below. To change the current policy and credential providers use the Configure button.

To configure and manage Identity store provider in the WebLogic domain, use the Oracle WebLogic Server Security Provider.

Provider Name	Provider Type	Location	Policy and Credential Store
system-jazn-data.xml	XML	./system-jazn-data.xml	✓

Web Services Manager Authentication Providers

You can configure the login modules and keystore for Web Services Manager authentication.

Login Modules

The following table lists all configured login modules for Web Services Manager. Use this list to create, configure or delete a login module.

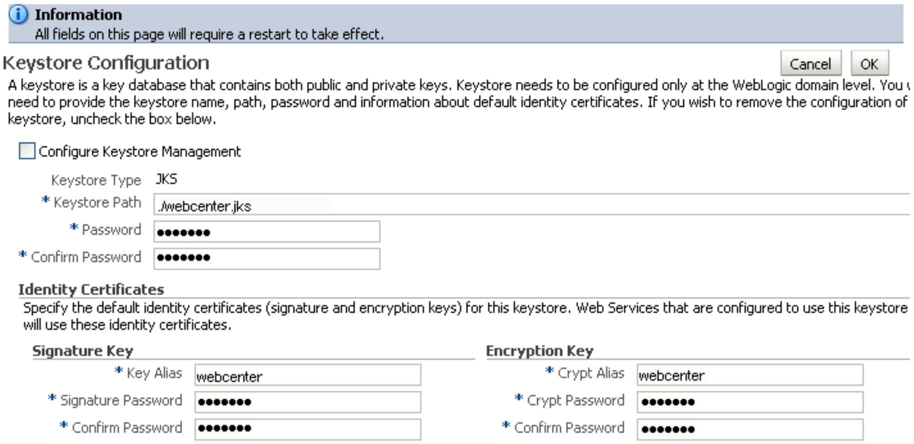
Name	Class	Control Flag	Description
saml.loginmodule	oracle.security.jps.internal.jaas.module.saml.JpsSAMLLoginModule	REQUIRED	SAML Login Mo
krb5.loginmodule	com.sun.security.auth.module.Krb5LoginModule	REQUIRED	Kerberos Login
digest.authenticator.logi	oracle.security.jps.internal.jaas.module.digest.DigestLoginModule	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.login	oracle.security.jps.internal.jaas.module.authentication.JpsUserAu	REQUIRED	User Authentic.
user.assertion.loginmodu	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 28–9).

Figure 28–9 Keystore Configuration Page



Information
All fields on this page will require a restart to take effect.

Keystore Configuration

Cancel | OK

A keystore is a key database that contains both public and private keys. Keystore needs to be configured only at the WebLogic domain level. You ι need to provide the keystore name, path, password and information about default identity certificates. If you wish to remove the configuration of keystore, uncheck the box below.

□ Configure Keystore Management

Keystore Type	JKS
* Keystore Path	./webcenter.jks
* Password	●●●●●●●
* Confirm Password	●●●●●●●

Identity Certificates

Specify the default identity certificates (signature and encryption keys) for this keystore. Web Services that are configured to use this keystore will use these identity certificates.

Signature Key		Encryption Key	
* Key Alias	webcenter	* Crypt Alias	webcenter
* Signature Password	●●●●●●●	* Crypt Password	●●●●●●●
* Confirm Password	●●●●●●●	* Confirm Password	●●●●●●●

6. Check **Configure Keystore Management** and 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.

28.2.1.4 Unconfiguring a Keystore Provider

If a keystore provider is already configured, you must unconfigure the existing keystore provider before configuring a new provider. If a keystore provider is not already configured, continue with the steps to configure the keystore in Section 28.2.1.3, "Configuring the Keystore Using Fusion Middleware Control."

To unconfigure a keystore provider using Fusion Middleware Control:

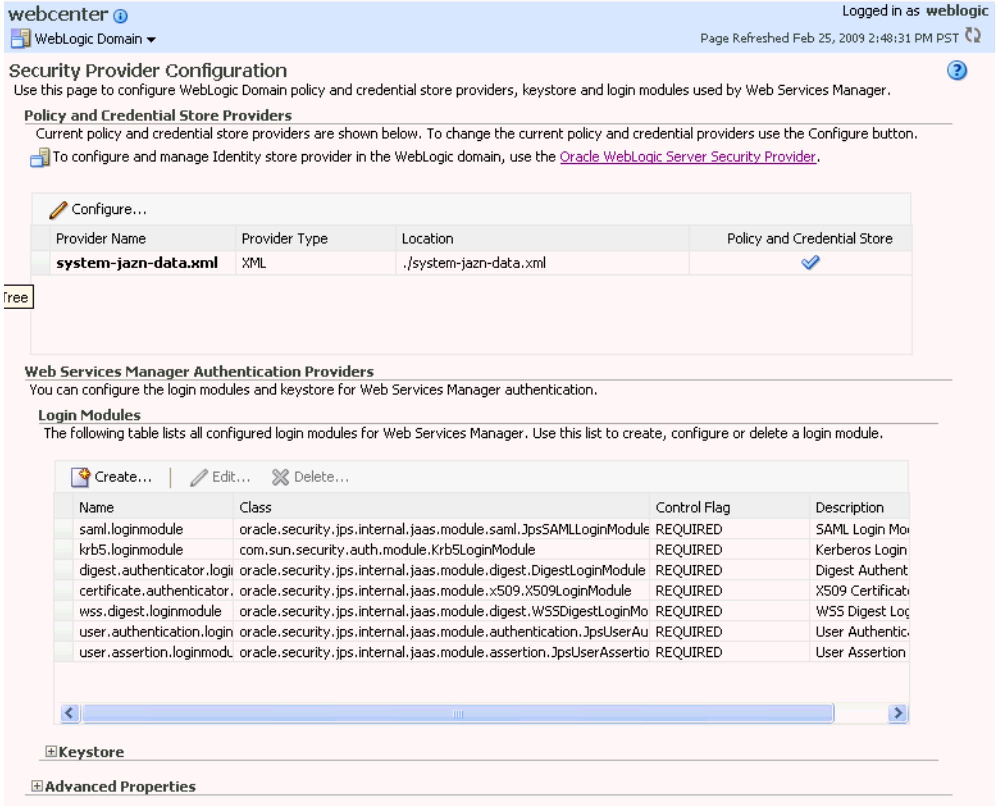
1. Open Fusion Middleware Control and log in to the target domain.

   For information on logging in to Fusion Middleware Control, see Section 6, "Starting Enterprise Manager Fusion Middleware Control."

2. From the WebLogic Domain menu, select **Security -> Security Provider Configuration**.

   The Security Provider Configuration page displays (see Figure 28–10).

Figure 28–10 Security Provider Configuration Page



webcenter

WebLogic Domain

Logged in as **weblogic**

Page Refreshed Feb 25, 2009 2:48:31 PM PST

Security Provider Configuration

Use this page to configure WebLogic Domain policy and credential store providers, keystore and login modules used by Web Services Manager.

Policy and Credential Store Providers

Current policy and credential store providers are shown below. To change the current policy and credential providers use the Configure button.

To configure and manage Identity store provider in the WebLogic domain, use the Oracle WebLogic Server Security Provider.

Configure...

Provider Name	Provider Type	Location	Policy and Credential Store
system-jazn-data.xml	XML	./system-jazn-data.xml	✓

Web Services Manager Authentication Providers

You can configure the login modules and keystore for Web Services Manager authentication.

Login Modules

The following table lists all configured login modules for Web Services Manager. Use this list to create, configure or delete a login module.

Name	Class	Control Flag	Description
saml.loginmodule	oracle.security.jps.internal.jaas.module.saml.JpsSAMLLoginModule	REQUIRED	SAML Login Mo
krb5.loginmodule	com.sun.security.auth.module.Krb5LoginModule	REQUIRED	Kerberos Login
digest.authenticator.logi	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 Log
user.authentication.login	oracle.security.jps.internal.jaas.module.authentication.JpsUserAu	REQUIRED	User Authentic.
user.assertion.loginmodu	oracle.security.jps.internal.jaas.module.assertion.JpsUserAssertio	REQUIRED	User Assertion

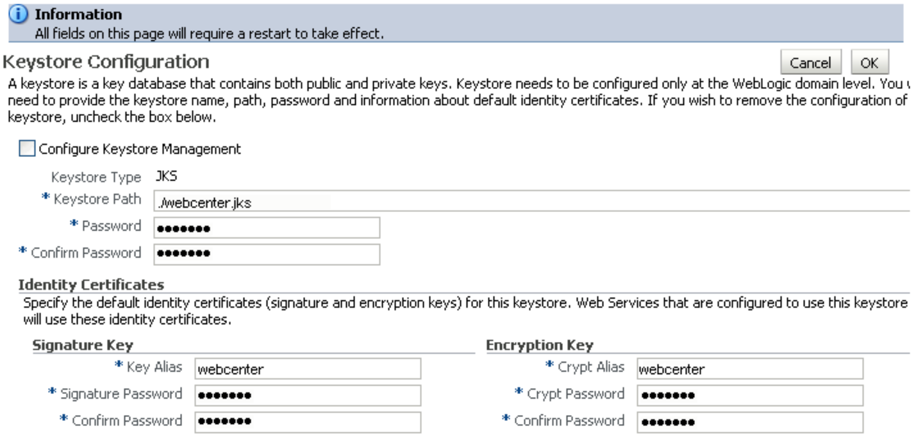
⊞ **Keystore**

⊞ **Advanced Properties**

3. Expand the Keystore section on the Security Provider Configuration page.
4. Click **Configure**.

   The Keystore Configuration page displays (see Figure 28–11).

Figure 28–11 Keystore Configuration Page



Information

All fields on this page will require a restart to take effect.

Keystore Configuration

A keystore is a key database that contains both public and private keys. Keystore needs to be configured only at the WebLogic domain level. You need to provide the keystore name, path, password and information about default identity certificates. If you wish to remove the configuration of keystore, uncheck the box below.

□ Configure Keystore Management

Keystore Type	JKS
* Keystore Path	./webcenter.jks
* Password	•••••••
* Confirm Password	•••••••

Identity Certificates

Specify the default identity certificates (signature and encryption keys) for this keystore. Web Services that are configured to use this keystore will use these identity certificates.

Signature Key

* Key Alias	webcenter
* Signature Password	•••••••
* Confirm Password	•••••••

Encryption Key

* Crypt Alias	webcenter
* Crypt Password	•••••••
* Confirm Password	•••••••

5. Uncheck **Configure Keystore Management**.
6. Click **OK**.

28.2.2 Configuring the Discussions Server for a Typical Topology

To use Oracle WebCenter Discussions with WebCenter Spaces or custom WebCenter applications, you must enable Web Services Security (WS-Security) trusted authentication. WS-Security establishes a trust relationship between your WebCenter application and Oracle WebCenter Discussions so that the application can pass the user identity information to the discussions server without knowing the user's credentials.

> **Note:** Discussions-specific Web Services messages sent by WebCenter applications to the Oracle WebCenter 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 27, "Securing WebCenter Applications and Components with SSL."

This section describes how to add the WS-Security-related properties within the discussions server connection that is configured for WebCenter Spaces or your custom WebCenter application. For information on how to add new properties, see Table 12–4, " Additional Discussion Connection Properties" in Section 12.3.1, "Registering Discussions Servers Using Fusion Middleware Control."

To configure WS-Security on the discussions server side, you must create a keystore certificate properties file, specify it for the ClassLoader, and modify the `webservices.soap.custom.crypto.fileName` system property.

These configuration steps are described in the following sub-sections:

- Section 28.2.2.1, "Importing the WebCenter Domain Certificate"
- Section 28.2.2.2, "Creating the Keystore Certificate Properties File"
- Section 28.2.2.3, "Specifying the Properties File for ClassLoader"
- Section 28.2.2.4, "Updating the System Properties for WS-Security"
- Section 28.2.2.5, "Configuring the Discussions Server Connection Settings"

28.2.2.1 Importing the WebCenter Domain Certificate

Create a keystore by importing the certificate containing public key of the WebCenter domain.

To import the WebCenter domain certificate:

1. Go to *`JDK_HOME`*`/jdk/bin` and open a command prompt.
2. Using keytool, import the certificate containing the public key of the WebCenter domain:

   ```
   keytool -importcert -alias df_webcenter_public -file webcenter_public.cer
   -keystore owc_discussions.jks -storepass keystore_password
   ```

   Where:

   - *`keystore_password`* is the keystore password, (for example, `welcome1`)

Example 28–9 Importing the WebCenter Domain Certificate

```
keytool -importcert -alias df_webcenter_public -file webcenter_public.cer
-keystore owc_discussions.jks -storepass welcome1
```

28.2.2.2 Creating the Keystore Certificate Properties File

The server-side keystore certificate configuration must be stored in a properties file (`keystore.properties`) and specified as a system property on the discussions server. The properties file must then be loaded in the ClassLoader for the WS-Secure Handler to pick it up.

> **Note:** When you are updating the properties file, be sure to remove any spaces from the property names and values. The properties file should not contain any extraneous spaces.

To create the properties file:

1. Create a properties file with the following entries:

   ```
   org.apache.ws.security.crypto.provider=<Specify your crypto provider
   (typically org.apache.ws.security.components.crypto.Merlin)>
   org.apache.ws.security.crypto.merlin.keystore.type=jks
   org.apache.ws.security.crypto.merlin.keystore.password=<Specify the keystore
    password of your server certificate.
    Note that the password stored in this file is in clear text because of a
   limitation of the Ws-Security provider WSS4J used in Oracle Discussions
   Server.>
   org.apache.ws.security.crypto.merlin.keystore.alias=df_orakey_public
   org.apache.ws.security.crypto.merlin.file=<Absolute path of directory
    containing the keystore (owc_discussions.jks) created above.>
   ```

2. Save the file as `keystore.properties`.

28.2.2.3 Specifying the Properties File for ClassLoader

There are two ways you can choose to specify your `keystore.properties` file based on your setup. Using the same file mounted across different servers is recommended when using a Clustered Discussions Server installation in Linux.

To specify the properties file for ClassLoader, do one of the following:

- Specify the properties file as the `CLASSPATH` in `setDomainEnv.sh`.

  For Linux:

  1. Place the `keystore.properties` file in a directory (for example, `. /home/user/keystore/`)
  2. Open `DOMAIN_HOME/bin/setDomainEnv.sh`.
  3. Towards the end of the file, add the following lines to specify this directory as the `CLASSPATH`.

     ```
     if [ "${CLASSPATH}" != "" ] ; then
       CLASSPATH="${CLASSPATH}${CLASSPATHSEP}/home/user/keystore/"
       export CLASSPATH
     else
       CLASSPATH="/home/user/keystore/"
       export CLASSPATH
     fi
     ```

     Note that the `CLASSPATH` directory name must end with "/".

  For Windows:

1. Place the `keystore.properties` file in a directory (for example, `c:\keystore\`).
2. Open `DOMAIN_HOME\bin\setDomainEnv.cmd`.
3. Towards the end of the file, add the following lines to specify this directory in `CLASSPATH`.

   ```
   if NOT "%CLASSPATH%"=="" (
     set CLASSPATH=%CLASSPATH%;c:\keystore\
   ) else (
     set CLASSPATH=c:\keystore\
   )
   ```

   Note that the `CLASSPATH` directory name must end with "\".

- Or, add the `keystore.properties` file to a `.JAR` file and place the `.JAR` file in your `DOMAIN_HOME/lib` directory. Be sure to also set the system property `webservices.soap.custom.crypto.fileName` to `keystore.properties` as described in Section 28.2.2.4, "Updating the System Properties for WS-Security."

28.2.2.4 Updating the System Properties for WS-Security

To update your system properties:

1. Log in to the Oracle WebCenter Discussions Admin Console at the following URL:

   `http://host:port/owc_discussions/admin`

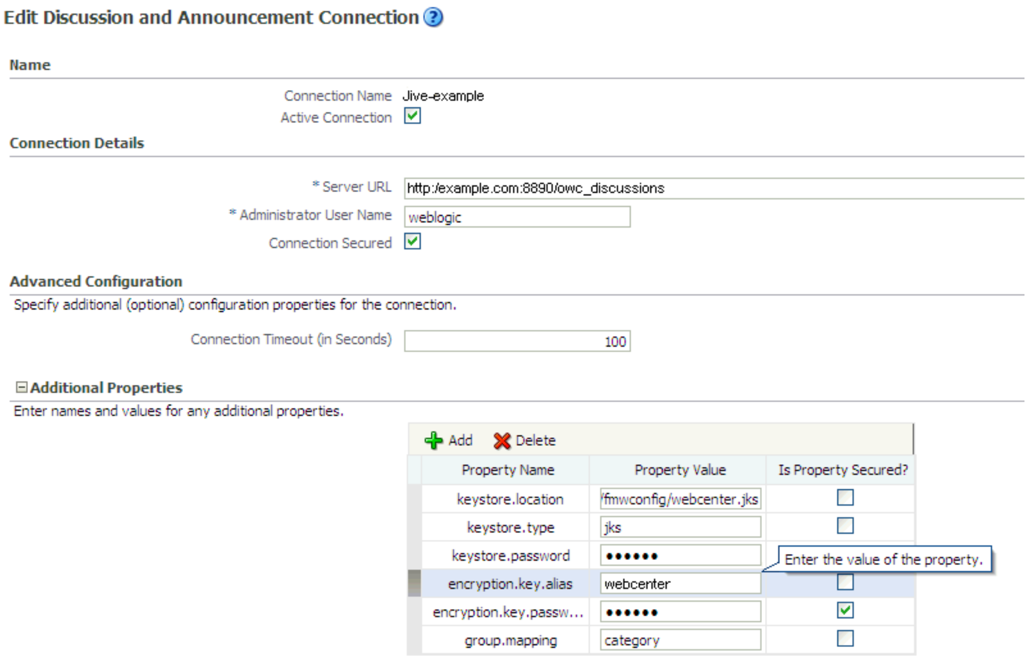
   Where `host` and `port` are the address and the port number of the server where you deployed Oracle WebCenter Discussions (for example, `http://localhost:7001/owc_discussions`).
2. Click **System Properties** under **Forum System** to display the Jive Properties page.
3. Modify the system property `webservices.soap.custom.crypto.fileName` and specify the properties file that you created (that is, `keystore.properties`).

   Be sure to specify the name of the file, and not the directory or `.JAR` name.
4. Click **OK**.
5. Restart the `WLS_Services` Managed Server.

28.2.2.5 Configuring the Discussions Server Connection Settings

After setting the system properties, you must supply the WS-Security client certificate information within the discussion server connection settings, as described in Section 12.3, "Registering Discussions Servers." Figure 28–12 shows example settings for the Edit Discussions and Announcement Connection page.

Figure 28–12 Edit Discussions and Announcement Connection Page



Edit Discussion and Announcement Connection

Name

Connection Name Jive-example

Active Connection ☑

Connection Details

* Server URL http:/example.com:8890/owc_discussions

* Administrator User Name weblogic

Connection Secured ☑

Advanced Configuration

Specify additional (optional) configuration properties for the connection.

Connection Timeout (in Seconds) 100

⊟ Additional Properties

Enter names and values for any additional properties.

Property Name	Property Value	Is Property Secured?
keystore.location	/fmwconfig/webcenter.jks	□
keystore.type	jks	□
keystore.password	••••••	Enter the value of the property.
encryption.key.alias	webcenter	□
encryption.key.passw...	••••••	☑
group.mapping	category	□

28.2.3 Setting Up the SOA Domain

This section describes how to set up the SOA domain keystore and contains the following subsections:

- Section 28.2.3.1, "Creating the SOA Domain Keystore"
- Section 28.2.3.2, "Configuring the Keystore Using WLST"
- Section 28.2.3.4, "Unconfiguring a Keystore Provider"
- Section 28.2.3.3, "Configuring the Keystore Using Fusion Middleware Control"

28.2.3.1 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 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 28–10 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 28–11 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 domain using the `orakey` alias:

   ```
   keytool -exportcert -v -alias orakey -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 28–12 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 28–13 Importing the Certificate

```
keytool -importcert -alias orakey -file orakay.cer -keystore webcenter.jks
-storepass welcome1
```

28.2.3.2 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.

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:

   ```
   createCred(map="oracle.wsm.security", key="keystore-csf-key", user="owsm",
   password="welcome1", desc="Keystore key")
   createCred(map="oracle.wsm.security", key="enc-csf-key", user="bpel",
   password="welcome1", desc="Encryption key")
   createCred(map="oracle.wsm.security", key="sign-csf-key", user="bpel",
   password="welcome1", desc="Signing key")
   ```

5. Restart all servers.

28.2.3.3 Configuring the Keystore Using Fusion Middleware Control

If a keystore provider is already configured, you must first unconfigure the existing keystore provider as described in Section 28.2.3.4, "Unconfiguring a Keystore Provider." Otherwise, continue with the steps below.

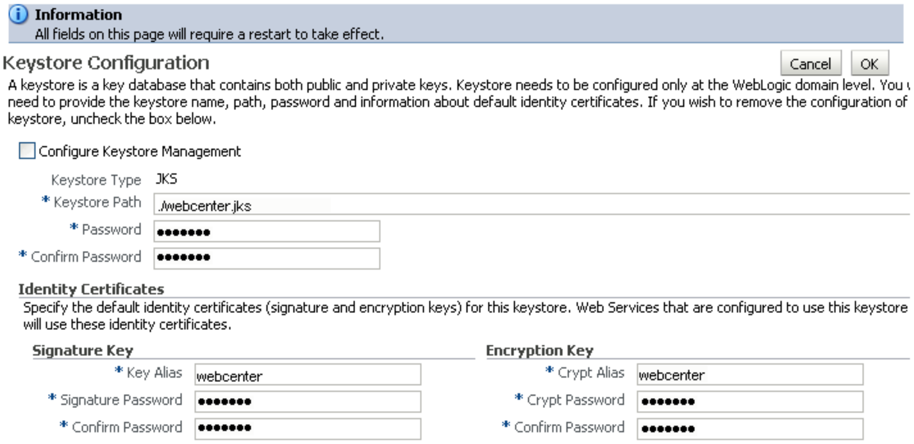
To configure the keystore provider:

1. Open Fusion Middleware Control and log in to the WebCenter domain.

   For information on logging in to 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 WebCenter domain (`webcenter` 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 28–13).

Figure 28–13 Keystore Configuration Page



Information
All fields on this page will require a restart to take effect.

Keystore Configuration

A keystore is a key database that contains both public and private keys. Keystore needs to be configured only at the WebLogic domain level. You ı need to provide the keystore name, path, password and information about default identity certificates. If you wish to remove the configuration of keystore, uncheck the box below.

□ Configure Keystore Management

Keystore Type JKS
* Keystore Path ./webcenter.jks
* Password •••••••
* Confirm Password •••••••

Identity Certificates

Specify the default identity certificates (signature and encryption keys) for this keystore. Web Services that are configured to use this keystore will use these identity certificates.

Signature Key
* Key Alias webcenter
* Signature Password •••••••
* Confirm Password •••••••

Encryption Key
* Crypt Alias webcenter
* Crypt Password •••••••
* Confirm Password •••••••

6. Check **Configure Keystore Management** and 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**: `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.

7. Click **OK** to save your settings.
8. Restart the Administration server for the domain.

28.2.3.4 Unconfiguring a Keystore Provider

If a keystore provider is already configured, you must unconfigure the existing keystore provider before configuring a new provider. If a keystore provider is not already configured, continue with the steps to configure the keystore in Section 28.2.3.3, "Configuring the Keystore Using Fusion Middleware Control."

To unconfigure a keystore provider using Fusion Middleware Control:

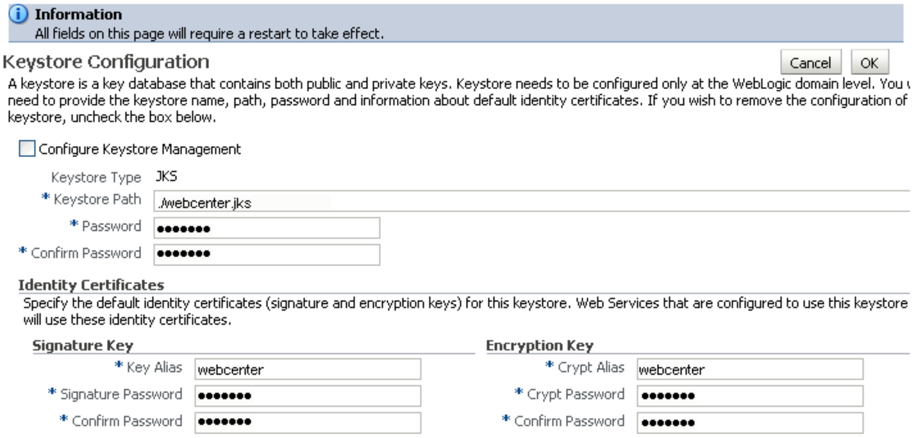
1. Open Fusion Middleware Control and log in to the target domain.

   For information on logging in to Fusion Middleware Control, see Section 6, "Starting Enterprise Manager Fusion Middleware Control."

2. From the WebLogic Domain menu, select **Security -> Security Provider Configuration**.
3. Expand the Keystore section on the Security Provider Configuration page.
4. Click **Configure**.

   The Keystore Configuration page displays (see Figure 28–14).

Figure 28–14 Keystore Configuration Page



Information
All fields on this page will require a restart to take effect.

Keystore Configuration

A keystore is a key database that contains both public and private keys. Keystore needs to be configured only at the WebLogic domain level. You
need to provide the keystore name, path, password and information about default identity certificates. If you wish to remove the configuration of
keystore, uncheck the box below.

☐ Configure Keystore Management

Keystore Type JKS
* Keystore Path ./webcenter.jks
* Password •••••••
* Confirm Password •••••••

Identity Certificates

Specify the default identity certificates (signature and encryption keys) for this keystore. Web Services that are configured to use this keystore will use these identity certificates.

Signature Key		Encryption Key	
* Key Alias	webcenter	* Crypt Alias	webcenter
* Signature Password	•••••••	* Crypt Password	•••••••
* Confirm Password	•••••••	* Confirm Password	•••••••

5. Uncheck **Configure Keystore Management**.
6. Click **OK**.

28.2.4 Configuring the BPEL Server for a Typical Topology

The BPEL server's Worklist connection must be configured to use message protected SAML service policy. The BPEL server's `oracle-webservices.xml` file must also be edited so that the server-side SAML policy matches that of the client's policy.

To configure the BPEL server:

1. To configure the Worklist connection on the BPEL server to use the SAML policy with message protection, follow the steps in Section 20.3.2, "Registering Worklist Connections," selecting `SAML Token With Message Client Policy` in Fusion Middleware Control, or entering `oracle/wss10_saml_token_with_message_protection_client_policy` as the policy value if using WLST.

2. Use `grep` to find the strings `TaskQueryServicePortSAML` and `provider-name` in all the BPEL server's `oracle-webservices.xml` files. For example:

```
cd <domain home>
find . | grep webservices.xml | xargs grep TaskQueryServicePortSAML | grep
provider-name
./servers/BPEL Server
1/tmp/_WL_user/soa-infra/ugh7wb/war/WEB-INF/oracle-webservices.xml:
<provider-name>TaskQueryServicePortSAML</provider-name>
```

3. Back up the file. For example:

```
cp
./servers/BPEL Server
1/tmp/_WL_user/soa-infra/ugh7wb/war/WEB-INF/oracle-webservices.xml
./servers/BPEL Server
1/tmp/_WL_user/soa-infra/ugh7wb/war/WEB-INF/oracle-webservices.xml.original
```

4. Edit the file, replacing:

```
<policy-reference uri="oracle/wss10_saml_token_service_policy"
category="security" enabled="true"/>
```

with:

```
<policy-reference
uri="oracle/wss10_saml_token_with_message_protection_service_policy"
category="security" enabled="true"/>
```

5. Save the file and restart the Managed Servers. The message protected SAML access is now configured. Examine the managed server diagnostic logs for exception stack information should the worklist service still not work to obtain information about configuration issues.

28.2.5 Command Summary for a Typical Topology

Use the following command summary to quickly configure the keystore and DF properties 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 Domain Keystore

Follow the steps below to configure the service instance reference for the WebCenter 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 Spaces domain as an admin user and run the following commands:

```
createCred(map="oracle.wsm.security", key="keystore-csf-key", user="owsm",
password="welcome1", desc="Keystore key")
createCred(map="oracle.wsm.security", key="enc-csf-key", user="webcenter",
password="welcome1", desc="Encryption key")
createCred(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:

```
createCred(map="oracle.wsm.security", key="keystore-csf-key", user="owsm",
password="welcome1", desc="Keystore key")
createCred(map="oracle.wsm.security", key="enc-csf-key", user="bpel",
password="welcome1", desc="Encryption key")
createCred(map="oracle.wsm.security", key="sign-csf-key", user="bpel",
password="welcome1", desc="Signing key")
```

Configure the DF Keystore Properties File

Using WLST, connect to the WebCenter Spaces domain as an admin user and run the following commands:

```
org.apache.ws.security.crypto.merlin.keystore.type=jks
org.apache.ws.security.crypto.merlin.keystore.password=welcome1
org.apache.ws.security.crypto.merlin.keystore.alias=df_webcenter_public
org.apache.ws.security.crypto.merlin.file=<dir_containing_keystore>/owc_discussion
s.jks
```

> **Note:** Be sure to trim any spaces from the line endings. If you are working in a Windows environment, also be sure to use "\\" as the file path separator.

Additional DF Connection properties are shown in Table 28–2.

Table 28–4 Additional DF Connection Properties

Property Name	Property Value	Secured
`keystore.location`	`<doamin_home>/config/fmwconfig/webcenter.jks`	No
`keystore.type`	`jks`	No

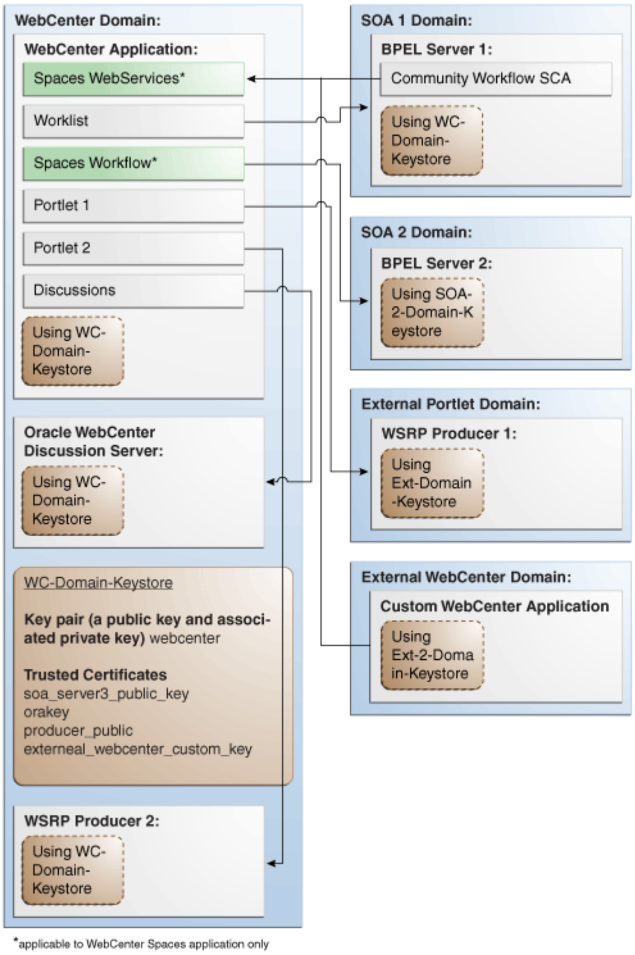
Table 28–4 (Cont.) Additional DF Connection Properties

Property Name	Property Value	Secured
`keystore.password`	`welcome1`	Yes
`encryption.key.alias`	`webcenter`	No
`encryption.key.password`	`welcome1`	Yes
`group.mapping`	`category`	No

28.3 Configuring WS-Security for a Complex Topology

This section describes how to configure WS-Security for a complex topology where the WebCenter 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 28–15).

Figure 28–15 Complex Configuration



The steps to configure WS-Security for a typical two domain WebCenter topology are described in the following sections:

- Section 28.3.1, "Setting Up the WebCenter Domain Keystore"

- Section 28.3.2, "Configuring the Discussions Server for a Complex Topology"
- Section 28.3.3, "Setting Up the First SOA Domain"
- Section 28.3.4, "Setting Up the Second SOA Domain"
- Section 28.3.5, "Configuring the BPEL Server for a Complex Topology"
- Section 28.3.6, "Setting Up the External Portlet Domain Keystore"
- Section 28.3.7, "Setting Up the External WebCenter Domain Keystore"
- Section 28.3.8, "Command Summary for a Complex Topology"

28.3.1 Setting Up the WebCenter Domain Keystore

The security credentials of WebCenter 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 28.3.1.1, "Creating the WebCenter Domain Keystore"
- Section 28.3.1.2, "Configuring the Keystore Using WLST"
- Section 28.3.1.3, "Configuring the Keystore Using Fusion Middleware Control"
- Section 28.3.1.4, "Unconfiguring a Keystore Provider"

28.3.1.1 Creating the WebCenter 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 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 28–14 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 wecenter.jks -storepass
   keystore_password -rfc -file webcenter_public.cer
   ```

   Where:

   - *`keystore_password`* is the keystore password, (for example, `welcome1`)

Example 28–15 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 28.3.1.2, "Configuring the Keystore Using WLST," or using Fusion Middleware Control, as described in Section 28.3.1.3, "Configuring the Keystore Using Fusion Middleware Control."

   Table 28–5 shows the keystore contents you should wind up with after creating and configuring the keystore.

Table 28–5 WebCenter Domain Keystore Contents for a Complex Topology

Key Alias	Description
`webcenter`	Key pair used to sign and encrypt outbound messages from WebCenter 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 WebCenter Spaces to WSRP Producer 1 registered in the WebCenter Spaces application.
`external_webcenter_custom_public_key`	Certificate containing the public key for the external_webcenter_custom private key used in the external WebCenter domain that hosts the custom WebCenter application that makes WebService call to the WebCenter Spaces WebService. This certificate is used to encrypt outbound messages from WebCenter Spaces to custom WebCenter applications in the external WebCenter domain.

28.3.1.2 Configuring the Keystore Using WLST

After creating the WebCenter 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:

```
createCred(map="oracle.wsm.security", key="keystore-csf-key", user="owsm",
password="welcome1", desc="Keystore key")
createCred(map="oracle.wsm.security", key="enc-csf-key", user="webcenter",
password="welcome1", desc="Encryption key")
createCred(map="oracle.wsm.security", key="sign-csf-key", user="webcenter",
password="welcome1", desc="Signing key")
```

5. Restart all servers.

28.3.1.3 Configuring the Keystore Using Fusion Middleware Control

If a keystore provider is already configured, you must first unconfigure the existing keystore provider as described in Section 28.3.1.4, "Unconfiguring a Keystore Provider." Otherwise, continue with the steps below.

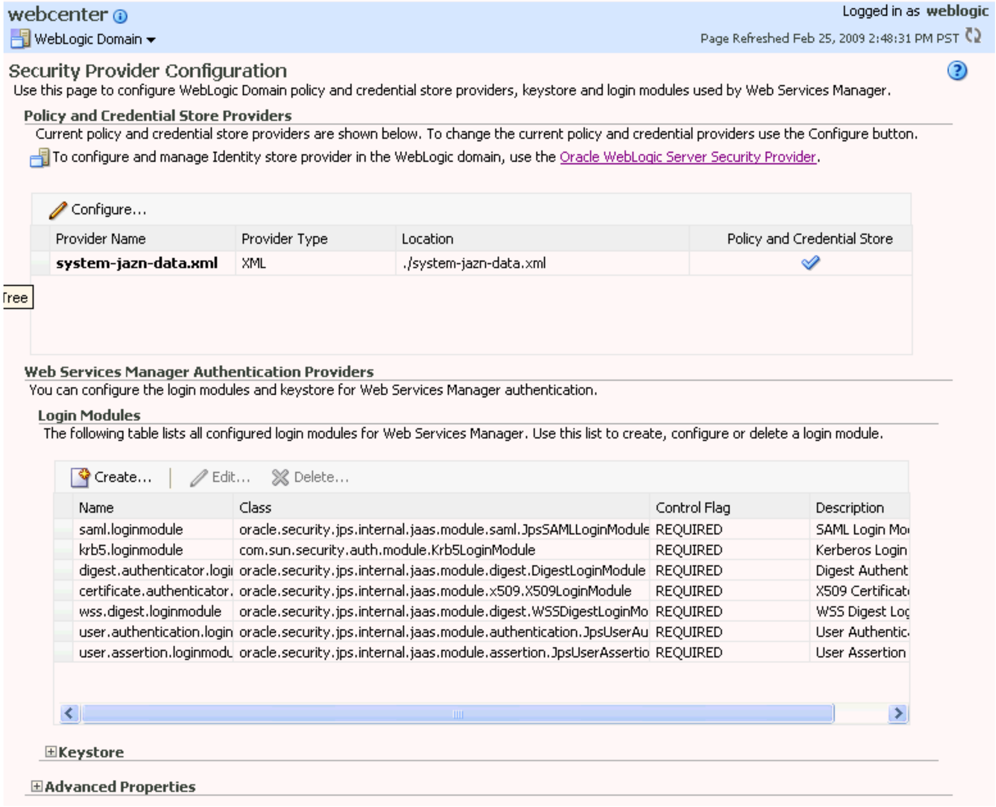
To configure the keystore provider:

1. Open Fusion Middleware Control and log in to the WebCenter domain.

   For information on logging in to 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 WebCenter domain (wc_domain by default).
3. From the WebLogic Domain menu, select **Security -> Security Provider Configuration**.

   The Security Provider Configuration page displays (see Figure 28–16).

Figure 28–16 Security Provider Configuration Page



webcenter ⓘ
WebLogic Domain ▾

Logged in as **weblogic**
Page Refreshed Feb 25, 2009 2:48:31 PM PST

Security Provider Configuration

Use this page to configure WebLogic Domain policy and credential store providers, keystore and login modules used by Web Services Manager.

Policy and Credential Store Providers

Current policy and credential store providers are shown below. To change the current policy and credential providers use the Configure button.

To configure and manage Identity store provider in the WebLogic domain, use the Oracle WebLogic Server Security Provider.

Provider Name	Provider Type	Location	Policy and Credential Store
system-jazn-data.xml	XML	./system-jazn-data.xml	✓

Web Services Manager Authentication Providers

You can configure the login modules and keystore for Web Services Manager authentication.

Login Modules

The following table lists all configured login modules for Web Services Manager. Use this list to create, configure or delete a login module.

Name	Class	Control Flag	Description
saml.loginmodule	oracle.security.jps.internal.jaas.module.saml.JpsSAMLLoginModule	REQUIRED	SAML Login Mo
krb5.loginmodule	com.sun.security.auth.module.Krb5LoginModule	REQUIRED	Kerberos Login
digest.authenticator.logi	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 Log
user.authentication.login	oracle.security.jps.internal.jaas.module.authentication.JpsUserAu	REQUIRED	User Authentic
user.assertion.loginmodu	oracle.security.jps.internal.jaas.module.assertion.JpsUserAssertio	REQUIRED	User Assertion

⊞**Keystore**

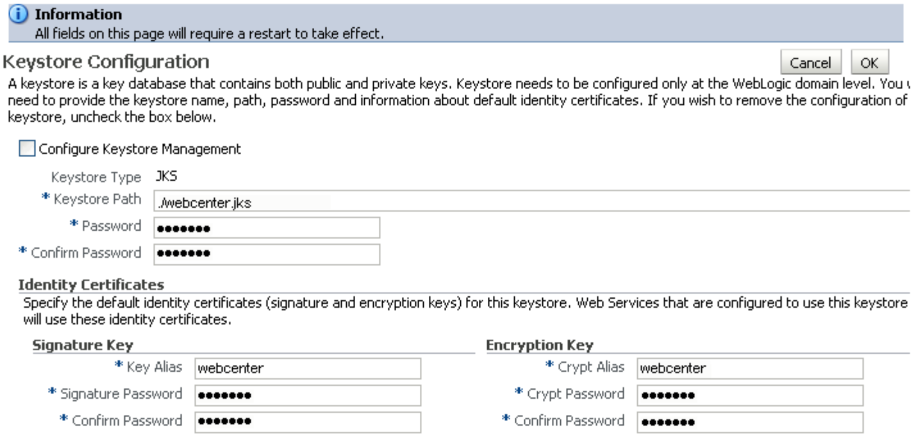
⊞**Advanced Properties**

4. Expand the Keystore section on the Security Provider Configuration page.

5. Click **Configure**.

   The Keystore Configuration page displays (see Figure 28–17).

Figure 28–17 Keystore Configuration Page



Information
All fields on this page will require a restart to take effect.

Keystore Configuration

A keystore is a key database that contains both public and private keys. Keystore needs to be configured only at the WebLogic domain level. You need to provide the keystore name, path, password and information about default identity certificates. If you wish to remove the configuration of keystore, uncheck the box below.

☐ Configure Keystore Management

Keystore Type	JKS
* Keystore Path	./webcenter.jks
* Password	•••••••
* Confirm Password	•••••••

Identity Certificates

Specify the default identity certificates (signature and encryption keys) for this keystore. Web Services that are configured to use this keystore will use these identity certificates.

Signature Key

* Key Alias	webcenter
* Signature Password	•••••••
* Confirm Password	•••••••

Encryption Key

* Crypt Alias	webcenter
* Crypt Password	•••••••
* Confirm Password	•••••••

This screenshot shows the Keystore Configuration page.

****

6. Check **Configure Keystore Management** and 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.

28.3.1.4 Unconfiguring a Keystore Provider

If a keystore provider is already configured, you must unconfigure the existing keystore provider before configuring a new provider. If a keystore provider is not already configured, continue with the steps to configure the keystore in Section 28.3.1.3, "Configuring the Keystore Using Fusion Middleware Control."

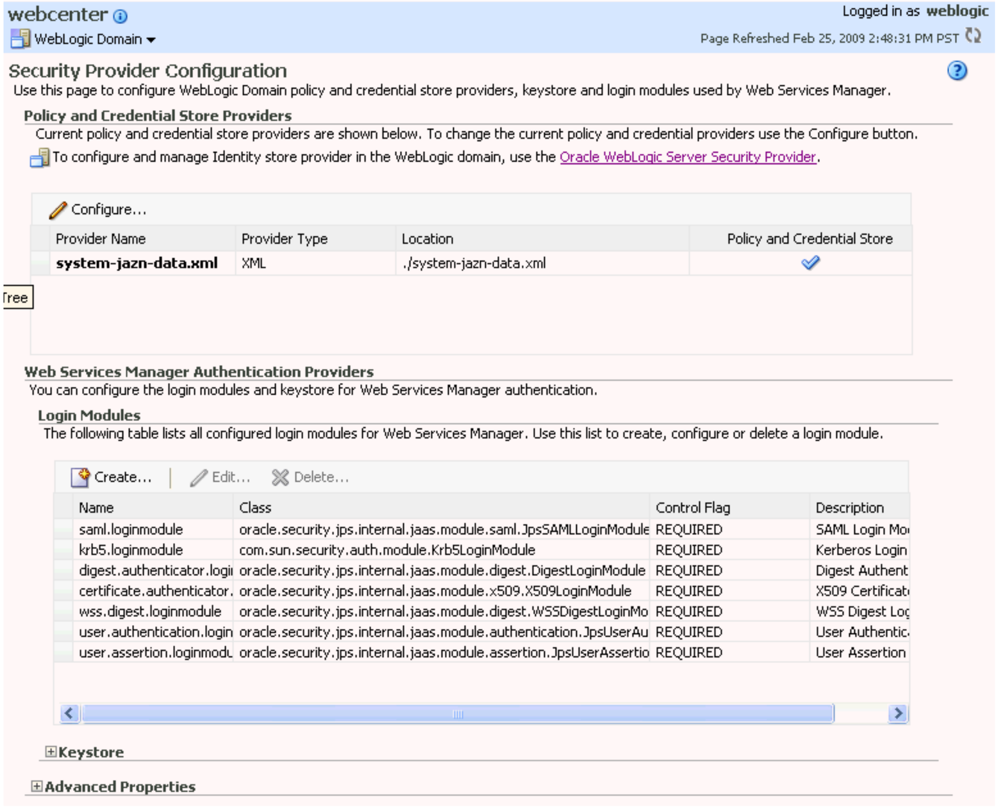
To unconfigure a keystore provider using Fusion Middleware Control:

1. Open Fusion Middleware Control and log in to the target domain.

   For information on logging in to Fusion Middleware Control, see Section 6, "Starting Enterprise Manager Fusion Middleware Control."
2. From the WebLogic Domain menu, select **Security -> Security Provider Configuration**.

   The Security Provider Configuration page displays (see Figure 28–18).

Figure 28–18 Security Provider Configuration Page



webcenter ⓘ

WebLogic Domain ▾

Logged in as **weblogic**

Page Refreshed Feb 25, 2009 2:48:31 PM PST

Security Provider Configuration

Use this page to configure WebLogic Domain policy and credential store providers, keystore and login modules used by Web Services Manager.

Policy and Credential Store Providers

Current policy and credential store providers are shown below. To change the current policy and credential providers use the Configure button.

To configure and manage Identity store provider in the WebLogic domain, use the Oracle WebLogic Server Security Provider.

Provider Name	Provider Type	Location	Policy and Credential Store
system-jazn-data.xml	XML	./system-jazn-data.xml	✓

Web Services Manager Authentication Providers

You can configure the login modules and keystore for Web Services Manager authentication.

Login Modules

The following table lists all configured login modules for Web Services Manager. Use this list to create, configure or delete a login module.

Name	Class	Control Flag	Description
saml.loginmodule	oracle.security.jps.internal.jaas.module.saml.JpsSAMLLoginModule	REQUIRED	SAML Login Mo
krb5.loginmodule	com.sun.security.auth.module.Krb5LoginModule	REQUIRED	Kerberos Login
digest.authenticator.logi	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 Log
user.authentication.login	oracle.security.jps.internal.jaas.module.authentication.JpsUserAu	REQUIRED	User Authentic
user.assertion.loginmodu	oracle.security.jps.internal.jaas.module.assertion.JpsUserAssertio	REQUIRED	User Assertion

⊞**Keystore**

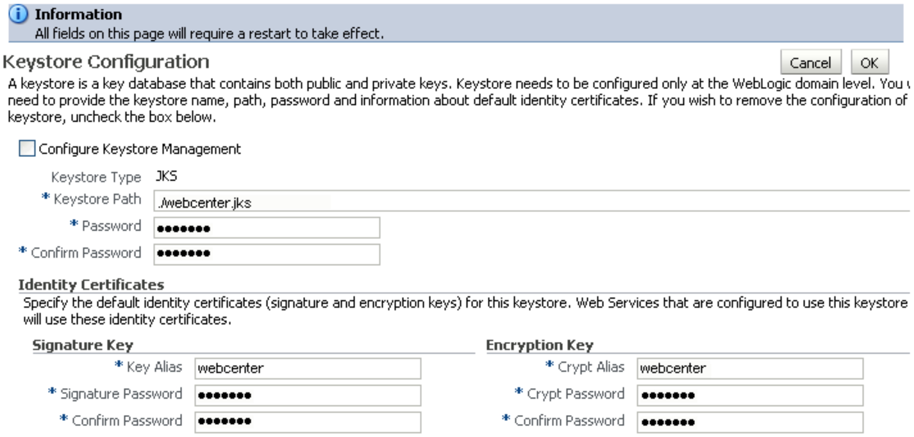
⊞**Advanced Properties**

3. Expand the Keystore section on the Security Provider Configuration page.

4. Click **Configure**.

   The Keystore Configuration page displays (see Figure 28–19).

Figure 28–19 Keystore Configuration Page



ⓘ **Information**

All fields on this page will require a restart to take effect.

Keystore Configuration

A keystore is a key database that contains both public and private keys. Keystore needs to be configured only at the WebLogic domain level. You need to provide the keystore name, path, password and information about default identity certificates. If you wish to remove the configuration of keystore, uncheck the box below.

□ Configure Keystore Management

Keystore Type JKS

* Keystore Path ./webcenter.jks

* Password •••••••

* Confirm Password •••••••

Identity Certificates

Specify the default identity certificates (signature and encryption keys) for this keystore. Web Services that are configured to use this keystore will use these identity certificates.

Signature Key

* Key Alias webcenter

* Signature Password •••••••

* Confirm Password •••••••

Encryption Key

* Crypt Alias webcenter

* Crypt Password •••••••

* Confirm Password •••••••

5. Uncheck **Configure Keystore Management**.

6. Click **OK**.

28.3.2 Configuring the Discussions Server for a Complex Topology

To use the Oracle WebCenter Discussions with WebCenter Spaces or custom WebCenter applications, you must enable Web Services Security (WS-Security) trusted authentication. WS-Security establishes a trust relationship between your WebCenter application and Oracle WebCenter Discussions so that the application can pass the user identity information to the discussions server without knowing the user's credentials.

> **Note:** Discussions-specific Web Services messages sent by WebCenter applications to the Oracle WebCenter 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 27, "Securing WebCenter Applications and Components with SSL."

This section describes how to add WS-Security-related properties to the discussion server connection that is configured for WebCenter Spaces or your custom WebCenter application. For information on how to add new properties, see Table 12–4, " Additional Discussion Connection Properties" in Section 12.3.1, "Registering Discussions Servers Using Fusion Middleware Control."

To configure WS-Security on the discussions server side, you must create a keystore certificate properties file, specify it for the ClassLoader, and modify the `webservices.soap.custom.crypto.fileName` system property. These configuration steps are described in the following sub-sections:

- Section 28.3.2.1, "Importing the WebCenter Domain Certificate"
- Section 28.3.2.2, "Creating the Keystore Certificate Properties File"
- Section 28.3.2.3, "Specifying the Properties File for ClassLoader"
- Section 28.3.2.4, "Updating the System Properties for WS-Security"

28.3.2.1 Importing the WebCenter Domain Certificate

Create a keystore by importing the certificate containing public key of the WebCenter domain.

To import the WebCenter domain certificate:

1. Go to *`JDK_HOME`*`/jdk/bin` and open a command prompt.
2. Using keytool, import the certificate containing the public key of the WebCenter domain:

   ```
   keytool -importcert -alias df_orakey_public -file webcenter_public.cer
   -keystore owc_discussions.jks -storepass keystore_password
   ```

   Where:

   - *`keystore_password`* is the keystore password, (for example, `welcome1`)

Example 28–16 Importing the WebCenter Domain Certificate

```
keytool -importcert -alias df_webcenter_public -file webcenter_public.cer
-keystore owc_discussions.jks -storepass welcome1
```

28.3.2.2 Creating the Keystore Certificate Properties File

The server-side keystore certificate configuration must be stored in a properties file (`keystore.properties`) and specified as a system property on the discussions server. The properties file must then be loaded in the ClassLoader for the WS-Secure Handler to pick it up.

> **Note:** When you are updating the properties file, be sure to remove any spaces from the property names and values. The properties file should not contain any extraneous spaces.

To create the properties file:

1. Create a properties file with the following entries:

```
org.apache.ws.security.crypto.provider= <Specify your crypto provider
(typically org.apache.ws.security.components.crypto.Merlin)>
org.apache.ws.security.crypto.merlin.keystore.type=jks
org.apache.ws.security.crypto.merlin.keystore.password=<Specify the keystore
password of your server certificate.
Note that the password stored in this file is in clear text because of a
limitation of the Ws-Security provider WSS4J used in Oracle Discussions
Server.>
org.apache.ws.security.crypto.merlin.keystore.alias=df_webcenter_public
org.apache.ws.security.crypto.merlin.file=<Absolute path of directory
 containing the keystore created above.>
```

2. Save the file as `keystore.properties`.

28.3.2.3 Specifying the Properties File for ClassLoader

There are two ways you can choose to specify your `keystore.properties` file based on your setup. Using the same file mounted across different servers is recommended when using a Clustered Discussions Server installation in Linux.

To specify the properties file for ClassLoader, do one of the following:

- Specify the properties file as the `CLASSPATH` in `setDomainEnv.sh`.

  For Linux:

  1. Place the `keystore.properties` file in a directory (for example, `. /home/user/keystore/`)
  2. Open `DOMAIN_HOME/bin/setDomainEnv.sh`.
  3. Towards the end of the file, add the following lines to specify this directory as the `CLASSPATH`.

```
if [ "${CLASSPATH}" != "" ] ; then
  CLASSPATH="${CLASSPATH}${CLASSPATHSEP}/home/user/keystore/"
  export CLASSPATH
else
  CLASSPATH="/home/user/keystore/"
  export CLASSPATH
fi
```

  Note that the `CLASSPATH` directory name must end with "/".

  For Windows:

1. Place the keystore.properties file in a directory (for example, c:\keystore\).
2. Open DOMAIN_HOME\bin\setDomainEnv.cmd.
3. Towards the end of the file, add the following lines to specify this directory in CLASSPATH.

   ```
   if NOT "%CLASSPATH%"=="" (
     set CLASSPATH=%CLASSPATH%;c:\keystore\
   ) else (
     set CLASSPATH=c:\keystore\
   )
   ```

   Note that the CLASSPATH directory name must end with "\".

- Or, add the keystore.properties file to a .JAR file and place the .JAR file in your DOMAIN_HOME/lib directory. Be sure to also set the system property webservices.soap.custom.crypto.fileName to keystore.properties as described in Section 28.3.2.4, "Updating the System Properties for WS-Security."

28.3.2.4 Updating the System Properties for WS-Security

To update your system properties:

1. Log in to the Oracle WebCenter Discussions Administration Console at the following URL:

   http://host:port/owc_discussions/admin

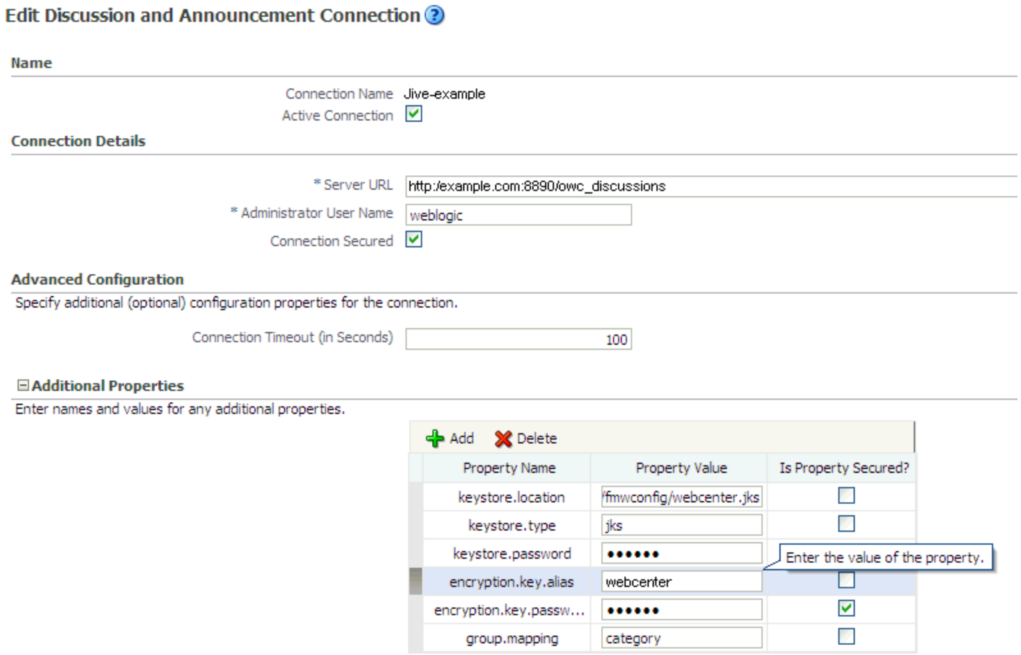
   Where host and port are the address and the port number of the server where you deployed Oracle WebCenter Discussions (for example, http://localhost:7001/owc_discussions).
2. Click **System Properties** under **Forum System** to display the Jive Properties page.
3. Modify the system property webservices.soap.custom.crypto.fileName and specify the properties file that you created (that is, keystore.properties).

   Be sure to specify the name of the file, and not the directory or .JAR name.
4. Click **OK**.
5. Restart the WLS_Services Managed Server.

28.3.2.5 Configuring the Discussions Server Connection Settings

After setting the system properties, you must supply the WS-Security client certificate information within the discussion server connection settings, as described in Section 12.3, "Registering Discussions Servers." Figure 28–20 shows example settings for the Edit Discussions and Announcement Connection page.

Figure 28–20 Edit Discussions and Announcement Connection Page



Edit Discussion and Announcement Connection

Name

Connection Name Jive-example

Active Connection ☑

Connection Details

* Server URL http:/example.com:8890/owc_discussions

* Administrator User Name weblogic

Connection Secured ☑

Advanced Configuration

Specify additional (optional) configuration properties for the connection.

Connection Timeout (in Seconds) 100

⊟ **Additional Properties**

Enter names and values for any additional properties.

Property Name	Property Value	Is Property Secured?
keystore.location	/fmwconfig/webcenter.jks	□
keystore.type	jks	□
keystore.password	••••••	
encryption.key.alias	webcenter	□
encryption.key.passw...	••••••	☑
group.mapping	category	□

Enter the value of the property.

28.3.3 Setting Up the First SOA Domain

This section describes how to set up the SOA domain keystore and contains the following subsections:

- Section 28.3.3.1, "Creating the SOA Domain Keystore"
- Section 28.3.3.2, "Configuring the Keystore Using WLST"
- Section 28.3.3.3, "Configuring the Keystore Using Fusion Middleware Control"
- Section 28.3.3.4, "Unconfiguring a Keystore Provider"

28.3.3.1 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 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 28–17 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 28–18 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 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 28–19 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 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 28–20 Importing the Certificate

```
keytool -importcert -alias orakey -file orakay.cer -keystore webcenter.jks
-storepass welcome1
```

6. Continue by configuring the keystore using either WLST as described in Section 28.3.3.2, "Configuring the Keystore Using WLST,", or using Fusion Middleware Control as described in Section 28.3.3.3, "Configuring the Keystore Using Fusion Middleware Control."

   Table 28–6 shows the keystore contents you should wind up with after creating and configuring the SOA 1 domain keystore.

Table 28–6 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 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.

28.3.3.2 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.

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:

```
createCred(map="oracle.wsm.security", key="keystore-csf-key", user="owsm",
password="welcome1", desc="Keystore key")
createCred(map="oracle.wsm.security", key="enc-csf-key", user="bpel",
password="welcome1", desc="Encryption key")
createCred(map="oracle.wsm.security", key="sign-csf-key", user="bpel",
password="welcome1", desc="Signing key")
```

5. Restart all servers.

28.3.3.3 Configuring the Keystore Using Fusion Middleware Control

If a keystore provider is already configured, you must first unconfigure the existing keystore provider as described in Section 28.3.3.4, "Unconfiguring a Keystore Provider." Otherwise, continue with the steps below.

To configure the keystore provider:

1. Open Fusion Middleware Control and log in to the WebCenter domain.

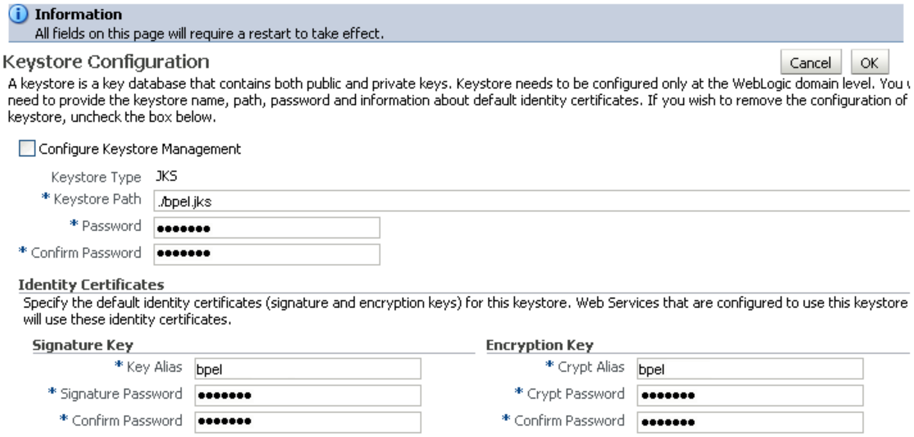
   For information on logging in to Fusion Middleware Control, see Section 6, "Starting Enterprise Manager Fusion Middleware Control."

2. In the Navigation pane, expand the WebLogic Domain node and click the 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 28–21).

Figure 28–21 Keystore Configuration Page



Information
All fields on this page will require a restart to take effect.

Keystore Configuration

A keystore is a key database that contains both public and private keys. Keystore needs to be configured only at the WebLogic domain level. You
need to provide the keystore name, path, password and information about default identity certificates. If you wish to remove the configuration of keystore, uncheck the box below.

☐ Configure Keystore Management

Keystore Type JKS
* Keystore Path ./bpel.jks
* Password •••••••
* Confirm Password •••••••

Identity Certificates

Specify the default identity certificates (signature and encryption keys) for this keystore. Web Services that are configured to use this keystore will use these identity certificates.

Signature Key
* Key Alias bpel
* Signature Password •••••••
* Confirm Password •••••••

Encryption Key
* Crypt Alias bpel
* Crypt Password •••••••
* Confirm Password •••••••

6. Check **Configure Keystore Management** and 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.

28.3.3.4 Unconfiguring a Keystore Provider

If a keystore provider is already configured, you must unconfigure the existing keystore provider before configuring a new provider. If a keystore provider is not already configured, continue with the steps to configure the keystore in Section 28.3.3.3, "Configuring the Keystore Using Fusion Middleware Control."

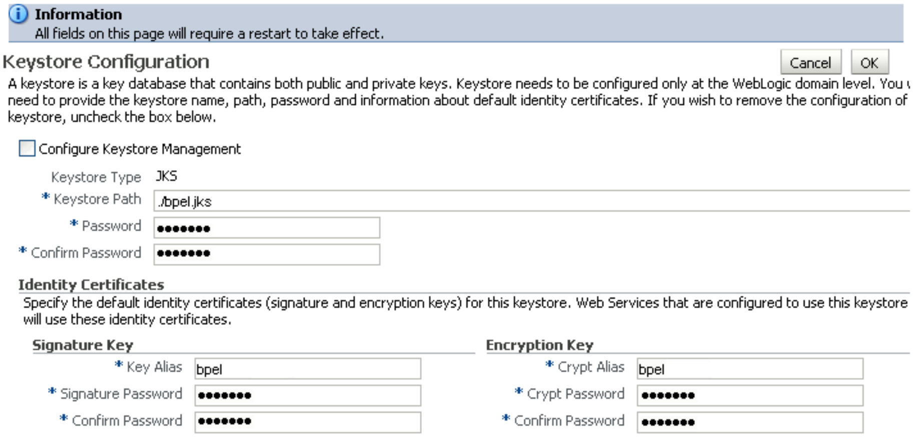
To unconfigure a keystore provider using Fusion Middleware Control:

1. Open Fusion Middleware Control and log in to the target domain.

   For information on logging in to Fusion Middleware Control, see Section 6, "Starting Enterprise Manager Fusion Middleware Control."
2. From the SOA Domain menu, select **Security -> Security Provider Configuration**.
3. Expand the Keystore section on the Security Provider Configuration page.
4. Click **Configure**.

The Keystore Configuration page displays (see Figure 28–22).

Figure 28–22 Keystore Configuration Page



Information
All fields on this page will require a restart to take effect.

Keystore Configuration

A keystore is a key database that contains both public and private keys. Keystore needs to be configured only at the WebLogic domain level. You
need to provide the keystore name, path, password and information about default identity certificates. If you wish to remove the configuration of
keystore, uncheck the box below.

□ Configure Keystore Management

Keystore Type JKS
* Keystore Path ./bpel.jks
* Password •••••••
* Confirm Password •••••••

Identity Certificates
Specify the default identity certificates (signature and encryption keys) for this keystore. Web Services that are configured to use this keystore will use these identity certificates.

Signature Key
* Key Alias bpel
* Signature Password •••••••
* Confirm Password •••••••

Encryption Key
* Crypt Alias bpel
* Crypt Password •••••••
* Confirm Password •••••••

5. Uncheck **Configure Keystore Management**.
6. Click **OK**.

28.3.4 Setting Up the Second SOA Domain

This section describes how to set up a second SOA domain keystore and contains the following subsections:

- Section 28.3.4.1, "Creating the SOA Domain Keystore"
- Section 28.3.4.2, "Configuring the Keystore Using WLST"
- Section 28.3.4.3, "Configuring the Keystore Using Fusion Middleware Control"
- Section 28.3.4.4, "Unconfiguring a Keystore Provider"

28.3.4.1 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. 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 28–21 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 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 28–22 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 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 28–23 Importing the Certificate

```
keytool -importcert -alias soa_server3_public_key -file soa_server3_public_key.cer
-keystore webcenter.jks -storepass welcome1
```

5. Continue by configuring the keystore using either WLST as described in Section 28.3.4.2, "Configuring the Keystore Using WLST,", or using Fusion Middleware Control as described in Section 28.3.4.3, "Configuring the Keystore Using Fusion Middleware Control."

   Table 28–7 shows the keystore contents you should wind up with after creating and configuring the SOA 2 domain keystore.

Table 28–7 SOA 2 Domain Keystore Contents for a Complex Topology

Key Alias	Description
webcenter	Key pair used to sign and encrypt outbound messages from WebCenter Spaces. This key is used by both OWSM (Portlets and Worklist) and Discussions.

Table 28–7 (Cont.) SOA 2 Domain Keystore Contents for a Complex Topology

Key Alias	Description
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 WebCenter Spaces to WSRP Producer 1 registered in the WebCenter Spaces application.
external_webcenter_custom_public_key	Certificate containing the public key for the external_webcenter_custom private key used in the external WebCenter domain that hosts the custom WebCenter application that makes WebService call to the WebCenter Spaces WebService. This certificate is used to encrypt outbound messages from WebCenter Spaces to custom WebCenter applications in the external WebCenter domain.

28.3.4.2 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.

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:

```
createCred(map="oracle.wsm.security", key="keystore-csf-key", user="owsm",
password="welcome1", desc="Keystore key")
createCred(map="oracle.wsm.security", key="enc-csf-key", user="soa_server3",
password="welcome1", desc="Encryption key")
createCred(map="oracle.wsm.security", key="sign-csf-key", user="soa_server3",
password="welcome1", desc="Signing key")
```

5. Restart all servers.

28.3.4.3 Configuring the Keystore Using Fusion Middleware Control

If a keystore provider is already configured, you must first unconfigure the existing keystore provider as described in Section 28.3.4.4, "Unconfiguring a Keystore Provider." Otherwise, continue with the steps below.

To configure the keystore provider:

1. Open Fusion Middleware Control and log in to the WebCenter domain.

   For information on logging in to 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 SOA domain.

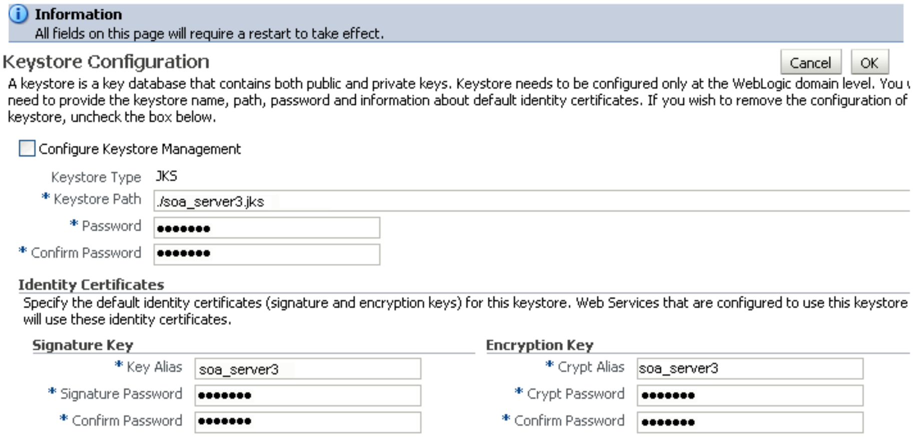
3. From the SOA Domain menu, select **Security -> Security Provider Configuration**.

4. Expand the Keystore section on the Security Provider Configuration page.

5. Click **Configure**.

   The Keystore Configuration page displays (see Figure 28–23).

Figure 28–23 Keystore Configuration Page



Information
All fields on this page will require a restart to take effect.

Keystore Configuration

A keystore is a key database that contains both public and private keys. Keystore needs to be configured only at the WebLogic domain level. You ι need to provide the keystore name, path, password and information about default identity certificates. If you wish to remove the configuration of keystore, uncheck the box below.

□ Configure Keystore Management

Keystore Type JKS
* Keystore Path ./soa_server3.jks
* Password ●●●●●●●
* Confirm Password ●●●●●●●

Identity Certificates

Specify the default identity certificates (signature and encryption keys) for this keystore. Web Services that are configured to use this keystore will use these identity certificates.

Signature Key
* Key Alias soa_server3
* Signature Password ●●●●●●●
* Confirm Password ●●●●●●●

Encryption Key
* Crypt Alias soa_server3
* Crypt Password ●●●●●●●
* Confirm Password ●●●●●●●

6. Check **Configure Keystore Management** and 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.

28.3.4.4 Unconfiguring a Keystore Provider

If a keystore provider is already configured, you must unconfigure the existing keystore provider before configuring a new provider. If a keystore provider is not already configured, continue with the steps to configure the keystore in Section 28.3.4.3, "Configuring the Keystore Using Fusion Middleware Control."

To unconfigure a keystore provider using Fusion Middleware Control:

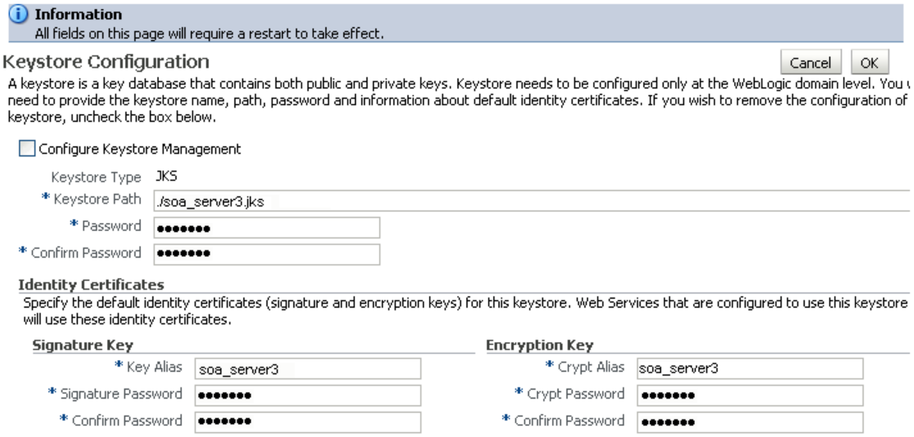
1. Open Fusion Middleware Control and log in to the target domain.

   For information on logging in to Fusion Middleware Control, see Section 6, "Starting Enterprise Manager Fusion Middleware Control."

2. From the SOA Domain menu, select **Security -> Security Provider Configuration**.
3. Expand the Keystore section on the Security Provider Configuration page.
4. Click **Configure**.

   The Keystore Configuration page displays (see Figure 28–24).

Figure 28–24 Keystore Configuration Page



Information
All fields on this page will require a restart to take effect.

Keystore Configuration

A keystore is a key database that contains both public and private keys. Keystore needs to be configured only at the WebLogic domain level. You need to provide the keystore name, path, password and information about default identity certificates. If you wish to remove the configuration of keystore, uncheck the box below.

□ Configure Keystore Management

Keystore Type JKS
* Keystore Path ./soa_server3.jks
* Password •••••••
* Confirm Password •••••••

Identity Certificates

Specify the default identity certificates (signature and encryption keys) for this keystore. Web Services that are configured to use this keystore will use these identity certificates.

Signature Key
* Key Alias soa_server3
* Signature Password •••••••
* Confirm Password •••••••

Encryption Key
* Crypt Alias soa_server3
* Crypt Password •••••••
* Confirm Password •••••••

5. Uncheck **Configure Keystore Management**.
6. Click **OK**.

28.3.5 Configuring the BPEL Server for a Complex Topology

WebCenter Spaces Worklist connections use `oracle/wss10_saml_token_with_message_protection_client_policy` as the secure OWSM policy for generating outbound SOAP messages to the SOA server. However, by default, this policy uses `orakey` to encrypt outbound messages.

When the WebCenter domain (where WebCenter Spaces is installed) is configured to use two or more Worklist connections simultaneously, and those connections use a secure message propagation OWSM policy, an additional OWSM policy must be created. This policy must be configured so that the recipient key alias matches the alias by which the certificate of the intended SOA server is stored on the WebCenter Spaces side.

The following steps are required to use more than one external SOA Domain configuration simultaneously on the WebCenter Spaces server:

1. Export the certificate from the external SOA domain and import it into the WebCenter domain under a specific 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 in step 1 above.
3. Create a connection to a BPEL server and use WLST to set the security policy to the policy created in step 2 above.

The following steps show how to perform steps 2 and 3 above. Note that the keystore should already have been created in Section 28.3.4, "Setting Up the Second SOA Domain."

To configure the BPEL server for multiple Worklist connections:

1. Create an OWSM security policy and register the new policy in WebCenter Spaces using Fusion Middleware Control.

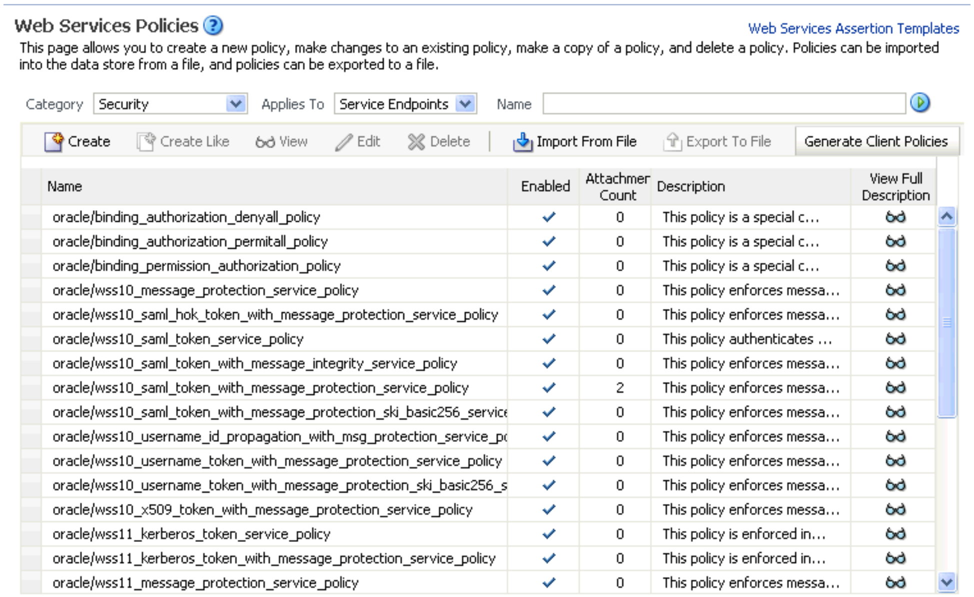
   a. Open Fusion Middleware Control and log in to the target domain.

      For information on logging in to Fusion Middleware Control, see Section 6, "Starting Enterprise Manager Fusion Middleware Control."

   b. From the WebLogic Domain menu, select **Web Services > Policies.**

      The Web Services Policies page displays (see Figure 28–25).

Figure 28–25 Web Services Policies Page



Web Services Policies

Web Services Assertion Templates

This page allows you to create a new policy, make changes to an existing policy, make a copy of a policy, and delete a policy. Policies can be imported into the data store from a file, and policies can be exported to a file.

Category: Security

Applies To: Service Endpoints

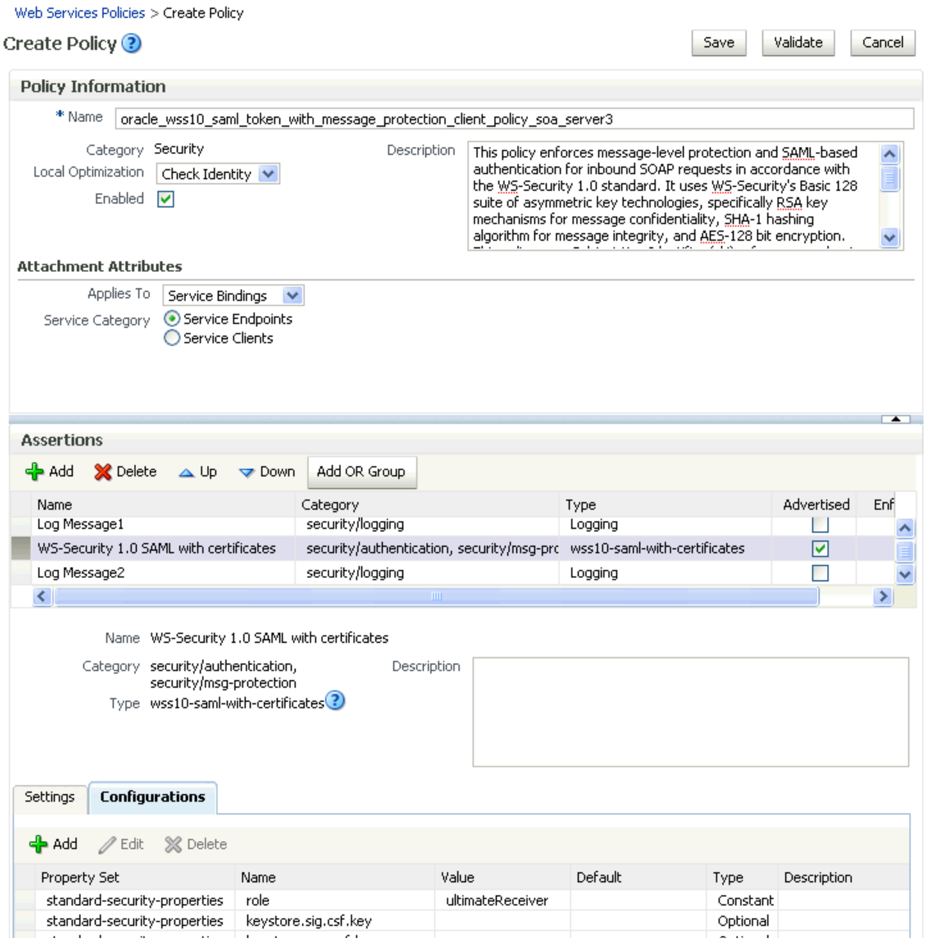
Name:

Name	Enabled	Attachmer Count	Description	View Full Description
oracle/binding_authorization_denyall_policy	✓	0	This policy is a special c...	👓
oracle/binding_authorization_permitall_policy	✓	0	This policy is a special c...	👓
oracle/binding_permission_authorization_policy	✓	0	This policy is a special c...	👓
oracle/wss10_message_protection_service_policy	✓	0	This policy enforces messa...	👓
oracle/wss10_saml_hok_token_with_message_protection_service_policy	✓	0	This policy enforces messa...	👓
oracle/wss10_saml_token_service_policy	✓	0	This policy authenticates ...	👓
oracle/wss10_saml_token_with_message_integrity_service_policy	✓	0	This policy enforces messa...	👓
oracle/wss10_saml_token_with_message_protection_service_policy	✓	2	This policy enforces messa...	👓
oracle/wss10_saml_token_with_message_protection_ski_basic256_service	✓	0	This policy enforces messa...	👓
oracle/wss10_username_id_propagation_with_msg_protection_service_pc	✓	0	This policy enforces messa...	👓
oracle/wss10_username_token_with_message_protection_service_policy	✓	0	This policy enforces messa...	👓
oracle/wss10_username_token_with_message_protection_ski_basic256_s	✓	0	This policy enforces messa...	👓
oracle/wss10_x509_token_with_message_protection_service_policy	✓	0	This policy enforces messa...	👓
oracle/wss11_kerberos_token_service_policy	✓	0	This policy is enforced in...	👓
oracle/wss11_kerberos_token_with_message_protection_service_policy	✓	0	This policy is enforced in...	👓
oracle/wss11_message_protection_service_policy	✓	0	This policy enforces messa...	👓

   c. Select a client policy to use as a base for creating a new policy and click **Create Like**.

      The Create Policy page displays (see Figure 28–26).

Figure 28–26 Create Policy Page



Web Services Policies > Create Policy

Create Policy

Save | Validate | Cancel

Policy Information

* Name: oracle_wss10_saml_token_with_message_protection_client_policy_soa_server3

Category: Security

Local Optimization: Check Identity

Enabled: ☑

Description: 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.

Attachment Attributes

Applies To: Service Bindings

Service Category: ● Service Endpoints ○ Service Clients

Assertions

Add | Delete | Up | Down | Add OR Group

Name	Category	Type	Advertised	Enf
Log Message1	security/logging	Logging	□	
WS-Security 1.0 SAML with certificates	security/authentication, security/msg-prc	wss10-saml-with-certificates	☑	
Log Message2	security/logging	Logging	□	

Name: WS-Security 1.0 SAML with certificates

Category: security/authentication, security/msg-protection

Type: wss10-saml-with-certificates

Description:

Settings | Configurations

Add | Edit | Delete

Property Set	Name	Value	Default	Type	Description
standard-security-properties	role	ultimateReceiver		Constant	
standard-security-properties	keystore.sig.csf.key			Optional	

d. Name the policy `oracle_wss10_saml_token_with_message_protection_client_policy_soa_server3`.

e. On the Configuration tab, select the row for `recipient.key.alias` and click **Edit**.

f. Enter `soa_server3_key` as the **Value** and click **OK**.

g. On the Create Policy page, click **Save**. The new policy should now be listed on the Web Services Policies page.

2. Create a BPEL connection that uses the new security policy with 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_serve
r3')
```

28.3.6 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 28.3.6.1, "Creating the External Portlet Domain Keystore"
- Section 28.3.6.2, "Configuring the Keystore Using WLST"
- Section 28.3.6.3, "Configuring the Keystore Using Fusion Middleware Control"
- Section 28.3.6.4, "Unconfiguring a Keystore Provider"

28.3.6.1 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 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 28–24 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 28–25 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 WebCenter 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 28–26 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 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 28–27 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 28.3.6.2, "Configuring the Keystore Using WLST,", or using Fusion Middleware Control as described in Section 28.3.6.3, "Configuring the Keystore Using Fusion Middleware Control."

28.3.6.2 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.

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:

   ```
   createCred(map="oracle.wsm.security", key="keystore-csf-key", user="owsm",
   password="welcome1", desc="Keystore key")
   createCred(map="oracle.wsm.security", key="enc-csf-key", user="producer",
   password="welcome1", desc="Encryption key")
   createCred(map="oracle.wsm.security", key="sign-csf-key", user="producer",
   password="welcome1", desc="Signing key")
   ```

5. Restart all servers.

28.3.6.3 Configuring the Keystore Using Fusion Middleware Control

If a keystore provider is already configured, you must first unconfigure the existing keystore provider as described in Section 28.3.6.4, "Unconfiguring a Keystore Provider." Otherwise, continue with the steps below.

To configure the keystore provider:

1. Open Fusion Middleware Control and log in to the WebCenter domain.

   For information on logging in to 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 WebCenter domain (`webcenter` by default).

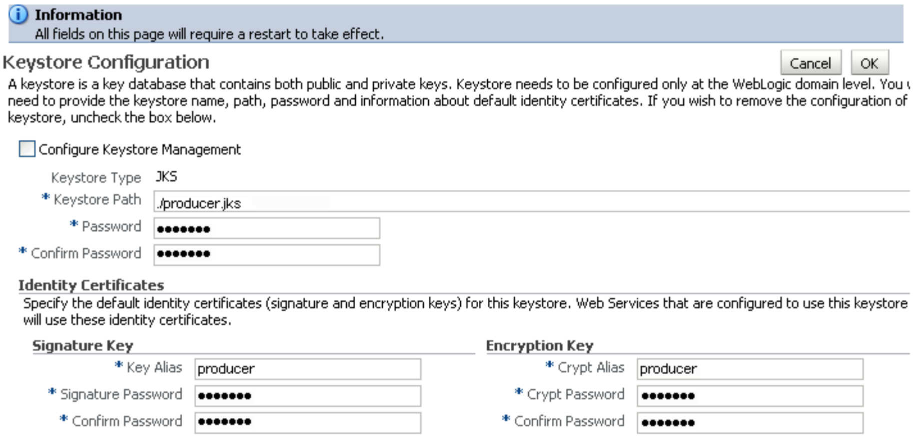
3. From the WebLogic Domain menu, select **Security -> Security Provider Configuration**.

4. Expand the Keystore section on the Security Provider Configuration page.

5. Click **Configure**.

   The Keystore Configuration page displays (see Figure 28–27).

Figure 28–27 Keystore Configuration Page



Information
All fields on this page will require a restart to take effect.

Keystore Configuration

A keystore is a key database that contains both public and private keys. Keystore needs to be configured only at the WebLogic domain level. You u
need to provide the keystore name, path, password and information about default identity certificates. If you wish to remove the configuration of
keystore, uncheck the box below.

□ Configure Keystore Management

Keystore Type JKS
* Keystore Path ./producer.jks
* Password ●●●●●●●
* Confirm Password ●●●●●●●

Identity Certificates
Specify the default identity certificates (signature and encryption keys) for this keystore. Web Services that are configured to use this keystore will use these identity certificates.

Signature Key
* Key Alias producer
* Signature Password ●●●●●●●
* Confirm Password ●●●●●●●

Encryption Key
* Crypt Alias producer
* Crypt Password ●●●●●●●
* Confirm Password ●●●●●●●

6. Check **Configure Keystore Management** and 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.

28.3.6.4 Unconfiguring a Keystore Provider

If a keystore provider is already configured, you must unconfigure the existing keystore provider before configuring a new provider. If a keystore provider is not already configured, continue with the steps to configure the keystore in Section 28.3.6.3, "Configuring the Keystore Using Fusion Middleware Control."

To unconfigure a keystore provider using Fusion Middleware Control:

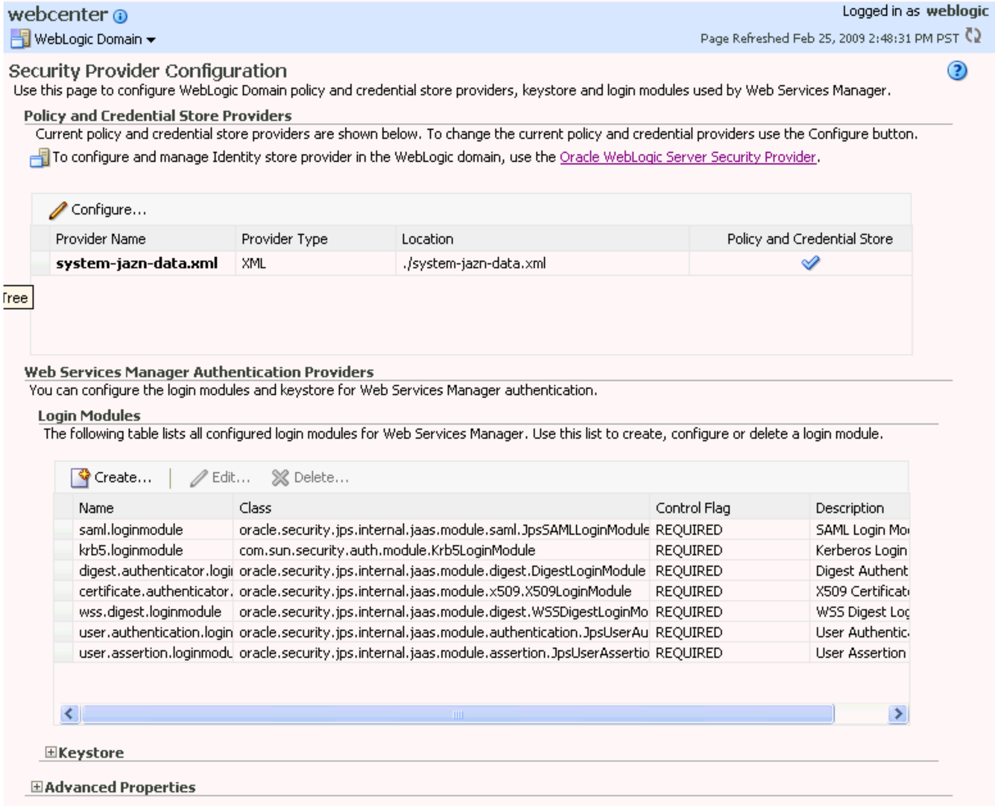
1. Open Fusion Middleware Control and log in to the target domain.

   For information on logging in to Fusion Middleware Control, see Section 6, "Starting Enterprise Manager Fusion Middleware Control."

2. From the WebLogic Domain menu, select **Security -> Security Provider Configuration**.

   The Security Provider Configuration page displays (see Figure 28–28).

Figure 28–28 Security Provider Configuration Page



webcenter

Logged in as **weblogic**

Page Refreshed Feb 25, 2009 2:48:31 PM PST

Security Provider Configuration

Use this page to configure WebLogic Domain policy and credential store providers, keystore and login modules used by Web Services Manager.

Policy and Credential Store Providers

Current policy and credential store providers are shown below. To change the current policy and credential providers use the Configure button.

To configure and manage Identity store provider in the WebLogic domain, use the Oracle WebLogic Server Security Provider.

Provider Name	Provider Type	Location	Policy and Credential Store
system-jazn-data.xml	XML	./system-jazn-data.xml	✓

Web Services Manager Authentication Providers

You can configure the login modules and keystore for Web Services Manager authentication.

Login Modules

The following table lists all configured login modules for Web Services Manager. Use this list to create, configure or delete a login module.

Name	Class	Control Flag	Description
saml.loginmodule	oracle.security.jps.internal.jaas.module.saml.JpsSAMLLoginModule	REQUIRED	SAML Login Mo
krb5.loginmodule	com.sun.security.auth.module.Krb5LoginModule	REQUIRED	Kerberos Login
digest.authenticator.logi	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 Log
user.authentication.login	oracle.security.jps.internal.jaas.module.authentication.JpsUserAu	REQUIRED	User Authentic.
user.assertion.loginmodu	oracle.security.jps.internal.jaas.module.assertion.JpsUserAssertio	REQUIRED	User Assertion

⊞**Keystore**

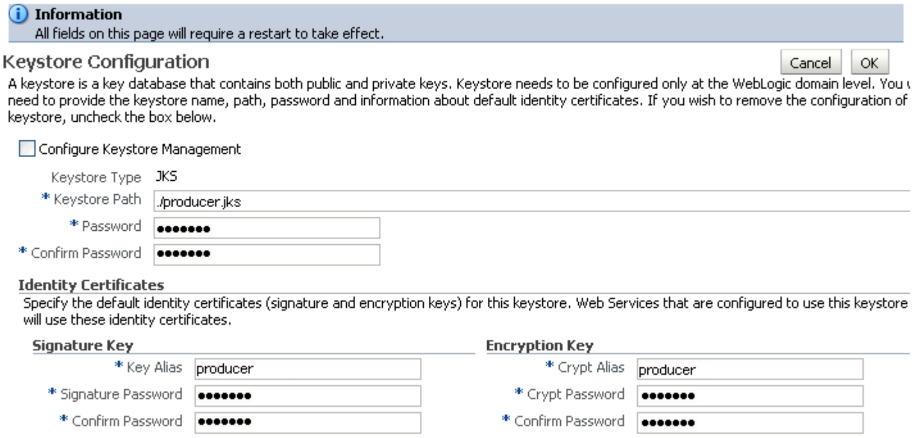
⊞**Advanced Properties**

3. Expand the Keystore section on the Security Provider Configuration page.

4. Click **Configure**.

   The Keystore Configuration page displays (see Figure 28–29).

Figure 28–29 Keystore Configuration Page



Information
All fields on this page will require a restart to take effect.

Keystore Configuration

A keystore is a key database that contains both public and private keys. Keystore needs to be configured only at the WebLogic domain level. You need to provide the keystore name, path, password and information about default identity certificates. If you wish to remove the configuration of keystore, uncheck the box below.

□ Configure Keystore Management

Keystore Type JKS
* Keystore Path ./producer.jks
* Password •••••••
* Confirm Password •••••••

Identity Certificates
Specify the default identity certificates (signature and encryption keys) for this keystore. Web Services that are configured to use this keystore will use these identity certificates.

Signature Key
* Key Alias producer
* Signature Password •••••••
* Confirm Password •••••••

Encryption Key
* Crypt Alias producer
* Crypt Password •••••••
* Confirm Password •••••••

5. Uncheck **Configure Keystore Management**.
6. Click **OK**.

28.3.7 Setting Up the External WebCenter Domain Keystore

This section describes how to set up an external WebCenter domain used by a custom WebCenter application making WebCenter Spaces WebService calls.

This section contains the following subsections:

- Section 28.3.7.1, "Creating the External WebCenter Domain Keystore"
- Section 28.3.7.2, "Configuring the Keystore Using WLST"
- Section 28.3.7.3, "Configuring the Keystore Using Fusion Middleware Control"
- Section 28.3.7.4, "Unconfiguring a Keystore Provider"

28.3.7.1 Creating the External WebCenter Domain Keystore

To create the external WebCenter domain keystore:

1. Go to *`JDK_HOME`*`/jdk/bin` and open a command prompt.
2. Using keytool, generate the keystore by importing the WebCenter 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 28–28 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 28–29 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.

4. Export the certificate containing the public key so that it can be imported into the WebCenter 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 28–30 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
```

5. Import the certificate to the WebCenter 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 28–31 Importing the Certificate

```
keytool -importcert -alias external_webcenter_custom_public_key -file external_
webcenter_custom_public_key.cer -keystore webcenter.jks -storepass welcome1
```

6. Continue by configuring the keystore using either WLST as described in Section 28.3.7.2, "Configuring the Keystore Using WLST,", or using Fusion Middleware Control as described in Section 28.3.7.3, "Configuring the Keystore Using Fusion Middleware Control."

28.3.7.2 Configuring the Keystore Using WLST

After creating the external WebCenter 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:

```
createCred(map="oracle.wsm.security", key="keystore-csf-key", user="owsm",
password="welcome1", desc="Keystore key")
createCred(map="oracle.wsm.security", key="enc-csf-key",
user="external_webcenter_custom", password="welcome1", desc="Encryption key")
createCred(map="oracle.wsm.security", key="sign-csf-key",
user="external_webcenter_custom", password="welcome1", desc="Signing key")
```

5. Restart all servers.

28.3.7.3 Configuring the Keystore Using Fusion Middleware Control

If a keystore provider is already configured, you must first unconfigure the existing keystore provider as described in Section 28.3.7.4, "Unconfiguring a Keystore Provider." Otherwise, continue with the steps below.

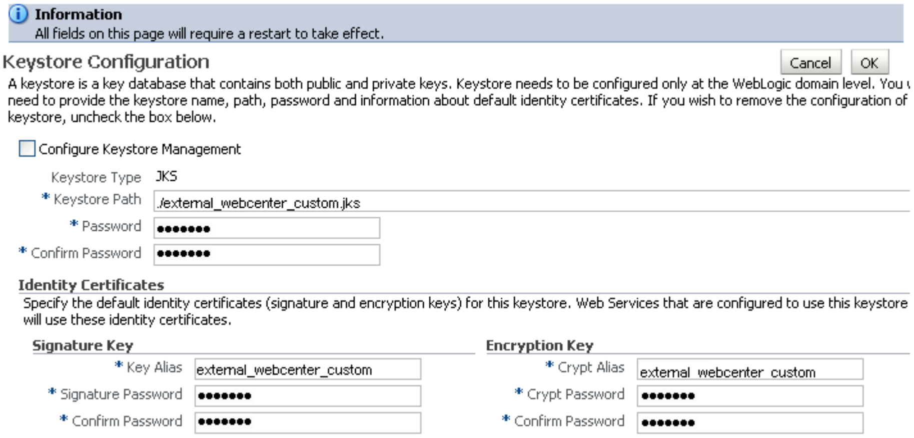
To configure the keystore provider:

1. Open Fusion Middleware Control and log in to the WebCenter domain.

   For information on logging in to 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 WebCenter domain (webcenter 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 28–30).

Figure 28–30 Keystore Configuration Page



Information
All fields on this page will require a restart to take effect.

Keystore Configuration

A keystore is a key database that contains both public and private keys. Keystore needs to be configured only at the WebLogic domain level. You ι need to provide the keystore name, path, password and information about default identity certificates. If you wish to remove the configuration of keystore, uncheck the box below.

□ Configure Keystore Management

Keystore Type JKS
* Keystore Path ./external_webcenter_custom.jks
* Password •••••••
* Confirm Password •••••••

Identity Certificates

Specify the default identity certificates (signature and encryption keys) for this keystore. Web Services that are configured to use this keystore will use these identity certificates.

Signature Key
* Key Alias external_webcenter_custom
* Signature Password •••••••
* Confirm Password •••••••

Encryption Key
* Crypt Alias external_webcenter_custom
* Crypt Password •••••••
* Confirm Password •••••••

6. Check **Configure Keystore Management** and 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.

28.3.7.4 Unconfiguring a Keystore Provider

If a keystore provider is already configured, you must unconfigure the existing keystore provider before configuring a new provider. If a keystore provider is not already configured, continue with the steps to configure the keystore in Section 28.3.7.3, "Configuring the Keystore Using Fusion Middleware Control."

To unconfigure a keystore provider using Fusion Middleware Control:

1. Open Fusion Middleware Control and log in to the target domain.

   For information on logging in to Fusion Middleware Control, see Section 6, "Starting Enterprise Manager Fusion Middleware Control."

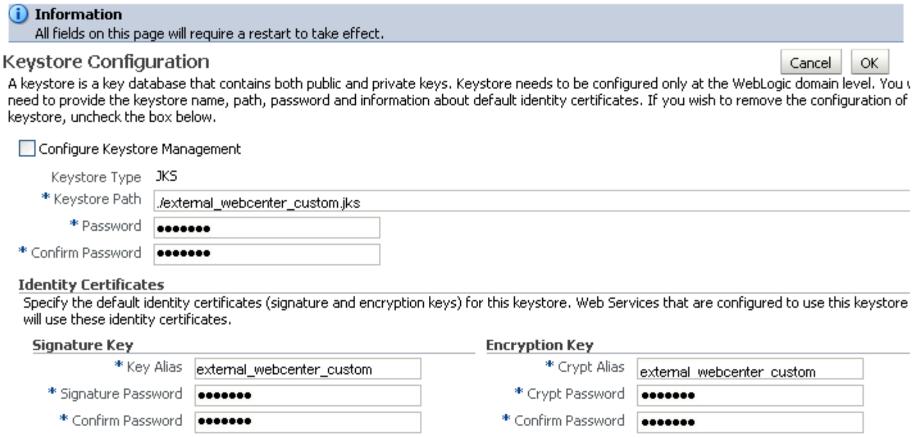
2. From the WebLogic Domain menu, select **Security -> Security Provider Configuration**.

3. Expand the Keystore section on the Security Provider Configuration page.

4. Click **Configure**.

   The Keystore Configuration page displays (see Figure 28–31).

Figure 28–31 Keystore Configuration Page



Information
All fields on this page will require a restart to take effect.

Keystore Configuration

A keystore is a key database that contains both public and private keys. Keystore needs to be configured only at the WebLogic domain level. You need to provide the keystore name, path, password and information about default identity certificates. If you wish to remove the configuration of keystore, uncheck the box below.

□ Configure Keystore Management

Keystore Type JKS
* Keystore Path ./external_webcenter_custom.jks
* Password ●●●●●●●
* Confirm Password ●●●●●●●

Identity Certificates
Specify the default identity certificates (signature and encryption keys) for this keystore. Web Services that are configured to use this keystore will use these identity certificates.

Signature Key
* Key Alias external_webcenter_custom
* Signature Password ●●●●●●●
* Confirm Password ●●●●●●●

Encryption Key
* Crypt Alias external_webcenter_custom
* Crypt Password ●●●●●●●
* Confirm Password ●●●●●●●

5. Uncheck **Configure Keystore Management**.

6. Click **OK**.

28.3.7.5 Calling WebCenter Spaces WebServices

In your client project, where you are setting up the `GroupSpaceWSContext`, set the recipient key alias to be the same as the WebCenter Spaces certificate alias as shown below:

```
GroupSpaceWSContext context = new GroupSpaceWSContext();
context.setRecipientKeyAlias("webcenter_public");
```

28.3.8 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 Domain Keystore

Follow the steps below to configure the service instance reference for the WebCenter 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 Spaces domain as an admin user and run the following commands:

```
createCred(map="oracle.wsm.security", key="keystore-csf-key", user="owsm",
password="welcome1", desc="Keystore key")
createCred(map="oracle.wsm.security", key="enc-csf-key", user="webcenter",
password="welcome1", desc="Encryption key")
createCred(map="oracle.wsm.security", key="sign-csf-key", user="webcenter",
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:

```
createCred(map="oracle.wsm.security", key="keystore-csf-key", user="owsm",
password="welcome1", desc="Keystore key")
createCred(map="oracle.wsm.security", key="enc-csf-key", user="bpel",
password="welcome1", desc="Encryption key")
createCred(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:

   ```
   createCred(map="oracle.wsm.security", key="keystore-csf-key", user="owsm",
   password="welcome1", desc="Keystore key")
   createCred(map="oracle.wsm.security", key="enc-csf-key", user="soa_server3",
   password="welcome1", desc="Encryption key")
   createCred(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 domain:

1. Navigate to the `<DOMAIN_HOME>/config/fmwconfig` directory.
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 admin user and run the following commands:

   ```
   createCred(map="oracle.wsm.security", key="keystore-csf-key", user="owsm",
   password="welcome1", desc="Keystore key")
   createCred(map="oracle.wsm.security", key="enc-csf-key",
   user="external_webcenter_custom", password="welcome1", desc="Encryption key")
   createCred(map="oracle.wsm.security", key="sign-csf-key",
   user="external_webcenter_custom", password="welcome1", desc="Signing key")
   ```

Configure the DF Keystore Properties File

Using WLST, connect to the WebCenter Spaces domain as an admin user and run the following commands:

```
org.apache.ws.security.crypto.merlin.keystore.type=jks
org.apache.ws.security.crypto.merlin.keystore.password=welcome1
org.apache.ws.security.crypto.merlin.keystore.alias=df_webcenter_public
org.apache.ws.security.crypto.merlin.file=<dir_containing_keystore>/owc_discussion
s.jks
```

> **Note:** Be sure to trim any trailing spaces from the line endings. If you are working in a Windows environment, also be sure to use "\\" as the file path separator.

Additional DF Connection properties are shown in Table 28–2.

Table 28–8 Additional DF Connection Properties

Property Name	Property Value	Secured
`keystore.location`	`<webcenter_spaces_doamin_home>/config/fmwconfig/webcenter.jks`	No
`keystore.type`	`jks`	No
`keystore.password`	`welcome1`	Yes

Table 28–8 (Cont.) Additional DF Connection Properties

Property Name	Property Value	Secured
encryption.key.alias	webcenter	No
encryption.key.password	welcome1	Yes
group.mapping	category	No

28.4 Securing Oracle WebLogic Communication Services (OWLCS) with WS-Security

Follow the steps below to configure WS-Security for Oracle WebLogic Communication Services (OWLCS):

1. Provide the **policyURI** when creating the Instant Messaging and Presence (IMP) connection.

   When you create the connection to the WS-Security enabled OWLCS server, you must provide the `policyURI`. The value of `policyURI` should be set to `oracle/wss11_saml_token_with_message_protection_client_policy`. If no `policyURI` is supplied, the application uses a non-secure connection. See also Section 14.1, "What You Should Know About Instant Messaging and Presence Connections."

2. Supply an alias name for the private key to the IMP connection.

   Provide an additional property in the WebCenter IMP connection named `recipient.alias`. Set the value of this property to the alias under which to import the OWLCS certificate. Ensure that this value is unique and is not used already by some other service. If no alias name is supplied, the application uses the default value `webcenter_owlcs`. See also Section 14.3, "Registering Instant Messaging and Presence Servers."

3. Determine the private key in the OWLCS keystore (located on the OWLCS instance at `DOMAIN_HOME/config/fmwconfig`).

   Use the following command to list the keystore contents:

   ```
   keytool -list -v -keystore Serversidekeystore.jks -storepass password
   ```

   Find the entry with the Entry type set to `keyEntry`. The alias name of this entry is the private key (`orakey` by default).

4. Export the private key from the OWLCS server keystore.

   Use the following command to export `orakey` to a certificate file (for example, `orakey.cer`).

   ```
   keytool -exportcert -v -alias orakey -keystore Serversidekeystore.jks
   -storepass welcome -rfc -file orakey.cer
   ```

5. Determine the private key in the WebCenter keystore (on the WebCenter instance at `DOMAIN_HOME/config/fmwconfig`).

   If no keystore is found, proceed to step 6. Otherwise, use the following command to list the keystore contents:

   ```
   keytool -list -v -keystore default-keystore.jks -storepass welcome
   ```

Find the entry with Entry type set to `keyEntry` or `PrivateKeyEntry`. The alias name of this entry is the private key.

If no such entry is found, proceed to step 6. Otherwise, continue at step 7.

6. Generate a private key on WebCenter.

   Go to `DOMAIN_HOME/config/fmwconfig` in your WebCenter installation and run the following command to add a key pair to the keystore. The command creates a keystore named `default-keystore.jks` if it does not exist, and adds a new private key entry with alias `orasig` and the password set to `welcome1`. You can optionally change the alias, password and domain name command when you run the command.

   ```
   keytool -genkeypair -keyalg RSA -dname "cn=consumer,dc=example,dc=com"
   -alias orasig -keypass welcome1 -keystore default-keystore.jks
   -storepass welcome1 -validity 360
   ```

7. Configure OWLCS on your WebCenter instance to use the private key.

   Run the WLST `createCred` command substituting the values for `user` and `password` in the first two commands with your private key alias and password.

   ```
   createCred(map='oracle.wsm.security', key='enc-csf-key', user='orasig',
   password='welcome1', desc='EncryptionKey')

   createCred(map='oracle.wsm.security', key='sign-csf-key', user='orasig',
   password='welcome1', desc='SigningKey')

   createCred(map='oracle.wsm.security', key='keystore-csf-key', user='owsm',
   password='welcome1', desc='KeystoreKey')
   ```

8. Export the private key pair to a certificate.

   Export the private key found in step 5 or created in step 6 to a certificate file using the following command:

   ```
   keytool -exportcert -v -alias orasig -keystore default-keystore.jks -storepass
   welcome1 -rfc -file orasig.cer
   ```

9. Import the certificate generated on the OWLCS Server to the WebCenter keystore.

   Copy the certificate generated in step 4 to a temporary location on the WebCenter instance. Import the certificate in the WebCenter instance using the alias name from step 2.

   Use the following command to import the certificate in the WebCenter keystore:

   ```
   keytool -importcert -alias webcenter_owlcs -file orakey.cer -keystore
   default-keystore.jks -storepass welcome1
   ```

10. Import the WebCenter certificate on the OWLCS instance.

    Copy the certificate created in step 8 to a temporary location on the OWLCS instance. Go to `DOMAIN_HOME/config/fmwconfig` and import the certificate in the keystore under a meaningful alias (for example, `webcenter_key`) using the following command:

    ```
    keytool -importcert -alias webcenter_key -file orasig.cer -keystore
    Serversidekeystore.jks -storepass welcome
    ```

28.5 Securing WebCenter Spaces for Applications Consuming Spaces Client APIs with WS-Security

This section describes the administrator tasks required to configure WS-Security for WebCenter Spaces so that the communication between the an application exposing WebCenter Spaces APIs (the consumer) and WebCenter Spaces (the producer) is secure, and that the identity of the user invoking the APIs is protected.

You must create a Java keystore and update the credential store so that WebCenter Spaces can verify the authenticity of the SAML-based security tokens received from your application. You must then register this keystore and update the credential store. For information about the developer tasks for developing applications that consume WebCenter Spaces client APIs, see "How to Set Up Your Custom WebCenter Application to Use the WebCenter Spaces APIs" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*.

This section includes the following subsections:

- Section 28.5.1, "Generating the Keystores"
- Section 28.5.2, "Providing the Keystores and Keystore Information to the Application Developer"
- Section 28.5.3, "Registering the Keystores"
- Section 28.5.4, "Updating the Credential Stores"

28.5.1 Generating the Keystores

Follow the steps below to generate Java keystores for the consumer (the custom WebCenter application) and producer (WebCenter Spaces).

To generate keystores for the consumer and producer:

1. Go to *JDK_HOME*/jdk/bin and open a command prompt.
2. Using keytool, generate a key pair:

```
keytool -genkeypair -keyalg RSA -dname "consumer_dname" -alias consumer_alias
-keypass key_password
-keystore keystore -storepass keystore_password -validity days_valid
```

Where:

- *consumer_dname* is the distinguished name of the consumer (for example, cn=consumer,dc=example,dc=com). The value could be anything but typically matches the distinguished name (DN) of the machine on which the keystore would reside.
- *consumer_alias* is the alias of the consumer (for example, consumer)
- *key_password* is the password for the new public key, (for example, welcome1)
- *keystore* is the keystore name, (for example, consumer.jks)
- *keystore_password* is the keystore password, (for example, welcome1)
- *days_valid* is the number of days for which the key password is valid (for example, 360).

Note: You must use the `-keyalg` parameter and specify `RSA` as its value as shown above as the default algorithm (DSA) used by `keytool` for generating the key is incompatible with Oracle WebServices Security Manager requirements.

3. Export the public key for the consumer:

```
keytool -exportcert -v -alias consumer_alias -keystore keystore -storepass
keystore_password -rfc -file certificate_file
```

   Where:

   - *`consumer_alias`* is the alias of the consumer (for example, `consumer`)
   - *`keystore`* is the keystore name, (for example, `consumer.jks`)
   - *`keystore_password`* is the keystore password, (for example, `welcome1`)
   - *`certificate_file`* is the file name for the certificate to export the key to (for example, `consumer.cer`)

4. Generate the producer keystore by importing the trusted certificate of the consumer:

```
keytool -importcert -alias consumer_alias -file certificate_file -keystore
keystore -storepass keystore_password
```

   Where:

   - *`consumer_alias`* is the alias of the consumer
   - *`certificate_file`* is the certificate file name
   - *`keystore`* is the keystore name
   - *`keystore_password`* is the keystore password

5. Generate the key pair for the producer:

```
keytool -genkeypair -keyalg RSA -dname "producer_dname" -alias producer_alias
-keypass key_password -keystore keystore -storepass keystore_password -validity
days_valid
```

   Where:

   - *`producer_dname`* is the name of the producer (for example, `cn=producer,dc=example,dc=com`)
   - *`producer_alias`* is the alias of the producer (for example, `producer`)
   - *`key_password`* is the password for the new public key, (for example, `welcome1`)
   - *`keystore`* is the keystore name, (for example, `producer.jks`)
   - *`keystore_password`* is the keystore password, (for example, `welcome1`)
   - *`days_valid`* is the number of days for which the key password is valid (for example, `1024`)

Note: You must use the `-keyalg` parameter and specify `RSA` as its value as shown above as the default algorithm (DSA) used by keytool for generating the key will not work.

6. List the contents of the keystore:

   ```
   keytool -list -v -keystore keystore_name -storepass password
   ```

   Where:

   - *keystore_name* is the name of the consumer keystore file (for example, `portal.jks`)
   - *password* is the keystore password.

   The keystore should now have two key entries.

7. Export the public key of the producer:

   ```
   keytool -exportcert -v -alias producer_alias -keystore keystore -storepass
   keystore_password -rfc -file certificate_file
   ```

   Where:

   - *producer_alias* is the alias of the producer (for example, `producer`)
   - *keystore* is the keystore name (for example, `producer.jks`)
   - *keystore_password* is the keystore password, (for example,`welcome1`
   - *certificate_file* is the certificate file name (for example, `producer.cer`)

8. Import the trusted certificate of the producer:

   ```
   keytool -importcert -alias producer_alias -file certificate_file -keystore
   keystore_name -storepass keystore_password
   ```

   Where:

   - *producer_alias* is the alias of the producer (for example, `producer`)
   - *certificate_file* is the file name or path for the producer's certificate file (for example,`../producer/producer.cer`)
   - *keystore_name* is the keystore name (for example, `consumer.jks`)
   - *keystore_password* is the keystore password, (for example, `welcome1`)

28.5.2 Providing the Keystores and Keystore Information to the Application Developer

Before registering the keystores, ensure that you have provided the following to the developer who is creating the application that will be consuming the WebCenter Spaces APIs:

- The consumer keystore to be used to secure the connection. This is a `.jks` file (for example, `consumer.jks`).
- The consumer public alias key stored in the keystore (for example, `consumer`).
- The password of the consumer public alias key (for example, `welcome1`).
- The producer public alias key stored in the consumer keystore (for example, `producer`). This is the alias used when importing the trusted certificate of the producer, and created in step 8 of Section 28.5.1, "Generating the Keystores."
- The consumer keystore password (for example, `welcome1`).

28.5.3 Registering the Keystores

After you have created the keystores, configure the keystore for WS-Security by performing the following steps. If a keystore provider is already configured, unconfigure the existing keystore provider before proceeding as described in Section 28.1.1.4, "Unconfiguring a Keystore Provider Using Fusion Middleware Control."

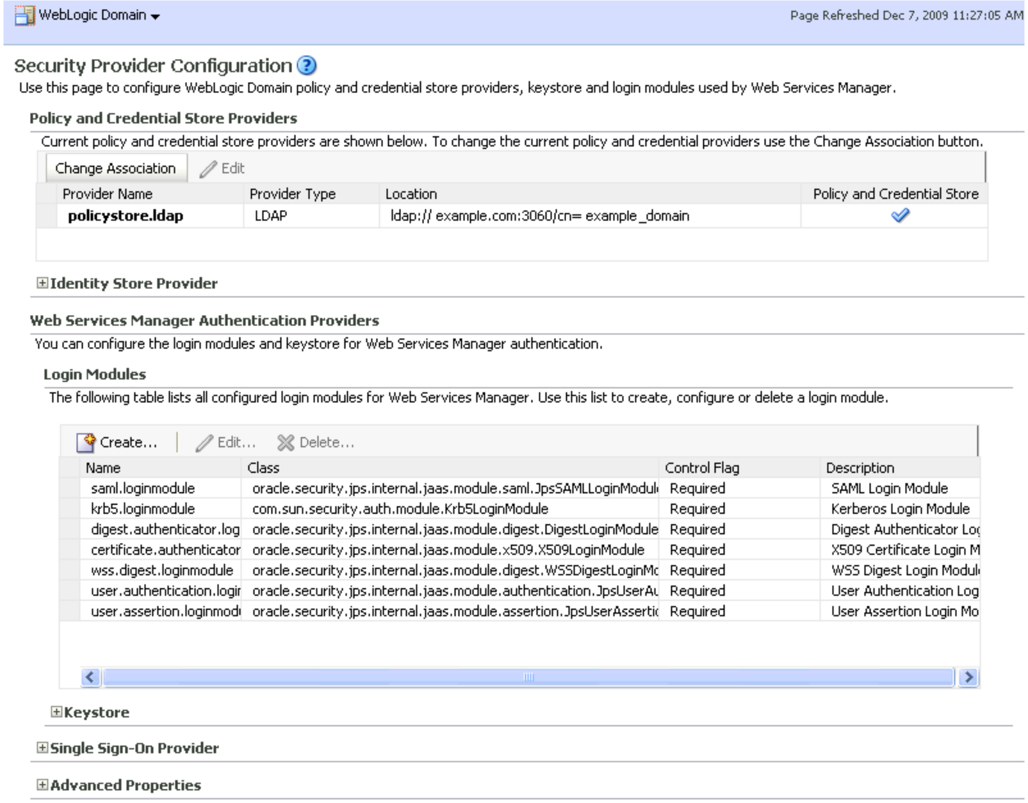
To register the keystore provider:

1. Copy the `producer.jks` file to the file system where your producer application is running (for example, `DOMAIN_HOME/config/fmwconfig`).
2. Log in to Fusion Middleware Control.

   For information on logging in to 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 domain (for example, `webcenter`).
4. From the WebLogic Domain menu, select **Security -> Security Provider Configuration**.

   The Security Provider Configuration page displays (see Figure 28–32).

Figure 28–32 Security Provider Configuration Page



Page Refreshed Dec 7, 2009 11:27:05 AM

Security Provider Configuration

Use this page to configure WebLogic Domain policy and credential store providers, keystore and login modules used by Web Services Manager.

Policy and Credential Store Providers

Current policy and credential store providers are shown below. To change the current policy and credential providers use the Change Association button.

Provider Name	Provider Type	Location	Policy and Credential Store
policystore.ldap	LDAP	ldap:// example.com:3060/cn= example_domain	✓

⊞ Identity Store Provider

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.JpsSAMLLoginModul	Required	SAML 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 Lo
certificate.authenticator	oracle.security.jps.internal.jaas.module.x509.X509LoginModule	Required	X509 Certificate Login M
wss.digest.loginmodule	oracle.security.jps.internal.jaas.module.digest.WSSDigestLoginMo	Required	WSS Digest Login Modul
user.authentication.logir	oracle.security.jps.internal.jaas.module.authentication.JpsUserAu	Required	User Authentication Log
user.assertion.loginmod	oracle.security.jps.internal.jaas.module.assertion.JpsUserAsserti	Required	User Assertion Login Mo

⊞ Keystore

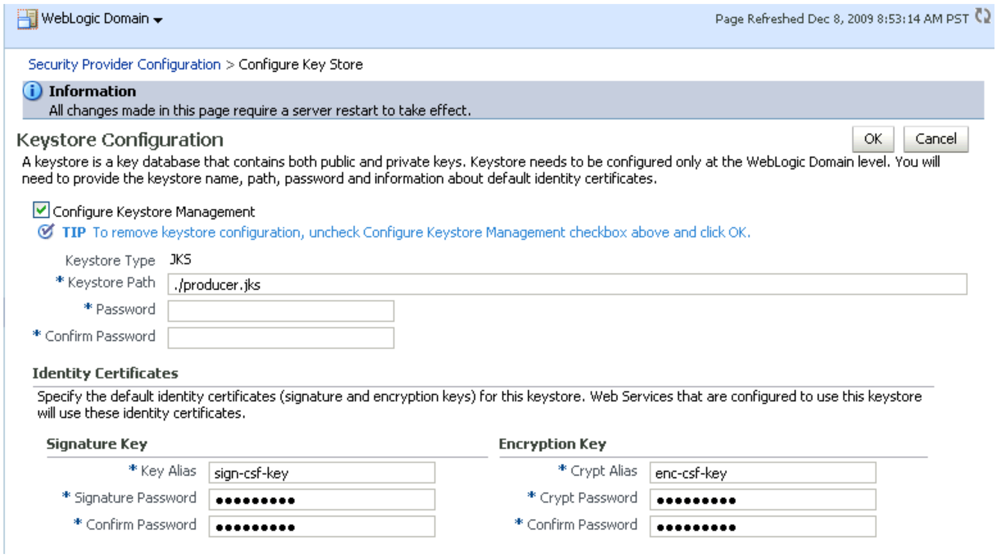
⊞ Single Sign-On Provider

⊞ Advanced Properties

5. Expand the Keystore section on the Security Provider Configuration page.
6. Click **Configure**.

   The Keystore Configuration page displays (see Figure 28–33).

Figure 28–33 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

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.

☑ Configure Keystore Management

TIP To remove keystore configuration, uncheck Configure Keystore Management checkbox above and click OK.

Keystore Type JKS
* Keystore Path ./producer.jks
* Password
* Confirm Password

Identity Certificates

Specify the default identity certificates (signature and encryption keys) for this keystore. Web Services that are configured to use this keystore will use these identity certificates.

Signature Key
* Key Alias sign-csf-key
* Signature Password ●●●●●●●●●
* Confirm Password ●●●●●●●●●

Encryption Key
* Crypt Alias enc-csf-key
* Crypt Password ●●●●●●●●●
* Confirm Password ●●●●●●●●●

7. In the **Keystore Path** field, specify the location of the keystore that contains the certificate and private key that is used for signing some parts (security token and SOAP message body) of the SOAP message, and enter and confirm the keystore **Password**.
8. In the Signature Key section, enter `sign-csf-key` as the **Key Alias**, and enter and confirm the signature key **Password** (the value used for *<key_password>* above) for the new public key, (for example, `welcome1`).
9. In the Encryption Key section, enter `enc-csf-key` in the **Crypt Alias** field, and enter and confirm the encryption key **Password** (the value used for *<key_password>* above) for the new public key, (for example, `welcome1`).
10. Click **OK** to save your settings.
11. Restart the Administration server for the domain.

28.5.4 Updating the Credential Stores

Follow the steps below to update the credential stores from the command line using WLST, or using Fusion Middleware Control.

This section contains the following subsections:

- Section 28.5.4.1, "Updating the Credential Store Using WLST"
- Section 28.5.4.2, "Updating the Credential Store Using Fusion Middleware Control"

28.5.4.1 Updating the Credential Store Using WLST

Update the credential store using the WLST `createCred` command. Use the following example values to add the `keystore-csf-key`, `enc-csf-key`, and `sign-csf-key` encryption keys. Before running the command, be sure to back up the `cwallet.sso` file.

Example 28–32 keystore-csf-key

```
createCred(map="oracle.wsm.security",key="keystore-csf-key",user="keystore-csf-key
",password="welcome1",desc="Keystore Password")
```

Example 28–33 enc-csf-key

```
createCred(map="oracle.wsm.security",key="enc-csf-key",user="producer",password="w
elcome1",desc="Enc Password")
```

Example 28–34 sign-csf-key

```
createCred(map="oracle.wsm.security",key="sign-csf-key",user="producer",password="
welcome1",desc="Enc Password")
```

28.5.4.2 Updating the Credential Store Using Fusion Middleware Control

1. Log in to Fusion Middleware Control.

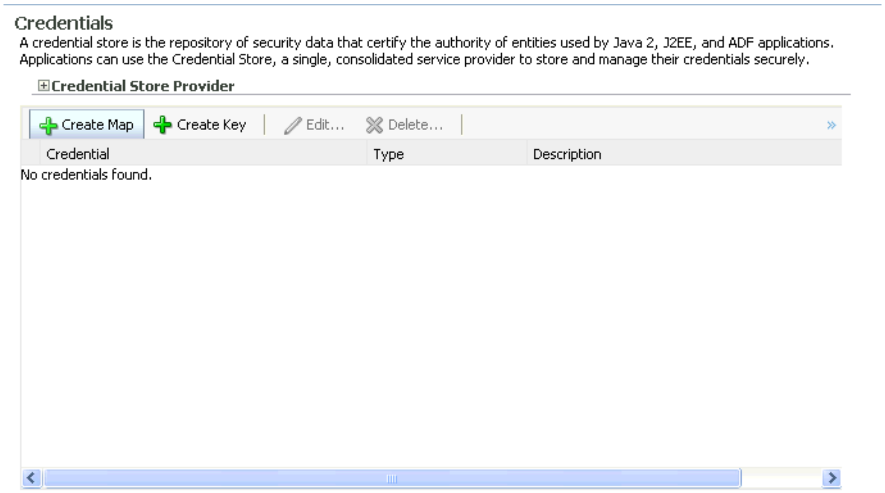
   For information on logging in to Fusion Middleware Control, see Section 6, "Starting Enterprise Manager Fusion Middleware Control."

2. In the Navigation pane, expand the WebLogic Domain node and click the domain (for example, `webcenter`).

3. From the WebLogic Domain menu, select **Security -> Credentials**.

   The Credentials page displays (see Figure 28–34).

Figure 28–34 Credentials Page



Credentials

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

⊞Credential Store Provider

Credential	Type	Description

No credentials found.

4. Click **Create Map**.

5. On the Create Map pop-up, enter `oracle.wsm.security` as the map name and click **OK**.

6. Click **Create Key**.

7. On the Create Key pop-up, select `oracle.wsm.security` as the map, enter `keystore-csf-key` as the **Key**, select `Password` as the **Type**, enter `keystore-csf-key` as the **User Name**, supply the **Password** (in this case, the keystore password of `producer.jks`) from when you created the keystores (for example, `welcome1`), enter an optional description, and click **OK**.

8. Click **Create Key**.

9. On the Create Key pop-up, select `oracle.wsm.security` as the map, enter `sign-csf-key` as the **Key**, select `Password` as the **Type**, enter the public key alias of the keystore used in the custom WebCenter application as the **User Name**,

enter the password of the public key used in the custom WebCenter application as the **Password**, enter an optional description, and click **OK**.

10. Click **Create Key**.

11. On the Create Key pop-up, select `oracle.wsm.security` as the map, enter `enc-csf-key` as the **Key**, select `Password` as the **Type**, enter the public key alias of the keystore used in the WebCenter instance (for example, `webcenter)` as the **User Name**, enter the password of the public key used in the custom WebCenter application as the **Password**, enter an optional description, and click **OK**.

12. Restart the Administration server and `WLS_Custom` or managed server on which the custom WebCenter application is hosted.

29

Managing Security for Portlet Producers

This chapter describes how to configure your WebCenter application to handle security for WSRP and JPDK portlet producers.

This chapter includes the following sections:

- Section 29.1, "Securing a WSRP Producer"
- Section 29.2, "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."

29.1 Securing a WSRP Producer

The following sections describe how to secure access to JSR-168 standards-based WSRP portlets from WebCenter applications:

- Section 29.1.1, "Deploying the Producer"
- Section 29.1.2, "Attaching a Policy to the Producer Endpoint"
- Section 29.1.3, "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*.

29.1.1 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 21.8, "Deploying Portlet Producer Applications."

29.1.2 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 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 RSA key mechanisms for message confidentiality, and 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.

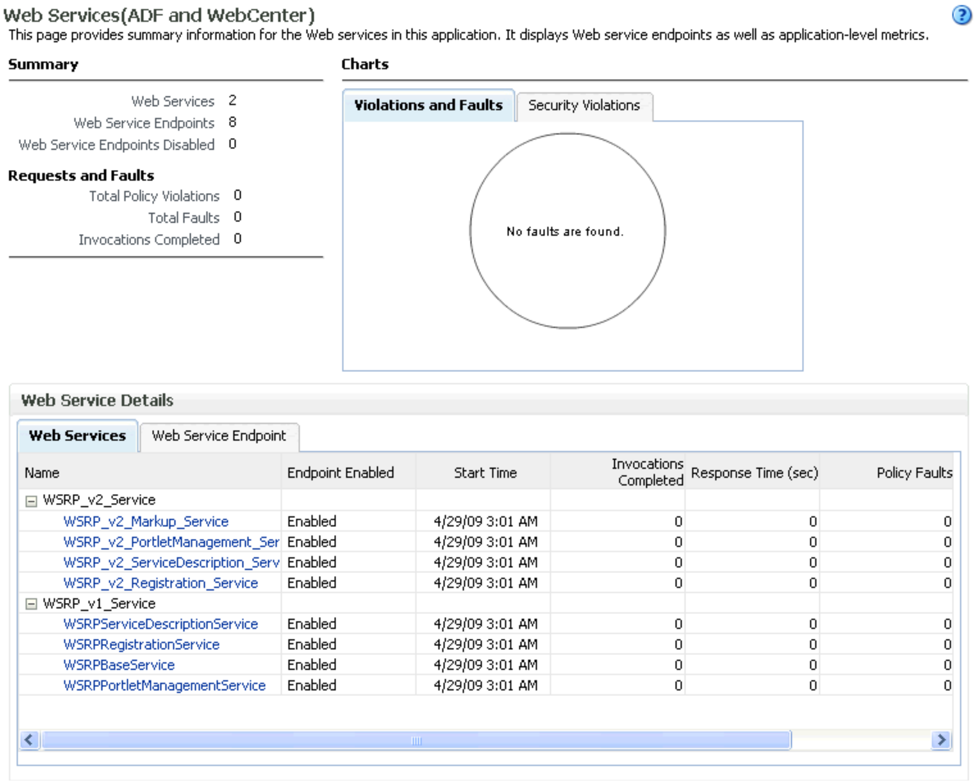
   For information on logging into Fusion Middleware Control, see Section 6, "Starting Enterprise Manager Fusion Middleware Control."

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 29–1).

Figure 29–1 Web Services Summary Page



Web Services(ADF and WebCenter)

This page provides summary information for the Web services in this application. It displays Web service endpoints as well as application-level metrics.

Summary

Web Services 2
Web Service Endpoints 8
Web Service Endpoints Disabled 0

Requests and Faults

Total Policy Violations 0
Total Faults 0
Invocations Completed 0

Charts

Web Service Details

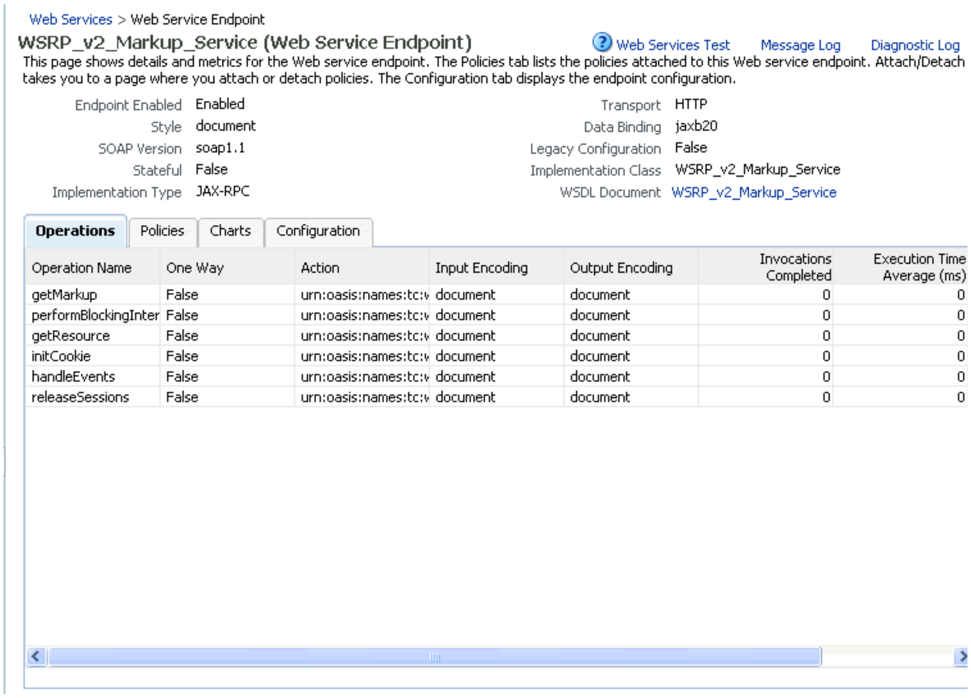
Name	Endpoint Enabled	Start Time	Invocations Completed	Response Time (sec)	Policy Faults
⊟ WSRP_v2_Service					
WSRP_v2_Markup_Service	Enabled	4/29/09 3:01 AM	0	0	0
WSRP_v2_PortletManagement_Ser	Enabled	4/29/09 3:01 AM	0	0	0
WSRP_v2_ServiceDescription_Serv	Enabled	4/29/09 3:01 AM	0	0	0
WSRP_v2_Registration_Service	Enabled	4/29/09 3:01 AM	0	0	0
⊟ WSRP_v1_Service					
WSRPServiceDescriptionService	Enabled	4/29/09 3:01 AM	0	0	0
WSRPRegistrationService	Enabled	4/29/09 3:01 AM	0	0	0
WSRPBaseService	Enabled	4/29/09 3:01 AM	0	0	0
WSRPPortletManagementService	Enabled	4/29/09 3:01 AM	0	0	0

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 29–2).

Figure 29–2 Web Service Endpoints Page



WSRP_v2_Markup_Service (Web Service Endpoint)

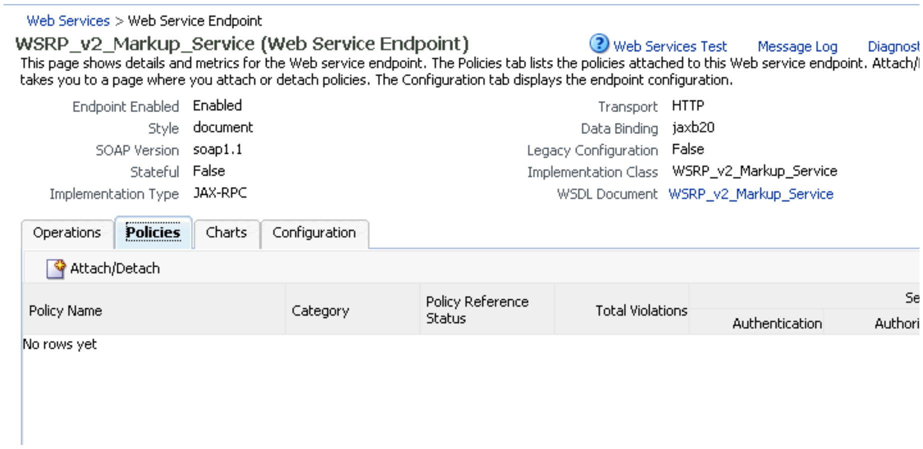
This page shows details and metrics for the Web service endpoint. The Policies tab lists the policies attached to this Web service endpoint. Attach/Detach takes you to a page where you attach or detach policies. The Configuration tab displays the endpoint configuration.

Endpoint Enabled	Enabled	Transport	HTTP
Style	document	Data Binding	jaxb20
SOAP Version	soap1.1	Legacy Configuration	False
Stateful	False	Implementation Class	WSRP_v2_Markup_Service
Implementation Type	JAX-RPC	WSDL Document	WSRP_v2_Markup_Service

Operation Name	One Way	Action	Input Encoding	Output Encoding	Invocations Completed	Execution Time Average (ms)
getMarkup	False	urn:oasis:names:tc:v	document	document	0	0
performBlockingInter	False	urn:oasis:names:tc:v	document	document	0	0
getResource	False	urn:oasis:names:tc:v	document	document	0	0
initCookie	False	urn:oasis:names:tc:v	document	document	0	0
handleEvents	False	urn:oasis:names:tc:v	document	document	0	0
releaseSessions	False	urn:oasis:names:tc:v	document	document	0	0

5. Open the Policies tab to display the currently attached policies for the producer (see Figure 29–3).

Figure 29–3 Web Services Endpoint Policies Page



WSRP_v2_Markup_Service (Web Service Endpoint)

This page shows details and metrics for the Web service endpoint. The Policies tab lists the policies attached to this Web service endpoint. Attach/
takes you to a page where you attach or detach policies. The Configuration tab displays the endpoint configuration.

Endpoint Enabled	Enabled	Transport	HTTP
Style	document	Data Binding	jaxb20
SOAP Version	soap1.1	Legacy Configuration	False
Stateful	False	Implementation Class	WSRP_v2_Markup_Service
Implementation Type	JAX-RPC	WSDL Document	WSRP_v2_Markup_Service

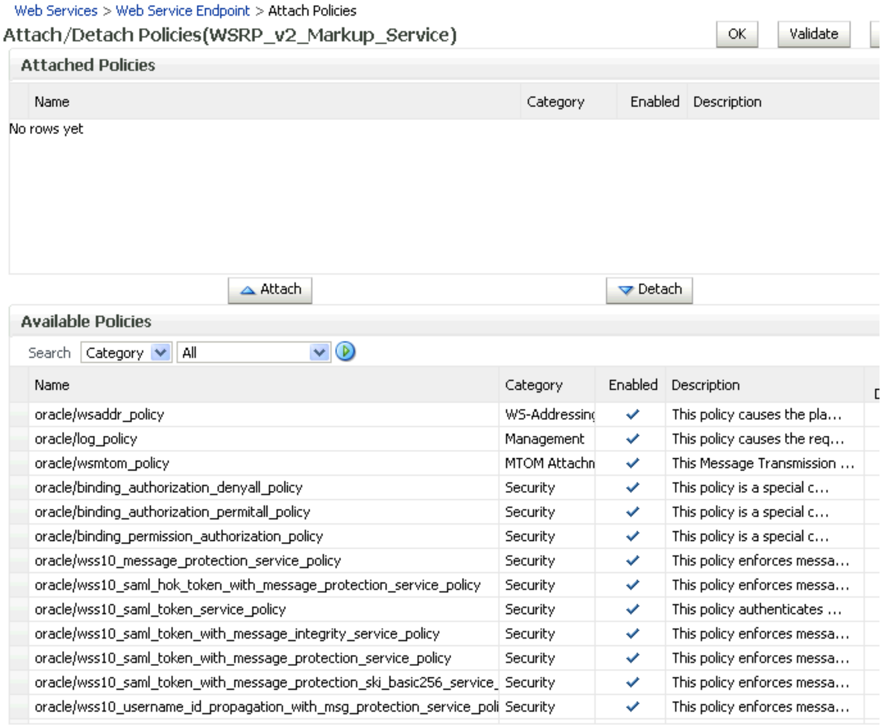
Policy Name	Category	Policy Reference Status	Total Violations	Se	
				Authentication	Authori

No rows yet

6. 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 29–4).

Figure 29–4 Attach/Detach Policies Page


Web Services > Web Service Endpoint > Attach Policies
Attach/Detach Policies(WSRP_v2_Markup_Service)
OK
Validate
Attached Policies
Attach
Detach
Available Policies
Search
Category
All

Name	Category	Enabled	Description

No rows yet

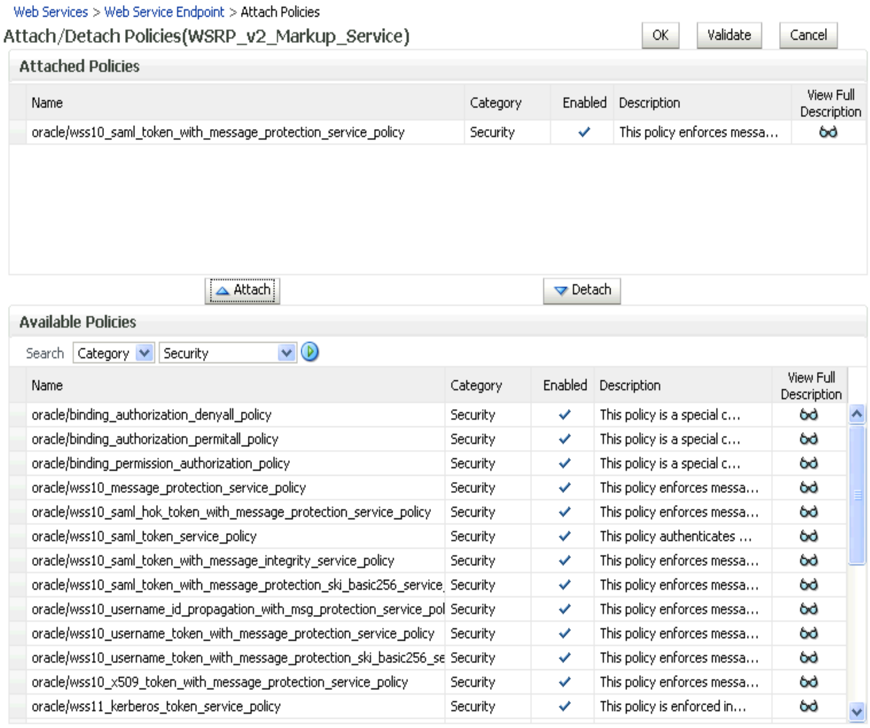
Name	Category	Enabled	Description
oracle/wsaddr_policy	WS-Addressing	✓	This policy causes the pla...
oracle/log_policy	Management	✓	This policy causes the req...
oracle/wsmtom_policy	MTOM Attachn	✓	This Message Transmission ...
oracle/binding_authorization_denyall_policy	Security	✓	This policy is a special c...
oracle/binding_authorization_permitall_policy	Security	✓	This policy is a special c...
oracle/binding_permission_authorization_policy	Security	✓	This policy is a special c...
oracle/wss10_message_protection_service_policy	Security	✓	This policy enforces messa...
oracle/wss10_saml_hok_token_with_message_protection_service_policy	Security	✓	This policy enforces messa...
oracle/wss10_saml_token_service_policy	Security	✓	This policy authenticates ...
oracle/wss10_saml_token_with_message_integrity_service_policy	Security	✓	This policy enforces messa...
oracle/wss10_saml_token_with_message_protection_service_policy	Security	✓	This policy enforces messa...
oracle/wss10_saml_token_with_message_protection_ski_basic256_service_	Security	✓	This policy enforces messa...
oracle/wss10_username_id_propagation_with_msg_protection_service_poli	Security	✓	This policy enforces messa...

7. Under Available Policies, select `Category` and `Security` as the policy category to search, and click the Search icon to list the security policies.

8. 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 29–5).

Figure 29–5 Attach Detach Policy Page with Policy Attached



Attach/Detach Policies(WSRP_v2_Markup_Service)

Attached Policies

Name	Category	Enabled	Description	View Full Description
oracle/wss10_saml_token_with_message_protection_service_policy	Security	✓	This policy enforces messa...	👓

Available Policies

Name	Category	Enabled	Description	View Full Description
oracle/binding_authorization_denyall_policy	Security	✓	This policy is a special c...	👓
oracle/binding_authorization_permitall_policy	Security	✓	This policy is a special c...	👓
oracle/binding_permission_authorization_policy	Security	✓	This policy is a special c...	👓
oracle/wss10_message_protection_service_policy	Security	✓	This policy enforces messa...	👓
oracle/wss10_saml_hok_token_with_message_protection_service_policy	Security	✓	This policy enforces messa...	👓
oracle/wss10_saml_token_service_policy	Security	✓	This policy authenticates ...	👓
oracle/wss10_saml_token_with_message_integrity_service_policy	Security	✓	This policy enforces messa...	👓
oracle/wss10_saml_token_with_message_protection_ski_basic256_service	Security	✓	This policy enforces messa...	👓
oracle/wss10_username_id_propagation_with_msg_protection_service_pol	Security	✓	This policy enforces messa...	👓
oracle/wss10_username_token_with_message_protection_service_policy	Security	✓	This policy enforces messa...	👓
oracle/wss10_username_token_with_message_protection_ski_basic256_se	Security	✓	This policy enforces messa...	👓
oracle/wss10_x509_token_with_message_protection_service_policy	Security	✓	This policy enforces messa...	👓
oracle/wss11_kerberos_token_service_policy	Security	✓	This policy is enforced in...	👓

9. When finished adding polices to attach to the producer endpoint, click **OK**.

29.1.3 Setting Up the Keystores

The steps to create and configure keystores for a WSRP producer depend on the topology of your WebCenter environment, and are covered in the following sections:

- Section 28.1, "Configuring WS-Security for a Simple Topology"
- Section 28.2, "Configuring WS-Security for a Typical Topology"
- Section 28.3, "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.

29.2 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 27.6, "Securing the WebCenter Spaces Connection to Portlet Producers with SSL."

29.2.1 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.

29.2.1.1 Defining a Shared Key Using Fusion Middleware Control

To define a shared key using Fusion Middleware Control:

1. Log into Fusion Middleware Control.

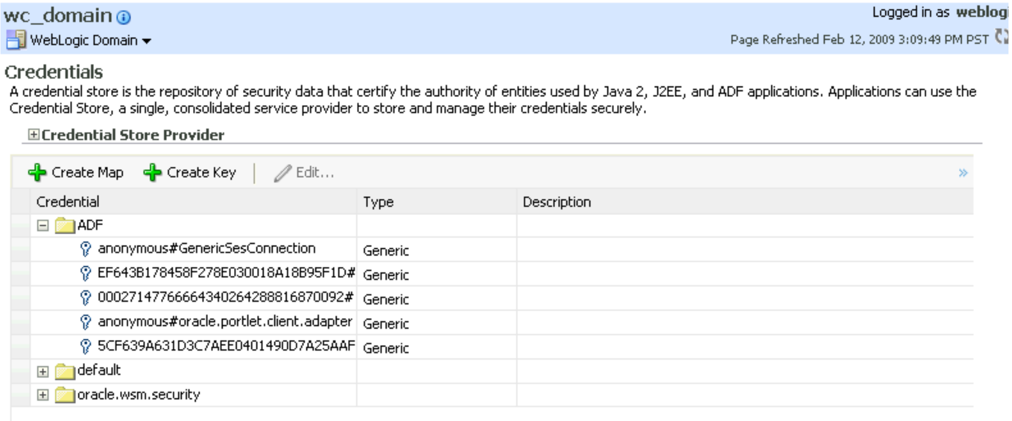
   For information on logging into Fusion Middleware Control, see Section 6, "Starting Enterprise Manager Fusion Middleware Control."

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 29–6).

Figure 29–6 Credentials Pane



wc_domain

WebLogic Domain ▾

Logged in as **weblogi**

Page Refreshed Feb 12, 2009 3:09:49 PM PST

Credentials

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

⊞**Credential Store Provider**

Credential	Type	Description
⊟ ADF		
anonymous#GenericSesConnection	Generic	
EF643B178458F278E030018A18B95F1D#	Generic	
00027147766664340264288816870092#	Generic	
anonymous#oracle.portlet.client.adapter	Generic	
5CF639A631D3C7AEE0401490D7A25AAF	Generic	
⊞ default		
⊞ oracle.wsm.security		

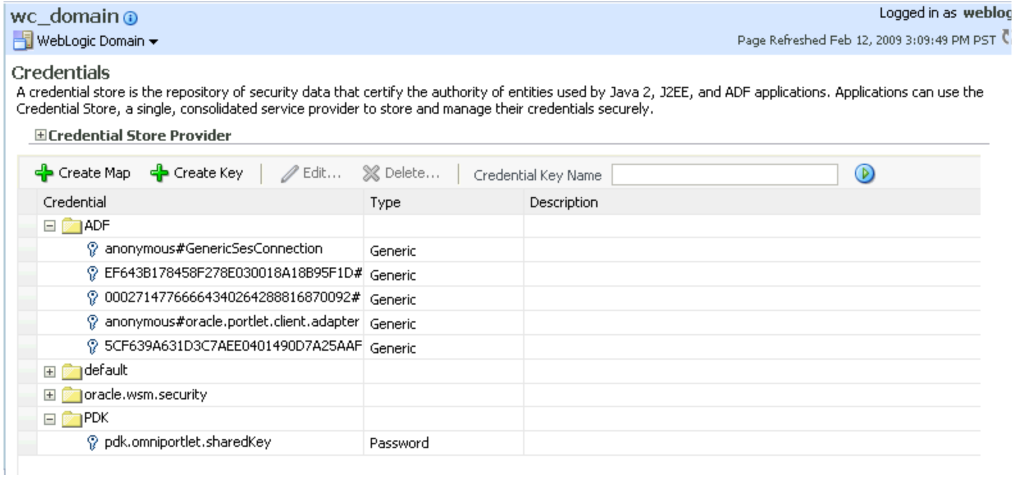
4. Click **Create Map** and enter `PDK` as the **Map Name** and click **OK**.

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 Credential pane (see Figure 29–7).

Figure 29–7 Credentials Pane with New Shared Key



Credentials

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

Credential	Type	Description
ADF		
anonymous#GenericSesConnection	Generic	
EF643B178458F278E030018A18B95F1D#	Generic	
000271477666643402642888168700092#	Generic	
anonymous#oracle.portlet.client.adapter	Generic	
5CF639A631D3C7AEE0401490D7A25AAF	Generic	
default		
oracle.wsm.security		
PDK		
pdk.omniportlet.sharedKey	Password	

29.2.1.2 Defining a Shared Key Using WLST

You can also define a shared key using WLST:

1. Start WLST as described in Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool (WLST) Commands," and connect to the Administration Server instance for the target domain.

2. Connect to the Administration Server for the target domain with the following command:

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

   Where:

   - *user_name* is the name of the user account with which to access the Administration Server (for example, weblogic)
   - *password* is the password with which to access the Administration Server
   - *host_id* is the host ID of the Administration Server
   - *port* is the port number of the Administration Server (for example, `7001`).

3. Add a shared key credential for a producer to the credential store using the WLST `createCred` command:

   ```
   createCred(map='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.

30

Monitoring Oracle WebCenter Performance

Fusion Middleware Control Console provides a Web-based user interface for monitoring the real-time performance of WebCenter applications, including any producers and portlets that WebCenter applications may use.

Performance monitoring helps administrators identify issues and performance bottlenecks in their environment. This chapter describes the range of performance metrics available for WebCenter applications and how to monitor them through Fusion Middleware Control. It also describes how to troubleshoot issues by analyzing information that is recorded in WebCenter diagnostic log files.

Administrators who monitor WebCenter applications regularly will learn to recognize trends as they develop and prevent performance problems in the future.

This chapter includes the following sections:

- Section 30.1, "Understanding WebCenter Performance Metrics"
- Section 30.2, "Viewing Performance Information"
- Section 30.3, "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".

30.1 Understanding WebCenter Performance Metrics

Through Fusion Middleware Control, administrators can monitor the performance and availability of all the components and services that make up WebCenter applications, 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's performance metrics are listed and described here for your reference. Some applications (such as WebCenter Spaces) 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:

- WebCenter Metric Collection: Recent History and Since Startup
- Common WebCenter Metrics

- Common WebCenter Performance Issues and Actions
- WebCenter Service-Specific Metrics
- WebCenter Service-Specific Performance Issues and Actions
- Group Space Metrics

30.1.1 WebCenter Metric Collection: Recent History and Since Startup

Performance metrics are automatically enabled for Oracle WebCenter. In other words, you do not need to set options or perform any extra configuration to collect performance metrics. If you encounter a problem, such as, an application running slowly or hanging, you can view particular metrics to find out more information about the problem as Fusion Middleware Control provides real-time data.

The following metrics are collected for Oracle WebCenter:

- **Since Startup**: At any given time, real-time metrics are available for the duration for which the WebLogic Server hosting WebCenter applications is up and running. Real-time metrics that are collected or aggregated since the startup of the container are displayed for WebCenter as **Since Startup**. These metrics provide data aggregated over the 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 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 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.

30.1.2 Common WebCenter Metrics

Fusion Middleware Control provides capabilities to monitor performance of WebCenter Services in the following ways:

- Services summary: Summary of performance metrics for each service used in a WebCenter application. Table 30–1 lists services that use common performance metrics. Table 30–2 describes service metrics.
- Most popular operations and response time for individual service operations. Table 30–3 describes these metrics.
- Per operation metrics: Performance metrics for individual service operations. Table 30–1 lists common performance metrics used to monitor performance of individual operations. Table 30–3 describes these metrics.

Table 30–1 Common Performance Metrics

Service	Services Summary (Since Startup and Recent History)	Per Operation Metrics (Since Startup and Recent History)
Announcements	The performance metrics include: ■ Status ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms)	The performance metrics include: ■ Most Popular Operations ■ Response Time ■ Invocations ■ Average Time (ms) ■ Maximum Time (ms) (Since Startup only)
BPEL Worklist	The performance metrics include: ■ Status ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms)	Not applicable
Discussion Forums	The performance metrics include: ■ Status ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms)	The performance metrics include: ■ Most Popular Operations ■ Response Time ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms) ■ Maximum Time (ms) (Since Startup only)

Table 30–1 (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: ■ Status ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms)	The performance metrics include: ■ Most Popular Operations ■ Response Time ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms) ■ Maximum Time (ms) (Since Startup only)
Events	The performance metrics include: ■ Status ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms)	The performance metrics include: ■ Most Popular Operations ■ Response Time ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms) ■ Maximum Time (ms) (Since Startup only)
Import/Export	The performance metrics include: ■ Status ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms)	The performance metrics include: ■ 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: ■ Status ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms)	The performance metrics include: ■ Most Popular Operations ■ Response Time ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms) ■ Maximum Time (ms) (Since Startup only)

Table 30–1 (Cont.) Common Performance Metrics

Service	Services Summary (Since Startup and Recent History)	Per Operation Metrics (Since Startup and Recent History)
Lists	The performance metrics include: ■ Status ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms)	The performance metrics include: ■ Most Popular Operations ■ Response Time ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms) ■ Maximum Time (ms) (Since Startup only)
Mail	The performance metrics include: ■ Status ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms)	The performance metrics include: ■ Most Popular Operations ■ Response Time ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms) ■ Maximum Time (ms) (Since Startup only)
Notes	The performance metrics include: ■ Status ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms)	The performance metrics include: ■ Most Popular Operations ■ Response Time ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms) ■ Maximum Time (ms) (Since Startup only)
Pages	The performance metrics include: ■ Status ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms)	The performance metrics include: ■ Most Popular Operations ■ Response Time ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms) ■ Maximum Time (ms) (Since Startup only)

Table 30–1 (Cont.) Common Performance Metrics

Service	Services Summary (Since Startup and Recent History)	Per Operation Metrics (Since Startup and Recent History)
Recent Activity	The performance metrics include: ■ Status ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms)	Not available
RSS	The performance metrics include: ■ Status ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms)	Not available
Search	The performance metrics include: ■ Status ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms)	The performance metrics include: ■ Most Popular Operations ■ Response Time ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms) ■ Maximum Time (ms) (Since Startup only)

Table 30–2 describes metrics used for monitoring performance of all operations.

Table 30–2 Description of Common Metrics - Summary (All Operations)

Metric	Description
Status	The current status of the service: ■ **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 application for some reason.
Successful Invocations (%)	Percentage of a service invocations that succeeded. Successful Invocations (%) equals the number of successful invocations divided by the invocation count: - Since Startup - Recent History If Successful Invocations (%) is below 100%, check the diagnostic logs to establish why service requests are failing. See, Section 30.3, "Viewing and Configuring Log Information".

Table 30–2 (Cont.) Description of Common Metrics - Summary (All Operations)

Metric	Description
Invocations	This metric shows number of service invocations per minute: - 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 Services in the application.
Average Time (ms)	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. - Since Startup - Recent History

Table 30–3 describes metrics used to monitor performance of each operation performed by a service or component.

Table 30–3 Description of Common Metrics - Per Operation

Metric	Description
Most Popular Operations	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.
Response Time	The average time to process operations associated with a service since the WebCenter 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.
Operation	The operation being monitored. See also, Section 30.1.4, "WebCenter Service-Specific Metrics".
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 Web 2.0 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.

30.1.3 Common WebCenter Performance Issues and Actions

This section provides information on 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 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.

30.1.4 WebCenter Service-Specific Metrics

This section describes *per operation* metrics for all services and components. This section includes the following sub sections:

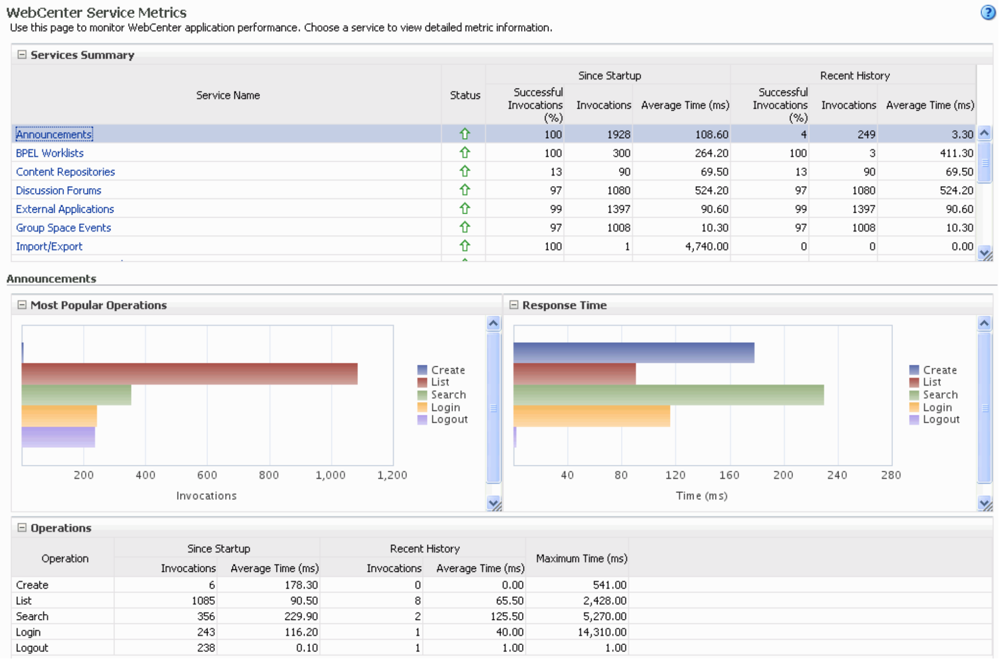
- Announcements Metrics
- BPEL Worklist Metrics
- Content Repository (Documents Service) Metrics
- Discussions Metrics
- External Application Metrics
- Events Metrics
- Instant Messaging and Presence (IMP) Metrics
- Import and Export Metrics
- List Metrics
- Mail Metrics
- Note Metrics
- Page Metrics
- Portlet Producer Metrics
- Portlet Metrics
- RSS News Feed Metrics
- Recent Activity Metrics
- Search Metrics

To access live performance metrics for your WebCenter application, see Section 30.2, "Viewing Performance Information."

30.1.4.1 Announcements Metrics

Performance metrics associated with the Announcements service (Figure 30–1) are described in Table 30–4 and Section 30.1.2, "Common WebCenter Metrics."

Figure 30–1 Announcement Metrics



WebCenter Service Metrics

Use this page to monitor WebCenter application performance. Choose a service to view detailed metric information.

Services Summary

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

Announcements

Operations

Operation	Since Startup		Recent History		Maximum Time (ms)
	Invocations	Average Time (ms)	Invocations	Average Time (ms)	
Create	6	178.30	0	0.00	541.00
List	1085	90.50	8	65.50	2,428.00
Search	356	229.90	2	125.50	5,270.00
Login	243	116.20	1	40.00	14,310.00
Logout	238	0.10	1	1.00	1.00

To monitor these metrics through Fusion Middleware Control, see Section 30.2, "Viewing Performance Information."

Table 30–4 Announcements Service - Operations Monitored

Operation	Description	Performance Issues - User Action
Login	Logs a WebCenter user (accessing the Announcements service) into the discussions server that is hosting announcements.	For service-specific causes, see Section 30.1.5.1, "Announcements Service." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."
Logout	Logs a WebCenter user out of the discussions server that is hosting announcements.	For service-specific causes, see Section 30.1.5.1, "Announcements Service." For common causes, see Section 30.1.3, "Common WebCenter 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 30.1.5.1, "Announcements Service." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."

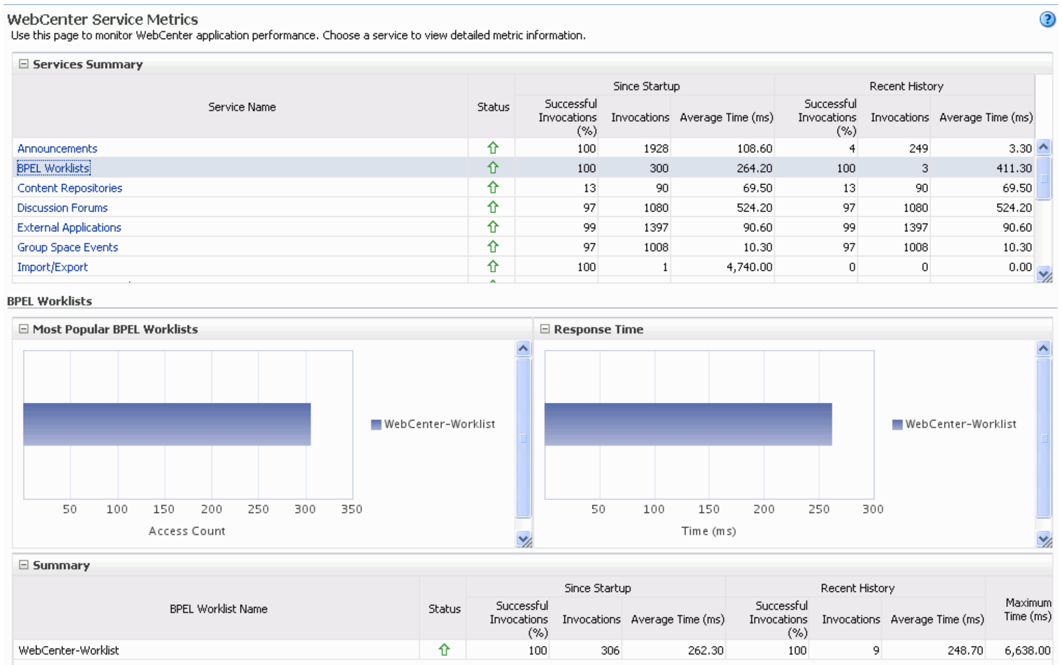
Table 30–4 (Cont.) Announcements Service - Operations Monitored

Operation	Description	Performance Issues - User Action
Create	Creates an announcement.	For service-specific causes, see Section 30.1.5.1, "Announcements Service.". For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."
List	Retrieves a list of announcements.	For service-specific causes, see Section 30.1.5.1, "Announcements Service." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."

30.1.4.2 BPEL Worklist Metrics

Performance metrics associated with the BPEL Worklist service (Figure 30–2) are described in Section 30.1.2, "Common WebCenter Metrics."

Figure 30–2 BPEL Worklist Metrics



WebCenter Service Metrics

Use this page to monitor WebCenter application performance. Choose a service to view detailed metric information.

⊟ Services Summary

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

BPEL Worklists

⊟ Most Popular BPEL Worklists

⊟ Response Time

⊟ Summary

BPEL Worklist Name	Status	Since Startup			Recent History			Maximum Time (ms)
		Successful Invocations (%)	Invocations	Average Time (ms)	Successful Invocations (%)	Invocations	Average Time (ms)	
WebCenter-Worklist	⇧	100	306	262.30	100	9	248.70	6,638.00

To monitor these metrics through Fusion Middleware Control, see Section 30.2, "Viewing Performance Information."

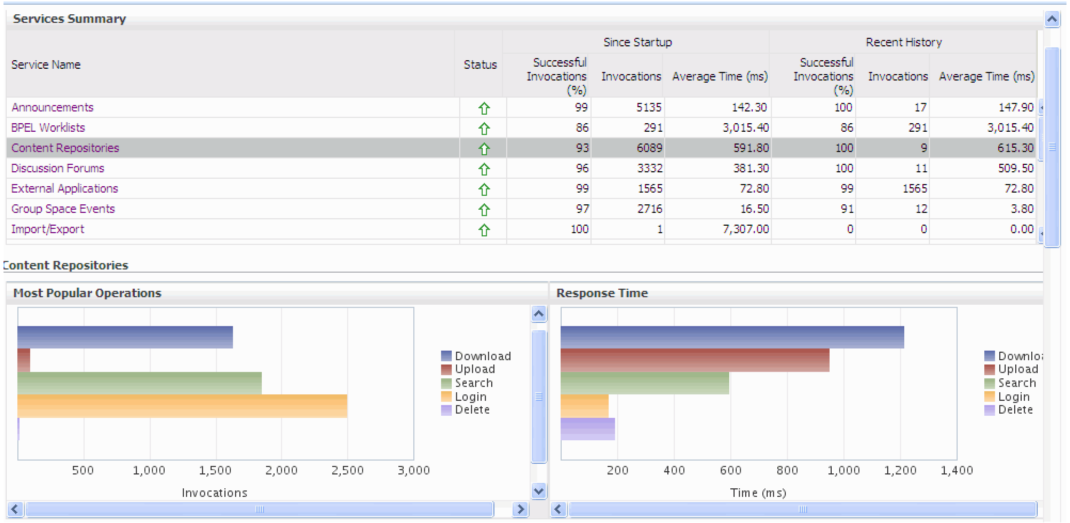
30.1.4.3 Content Repository (Documents Service) Metrics

Performance metrics associated with the Documents service (Figure 30–3 and Figure 30–4) are described in the following tables:

- Table 30–5, " Documents Service - Operations Monitored"
- Table 30–6, " Content Repository Metrics - Summary (All Repositories)"
- Table 30–7, " Content Repository Metrics - Operation Summary Per Repository"

- Table 30–8, " Content Repository Metrics - Operation Detail Per Repository"

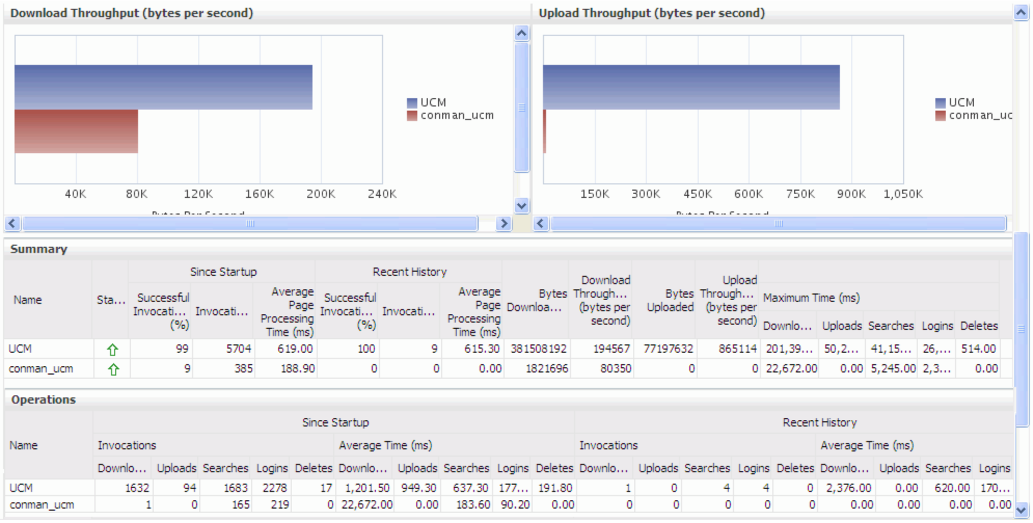
Figure 30–3 Content Repository Metrics



Services Summary

Service Name	Status	Since Startup Successful Invocations (%)	Since Startup Invocations	Since Startup Average Time (ms)	Recent History Successful Invocations (%)	Recent History Invocations	Recent History Average Time (ms)
Announcements	⇧	99	5135	142.30	100	17	147.90
BPEL Worklists	⇧	86	291	3,015.40	86	291	3,015.40
Content Repositories	⇧	93	6089	591.80	100	9	615.30
Discussion Forums	⇧	96	3332	381.30	100	11	509.50
External Applications	⇧	99	1565	72.80	99	1565	72.80
Group Space Events	⇧	97	2716	16.50	91	12	3.80
Import/Export	⇧	100	1	7,307.00	0	0	0.00

Figure 30–4 Content Repository Metrics - Per Operation



Summary

Name	Sta...	Since Startup Successful Invocati... (%)	Since Startup Invocati...	Since Startup Average Page Processing Time (ms)	Recent History Successful Invocati... (%)	Recent History Invocati...	Recent History Average Page Processing Time (ms)	Bytes Downloa...	Download Through... (bytes per second)	Bytes Uploaded	Upload Through... (bytes per second)	Maximum Time (ms) Downlo...	Maximum Time (ms) Uploads	Maximum Time (ms) Searches	Maximum Time (ms) Logins	Maximum Time (ms) Deletes
UCM	⇧	99	5704	619.00	100	9	615.30	381508192	194567	77197632	865114	201,39...	50,2...	41,15...	26,...	514.00
conman_ucm	⇧	9	385	188.90	0	0	0.00	1821696	80350	0	0	22,672.00	0.00	5,245.00	2,3...	0.00

Operations

Name	Since Startup Invocations Downlo...	Uploads	Searches	Logins	Deletes	Since Startup Average Time (ms) Downlo...	Uploads	Searches	Logins	Deletes	Recent History Invocations Downlo...	Uploads	Searches	Logins	Deletes	Recent History Average Time (ms) Downlo...	Uploads	Searches	Logins
UCM	1632	94	1683	2278	17	1,201.50	949.30	637.30	177...	191.80	1	0	4	4	0	2,376.00	0.00	620.00	170...
conman_ucm	1	0	165	219	0	22,672.00	0.00	183.60	90.20	0.00	0	0	0	0	0	0.00	0.00	0.00	0.00

To monitor these metrics through Fusion Middleware Control, see Section 30.2, "Viewing Performance Information."

Table 30–5 Documents Service - Operations Monitored

Operation	Description	Performance Issues - User Action
Download	Downloads one or more documents from a content repository.	For service-specific causes, see Section 30.1.5.3, "Content Repository (Documents) Service." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."

Table 30–5 (Cont.) Documents Service - Operations Monitored

Operation	Description	Performance Issues - User Action
Upload	Uploads one or more documents to a content repository.	For service-specific causes, see Section 30.1.5.3, "Content Repository (Documents) Service." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."
Search	Searches for documents stored in a content repository.	For service-specific causes, see Section 30.1.5.3, "Content Repository (Documents) Service." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."
Login	Establishes a connection to the content repository and authenticates the user.	For service-specific causes, see Section 30.1.5.3, "Content Repository (Documents) Service." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."
Delete	Deletes one or more documents stored in a content repository.	For service-specific causes, see Section 30.1.5.3, "Content Repository (Documents) Service." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."

Table 30–6 Content Repository Metrics - Summary (All Repositories)

Metric	Description
Status	The current status of the Documents service: ■ **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**. If you are having problems with the Documents service, check the diagnostic logs to establish why this service is "Down". See, Section 30.3, "Viewing and Configuring Log Information." Some typical causes of failure include: - 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. ■ **Clock** - Unable to query the status of the service for some reason.

Table 30–6 (Cont.) Content Repository Metrics - Summary (All Repositories)

Metric	Description
Successful Invocations (%)	The percentage of Documents service invocations that succeeded (Upload, Download, Search Login, Delete): - Since Startup - Recent History If Successful Invocations (%) is below 100%, check the diagnostic logs to establish why service requests are failing. See, Section 30.3, "Viewing and Configuring Log Information."
Invocations	The number of Documents service invocations per minute (Upload, Download, Search Login, Delete): - 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 Services in the application.
Average Time (ms)	The average time taken to process operations associated with the Documents service (Upload, Download, Search Login, Delete): - Since Startup - Recent History
Most Popular Operations	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 operations is used the least.
Response Time	The average time to process operations associated with the Documents service since the WebCenter application started up (displayed on a chart). The highest value on the chart indicates the worst performing operation. The lowest value indicates which operations is performing the best.
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 30–7 Content Repository Metrics - Operation Summary Per Repository

Metric	Description
Status	The current status of the content repository: ■ **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**. If you are having problems with a content repository, check the diagnostic logs to establish why this service is "Down". See, Section 30.3, "Viewing and Configuring Log Information." Some typical causes of failure include: - 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. ■ **Clock** - Unable to query the status of the service for some reason.
Successful Invocations (%)	The percentage of Documents service invocations that succeeded (Upload, Download, Search, Login, Delete) for this content repository: - Since Startup - Recent History If Successful Invocations (%) is below 100%, check the diagnostic logs to establish why service requests are failing. See, Section 30.3, "Viewing and Configuring Log Information".
Invocations	The number of Documents service invocations per minute (Upload, Download, Search, Login, Delete) for this content repository: - 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 Services in the application.
Average Page Processing Time (ms)	The average time taken to process operations associated with the Documents service (Upload, Download, Search, Login, Delete) for this content repository: - Since Startup - Recent History
Bytes Downloaded	The volume of data that the Documents service has downloaded from this content repository.
Download Throughput (bytes per second)	The rate at which the Documents service downloads documents from this content repository.
Bytes Uploaded	The volume of data that the Documents service has uploaded from this content repository.

Table 30–7 (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.

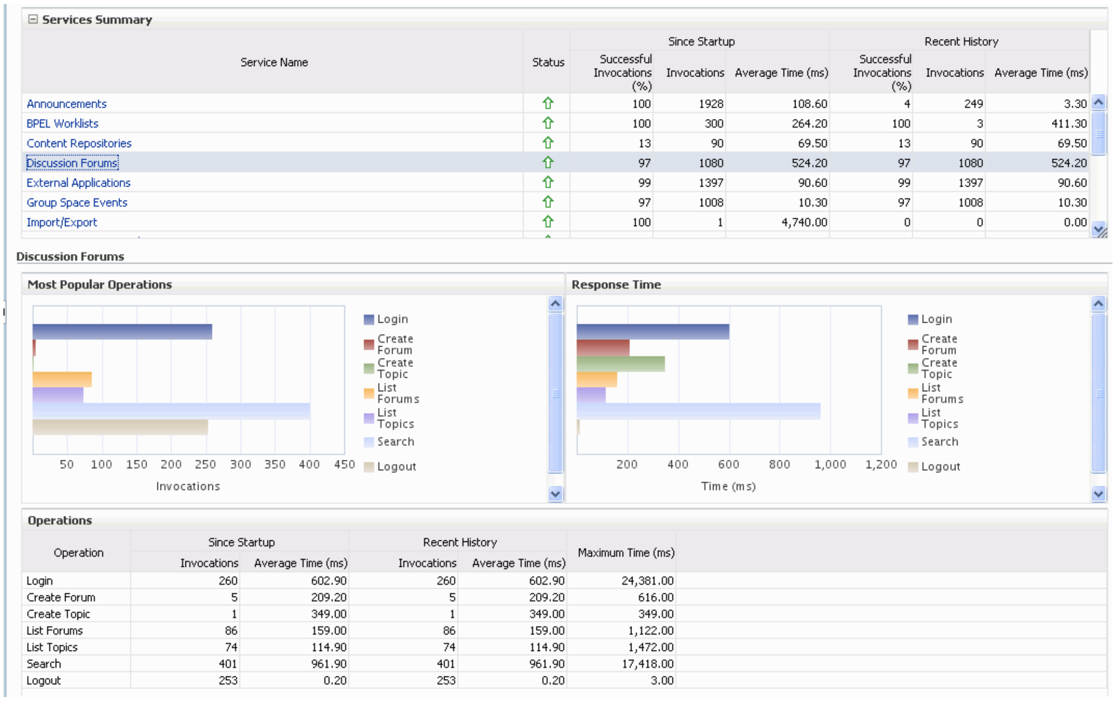
Table 30–8 Content Repository Metrics - Operation Detail Per Repository

Metric	Description
Invocations	The number of Documents service invocations per operation (Upload, Download, Search, Login, Delete): - 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 Services in the application.
Average Processing Time (ms)	The average time taken to process each operation associated with the Documents service (Upload, Download, Search, Login, Delete): - Since Startup - Recent History

30.1.4.4 Discussions Metrics

Performance metrics associated with the Discussions service (Figure 30–5) are described in Table 30–9 and Section 30.1.2, "Common WebCenter Metrics."

Figure 30–5 Discussion Metrics



⊟ Services Summary

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

Discussion Forums

Operations

Operation	Since Startup		Recent History		Maximum Time (ms)
	Invocations	Average Time (ms)	Invocations	Average Time (ms)	
Login	260	602.90	260	602.90	24,381.00
Create Forum	5	209.20	5	209.20	616.00
Create Topic	1	349.00	1	349.00	349.00
List Forums	86	159.00	86	159.00	1,122.00
List Topics	74	114.90	74	114.90	1,472.00
Search	401	961.90	401	961.90	17,418.00
Logout	253	0.20	253	0.20	3.00

To monitor these metrics through Fusion Middleware Control, see Section 30.2, "Viewing Performance Information."

Table 30–9 Discussions Service - Operations Monitored

Operation	Description	Performance Issues - User Action
Login	Logs a WebCenter user (accessing the Discussions service) into the discussions server that is hosting discussions forums.	For service-specific causes, see Section 30.1.5.4, "Discussions Service." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."
Logout	Logs a WebCenter user out of the discussions server that is hosting discussion forums.	For service-specific causes, see Section 30.1.5.4, "Discussions Service." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."
Create Forum	Creates a discussion forum in the discussions server, under a specific category.	If you are having problems creating forums, it may be due to: ▪ Category under which discussion forums must be created has been deleted. ▪ User does not have permissions to create discussion forums. For other service-specific causes, see Section 30.1.5.4, "Discussions Service." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."
Create Topic	Creates a topic in the discussions server, under a specific forum.	If you are having problems creating forums, it may be due to: ▪ Discussion forum under which topics must be created has been deleted. ▪ User does not have permissions to create topics. For other service-specific causes, see Section 30.1.5.4, "Discussions Service". For information on common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions".

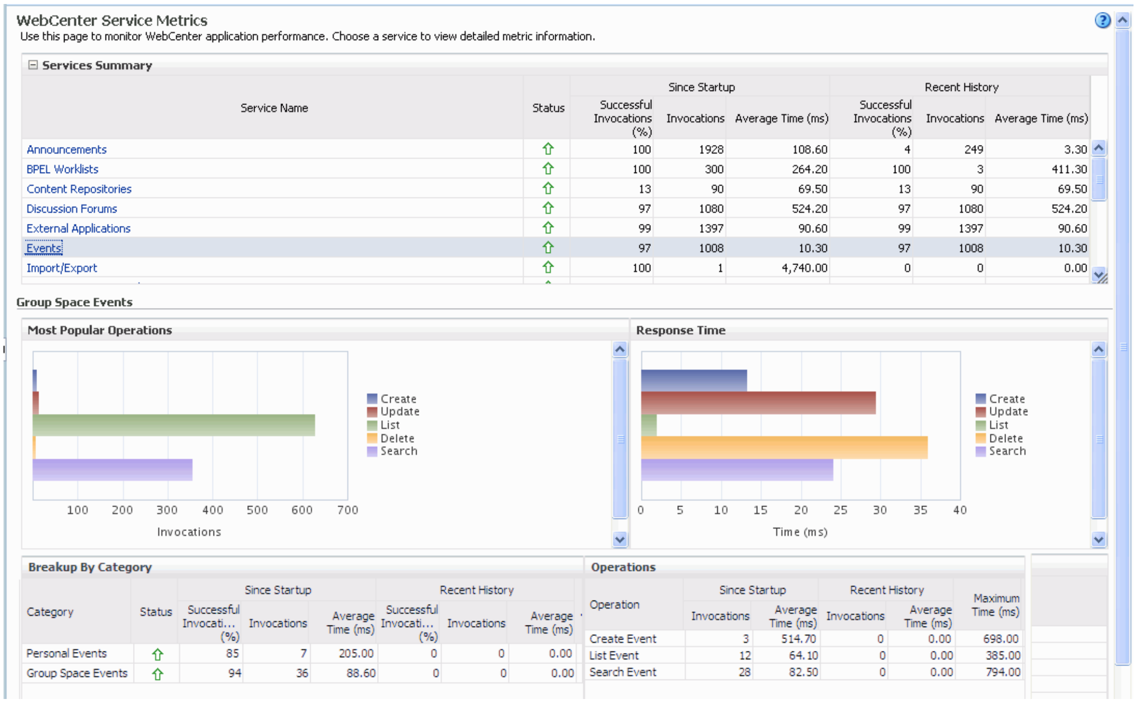
Table 30–9 (Cont.) Discussions Service - Operations Monitored

Operation	Description	Performance Issues - User Action
List Forums	Retrieves a list of forums, under a specific category, from the discussion server.	If you are having problems creating forums, it may be due to: ▪ User does not have permissions to view forums in the category. ▪ Category from which to fetch forums has been deleted. For other service-specific causes, see Section 30.1.5.4, "Discussions Service." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."
List Topics	Retrieves a list of topics, under a specific forum, from the discussion server.	If you are having problems creating forums, it may be due to: ▪ User does not have permissions to view topics in the forum. ▪ Forum from which to fetch topics has been deleted. For other service-specific causes, see Section 30.1.5.4, "Discussions Service." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."
Search	Searches for terms within discussion forum text, in the discussions server.	If you are having problems creating forums, it may be due to: ▪ No topic/messages exist with the specified search term. ▪ Category or forum in which the search term object resides has been deleted. For other service-specific causes, see Section 30.1.5.4, "Discussions Service." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."

30.1.4.5 Events Metrics

Performance metrics associated with the Group Space Events and Personal Events services are described in Table 30–10 and Section 30.1.2, "Common WebCenter Metrics."

Figure 30–6 Group Space Events Metrics



WebCenter Service Metrics

Use this page to monitor WebCenter application performance. Choose a service to view detailed metric information.

⊟ Services Summary

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
Events	⇧	97	1008	10.30	97	1008	10.30
Import/Export	⇧	100	1	4,740.00	0	0	0.00

Group Space Events

Most Popular Operations

Response Time

Breakup By Category

Category	Status	Since Startup			Recent History		
		Successful Invocati... (%)	Invocations	Average Time (ms)	Successful Invocati... (%)	Invocations	Average Time (ms)
Personal Events	⇧	85	7	205.00	0	0	0.00
Group Space Events	⇧	94	36	88.60	0	0	0.00

Operations

Operation	Since Startup		Recent History		Maximum Time (ms)
	Invocations	Average Time (ms)	Invocations	Average Time (ms)	
Create Event	3	514.70	0	0.00	698.00
List Event	12	64.10	0	0.00	385.00
Search Event	28	82.50	0	0.00	794.00

To monitor these metrics through Fusion Middleware Control, see Section 30.2, "Viewing Performance Information."

Table 30–10 Events Service - Operations Monitored

Operation	Description	Performance Issues - User Action
Create Event	Creates a group space or personal event in the WebCenter repository.	For service-specific causes, see Section 30.1.5.6, "Events Service." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."
Update Event	Updates a group space or personal event stored in the WebCenter repository.	For service-specific causes, see Section 30.1.5.6, "Events Service." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."
Delete Event	Deletes a group space or personal event in the WebCenter repository.	For service-specific causes, see Section 30.1.5.6, "Events Service." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."
List Event	Retrieves a list of events from the WebCenter repository.	For service-specific causes, see Section 30.1.5.6, "Events Service." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."

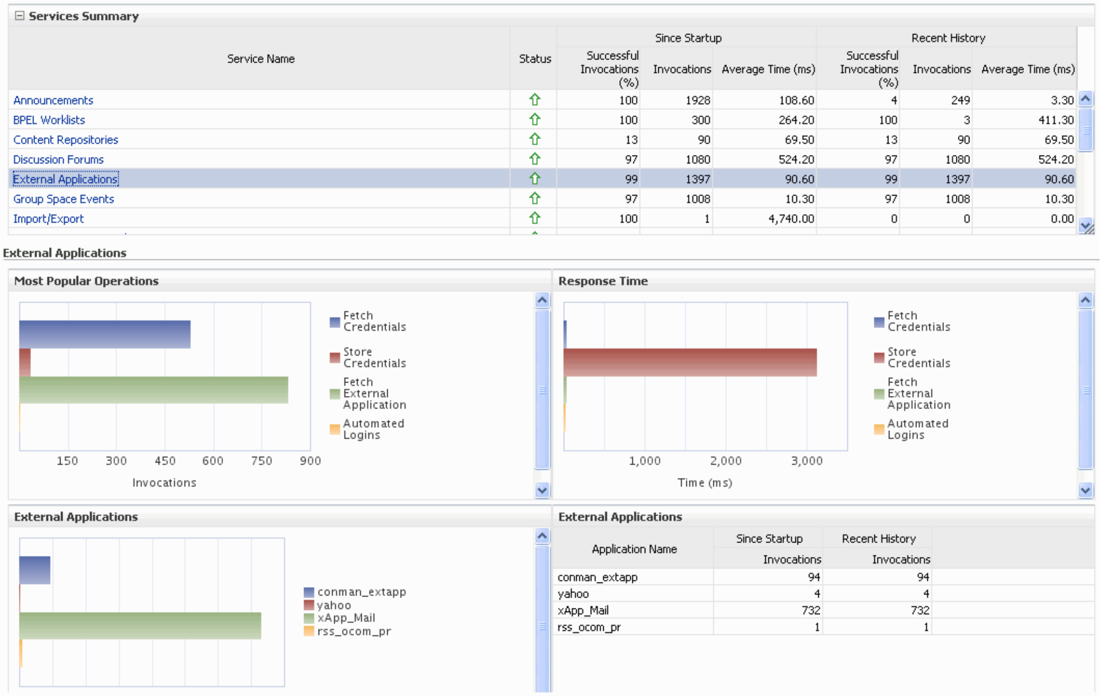
Table 30–10 (Cont.) Events Service - Operations Monitored

Operation	Description	Performance Issues - User Action
Search Event	Searches for terms within event text.	For service-specific causes, see Section 30.1.5.6, "Events Service." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."

30.1.4.6 External Application Metrics

Performance metrics associated with the External Application service are described in Table 30–11 and Section 30.1.2, "Common WebCenter Metrics."

Figure 30–7 External Application Metrics



⊟ Services Summary

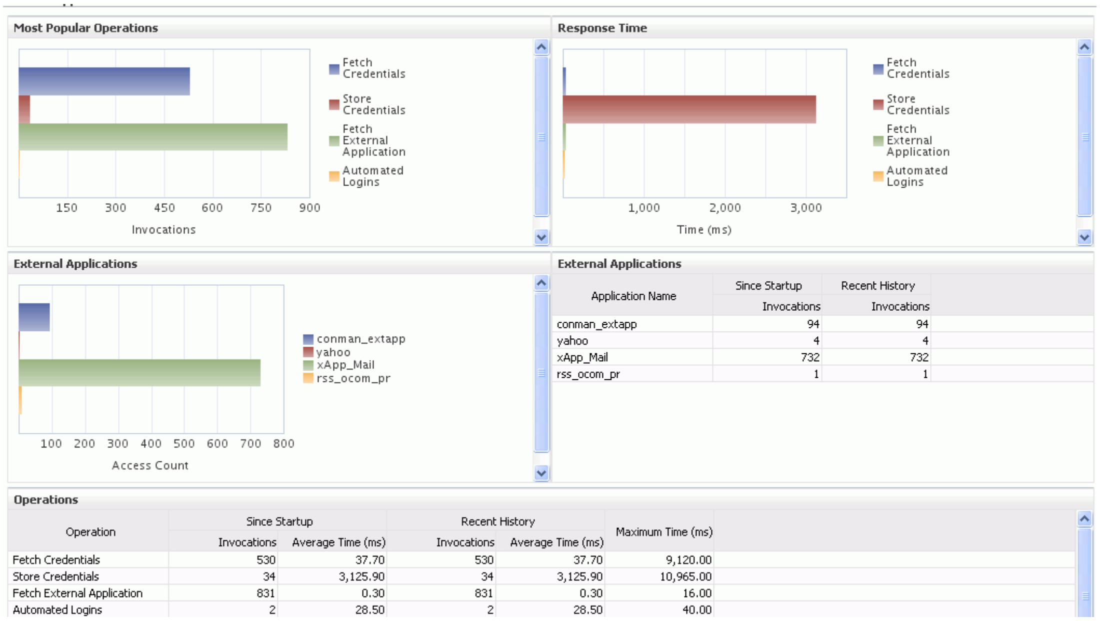
Service Name	Status	Since Startup			Recent History		
		Successful Invocations (%)	Invocations	Average Time (ms)	Successful Invocations (%)	Invocations	Average Time (ms)
Announcements	⇧	100	1928	108.60	4	249	3.30
BPEL Worklists	⇧	100	300	264.20	100	3	411.30
Content Repositories	⇧	13	90	69.50	13	90	69.50
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

External Applications

External Applications

Application Name	Since Startup	Recent History
	Invocations	Invocations
conman_extapp	94	94
yahoo	4	4
xApp_Mail	732	732
rss_ocom_pr	1	1

Figure 30–8 External Application Metrics - Per Operation



External Applications

Application Name	Since Startup	Recent History
	Invocations	Invocations
conman_extapp	94	94
yahoo	4	4
xApp_Mail	732	732
rss_ocom_pr	1	1

Operations

Operation	Since Startup		Recent History		Maximum Time (ms)
	Invocations	Average Time (ms)	Invocations	Average Time (ms)	
Fetch Credentials	530	37.70	530	37.70	9,120.00
Store Credentials	34	3,125.90	34	3,125.90	10,965.00
Fetch External Application	831	0.30	831	0.30	16.00
Automated Logins	2	28.50	2	28.50	40.00

To monitor these metrics through Fusion Middleware Control, see Section 30.2, "Viewing Performance Information."

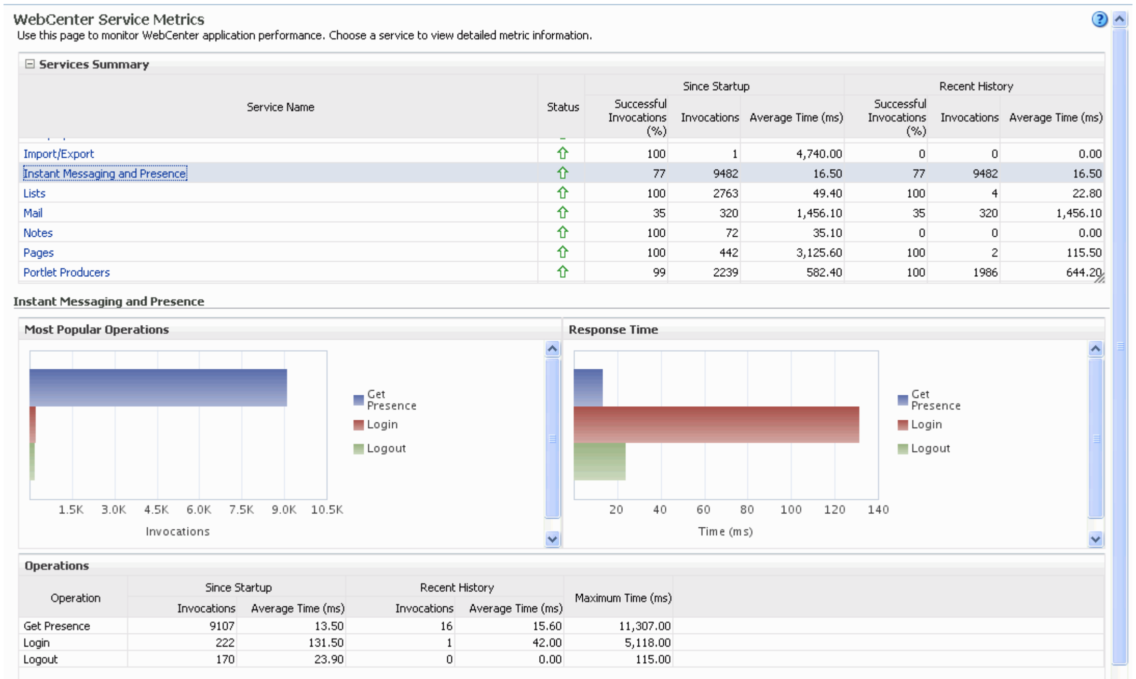
Table 30–11 External Applications - Operations Monitored

Operation	Description	Performance Issues - User Action
Fetch Credentials	Retrieves credentials for an external application.	For service-specific causes, see Section 30.1.5.5, "External Applications Service." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."
Store Credentials	Stores user credentials for an external application.	For service-specific causes, see Section 30.1.5.5, "External Applications Service." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."
Fetch External Application	Retrieves an external application.	For service-specific causes, see Section 30.1.5.5, "External Applications Service." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."
Automated Logins	Logs a WebCenter user in to an external application (using the automated login feature).	For service-specific causes, see Section 30.1.5.5, "External Applications Service." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."

30.1.4.7 Instant Messaging and Presence (IMP) Metrics

Performance metrics associated with the Instant Messaging and Presence (IMP) service (Figure 30–9) are described in Table 30–12 and Section 30.1.2, "Common WebCenter Metrics."

Figure 30–9 IMP Metrics



WebCenter Service Metrics

Use this page to monitor WebCenter application performance. Choose a service to view detailed metric information.

Services Summary

Service Name	Status	Since Startup			Recent History		
		Successful Invocations (%)	Invocations	Average Time (ms)	Successful Invocations (%)	Invocations	Average Time (ms)
Import/Export	⇧	100	1	4,740.00	0	0	0.00
Instant Messaging and Presence	⇧	77	9482	16.50	77	9482	16.50
Lists	⇧	100	2763	49.40	100	4	22.80
Mail	⇧	35	320	1,456.10	35	320	1,456.10
Notes	⇧	100	72	35.10	0	0	0.00
Pages	⇧	100	442	3,125.60	100	2	115.50
Portlet Producers	⇧	99	2239	582.40	100	1986	644.20

Instant Messaging and Presence

Operations

Operation	Since Startup		Recent History		Maximum Time (ms)
	Invocations	Average Time (ms)	Invocations	Average Time (ms)	
Get Presence	9107	13.50	16	15.60	11,307.00
Login	222	131.50	1	42.00	5,118.00
Logout	170	23.90	0	0.00	115.00

To monitor these metrics through Fusion Middleware Control, see Section 30.2, "Viewing Performance Information."

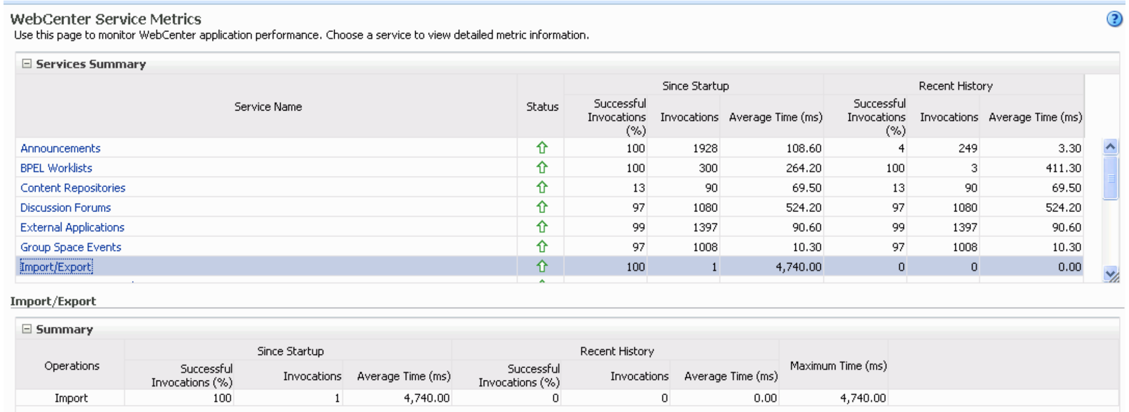
Table 30–12 Instant Messaging and Presence Service - Operations Monitored

Operation	Description	Performance Issues - User Action
Get Presence	Retrieves user presence information from the IMP server.	For service-specific causes, see Section 30.1.5.7, "Instant Messaging and Presence (IMP) Service." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."
Login	Logs a WebCenter user (accessing the IMP service) into the IMP server.	For service-specific causes, see Section 30.1.5.7, "Instant Messaging and Presence (IMP) Service." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."
Logout	Logs a WebCenter user (accessing the IMP service) out of the IMP server.	For service-specific causes, see Section 30.1.5.7, "Instant Messaging and Presence (IMP) Service." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."

30.1.4.8 Import and Export Metrics

Performance metrics associated with import and export services (Figure 30–10) are described in Table 30–13 and Section 30.1.2, "Common WebCenter Metrics." These metrics apply to WebCenter Spaces only.

Figure 30–10 Import/Export Metrics



WebCenter Service Metrics

Use this page to monitor WebCenter application performance. Choose a service to view detailed metric information.

⊟ Services Summary

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

Import/Export

⊟ Summary

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 30.2, "Viewing Performance Information."

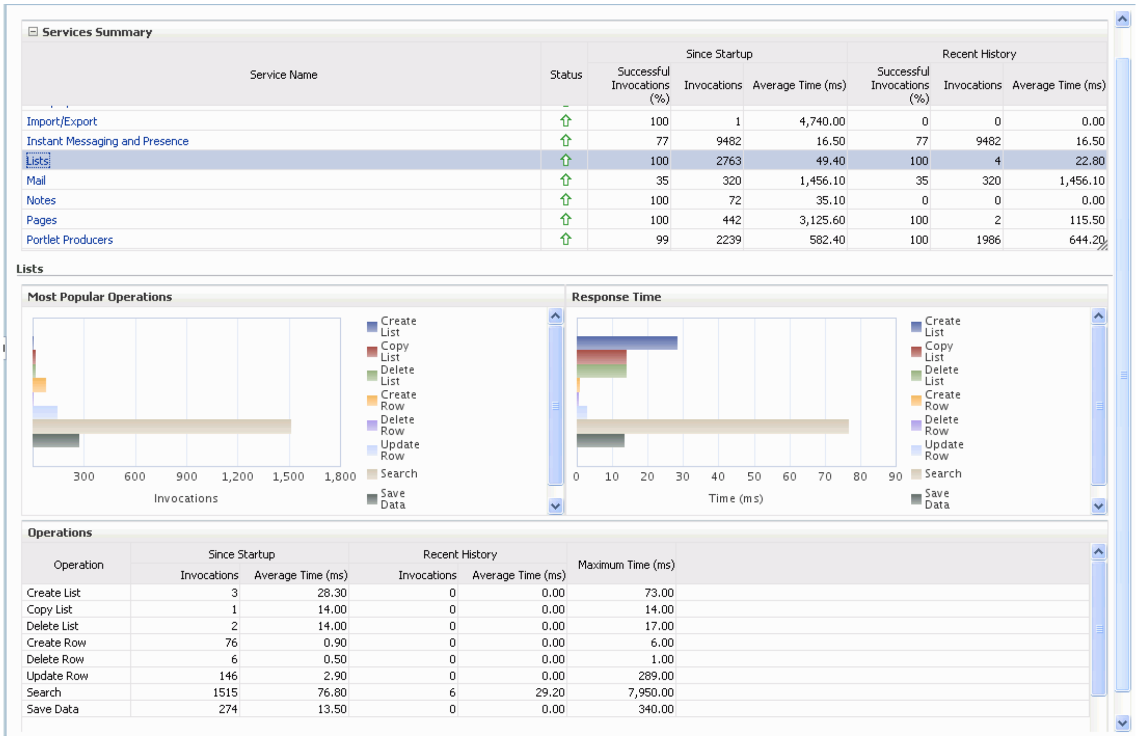
Table 30–13 Import/Export - Operations Monitored

Operation	Description	Performance Issues - User Action
Export	Exports an entire WebCenter application.	For service-specific causes, see Section 30.1.5.8, "Import and Export." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."
Import	Imports entire WebCenter application.	For service-specific causes, see Section 30.1.5.8, "Import and Export." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."

30.1.4.9 List Metrics

(WebCenter Spaces only) Performance metrics associated with the List service (Figure 30–11) are described in Table 30–14 and Section 30.1.2, "Common WebCenter Metrics."

Figure 30–11 List Metrics



Services Summary

Service Name	Status	Since Startup			Recent History		
		Successful Invocations (%)	Invocations	Average Time (ms)	Successful Invocations (%)	Invocations	Average Time (ms)
Import/Export	⇧	100	1	4,740.00	0	0	0.00
Instant Messaging and Presence	⇧	77	9482	16.50	77	9482	16.50
Lists	⇧	100	2763	49.40	100	4	22.80
Mail	⇧	35	320	1,456.10	35	320	1,456.10
Notes	⇧	100	72	35.10	0	0	0.00
Pages	⇧	100	442	3,125.60	100	2	115.50
Portlet Producers	⇧	99	2239	582.40	100	1986	644.20

Lists

Operations

Operation	Since Startup		Recent History		Maximum Time (ms)
	Invocations	Average Time (ms)	Invocations	Average Time (ms)	
Create List	3	28.30	0	0.00	73.00
Copy List	1	14.00	0	0.00	14.00
Delete List	2	14.00	0	0.00	17.00
Create Row	76	0.90	0	0.00	6.00
Delete Row	6	0.50	0	0.00	1.00
Update Row	146	2.90	0	0.00	289.00
Search	1515	76.80	6	29.20	7,950.00
Save Data	274	13.50	0	0.00	340.00

To monitor these metrics through Fusion Middleware Control, see Section 30.2, "Viewing Performance Information."

Table 30–14 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 30.1.5.9, "Lists Service."
	The Save Data operation commits new lists to the MDS repository.	For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."
Copy List	Copies a list and its data in the user session.	For service-specific causes, see Section 30.1.5.9, "Lists Service."
	The Save Data operation commits copied lists and list data to the MDS repository and the WebCenter repository (the database where list data is stored).	For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."
Delete List	Deletes a list and its data in the user session.	For service-specific causes, see Section 30.1.5.9, "Lists Service."
	The Save Data operation commits list changes to the MDS repository and the WebCenter repository (the database where list data is stored).	For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."

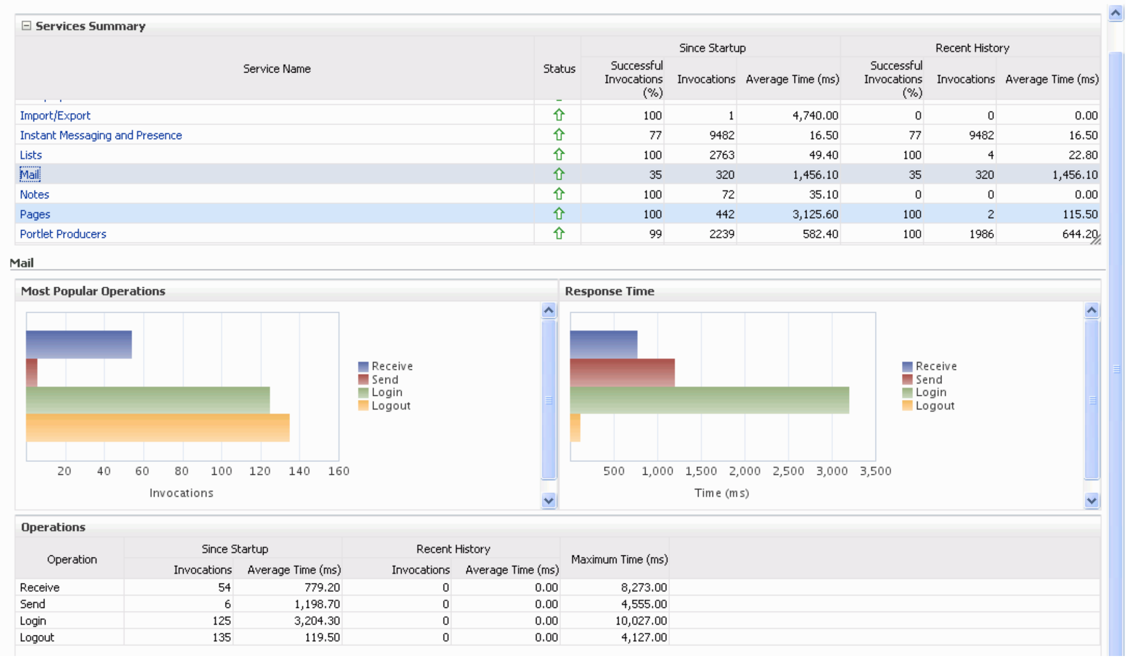
Table 30–14 (Cont.) List service - Operations Monitored

Operation	Description	Performance Issues - User Action
Create Row	Creates row of list data in the user session. The Save Data operation commits list data changes to the WebCenter repository (the database where list data is stored).	For service-specific causes, see Section 30.1.5.9, "Lists Service." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."
Update Row	Updates row of list data in the user session. The Save Data operation commits list data changes to the WebCenter repository (the database where list data is stored).	For service-specific causes, see Section 30.1.5.9, "Lists Service." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."
Delete Row	Deletes row of list data in the user session. The Save Data operation commits list data changes to the WebCenter repository (the database where list data is stored).	For service-specific causes, see Section 30.1.5.9, "Lists Service." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."
Search	Retrieves a list by its ID from the Metadata repository.	For service-specific causes, see Section 30.1.5.9, "Lists Service." For common causes, see Section 30.1.3, "Common WebCenter 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 repository (the database where list information is stored).	For service-specific causes, see Section 30.1.5.9, "Lists Service." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."

30.1.4.10 Mail Metrics

Performance metrics associated with the Mail service (Figure 30–12) are described in Table 30–15 and Section 30.1.2, "Common WebCenter Metrics."

Figure 30–12 Mail Metrics



Services Summary

Service Name	Status	Since Startup			Recent History		
		Successful Invocations (%)	Invocations	Average Time (ms)	Successful Invocations (%)	Invocations	Average Time (ms)
Import/Export	⇧	100	1	4,740.00	0	0	0.00
Instant Messaging and Presence	⇧	77	9482	16.50	77	9482	16.50
Lists	⇧	100	2763	49.40	100	4	22.80
Mail	⇧	35	320	1,456.10	35	320	1,456.10
Notes	⇧	100	72	35.10	0	0	0.00
Pages	⇧	100	442	3,125.60	100	2	115.50
Portlet Producers	⇧	99	2239	582.40	100	1986	644.20

Operations

Operation	Since Startup		Recent History		Maximum Time (ms)
	Invocations	Average Time (ms)	Invocations	Average Time (ms)	
Receive	54	779.20	0	0.00	8,273.00
Send	6	1,198.70	0	0.00	4,555.00
Login	125	3,204.30	0	0.00	10,027.00
Logout	135	119.50	0	0.00	4,127.00

To monitor these metrics through Fusion Middleware Control, see Section 30.2, "Viewing Performance Information."

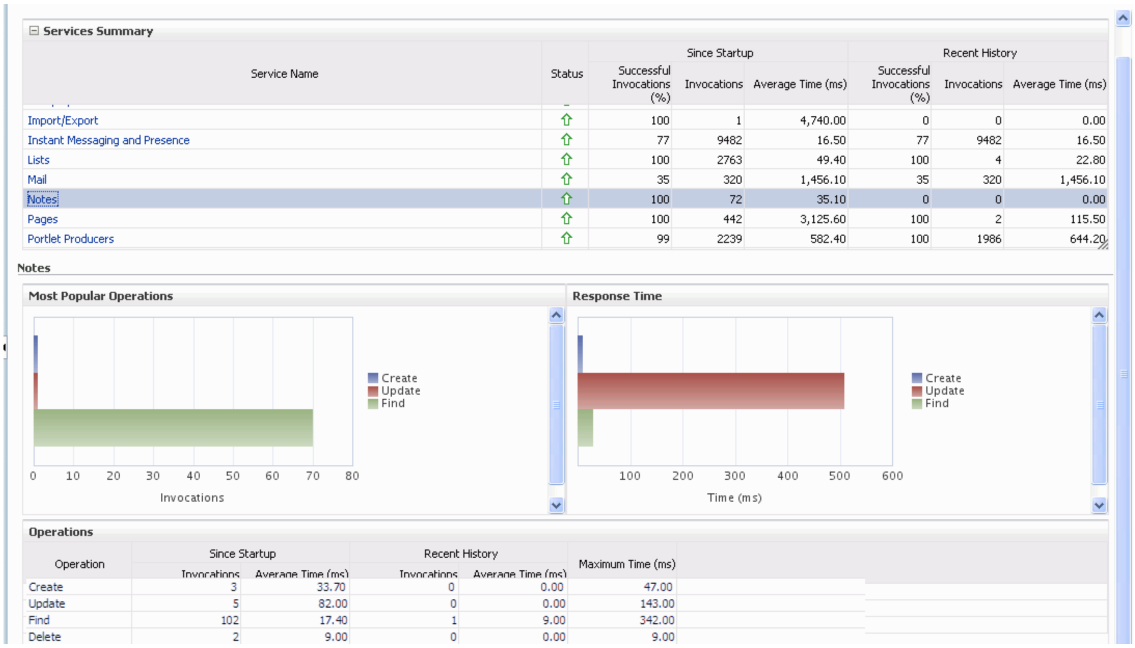
Table 30–15 Mail Service - Operations Monitored

Operation	Description	Performance Issues - User Action
Login	Logs a WebCenter user into the mail server that is hosting mail services.	For service-specific causes, see Section 30.1.5.10, "Mail Service." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."
Logout	Logs a WebCenter user out of the mail server that is hosting mail services.	For service-specific causes, see Section 30.1.5.10, "Mail Service." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."
Receive	Receives a mail.	For service-specific causes, see Section 30.1.5.10, "Mail Service." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."
Send	Sends a mail.	For service-specific causes, see Section 30.1.5.10, "Mail Service." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."
Search	Searches for mail that contains a specific term.	For service-specific causes, see Section 30.1.5.10, "Mail Service." For information on common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."

30.1.4.11 Note Metrics

Performance metrics associated with the Notes service (Figure 30–13) are described in Table 30–16 and Section 30.1.2, "Common WebCenter Metrics."

Figure 30–13 Notes Metrics



Services Summary

Service Name	Status	Since Startup			Recent History		
		Successful Invocations (%)	Invocations	Average Time (ms)	Successful Invocations (%)	Invocations	Average Time (ms)
Import/Export	⇧	100	1	4,740.00	0	0	0.00
Instant Messaging and Presence	⇧	77	9482	16.50	77	9482	16.50
Lists	⇧	100	2763	49.40	100	4	22.80
Mail	⇧	35	320	1,456.10	35	320	1,456.10
Notes	⇧	100	72	35.10	0	0	0.00
Pages	⇧	100	442	3,125.60	100	2	115.50
Portlet Producers	⇧	99	2239	582.40	100	1986	644.20

Notes

Operations

Operation	Since Startup		Recent History		Maximum Time (ms)
	Invocations	Average Time (ms)	Invocations	Average Time (ms)	
Create	3	33.70	0	0.00	47.00
Update	5	82.00	0	0.00	143.00
Find	102	17.40	1	9.00	342.00
Delete	2	9.00	0	0.00	9.00

To monitor these metrics through Fusion Middleware Control, see Section 30.2, "Viewing Performance Information."

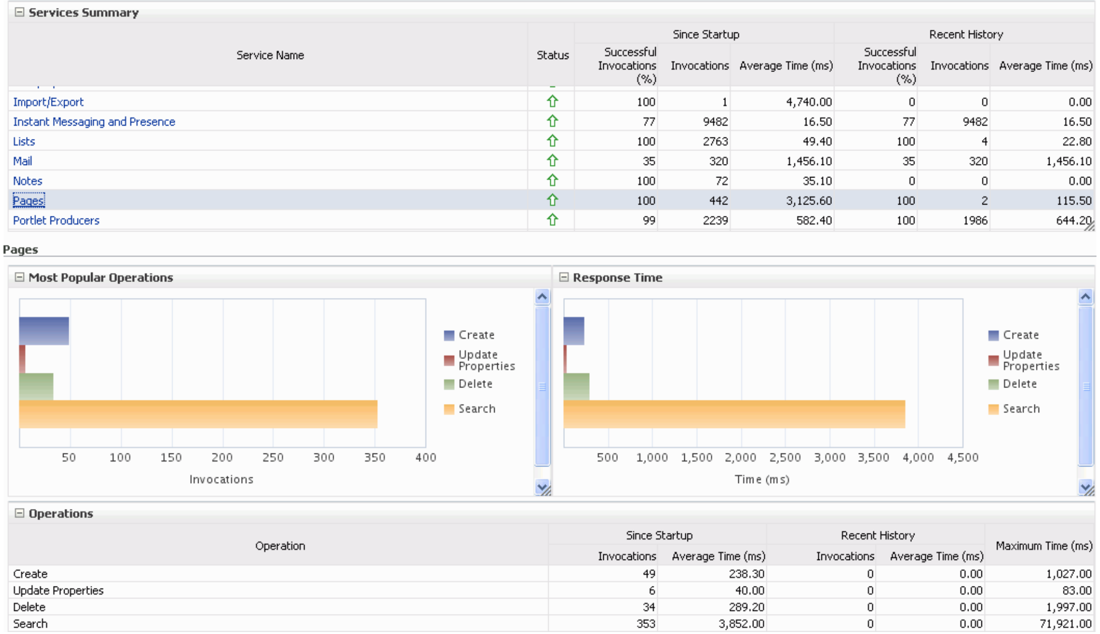
Table 30–16 Notes Service - Operations Monitored

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 30.1.5.11, "Notes Service." For common causes, see Section 30.1.3, "Common WebCenter 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 30.1.5.11, "Notes Service." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."
Find	Retrieves a note from the MDS repository.	For service-specific causes, see Section 30.1.5.11, "Notes Service." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."
Delete	Deletes a note from the MDS repository.	For service-specific causes, see Section 30.1.5.11, "Notes Service." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."

30.1.4.12 Page Metrics

Performance metrics associated with the Page service (Figure 30–14) are described in Table 30–17 and Section 30.1.2, "Common WebCenter Metrics."

Figure 30–14 Page Metrics



⊟ Services Summary

Service Name	Status	Since Startup			Recent History		
		Successful Invocations (%)	Invocations	Average Time (ms)	Successful Invocations (%)	Invocations	Average Time (ms)
Import/Export	⇧	100	1	4,740.00	0	0	0.00
Instant Messaging and Presence	⇧	77	9482	16.50	77	9482	16.50
Lists	⇧	100	2763	49.40	100	4	22.80
Mail	⇧	35	320	1,456.10	35	320	1,456.10
Notes	⇧	100	72	35.10	0	0	0.00
Pages	⇧	100	442	3,125.60	100	2	115.50
Portlet Producers	⇧	99	2239	582.40	100	1986	644.20

Pages

⊟ Operations

Operation	Since Startup		Recent History		Maximum Time (ms)
	Invocations	Average Time (ms)	Invocations	Average Time (ms)	
Create	49	238.30	0	0.00	1,027.00
Update Properties	6	40.00	0	0.00	83.00
Delete	34	289.20	0	0.00	1,997.00
Search	353	3,852.00	0	0.00	71,921.00

To monitor these metrics through Fusion Middleware Control, see Section 30.2, "Viewing Performance Information."

Table 30–17 Page Service - Operations Monitored

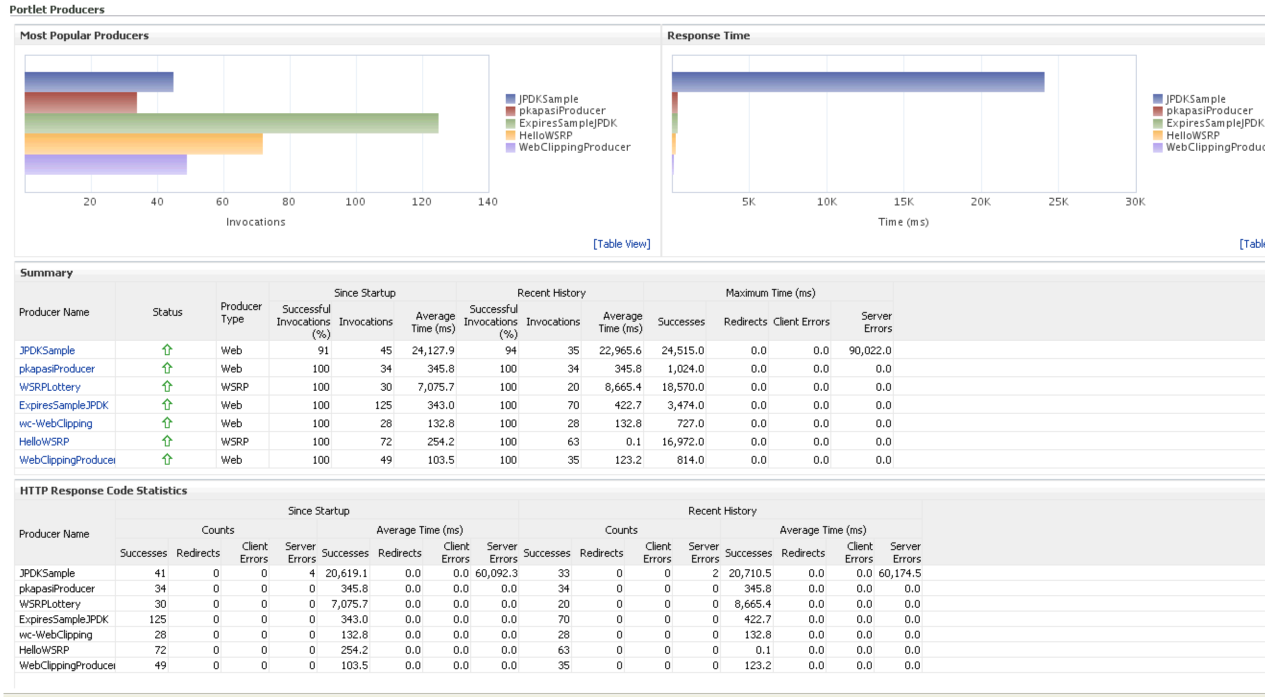
Operation	Description	Performance Issues - User Action
Create	Creates a page in the WebCenter application.	For service-specific causes, see Section 30.1.5.12, "Page Service." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."
Copy	Copies a page.	For service-specific causes, see Section 30.1.5.12, "Page Service." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."
Delete	Deletes a page.	For service-specific causes, see Section 30.1.5.12, "Page Service." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."
Search	Searches for pages that contain a specific term.	For service-specific causes, see Section 30.1.5.12, "Page Service." For common causes, see Section 30.1.3, "Common WebCenter Performance Issues and Actions."

30.1.4.13 Portlet Producer Metrics

Performance metrics associated with the portlet producers (Figure 30–15) are described in the following tables:

- Table 30–18, " Portlet Producers - Summary"
- Table 30–19, " Portlet Producer - Detail"

Figure 30–15 Portlet Producer Metrics



Summary

Producer Name	Status	Producer Type	Since Startup			Recent History			Maximum Time (ms)			
			Successful Invocations (%)	Invocations	Average Time (ms)	Successful Invocations (%)	Invocations	Average Time (ms)	Successes	Redirects	Client Errors	Server Errors
JPDKSample	⇧	Web	91	45	24,127.9	94	35	22,965.6	24,515.0	0.0	0.0	90,022.0
pkapasiProducer	⇧	Web	100	34	345.8	100	34	345.8	1,024.0	0.0	0.0	0.0
WSRPLottery	⇧	WSRP	100	30	7,075.7	100	20	8,665.4	18,570.0	0.0	0.0	0.0
ExpiresSampleJPDK	⇧	Web	100	125	343.0	100	70	422.7	3,474.0	0.0	0.0	0.0
wc-WebClipping	⇧	Web	100	28	132.8	100	28	132.8	727.0	0.0	0.0	0.0
HelloWSRP	⇧	WSRP	100	72	254.2	100	63	0.1	16,972.0	0.0	0.0	0.0
WebClippingProducer	⇧	Web	100	49	103.5	100	35	123.2	814.0	0.0	0.0	0.0

HTTP Response Code Statistics

Producer Name	Since Startup								Recent History							
	Counts				Average Time (ms)				Counts				Average Time (ms)			
	Successes	Redirects	Client Errors	Server Errors	Successes	Redirects	Client Errors	Server Errors	Successes	Redirects	Client Errors	Server Errors	Successes	Redirects	Client Errors	Server Errors
JPDKSample	41	0	0	4	20,619.1	0.0	0.0	60,092.3	33	0	0	2	20,710.5	0.0	0.0	60,174.5
pkapasiProducer	34	0	0	0	345.8	0.0	0.0	0.0	34	0	0	0	345.8	0.0	0.0	0.0
WSRPLottery	30	0	0	0	7,075.7	0.0	0.0	0.0	20	0	0	0	8,665.4	0.0	0.0	0.0
ExpiresSampleJPDK	125	0	0	0	343.0	0.0	0.0	0.0	70	0	0	0	422.7	0.0	0.0	0.0
wc-WebClipping	28	0	0	0	132.8	0.0	0.0	0.0	28	0	0	0	132.8	0.0	0.0	0.0
HelloWSRP	72	0	0	0	254.2	0.0	0.0	0.0	63	0	0	0	0.1	0.0	0.0	0.0
WebClippingProducer	49	0	0	0	103.5	0.0	0.0	0.0	35	0	0	0	123.2	0.0	0.0	0.0

To monitor these metrics through Fusion Middleware Control, see Section 30.2, "Viewing Performance Information."

Table 30–18 Portlet Producers - Summary

Metric	Description
Status	The current status of portlet producers used in the WebCenter application: ■ **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 30–18 (Cont.) Portlet Producers - Summary

Metric	Description
Successful Invocations (%)	The percentage of portlet producer invocations that succeeded: - Since Startup - Recent History Any request that fails will impact availability. This includes WebCenter 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. If Successful Invocations (%) is below 100%, check the diagnostic logs to establish why service requests are failing. See, Section 30.3, "Viewing and Configuring Log Information."
Invocations	The number of portlet producer invocations per minute: - Since Startup - Recent History This metric measures each WebCenter application-related portlet request and therefore, due to cache hits, errors, or timeouts on the application, this total may be higher than the number of actual HTTP requests made to the producer server.
Average Time (ms)	The average time taken to make a portlet request, regardless of the result: - Since Startup - Recent History

Table 30–19 Portlet Producer - Detail

Metric	Description
Most Popular Producers	The number of invocations per producer (displayed on a chart). The highest value on the chart indicates which portlet producer is used the most. The lowest value indicates which portlet producer is used the least.
Response Time	The average time each portlet producer takes to process producer requests since the WebCenter application started up (displayed on a chart). The highest value on the chart indicates the worst performing portlet producer. The lowest value indicates which portlet producer is performing the best.
Producer Name	The name of the portlet producer being monitored. Click the name of a portlet producer to pop up more detailed information about each portlet that the application uses. See also Table 30–21, " Portlet - Detail".

Table 30–19 (Cont.) Portlet Producer - Detail

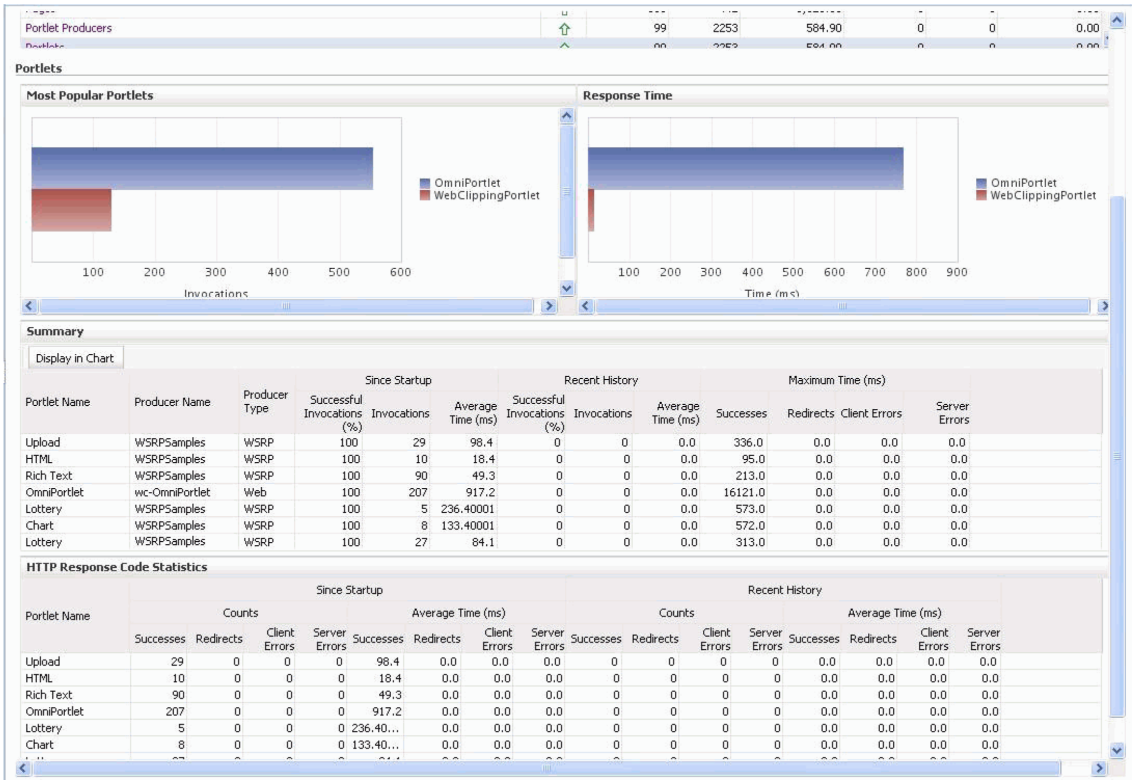
Metric	Description
Status	The current status of each portlet producer: - **Up** (Green Up Arrow) - Indicates that the portlet producer is up and running. - **Down** (Red Down Arrow) - Indicates that the portlet producer is currently unavailable. The producer instance might be down, or there could be some network connectivity issues. - **Clock** - Unable to query the status of portlet producer for some reason.
Producer Type	The portlet producer type: Web or WSRP - 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 producer invocations that succeeded: - Since Startup - Recent History
Invocations	The number of invocations, per producer: - Since Startup - Recent History By sorting the table on this column, you can find the most frequently accessed portlet producer in your WebCenter application.
Average Time (ms)	The average time taken to make a portlet request, regardless of the result: - Since Startup - Recent History 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.
Maximum Time (ms)	The maximum time taken to process producer requests: - Successes - HTTP200xx response code - Re-directs - HTTP300xx response code - Client Errors - HTTP400xx response code - Server Errors - HTTP500xx response code

30.1.4.14 Portlet Metrics

Performance metrics associated with portlets (Figure 30–16) are described in the following tables:

- Table 30–20, " Portlets - Summary"
- Table 30–21, " Portlet - Detail"
- Table 30–22, " Portlet - HTTP Response Code Statistics"
- Table 30–23, " HTTP Response Codes"

Figure 30–16 Portlet Metrics



Portlet Producers	⇧	99	2253	584.90	0	0	0.00

Portlets

Summary

			Since Startup			Recent History			Maximum Time (ms)			
Portlet Name	Producer Name	Producer Type	Successful Invocations (%)	Invocations	Average Time (ms)	Successful Invocations (%)	Invocations	Average Time (ms)	Successes	Redirects	Client Errors	Server Errors
Upload	WSRPSamples	WSRP	100	29	98.4	0	0	0.0	336.0	0.0	0.0	0.0
HTML	WSRPSamples	WSRP	100	10	18.4	0	0	0.0	95.0	0.0	0.0	0.0
Rich Text	WSRPSamples	WSRP	100	90	49.3	0	0	0.0	213.0	0.0	0.0	0.0
OmniPortlet	wc-OmniPortlet	Web	100	207	917.2	0	0	0.0	16121.0	0.0	0.0	0.0
Lottery	WSRPSamples	WSRP	100	5	236.40001	0	0	0.0	573.0	0.0	0.0	0.0
Chart	WSRPSamples	WSRP	100	8	133.40001	0	0	0.0	572.0	0.0	0.0	0.0
Lottery	WSRPSamples	WSRP	100	27	84.1	0	0	0.0	313.0	0.0	0.0	0.0

HTTP Response Code Statistics

	Since Startup								Recent History							
	Counts				Average Time (ms)				Counts				Average Time (ms)			
Portlet Name	Successes	Redirects	Client Errors	Server Errors	Successes	Redirects	Client Errors	Server Errors	Successes	Redirects	Client Errors	Server Errors	Successes	Redirects	Client Errors	Server Errors
Upload	29	0	0	0	98.4	0.0	0.0	0.0	0	0	0	0	0.0	0.0	0.0	0.0
HTML	10	0	0	0	18.4	0.0	0.0	0.0	0	0	0	0	0.0	0.0	0.0	0.0
Rich Text	90	0	0	0	49.3	0.0	0.0	0.0	0	0	0	0	0.0	0.0	0.0	0.0
OmniPortlet	207	0	0	0	917.2	0.0	0.0	0.0	0	0	0	0	0.0	0.0	0.0	0.0
Lottery	5	0	0	0	236.40...	0.0	0.0	0.0	0	0	0	0	0.0	0.0	0.0	0.0
Chart	8	0	0	0	133.40...	0.0	0.0	0.0	0	0	0	0	0.0	0.0	0.0	0.0

To monitor these metrics through Fusion Middleware Control, see Section 30.2, "Viewing Performance Information."

Table 30–20 Portlets - Summary

Metric	Description
Status	The current status of portlets used in the WebCenter application: ■ **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 30.1.5.13, "Portlets and Producers." ■ **Clock** - Unable to query the status of portlets for some reason.
Successful Invocations (%)	The percentage of portlet invocations that succeeded: - Since Startup - Recent History Any request that fails will impact availability. This includes WebCenter application-related failures such as timeouts and internal errors, and also client/server errors. If Successful Invocations (%) is below 100%, check the diagnostic logs to establish why service requests are failing. See, Section 30.3, "Viewing and Configuring Log Information."

Table 30–20 (Cont.) Portlets - Summary

Metric	Description
Invocations	The number of portlet invocations per minute: - Since Startup - Recent History This metric measures each WebCenter application-related portlet request and therefore, due to cache hits, errors, or timeouts on the application, this total may be higher than the number of actual HTTP requests made to the portlet producer.
Average Time (ms)	The average time taken to process operations associated with portlets, regardless of the result: - Since Startup - Recent History

Table 30–21 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 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: ■ **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 ■ 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 30.3, "Viewing and Configuring Log Information."

Table 30–21 (Cont.) Portlet - Detail

Metric	Description
Invocations	The number of invocations, per portlet: - Since Startup - Recent History By sorting the table on this column, you can find the most frequently accessed portlet in your WebCenter application.
Average Time (ms)	The average time each portlet takes to process requests, regardless of the result: - Since Startup - Recent History 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.
Maximum Time (ms)	The maximum time taken to process portlet requests: - Successes - HTTP200xx - Redirects - HTTP300xx - Client Errors - HTTP400xx - Server Errors - HTTP500xx 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.

Table 30–22 Portlet - HTTP Response Code Statistics

Metric	Description
Portlet Name	The name of the portlet being monitored.
Invocations Count - Successes - Redirects - Client Errors - Server Errors	The number of invocations, by type (HTTP response code): - Since Startup - Recent History See also, Table 30–23, " HTTP Response Codes".
Average Time (ms) - Successes - Redirects - Client Errors - Server Errors	The average time each portlet takes to process requests: - Since Startup - Recent History 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.

Table 30–23 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.

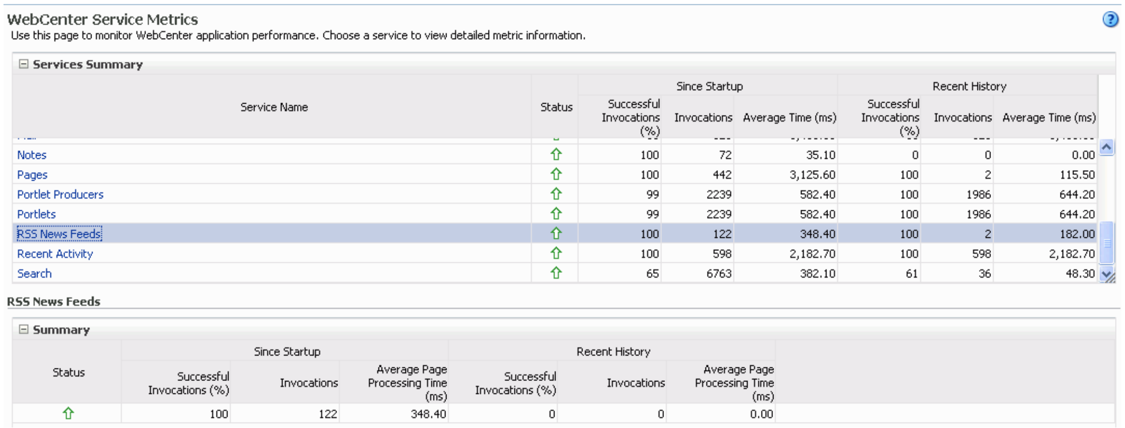
Table 30–23 (Cont.) HTTP Response Codes

HTTP Response and Error Code	Description
300 -Unresolved Redirections	Portlet requests that return any HTTP3xx response code.
400 -Unsuccessful Request Incomplete	Portlet requests that return any HTTP4xx response code.
500 -Unsuccessful Server Errors	Portlet requests that failed for any reason, including requests that return HTTP5xx response codes, or which failed due to a WebCenter application-related error, timeout, bad content type response, or SOAP fault.

30.1.4.15 RSS News Feed Metrics

Performance metrics associated with the RSS service (Figure 30–17) are described in Section 30.1.2, "Common WebCenter Metrics."

Figure 30–17 RSS News Feed Metrics



WebCenter Service Metrics

Use this page to monitor WebCenter application performance. Choose a service to view detailed metric information.

⊟ Services Summary

Service Name	Status	Since Startup			Recent History		
		Successful Invocations (%)	Invocations	Average Time (ms)	Successful Invocations (%)	Invocations	Average Time (ms)
Notes	⇧	100	72	35.10	0	0	0.00
Pages	⇧	100	442	3,125.60	100	2	115.50
Portlet Producers	⇧	99	2239	582.40	100	1986	644.20
Portlets	⇧	99	2239	582.40	100	1986	644.20
RSS News Feeds	⇧	100	122	348.40	100	2	182.00
Recent Activity	⇧	100	598	2,182.70	100	598	2,182.70
Search	⇧	65	6763	382.10	61	36	48.30

RSS News Feeds

⊟ Summary

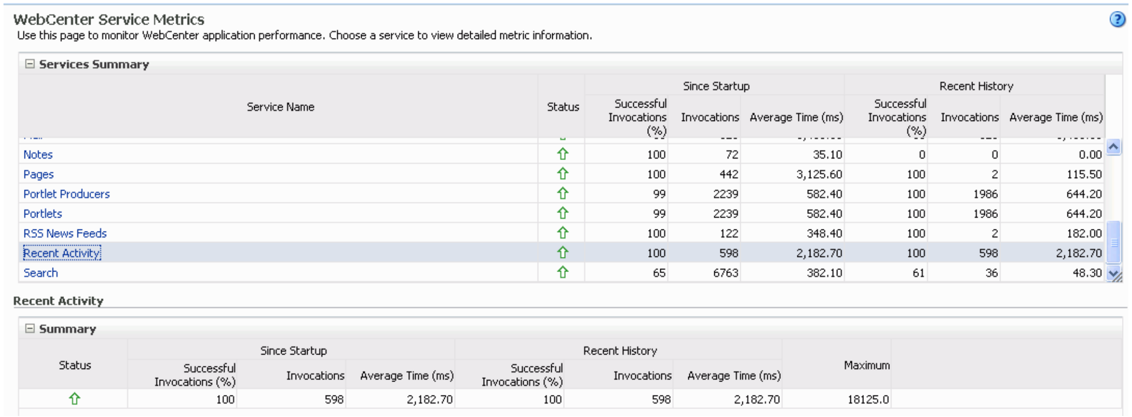
Status	Since Startup			Recent History		
	Successful Invocations (%)	Invocations	Average Page Processing Time (ms)	Successful Invocations (%)	Invocations	Average Page Processing Time (ms)
⇧	100	122	348.40	0	0	0.00

To monitor these metrics through Fusion Middleware Control, see Section 30.2, "Viewing Performance Information."

30.1.4.16 Recent Activity Metrics

Performance metrics associated with the Recent Activities service (Figure 30–18) are described in Section 30.1.2, "Common WebCenter Metrics."

Figure 30–18 Recent Activity Metrics



WebCenter Service Metrics

Use this page to monitor WebCenter application performance. Choose a service to view detailed metric information.

Services Summary

Service Name	Status	Since Startup			Recent History		
		Successful Invocations (%)	Invocations	Average Time (ms)	Successful Invocations (%)	Invocations	Average Time (ms)
Notes	⇧	100	72	35.10	0	0	0.00
Pages	⇧	100	442	3,125.60	100	2	115.50
Portlet Producers	⇧	99	2239	582.40	100	1986	644.20
Portlets	⇧	99	2239	582.40	100	1986	644.20
RSS News Feeds	⇧	100	122	348.40	100	2	182.00
Recent Activity	⇧	100	598	2,182.70	100	598	2,182.70
Search	⇧	65	6763	382.10	61	36	48.30

Recent Activity

Summary

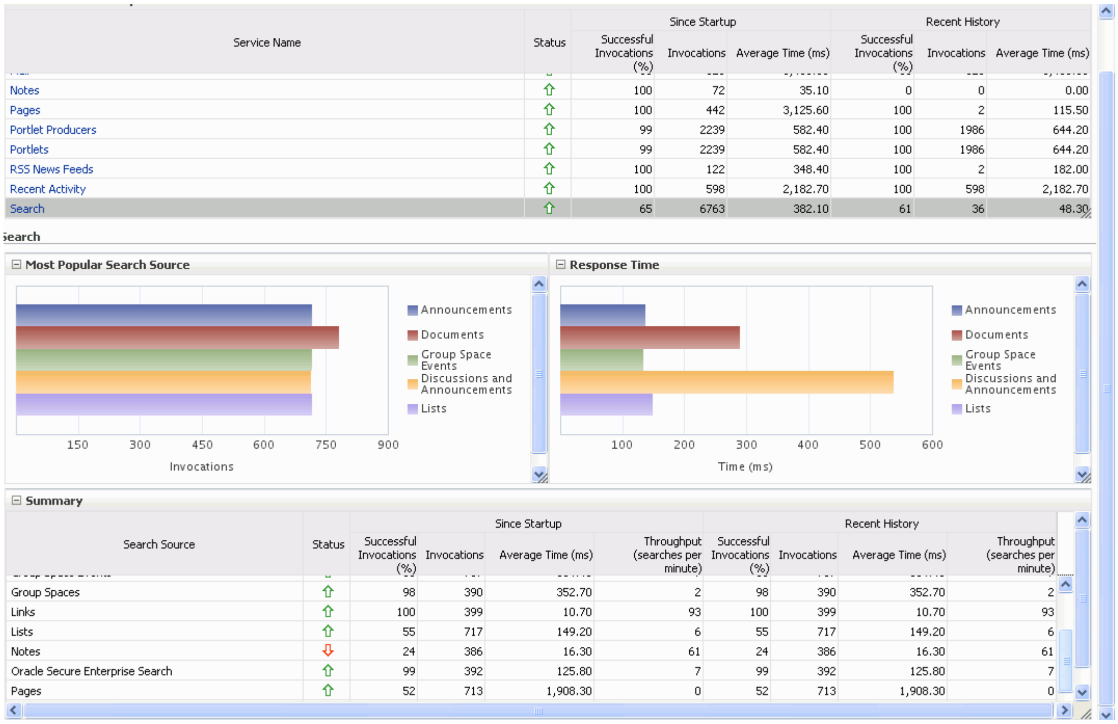
Status	Since Startup			Recent History			Maximum
	Successful Invocations (%)	Invocations	Average Time (ms)	Successful Invocations (%)	Invocations	Average Time (ms)	
⇧	100	598	2,182.70	100	598	2,182.70	18125.0

To monitor these metrics through Fusion Middleware Control, see Section 30.2, "Viewing Performance Information."

30.1.4.17 Search Metrics

Performance metrics associated with the Search service (Figure 30–19) are described in Table 30–24 and Section 30.1.2, "Common WebCenter Metrics."

Figure 30–19 Search Metrics



Service Name	Status	Since Startup			Recent History		
		Successful Invocations (%)	Invocations	Average Time (ms)	Successful Invocations (%)	Invocations	Average Time (ms)
Notes	⇧	100	72	35.10	0	0	0.00
Pages	⇧	100	442	3,125.60	100	2	115.50
Portlet Producers	⇧	99	2239	582.40	100	1986	644.20
Portlets	⇧	99	2239	582.40	100	1986	644.20
RSS News Feeds	⇧	100	122	348.40	100	2	182.00
Recent Activity	⇧	100	598	2,182.70	100	598	2,182.70
Search	⇧	65	6763	382.10	61	36	48.30

Summary

Search Source	Status	Since Startup				Recent History			
		Successful Invocations (%)	Invocations	Average Time (ms)	Throughput (searches per minute)	Successful Invocations (%)	Invocations	Average Time (ms)	Throughput (searches per minute)
Group Spaces	⇧	98	390	352.70	2	98	390	352.70	2
Links	⇧	100	399	10.70	93	100	399	10.70	93
Lists	⇧	55	717	149.20	6	55	717	149.20	6
Notes	⇩	24	386	16.30	61	24	386	16.30	61
Oracle Secure Enterprise Search	⇧	99	392	125.80	7	99	392	125.80	7
Pages	⇧	52	713	1,908.30	0	52	713	1,908.30	0

To monitor these metrics through Fusion Middleware Control, see Section 30.2, "Viewing Performance Information."

Table 30–24 Search Service - Search Sources

Operation	Description
Announcements	Announcement text is searched.

Table 30–24 (Cont.) Search Service - Search Sources

Operation	Description
Documents	Contents in files and folders are searched.
Discussion Forums	Forums and topics are searched.
Group Spaces	Contents saved in a group space, such as links, lists, notes, tags, and group space events are searched.
Group Space Events	Group space events are searched.
Links	Objects to which links have been created are searched (for example, announcements, discussion forum topics, documents, and events).
Lists	Information stored in lists is searched.
Notes	Notes text, such as reminders, is searched.
Oracle Secure Enterprise Search	Contents from the Document Library task flow, discussions, tag clouds, notes, and other WebCenter services are searched.
Pages	Contents added to application, personal, public, wiki, and blog pages are searched.

30.1.5 WebCenter 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 Services, see Appendix A, "WebCenter Configuration."

- Announcements Service
- BPEL Worklist Service
- Content Repository (Documents) Service
- Discussions Service
- External Applications Service
- Events Service
- Instant Messaging and Presence (IMP) Service
- Import and Export
- Lists Service
- Mail Service
- Notes Service
- Page Service
- Portlets and Producers
- RSS Service
- Recent Activities Service
- Search Service

30.1.5.1 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.

30.1.5.2 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.

30.1.5.3 Content Repository (Documents) 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 Content Server and Oracle Portal, verify that the back-end server is up and running.
- For Oracle Content Server, verify that the socket connection is open for the client for which the service is not functioning properly.
- For Oracle Portal, verify the status of the JDBC connection using Oracle WebLogic Administration Console.
- (Functional check) Check logs on the back-end server. For Oracle Content Server, go to Oracle Content Server > Administration > Log files > Content Server Logs. For Oracle Portal use Fusion Middleware Control.
- (Functional check) Search for log entries in which the module name starts with `oracle.vcr`, `oracle.webcenter.content`, `oracle.webcenter.doclib`, and `oracle.stellent`.

30.1.5.4 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 discussions server.
- Connection configuration information associated with the Discussions service is incorrect or no longer valid.

30.1.5.5 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.

30.1.5.6 Events Service

If you are experiencing problems with the Group 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 repository is not available (the database where event information is stored).
- Network connectivity issues exist between the application and the WebCenter repository.
- Connection configuration information associated with the Group Space Events or Personal Events service is incorrect or no longer valid.

30.1.5.7 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.

30.1.5.8 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.

30.1.5.9 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 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.

30.1.5.10 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.

30.1.5.11 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).

30.1.5.12 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 repository is not available (the database where page information is stored).
- Network connectivity issues exist between the application and the WebCenter repository.

30.1.5.13 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.

30.1.5.14 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.

30.1.5.15 Recent Activities Service

If you are facing problems with the Recent Activities service and the status is **Down**, check the diagnostic logs to establish why this service is unavailable. Some typical causes of failure include:

- Search Service is not available.
- A service being searched for recent activity has failed

30.1.5.16 Search Service

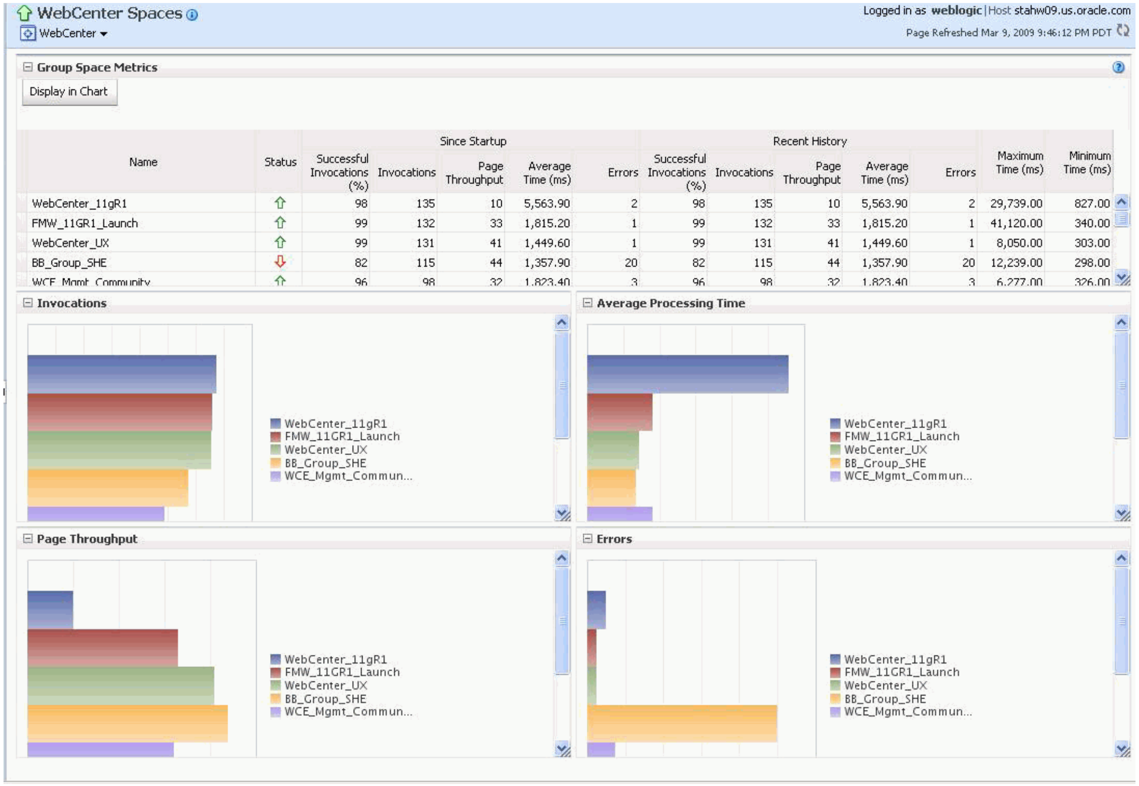
If you are facing problems with the Search service (a service executor) and the status is **Down**, check the diagnostic logs to establish why this executor is unavailable. Some typical causes of failure include:

- The repository of the executor is not available.
- Network connectivity issues exist between the application and the repository of the executor.
- Connection configuration information associated with the executor is incorrect or no longer valid.
- Content repositories being searched is currently unavailable.

30.1.6 Group Space Metrics

(WebCenter Spaces only) Performance metrics associated with group space activity (Figure 30–20) are described in Table 30–25 and Section 30.1.2, "Common WebCenter Metrics."

Figure 30–20 Group Space Metrics



Name	Status	Since Startup					Recent History					Maximum Time (ms)	Minimum Time (ms)
		Successful Invocations (%)	Invocations	Page Throughput	Average Time (ms)	Errors	Successful Invocations (%)	Invocations	Page Throughput	Average Time (ms)	Errors		
WebCenter_11gR1	⇧	98	135	10	5,563.90	2	98	135	10	5,563.90	2	29,739.00	827.00
FMW_11GR1_Launch	⇧	99	132	33	1,815.20	1	99	132	33	1,815.20	1	41,120.00	340.00
WebCenter_UX	⇧	99	131	41	1,449.60	1	99	131	41	1,449.60	1	8,050.00	303.00
BB_Group_SHE	⇩	82	115	44	1,357.90	20	82	115	44	1,357.90	20	12,239.00	298.00
WCE_Mgmt_Community	⇧	96	98	32	1,823.40	3	96	98	32	1,823.40	3	6,277.00	326.00

To monitor these metrics through Fusion Middleware Control, see Section 30.2, "Viewing Performance Information."

Table 30–25 Group Space Metrics

Metric	Description
WebCenter Spaces URL	The WebCenter Spaces application being managed.
WebLogic Server	The WebLogic Server instance in which WebCenter Spaces is deployed.
J2EE Application	The name of the WebCenter Spaces application.
Group Space Page Response	The current average response time (in milliseconds) of group space pages.
Most Popular Group Spaces	Graph showing the most popular group spaces, that is, group spaces recording the most invocations. To compare a different set of group spaces, select one or more group spaces in the table, and then click **Display in Chart**.
Group Space Page Throughput	Graph showing the average number of pages processed per minute for each group space. To compare a different set of group spaces, select one or more group spaces in the table, and then click **Display in Chart**.
Group Space Page Response Time	Graph showing the average page response time (in milliseconds) per group space. To compare a different set of group spaces, select one or more group spaces in the table, and then click **Display in Chart**.
Status	The current status of each group space: ▪ **Up** (Green Up Arrow) - Indicates that the last group space operation was successful. The group space is up and running. ▪ **Down** (Red Down Arrow) - Indicates that the group space is not currently available or the last group space operation was unsuccessful due to an unexpected error or exception. User errors, such as an authentication failure, do not change the status to "Down".
Successful Invocations (%)	The percentage of group space 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 30.3, "Viewing and Configuring Log Information."
Invocations	The number of group space invocations per minute: - Since Startup - Recent History
Page Throughput	The average number of pages processed per minute for each group space: - Since Startup - Recent History
Average Time (ms)	The average time (in ms) to display group space pages: - Since Startup - Recent History
Maximum Time (ms)	The maximum time taken to display a group space page.

Table 30–25 (Cont.) Group Space Metrics

Metric	Description
Minimum Time (ms)	The minimum time taken to display a group space page.

30.2 Viewing Performance Information

Fusion Middleware Control monitors a wide range of performance metrics for WebCenter applications. You can view performance data for all the dependent services, external applications, and portlet producers used by your WebCenter application.

This section includes the following sub sections:

- Monitoring WebCenter Spaces
- Monitoring Custom WebCenter Applications

30.2.1 Monitoring WebCenter Spaces

Administrators can monitor the performance and availability of all the components and services that make up WebCenter Spaces, 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 WebCenter Spaces home page. You can see at a glance which group spaces are the most popular, identify the best and worst performing group spaces and more. For details, see Section 30.1.6, "Group Space Metrics".

The WebCenter Spaces Home page also summarizes the status and performance of individual services, external applications, and any portlet producers that the application uses. When a service is **Down** or running slowly you can drill down to more detailed metrics to troubleshoot the problem, and take corrective action. For metric information, see Section 30.1, "Understanding WebCenter Performance Metrics."

To access performance metrics for WebCenter Spaces:

1. In Fusion Middleware Control Console, navigate to the home page for WebCenter Spaces.

   See Section 6.2, "Navigating to the Home Page for WebCenter Spaces".

2. From the **WebCenter** menu, choose **Monitoring** > **Service Metrics**.

   Use **Services Summary** at the top of the **WebCenter Service Metrics** page to quickly see which services are up and running, and to review individual and relative performances of those services used by WebCenter Spaces.

   Statistics become available when a service, application, or portlet is accessed for the first time. If a service is not configured or has never been used it will not appear in the **Summary** table.

3. Click the name of a service to drill down to more detailed metrics.

To learn more about individual metrics, see Section 30.1, "Understanding WebCenter Performance Metrics".

To access performance summary for WebCenter Spaces:

1. In Fusion Middleware Control Console, navigate to the home page for WebCenter Spaces.

   See Section 6.2, "Navigating to the Home Page for WebCenter Spaces".

2. From the **WebCenter** menu, choose **Monitoring** > **Performance Summary**.

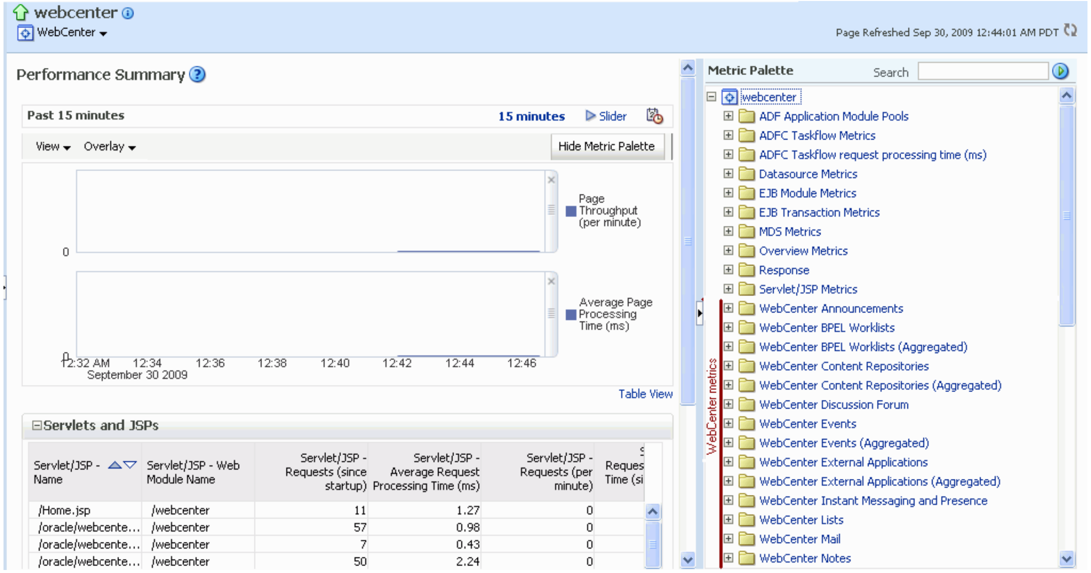
   Use the **Show Metric Palette** button at the top of the **Performance Summary** page to display the **Metric Palette**. This palette enables you to select metrics for services that are up and running, and to review live performances of individual services in graphical and tabular formats.

   Statistics become available when a service, application, or portlet is accessed for the first time. If a service is not configured or has never been used it will not appear in the performance summary graphs and tables.

3. In the **Metric Palette**, expand a service folder and select the metric checkboxes to view the service performance in graphical or tabular format.

   Figure 30–21 shows the Performance Summary page and Metric Palette. In addition to WebCenter 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 30–21 WebCenter Spaces - Performance Summary and Metric Palette



Servlet/JSP - Name	Servlet/JSP - Web Module Name	Servlet/JSP - Requests (since startup)	Servlet/JSP - Average Request Processing Time (ms)	Servlet/JSP - Requests (per minute)	S Reques Time (si
/Home.jsp	/webcenter	11	1.27	0	
/oracle/webcente...	/webcenter	57	0.98	0	
/oracle/webcente...	/webcenter	7	0.43	0	
/oracle/webcente...	/webcenter	50	2.24	0	

30.2.2 Monitoring Custom WebCenter Applications

Administrators can monitor the performance and availability of all the components and services that make up custom WebCenter applications, 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.

To access performance metrics for a custom WebCenter application:

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

See Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications".

2. From the **Application Deployment** menu, choose **WebCenter** > **Service Metrics**.

   Use the **Services Summary** at the top of the **WebCenter Service Metric**s page to quickly see which services are up and running, and to review individual and relative performances of all the services used by the WebCenter application.

   Statistics become available when a service, application, or portlet is accessed for the first time. If a service is not configured or has never been used it will not appear in the Services Summary table.

3. Click the name of a service to drill down to more detailed metrics (Figure 30–21). 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 30.1, "Understanding WebCenter Performance Metrics".

To access performance summary for a custom WebCenter application:

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

   See Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications".

2. From the **Application Deployment** menu, choose **Performance Summary**.

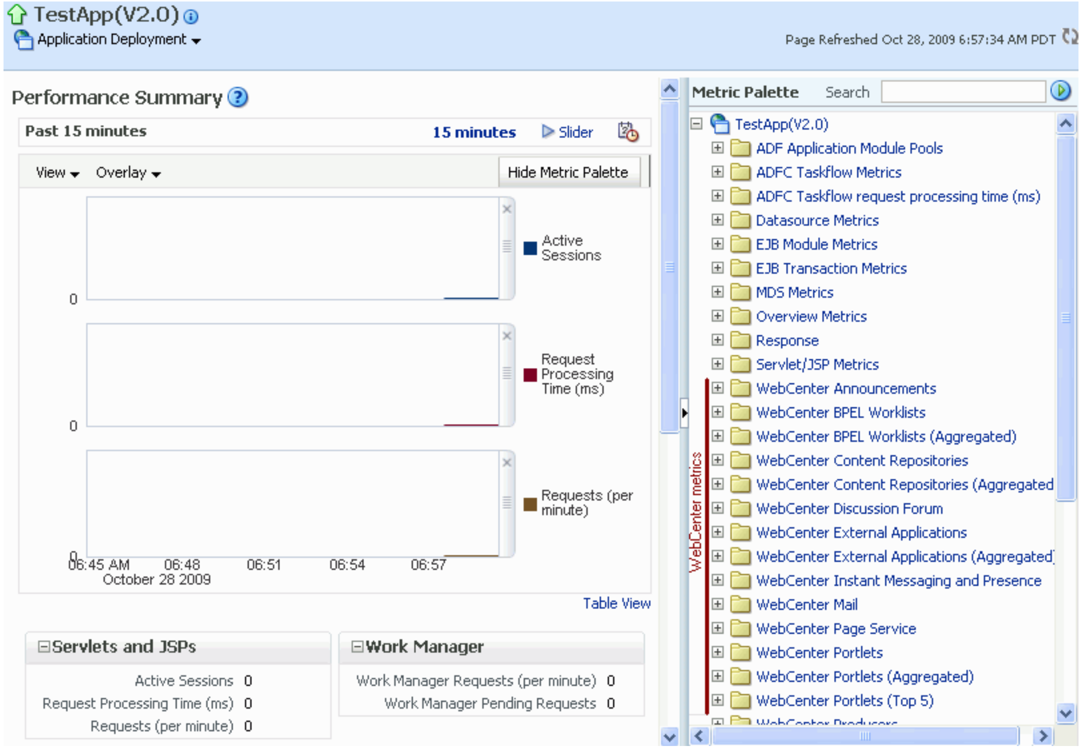
   Use the **Show Metric Palette** button at the top of the **Performance Summary** page to display the **Metric Palette**. This palette enables you to select metrics for services that are up and running, and to review live performances of individual services in graphical and tabular formats.

   Statistics become available when a service, application, or portlet is accessed for the first time. If a service is not configured or has never been used it will not appear in the performance summary graphs and tables.

3. In the **Metric Palette**, expand a service folder and select the metric checkboxes to view the service performance in graphical or tabular format.

   Figure 30–22 shows the Performance Summary page and Metric Palette. In addition to WebCenter 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 30–22 Custom WebCenter Application - Performance Summary and Metric Palette



Servlets and JSPs

Active Sessions	0
Request Processing Time (ms)	0
Requests (per minute)	0

Work Manager

Work Manager Requests (per minute)	0
Work Manager Pending Requests	0

30.3 Viewing and Configuring Log Information

All diagnostic information related to startup and shutdown information, errors, warning messages, access information on HTTP requests, and additional information get stored in log files. To learn how to find information about the cause of an error and its corrective action, see the chapter "Managing Log Files and Diagnostic Data" in *Oracle Fusion Middleware Administrator's Guide*. To learn how to enable diagnostic logging to identify issues, see the section "Configuring Settings for Log Files" in *Oracle Fusion Middleware Administrator's Guide*.

For WebCenter Spaces, the log file, `WLS_Spaces-diagnostic.log` is stored in the *`DOMAIN_HOME`*`/servers/WLS_Spaces/logs` directory.

For custom WebCenter applications, the log file is available in the *`DOMAIN_HOME`*`/servers/`*`ServerName`*`/logs` directory. The log file follows the naming convention of *`ServerName`*`-diagnostics.log`.

For example, for a managed server, `WLS_Custom`, the logs will be stored in the *`DOMAIN_HOME`*`/servers/WLS_Custom/logs`, and the log file name will be `WLS_Custom-diagnostics.log`.

This section includes the following sub sections:

- WebCenter Spaces Logs
- Custom WebCenter Application Logs

30.3.1 WebCenter Spaces Logs

To view log messages for WebCenter Spaces:

1. In Fusion Middleware Control Console, navigate to the home page for WebCenter Spaces.

   See Section 6.2, "Navigating to the Home Page for WebCenter Spaces".

2. From the **WebCenter** menu, choose **Logs** > **View Log Messages**.
3. In the **Log Messages** page, search for warnings, errors, notifications, and so on.

To configure log files for WebCenter Spaces:

1. In Fusion Middleware Control Console, navigate to the home page for WebCenter Spaces.

   See Section 6.2, "Navigating to the Home Page for WebCenter Spaces".

2. From the **WebCenter** menu, choose **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*.

30.3.2 Custom WebCenter Application Logs

To view log messages for custom WebCenter applications:

1. In Fusion Middleware Control Console, navigate to the home page for WebCenter applications.

   See Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications".

2. From the **Application Deployment** menu, choose **Logs > View Log Messages**.
3. In the **Log Messages** page, search for warnings, errors, notifications, and so on.

To configure log files for custom WebCenter applications:

1. In Fusion Middleware Control Console, navigate to the home page for WebCenter applications.

   See Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications".

2. From the **Application Deployment** menu, choose **Logs > Log Configuration**.
3. In the **Log Configuration** page, in the **Log Files** tab, configure log settings.

For more information, see the section "Searching and Viewing Log Files" in *Oracle Fusion Middleware Administrator's Guide*.

31

Managing Export, Import, Backup, and Recovery of WebCenter

Oracle WebCenter 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 provides a set of utilities that enable you to back up this data, move the data between WebCenter applications in staging and production environments. This chapter describes the backup, import, and export capabilities and tools available. It includes the following sections:

- Section 31.1, "Exporting and Importing WebCenter Spaces for Data Migration"
- Section 31.2, "Exporting and Importing Custom WebCenter Applications for Data Migration"
- Section 31.3, "Backing Up and Recovering WebCenter Applications"
- Section 31.4, "Troubleshooting Import and Export Issues for WebCenter Spaces"

To best plan the proper usage of these tools, record which WebCenter features your WebCenter applications are using: WebCenter Framework, WebCenter Spaces, Oracle WebCenter Discussions Server, Oracle WebCenter Wiki and Blog Server, and so on.

Audience

The content of this chapter is intended for Fusion Middleware administrators (users granted the `Admin` role through the Oracle WebLogic Server Administration Console) and WebCenter Spaces administrators (users granted the WebCenter Spaces `Administrator` role or a custom role that grants the `Application-Manage` permission).

See also, Section 1.8, "Understanding Administrative Operations, Roles, and Tools".

31.1 Exporting and Importing WebCenter Spaces for Data Migration

WebCenter Spaces provides a set of export and import utilities that enable you to back up or move content between WebCenter Spaces applications and stage or production environments. This section describes how to export and import the whole WebCenter Spaces application, and also individual group spaces and group space templates. It includes the following subsections:

- Section 31.1.1, "Understanding WebCenter Spaces Export and Import"
- Section 31.1.2, "Prerequisites for WebCenter Spaces Export and Import"

Migrating an entire WebCenter Spaces application:

- Section 31.1.3, "Migrating Back-end Components for an Entire WebCenter Spaces Application"
- Section 31.1.4, "Exporting an Entire WebCenter Spaces Application"
- Section 31.1.5, "Importing an Entire WebCenter Spaces Application"

Migrating group spaces:

- Section 31.1.6, "Prerequisites for Group Space Export and Import"
- Section 31.1.7, "Migrating Back-end Components for Individual Group Spaces"
- Section 31.1.8, "Exporting Group Spaces"
- Section 31.1.9, "Importing Group Spaces"

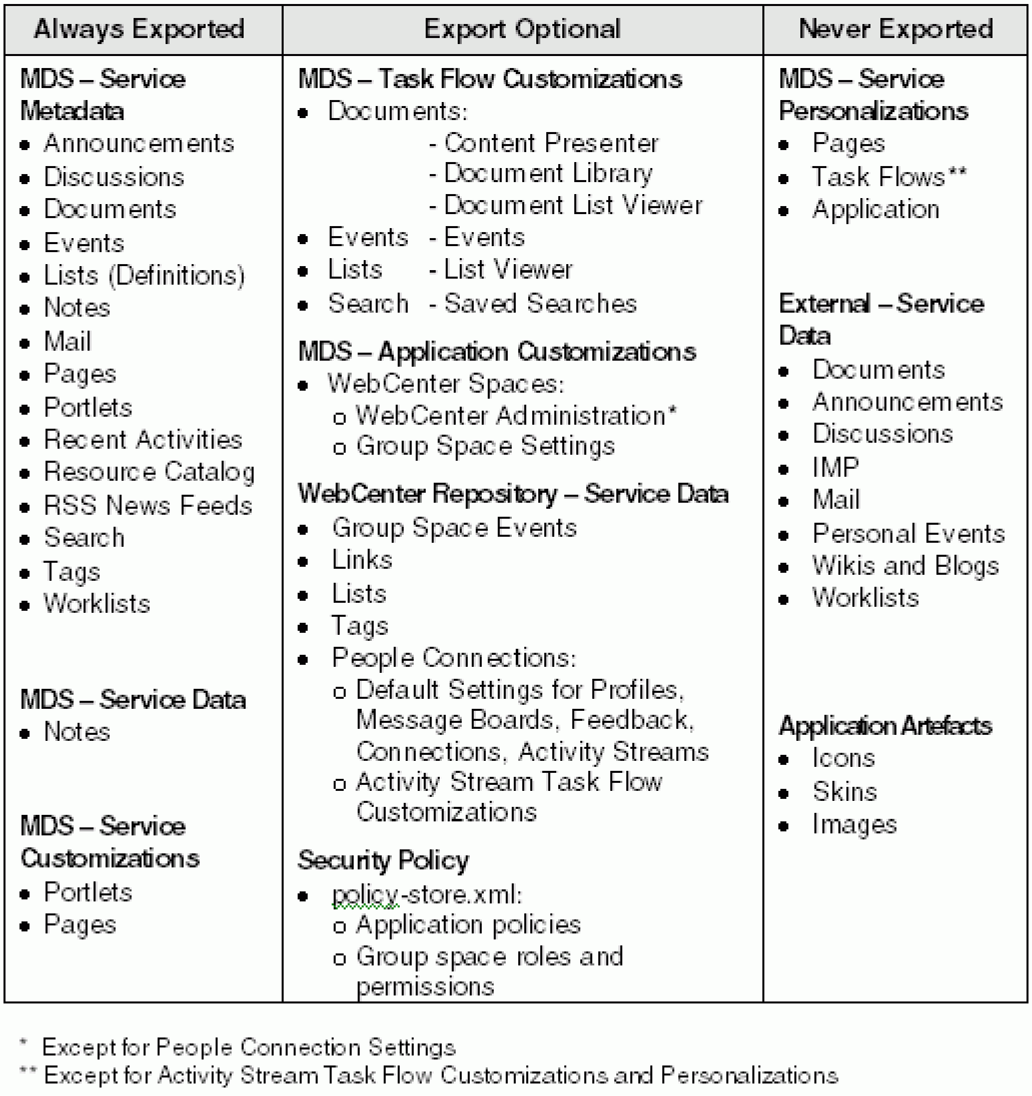
Migrating group space templates:

- Section 31.1.10, "Migrating Back-end Components for Group Space Templates"
- Section 31.1.11, "Exporting Group Space Templates"
- Section 31.1.12, "Importing Group Space Templates"

31.1.1 Understanding WebCenter Spaces Export and Import

Using export and import, Fusion Middleware administrators can migrate entire WebCenter Spaces applications between stage and production environments. This includes every personal space, group space, group space template, and also application and service customizations (applied to the application, pages, and task flows), application and service metadata (object definitions), and data, as outlined in Figure 31–1.

Figure 31–1 Information Exported with WebCenter Spaces



Always Exported	Export Optional	Never Exported
MDS – Service Metadata • Announcements • Discussions • Documents • Events • Lists (Definitions) • Notes • Mail • Pages • Portlets • Recent Activities • Resource Catalog • RSS News Feeds • Search • Tags • Worklists **MDS – Service Data** • Notes **MDS – Service Customizations** • Portlets • Pages	**MDS – Task Flow Customizations** • Documents: - Content Presenter - Document Library - Document List Viewer • Events - Events • Lists - List Viewer • Search - Saved Searches **MDS – Application Customizations** • WebCenter Spaces: o WebCenter Administration* o Group Space Settings **WebCenter Repository – Service Data** • Group Space Events • Links • Lists • Tags • People Connections: o Default Settings for Profiles, Message Boards, Feedback, Connections, Activity Streams o Activity Stream Task Flow Customizations **Security Policy** • policy-store.xml: o Application policies o Group space roles and permissions	**MDS – Service Personalizations** • Pages • Task Flows** • Application **External – Service Data** • Documents • Announcements • Discussions • IMP • Mail • Personal Events • Wikis and Blogs • Worklists **Application Artefacts** • Icons • Skins • Images

* Except for People Connection Settings
** Except for Activity Stream Task Flow Customizations and Personalizations

This migration can be performed using Fusion Middleware Control Console or WLST commands. For details, see:

- Section 31.1.4.1, "Exporting WebCenter Spaces Using Fusion Middleware Control"
- Section 31.1.4.2, "Exporting WebCenter Spaces Using WLST"
- Section 31.1.5.1, "Importing WebCenter Spaces Using Fusion Middleware Control"
- Section 31.1.5.2, "Importing WebCenter Spaces Using WLST"

Group Space and Group Space Template Export and Import

WebCenter Spaces administrators can also export and import individual group spaces and group space templates, and their related objects, through WebCenter Spaces Administration and using WLST Commands.

The primary purpose of these export and import features is to enable cloning and migration of data. The export and import combination enables WebCenter Spaces administrators to:

- Move content between stage and production environments.

- Move content to remote instances.

For more detail, see.

- Section 31.1.8, "Exporting Group Spaces"
- Section 31.1.9, "Importing Group Spaces"
- Section 31.1.11, "Exporting Group Space Templates"
- Section 31.1.12, "Importing Group Space Templates"

Customizations and Personalizations

Some WebCenter Spaces customizations are optional on export, as noted in Figure 31–1. If you want to migrate these customizations you must set the export option "Include Customizations". For more information, reference Table 31–3, " WebCenter Spaces - Service Customizations" and Table 31–4, " WebCenter Spaces - Application and Group Space Customizations" at the end of this chapter.

User personalizations are not migrated during export and import. For more information on customization and personalization and the difference between them, see "Customizing and Personalizing Page Content" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

31.1.2 Prerequisites for WebCenter Spaces Export and Import

The database in which the application metadata or schema is stored must be up and running for the successful completion of the export and import operation.

All the back-end components must be migrated *before* you export or import a WebCenter Spaces application. For more information, refer to the next section, Section 31.1.3, "Migrating Back-end Components for an Entire WebCenter Spaces Application".

WebCenter Spaces is temporarily unavailable during import and export operations to prevent data conflicts. Any user who tries to login or access WebCenter Spaces pages will see an "application unavailable" page.

31.1.3 Migrating Back-end Components for an Entire WebCenter Spaces Application

Before migrating a WebCenter Spaces application, you must migrate all the back-end components that are used by the application. This section tells you how to migrate the Identity Store, Credential Store, Policy Store, Oracle WebCenter Discussions Server, Oracle WebCenter Wiki Server, Oracle 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 will fail.

This section includes the following sub-sections:

- Section 31.1.3.1, "Exporting the LDAP Identity Store"
- Section 31.1.3.2, "Importing the LDAP Identity Store"
- Section 31.1.3.3, "Exporting and Importing the LDAP Credential Store"
- Section 31.1.3.4, "Exporting and Importing the LDAP Policy Store"

- Section 31.1.3.5, "Exporting and Importing a File-based Credential Store"
- Section 31.1.3.6, "Exporting and Importing a File-based Policy Store"
- Section 31.1.3.7, "Exporting Oracle WebCenter Discussions Server"
- Section 31.1.3.8, "Importing Oracle WebCenter Discussions Server"
- Section 31.1.3.9, "Exporting Oracle WebCenter Wiki Server"
- Section 31.1.3.10, "Importing Oracle WebCenter Wiki Server"
- Section 31.1.3.11, "Exporting Oracle Content Server"
- Section 31.1.3.12, "Importing Oracle Content Server"
- Section 31.1.3.13, "Exporting Oracle WebLogic Communications Server"
- Section 31.1.3.14, "Importing Oracle WebLogic Communications Server"
- Section 31.1.3.15, "Exporting Portlet Producers"
- Section 31.1.3.16, "Importing Portlet Producers"

31.1.3.1 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 31–1 shows the `ldapsearch` command for exporting an LDAP identity store. Where `LDAP_OH/bin` is the OID/IdM `IDM_ORACLE_HOME/bin` directory:

Example 31–1 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, for as shown in Example 31–1.

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 Fusion Middleware User Reference for Oracle Identity Management*.

For information on migrating an external LDAP identity store, refer to "Managing Directory Entries" and "Performing Bulk Operations" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

> **Note:** To migrate users, groups, and passwords between two *embedded* LDAP servers, refer to "Exporting and Importing Information in the Embedded LDAP Server" in *Oracle Fusion Middleware Securing Oracle WebLogic Server*. 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.

31.1.3.2 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 31–2 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 31–2 ldapaddmt Utility to Import the ldif File

```
LDAP_OH/bin/ldapaddmt -h ldap_hostname -p ldap_port -D "cn=ldap_user" -w password
-c -r -f my_users.ldif
```

For detailed syntax and examples, see "ldapaddmt" in *Oracle Fusion Middleware User Reference for Oracle Identity Management*.

For information on migrating the LDAP identity store, refer to "Managing Directory Entries" and "Performing Bulk Operations" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

> **Note:** To import users, groups, and passwords from another embedded LDAP server, refer to "Exporting and Importing Information in the Embedded LDAP Server" in *Oracle Fusion Middleware Securing Oracle WebLogic Server*.
>
> 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.

31.1.3.3 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.xm
   l
   ```

   , 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.xm
   l
   ```

   b. In the `jps-config-cred.xml` file, duplicate the following section:

   ```
   <serviceInstance provider="ldap.credentialstore.provider"
   name="credstore.ldap">
     ...
   </serviceInstance>
   ```

The next few steps describes how to edit this new section to point to your *source* credential store. Once complete, `jps-config-cred.xml` file will contain both source and target information for the migration process.

c. First, change the name of the new element to indicate that it contains *source* information. For example, change:

From: `name="credstore.ldap."`

To: `name="credstore.ldap.s"`

d. Modify the domain name, JPS root, and LDAP URL values as appropriate. For example:

```
<serviceInstance provider="ldap.credentialstore.provider"
name="credstore.ldap.s">
            <property value="bootstrap"
name="bootstrap.security.principal.key"/>
            <property value="cn=my_domain"
name="oracle.security.jps.farm.name"/>
            <property value="cn=jpsroot_webcenter_mytest_to_prod"
name="oracle.security.jps.ldap.root.name"/>
            <property value="ldap:myhost:myport" name="ldap.url"/>
        </serviceInstance>
```

e. Since we're only concerned with the credential store, modify the `<jpsContext name="default">` element, removing references to the identity store and the policy store. For example:

```
<jpsContext name="default">
     <serviceInstanceRef ref="keystore"/>
     <serviceInstanceRef ref="audit"/>
     <serviceInstanceRef ref="credstore.ldap"/>
</jpsContext>
```

f. Duplicate the `<jpsContext>` element, and change the name in the new `<jpsContext>` element to "`source`". For example, change:

From: `<jpsContext name="default">`

To: `<jpsContext name="source">`

g. Modify the credential store reference to point to the value specified in step c. For example:

```
<jpsContext name="source">
     <serviceInstanceRef ref="keystore"/>
     <serviceInstanceRef ref="audit"/>
     <serviceInstanceRef ref="credstore.ldap.s"/>
</jpsContext>
```

2. Find the name of the source folder using the `ldapsearch` utility.

For example, enter:

```
LDAP_OH/bin/ldapsearch -h srcldap_hostname -p ldap_port -D  "cn=ldap_user" -w
password -b "" -s sub "cn=<application_name>-*"
```

Where `<application_name>` is the name of the source WebCenter application.

The folder name returned is named: `<application_name>-xxxx`

For WebCenter Spaces, `<application_name>` is always `webcenter`. If, for example, the source folder is named webcenter-1646, the following information might be returned:

```
cn=webcenter-1646,cn=CredentialStore,cn=my_domain, cn=JPSContext,
cn=jpsroot_webcenter_t2ptest
objectclass=top
objectclass=orclContainer
cn=webcenter-1646
```

3. Find the name of the destination folder using the `ldapsearch` utility.

   For example, enter:

   ```
   LDAP_OH/bin/ldapsearch -h dstldap_hostname -p ldap_port -D  "cn=ldap_user" -w
   password -b "" -s sub "cn=<application_name>-*"
   ```

   Where `<application_name>` is the name of the destination WebCenter application.

   The folder name returned is named: `<application_name>-xxxx`

   For WebCenter Spaces, `<application_name>` is always `webcenter`.

4. To import the credential store, run the WLST command `migrateSecurityStore`.

   For example (Example 31–3):

Example 31–3 migrateSecurityStore - Credential Store

```
migrateSecurityStore(type="credStore",
configFile="/MW_HOME/user_projects/domains/my_domain/config/fmwconfig/jps-config-c
red.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*.

31.1.3.4 Exporting and Importing the LDAP Policy Store

With WebCenter Spaces, there is no need for manual policy store migration because the WebCenter Spaces export/import commands migrate security policy data for you. For details, see Section 31.1.4, "Exporting an Entire WebCenter Spaces Application".

While Oracle does not recommend that you perform policy store migration manually for WebCenter Spaces, there may be circumstances where this is required. In such cases, use the WLST command `migrateSecurityStore` to perform the migration as described below.

For custom WebCenter applications, always use the `migrateSecurityStore` command to migrate security policy data.

Before running the `migrateSecurityStore` command you must specify details relating to your *source* policy store in a `jps-config.xml` file.

1. Create your own `jps-config.xml` (named`jps-config-policy.xml` in this example) and then specify the domain name, JPS root, and LDAP URL of the source policy store:

a. Create a copy of your target's `jps-config.xml` file, located at *`DOMAIN_HOME`*`/config/fmwconfig/jps-config.xml`, and name the copy `jps-config-policy.xml` as follows:

```
cp MW_HOME/user_projects/domains/my_domain/config/fmwconfig/jps-config.xml
MW_HOME/user_projects/domains/my_domain/config/fmwconfig/jps-config-policy.
xml
```

b. In the `jps-config-policy.xml` file, duplicate the following section:

```
<serviceInstance provider="ldap.policystore.provider"
name="policystore.ldap">
  ...
</serviceInstance>
```

The next few steps describes how to edit this new section to point to your *source* policy store. Once complete, `jps-config-policy.xml` file will contain both source and target information for the migration process.

c. First, change the name of the new element to indicate that it contains *source* information. For example, change:

From: `name="policystore.ldap."`

To: `name="policystore.ldap.s"`

d. Modify the domain name, JPS root, and LDAP URL values as appropriate. For example:

```
<serviceInstance provider="ldap.policytore.provider"
name="policystore.ldap.s">
            <property value="bootstrap"
name="bootstrap.security.principal.key"/>
            <property value="cn=my_domain"
name="oracle.security.jps.farm.name"/>
            <property value="cn=jpsroot_webcenter_mytest_to_prod"
name="oracle.security.jps.ldap.root.name"/>
            <property value="ldap:myhost:myport" name="ldap.url"/>
        </serviceInstance>
```

e. Duplicate the `<jpsContext>` element, and change the name in the new `<jpsContext>` element to "`source`". For example, change:

From: `<jpsContext name="default">`

To: `<jpsContext name="source">`

f. Modify the policy store reference to point to the value specified in step c, removing references to the identity store and the credential store. For example:

```
<jpsContext name="source">
    <serviceInstanceRef ref="keystore"/>
    <serviceInstanceRef ref="audit"/>
    <serviceInstanceRef ref="policystore.ldap.s"/>
</jpsContext>
```

g. Modify the `<jpsContext name="default">` element, removing references to the identity store and the credential store. For example:

```
<jpsContext name="default">
     <serviceInstanceRef ref="keystore"/>
     <serviceInstanceRef ref="audit"/>
     <serviceInstanceRef ref="policystore.ldap"/>
</jpsContext>
```

2. Find the full name of the source WebCenter application using the `ldapsearch` utility.

   For example, enter:

   ```
   LDAP_OH/bin/ldapsearch -h srcldap_hostname -p srcldap_port -D  "cn=ldap_user"
   -w password -b "" -s sub "orclapplicationcommonname=<application_name>*"
   ```

   Where `<application_name>` is the name of the source WebCenter application.

   The application name returned is: `<application_name>xxxx`

   For WebCenter Spaces, `<application_name>` is always `webcenter.` If, for example, the full source application name is `webcenter#V2.0`, the following information might be returned:

   ```
   cn=webcenter\#V2.0,cn=my_domain,cn=JPSContext,cn=jpsroot_webcenter_t2ptest
   objectclass=top
   objectclass=orclJavaApplicationEntity
   orclapplicationcommonname=webcenter#V2.0
   cn=webcenter#V2.0
   ```

3. Find the full name of the destination WebCenter application using the `ldapsearch` utility.

   For example, enter:

   ```
   LDAP_OH/bin/ldapsearch -h dstldap_hostname -p dstldap_port -D  "cn=ldap_user"
   -w password -b "" -s sub "orclapplicationcommonname=<application_name>*"
   ```

   Where `<application_name>` is the name of the destination WebCenter application.

   The application name returned is: `<application_name>xxxx`

   For WebCenter Spaces, `<application_name>` is always `webcenter`.

4. To import the policy store, run the WLST command `migrateSecurityStore`.

   For example (Example 31–4):

Example 31–4 migrateSecurityStore - Policy Store

```
migrateSecurityStore(type="appPolicies",
configFile="/MW_HOME/user_projects/domains/my_domain/config/fmwconfig/jps-config-p
olicy.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*.

31.1.3.5 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 31–5):

Example 31–5 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.
```

31.1.3.6 Exporting and Importing a File-based Policy Store

With WebCenter Spaces, there is no need for manual policy store migration because the WebCenter Spaces export/import commands migrate security policy data for you. For details, see Section 31.1.4, "Exporting an Entire WebCenter Spaces Application".

While Oracle does not recommend that you perform policy store migration manually for WebCenter Spaces, there may be circumstances where this is required. In such cases, use the WLST command `migrateSecurityStore` to perform the migration as described below.

For custom WebCenter applications, always use the `migrateSecurityStore` command to migrate security policy data.

Before running the `migrateSecurityStore` command you must specify details relating to your *source* policy store in 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/syste
      m-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 31–6):

Example 31–6 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>
```

31.1.3.7 Exporting Oracle WebCenter Discussions Server

To export Oracle WebCenter 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 31–7.
- 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 31–7 Export Database Utility

```
DB_ORACLE_HOME/bin/expdp \"sys/password@serviceid as sysdba\"
OWNER=srcrcuprefix_DISCUSSIONS FILE=/tmp/df.dmp STATISTICS=none
```

where:

- DB_ORACLE_HOME is the directory in which the database for Oracle WebCenter Discussions 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.
- FILE contains the exported data.

31.1.3.8 Importing Oracle WebCenter Discussions Server

To import Oracle WebCenter Discussions Server, 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 Oracle WebCenter Discussions Server.
2. Go to `DB_ORACLE_HOME/bin` of the database where Oracle WebCenter 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;
   ```

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 31–8.

Example 31–8 Database Import Utility

```
DB_ORACLE_HOME/bin/impdp \"sys/password@serviceid as sysdba\"
FROMUSER=srcrcuprefix_DISCUSSIONS TOUSER=tgtrcuprefix_DISCUSSIONS FILE=/tmp/df.dmp
STATISTICS=none
```

where:

- `DB_ORACLE_HOME` is the directory in which the database for Oracle WebCenter Discussions Server schema is installed.
- `password` is the password for the system database user.
- `serviceid` is the service ID of the database connection.
- `FROMUSER` is the exported schema.
- `TOUSER` is the imported schema. This is the RCU suffix that was used during installation, _DISCUSSIONS, along with the user supplied prefix. For example, DEV_DISCUSSIONS.
- `FILE` contains the data to be imported.

31.1.3.9 Exporting Oracle WebCenter Wiki Server

To export Oracle WebCenter Wiki 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 31–9.
- 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 WIKI schema. Therefore Oracle recommends using Oracle Database Utilities. See also, the Oracle Database Utilities guide.

Example 31–9 Data Pump Export Utility

```
DB_ORACLE_HOME/bin/expdp \"sys/password@serviceid as sysdba\"
OWNER=srcrcuprefix_WIKI FILE=/tmp/wiki.dmp STATISTICS=none
```

where:

- `DB_ORACLE_HOME` is the directory in which the database for Oracle WebCenter Wiki 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, _WIKI, along with the user supplied prefix. For example, DEV_WIKI.
- `FILE` contains the exported data.

31.1.3.10 Importing Oracle WebCenter Wiki Server

To import Oracle WebCenter Wiki Server data, use the appropriate 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 WIKI schema. Therefore, Oracle recommends using Oracle Database Utilities. See also, the Oracle Database Utilities guide.

1. Shut down the target Oracle WebCenter Wiki Server.
2. Go to *`DB_ORACLE_HOME`*`/bin` of the database where Oracle WebCenter Wiki 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_WIKI cascade;
   ```

4. Create the target user:

   ```
   create user tgtrcuprefix_WIKI identified by password default tablespace
   tgtrcuprefix_WIKI temporary tablespace name_TEMP;
   ```

5. Grant connect and resource to the user:

   ```
   grant connect,resource to tgtrcuprefix_WIKI;
   ```

6. Exit `sqlplus`.
7. Run the import tool as described in Example 31–10.

Example 31–10 Database Import Utility

```
DB_ORACLE_HOME/bin/impdp \"sys/password@serviceid as sysdba\"
FROMUSER=srcrcuprefix_WIKI TOUSER=tgtrcuprefix_WIKI FILE=/tmp/wiki.dmp
STATISTICS=none
```

where:

- `DB_ORACLE_HOME` is the directory in which the database for Oracle WebCenter Wiki Server schema is installed.
- `password` is the password for the system database user.
- `serviceid` is the service ID of the database connection.
- `FROMUSER` is the exported schema.
- `TOUSER` is the imported schema. This is the RCU suffix that was used during installation, _WIKI, along with the user supplied prefix. For example, DEV_WIKI.
- `FILE` contains the data to be imported.

31.1.3.11 Exporting Oracle Content Server

First use Oracle Data Pump to export the Oracle 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 Oracle Content Server using the Oracle Data Pump export utility.

   For example, go to *ORACLE_HOME*`/bin` of your database and run the command described in Example 31–11.

   > **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 31–11 Data Pump Utility (Export)

```
DB_ORACLE_HOME/bin/expdp \"sys/password@serviceid as sysdba\"
OWNER=srcrcuprefix_OCSERVER FILE=/tmp/ucm.dmp STATISTICS=none
```

where:

- `DB_ORACLE_HOME` is the directory in which the database for Oracle 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, `_OCSERVER`, along with the user supplied prefix. For example, `DEV_OCSERVER`.
- `FILE` 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
     ```

31.1.3.12 Importing Oracle Content Server

First use Oracle Data Pump to import the source Oracle 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. Import Oracle Content Server using the Oracle Data Pump import utility.

   For example, go to *`ORACLE_HOME`*`/bin` of your database and run the command described in Example 31–12.

> **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 31–12 Data Pump Utility (Import)

```
DB_ORACLE_HOME/bin/impdp  \"sys/password@serviceid as sysdba\"
FROMUSER=srcrcuprefix_OCSERVER TOUSER=tgtrcuprefix_OCSERVER FILE=/tmp/UCM.dmp
STATISTICS=none TRANSFORM=oid:n
```

where:

- `DB_ORACLE_HOME` is the directory in which the database for Oracle Content Server schema is installed.
- `password` is the password for system database user.
- `serviceid` is the service ID of the database connection.
- `FROMUSER` is the exported schema.

- TOUSER is the imported schema. This is the RCU suffix that was used during installation, _OCSERVER, along with the user supplied prefix. For example, DEV_OCSERVER.
- FILE contains the data to be imported.

2. 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 Content Server, log in to WebCenter Spaces and open any imported group space. Verify that the Documents service is enabled in that group space and that imported group space folders are available as expected.

31.1.3.13 Exporting Oracle WebLogic Communications Server

For information on exporting Oracle WebLogic Communications Server, see *Oracle WebLogic Communication Services Administrator's Guide*.

31.1.3.14 Importing Oracle WebLogic Communications Server

For information on importing Oracle WebLogic Communications Server, see *Oracle WebLogic Communication Services Administrator's Guide*.

31.1.3.15 Exporting Portlet Producers

This step is only require to migrate entire producer metadata and not just the producer metadata associated with your WebCenter Spaces application. For information on how to export entire producer metadata, see the appendix "Portlet Preference Store Migration Utilities" in *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*.

31.1.3.16 Importing Portlet Producers

This step is only required to migrate entire producer metadata and not just the producer metadata associated with your WebCenter Spaces application. For information on how to import entire producer metadata, see the appendix "Portlet Preference Store Migration Utilities" in *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*.

31.1.4 Exporting an Entire WebCenter Spaces Application

This section describes how to export an entire WebCenter Spaces application using Oracle Enterprise Manager Fusion Middleware Control and WLST commands.

A WebCenter Spaces application is exported into a single export archive (.ear file). The EAR file contains a metadata archive (.mar file) and a single XML file containing the security policy information. You can save export archives to your local file system or to a remote server file system. For more information about what is exported, read Section 31.1.1, "Understanding WebCenter Spaces Export and Import".

WebCenter Spaces is temporarily unavailable during import and export operations to prevent data conflicts. Any user who tries to login or access WebCenter Spaces pages will see an "application unavailable" page.

The export process does not include data associated with external services, that is, Mail, Discussions, Announcements, Worklists, Wiki, Blogs, Personal Events, Instant Messaging and Presence (IMP), and Documents. To learn how to move data associated with these services, see Section 31.1.3, "Migrating Back-end Components for an Entire WebCenter Spaces Application".

If a shared identity store is not used and the users in both the export and import environment must be identical, then these users must also be migrated. Refer to Section 31.1.3, "Migrating Back-end Components for an Entire WebCenter Spaces Application".

> **Note:** No icons, skins, images, out-of-the-box templates, or personalizations are exported. For more information on personalizations, see the section "Personalizing Your Page View" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

This section includes the following:

- Section 31.1.4.1, "Exporting WebCenter Spaces Using Fusion Middleware Control"
- Section 31.1.4.2, "Exporting WebCenter Spaces Using WLST"

31.1.4.1 Exporting WebCenter Spaces Using Fusion Middleware Control

Fusion Middleware administrators can export an entire WebCenter application using Fusion Middleware Control.

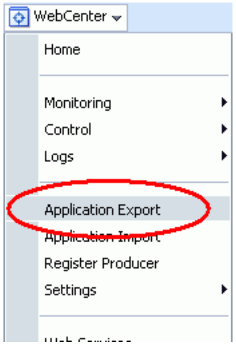
To export WebCenter Spaces:

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

   See Section 6.2, "Navigating to the Home Page for WebCenter Spaces".

2. From the **WebCenter** menu, select **Application Export**, as shown in Figure 31–2.

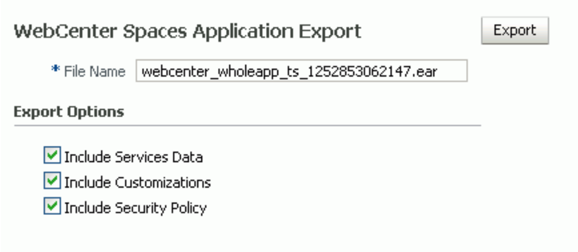
Figure 31–2 WebCenter Menu - Application Export Option



3. Change the **File Name** for the export archive or accept the default name.

   To ensure uniqueness, the default `.ear` filename contains a timestamp: `webcenter_wholeapp_ts_`*`timestamp`*`.ear`, as shown in Figure 31–3.

Figure 31–3 Naming the Export Archive



WebCenter Spaces Application Export

* File Name webcenter_wholeapp_ts_1252853062147.ear

Export Options

☑ Include Services Data
☑ Include Customizations
☑ Include Security Policy

4. Set export options as required. For details, see Table 31–1.

Table 31–1 WebCenter Spaces Application Export Options

Field	Description

Include Services Data	Select to export data stored in the WebCenter repository for the following services: Activity Streams, Events, Feedback, Lists, Links, Message Boards, Connections, and Profiles. Note data stored in the MDS repository is exported too.
	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.
	If the application selected for export contain a large amount of data, consider using the database export utilities to export (and import) the WebCenter schema data instead. For example:
	`DB_ORACLE_HOME/bin/expdp \"sys/password@serviceid as sysdba\" OWNER=srcrcuprefix_WEBCENTER FILE=/tmp/WCS.dmp STATISTICS=none`
	`DB_ORACLE_HOME/bin/impdp \"sys/password@serviceid as sysdba\" FROMUSER=srcrcuprefix_WEBCENTER TOUSER=tgtrcuprefix_WEBCENTER FILE=/tmp/WCS.dmp STATISTICS=none TRANSFORM=oid:n`
	For details, refer to the *Oracle Database Utilities* guide.
	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.
	Note: The export process does *not* 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 31.1.3, "Migrating Back-end Components for an Entire WebCenter Spaces Application".

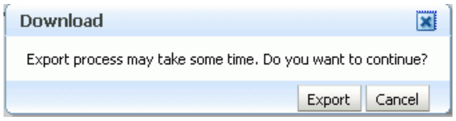
Include Customizations	Select to export application customizations. For information about which customizations are optional on export, see Table 31–3 and Table 31–4. If you deselect this option, WebCenter Spaces is exported without these application customizations. Portlet and page customizations are always exported. See also Figure 31–1, "Information Exported with WebCenter Spaces".

Table 31–1 (Cont.) WebCenter Spaces Application Export Options

Field	Description
Include Security Policy	Select to generate an XML file (`policy-store.xml`) listing: - WebCenter Spaces application roles (and permissions assigned to each role). - WebCenter user role assignments. - Group space members (and their role assignments). Deselect this option if you do not want to export user details, that is, users and their current role assignments. When you import an application without any user data, existing permissions (if any) are removed and the WebCenter Spaces administrator who is importing the application becomes the default moderator for any group spaces that are imported. This option is useful when exporting an application between a stage and production environment for the first time and where users added during the testing phase are no longer required. **Tip**: Always *select* this option when backing up WebCenter Spaces so that you can restore the application's security policy. If you deselect this option, no security policy will exist after the import/restore operation.

5. Click **Export**.
6. In the Download dialog, as shown in Figure 31–3, click **Export** to confirm that you want to go ahead.

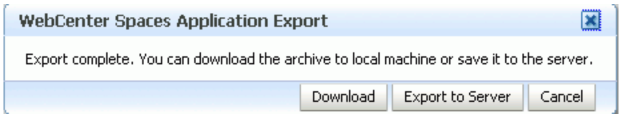
Figure 31–4 Downloading an Export Archive



Progress information is displayed during the export process. The application being exported cannot be accessed during export operations.

7. When the export process is complete, specify a location for the export archive (`.ear`).

Figure 31–5 Saving an Export Archive


WebCenter Spaces Application Export
Export complete. You can download the archive to local machine or save it to the server.
Download
Export to Server
Cancel

Select one of:

- **Download** - Saves the export EAR file to your local file system.

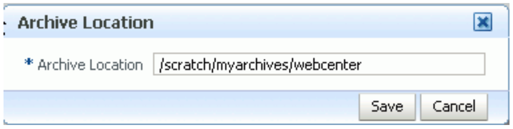
  Your Browser will download and save the archive locally. The actual download location depends on your Browser set up.

- **Save to Server** - Saves the export EAR file to a server location.

  When the Archive Location dialog box displays (Figure 31–6), 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 31–6 Saving Export Archives to a Server Location



Archive Location: /scratch/myarchives/webcenter

8. Click **Close** to dismiss the Export window.

The export archive (.EAR) is saved to the specified location.

Check the diagnostic log file, `WLS_Spaces-diagnostics.log`, for 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 30.3, "Viewing and Configuring Log Information". See also Section 31.4, "Troubleshooting Import and Export Issues for WebCenter Spaces".

31.1.4.2 Exporting WebCenter Spaces Using WLST

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

WebCenter Spaces is temporarily unavailable during export operations to prevent data conflicts. Any user who tries to login or access WebCenter Spaces pages will see an "application unavailable" page.

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

> **Note:** No icons, skins, images, out-of-the-box templates, or personalizations are exported. For more information on personalizations, see the section "Personalizing Your Page View" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

31.1.5 Importing an Entire WebCenter Spaces Application

This section describes how to import an entire WebCenter Spaces application using Fusion Middleware Control and WLST commands.

Before importing WebCenter Spaces:

- Migrate the LDAP Identity Store, Credential Store, Policy Store, Oracle WebCenter Discussions Server, Oracle WebCenter Wiki Server, Oracle Content Server, Oracle WebLogic Communications Server, and portlet producers. See Section 31.1.3, "Migrating Back-end Components for an Entire WebCenter Spaces Application".

  Personal pages 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 repository, MDS, and your policy store. See Section 31.3, "Backing Up and Recovering WebCenter Applications".

- Check that all users assigned to the `Administrator` role exist in the target identity store. On import, users listed in the WebCenter Spaces security policy are checked against the identity store that is configured for the domain. If a user is not found, any policies associated with that user are removed. See also, Section 24.5, "Moving the Administrator Account to an External LDAP Server."

- Confirm that the WebCenter Spaces archive (.ear) that you want to import was exported from WebCenter Spaces 11.1.1.2.0 or later. You cannot import archives from earlier versions (such as 11.1.1.1.0) directly into WebCenter Spaces 11.1.1.3.0. If necessary, you must upgrade to 11.1.1.2.0 or 11.1.1.3.0 before you create the export archive.

WebCenter Spaces is temporarily unavailable during import and export operations to prevent data conflicts. Any user who tries to login or access WebCenter Spaces pages will see an "application unavailable" page.

This section includes the following:

- Section 31.1.5.1, "Importing WebCenter Spaces Using Fusion Middleware Control"
- Section 31.1.5.2, "Importing WebCenter Spaces Using WLST"

31.1.5.1 Importing WebCenter Spaces Using Fusion Middleware Control

Fusion Middleware administrators can import an entire WebCenter application using Fusion Middleware Control.

To import a WebCenter Spaces application using Fusion Middleware Control:

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

   See Section 6.2, "Navigating to the Home Page for WebCenter Spaces".

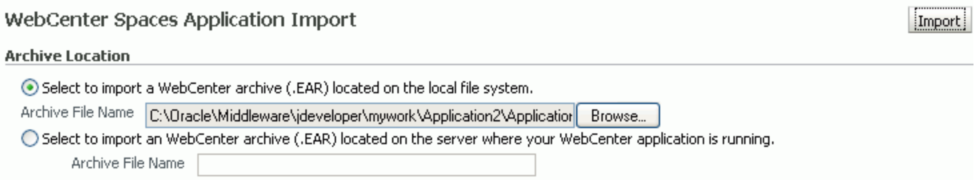
2. From the **WebCenter** menu, select **Application Import**.

3. In the WebCenter Spaces Application Import page, as shown in Figure 31–7, specify the location of your WebCenter Spaces application archive (`.ear`). Select one of the following:

   - **Archive Located on Local File System** - Enter the **File System Location**. Alternatively, click **Browse** to locate the directory on the local file system where the `.ear` file is stored.
   - **Archive Located on Server File System** - Enter the **Server Location**. Any shared location accessible from this WebCenter Spaces application.

   The `.ear` you select must contain an entire WebCenter Spaces application export—you cannot import individual group spaces from here. Refer to Chapter 38, "Exporting and Importing Group Spaces" for more information.

Figure 31–7 WebCenter Spaces Application Import Page



WebCenter Spaces Application Import

Archive Location

● Select to import a WebCenter archive (.EAR) located on the local file system.

Archive File Name: C:\Oracle\Middleware\jdeveloper\mywork\Application2\Applicatior

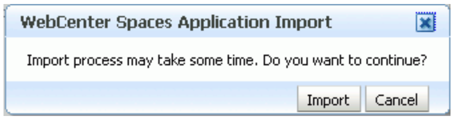
○ Select to import an WebCenter archive (.EAR) located on the server where your WebCenter application is running.

Archive File Name:

4. Click **Import**.

5. In the WebCenter Spaces Application Import dialog, as shown in Figure 31–8, click **Import**.

Figure 31–8 WebCenter Spaces Application Import dialog



WebCenter Spaces Application Import

Import process may take some time. Do you want to continue?

Once the import is complete, a success message displays.

6. Restart the managed server on which the newly imported WebCenter Spaces application is deployed.

   In a cluster environment, restart each managed server in the cluster. See also, see Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments".

7. Initiate the Oracle Secure Enterprise Search crawler to index newly imported data.

   See also, *Oracle Secure Enterprise Search Administrator's Guide*.

31.1.5.2 Importing WebCenter Spaces Using WLST

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

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

Note: After import:

- Restart the managed server on which the newly imported WebCenter Spaces application is deployed. In a cluster environment, restart each managed server in the cluster. See also, see Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments".
- Initiate the Oracle Secure Enterprise Search crawler to index newly imported data.

31.1.6 Prerequisites for Group Space Export and Import

To export one or more group spaces, the WebCenter Spaces application which contains the group spaces must be up and running, and all the group spaces you want to export must be offline to prevent data conflicts. See, Section 37.3.1, "Taking Any Group Space Offline".

Group space data associated with some back-end components, specifically Oracle WebCenter Discussions Server and Oracle WebCenter Wiki Server, must be migrated *after* you export or import group spaces. See next section, Section 31.1.7, "Migrating Back-end Components for Individual Group Spaces".

Note: The simultaneous export or import of large numbers of group spaces is not recommended as, depending on server configuration, it may affect system performance. If a serious deterioration in performance is observed, break the export or import down into several smaller groups.

31.1.7 Migrating Back-end Components for Individual Group Spaces

When migrating one or more group spaces, you must also migrate the back-end components used by the group space. This section tells you how.

This section includes the following sub sections:

- Section 31.1.7.1, "Exporting Discussions for a Group Space"
- Section 31.1.7.2, "Importing Discussions for a Group Space"
- Section 31.1.7.3, "Exporting Wikis and Blogs for a Group Space"
- Section 31.1.7.4, "Importing Wikis and Blogs for a Group Space"
- Section 31.1.7.5, "Exporting Documents for a Group Space"
- Section 31.1.7.6, "Importing Documents for a Group Space"

You must import the group spaces on to the target *before* importing these back-end components.

31.1.7.1 Exporting Discussions for a Group Space

Use the Oracle WebCenter Discussions Server Admin Console to export discussions associated with a particular group space.

Group space discussions are exported to an `.xml` file, and saved to a `.zip` file in the `DOMAIN_HOME/config/fmwconfig/servers/<target_server_name>/owc_discussions_11.1.1.2.0/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/WLS_Services/owc_discussions_11.1.1.2.0/data/`.

Before importing group space discussions on the target system, the target group space must exist. See Section 31.1.9.1, "Importing Group Spaces Using WebCenter Spaces".

To export group space discussions:

1. Login to the Oracle WebCenter Discussions Server Admin Console.

   You can login directly if you know the console's URL. For example: `http://example.com:8890/owc_discussions/admin`

   Alternatively, login through WebCenter Spaces as follows:

   a. Login to WebCenter Spaces with administrative privileges.

      See Section 32.1, "Logging into WebCenter Spaces as an Administrator."

   b. Click the **Administration** link at the top of the application.

   c. Click the **Group Spaces** tab.

   d. From the **Actions** menu, choose **Edit Group Space**, for the group space you want to export.

   e. Click the **Services** tab, then **Discussions**.

   f. Note down the **Forum Name/ID** or **Category Name/ID** associated with this group space.

      Oracle WebCenter Discussions Server generates discussion category and forum IDs sequentially. If this ID exists on the target system, the imported forum (or category) will be assigned a new, unique ID, and therefore you must reconfigure the imported group space, to point to the new ID. For details, see Section 31.1.9.1, "Importing Group Spaces Using WebCenter Spaces" - Step 11.

g. Click **Forum Administration**, and login to the Admin Console.

2. In the Admin Console, select the **System** menu and choose **XML Export & Import** in the sidebar.

3. Select **Data Export**.

4. Set the following options (Figure 31–9):

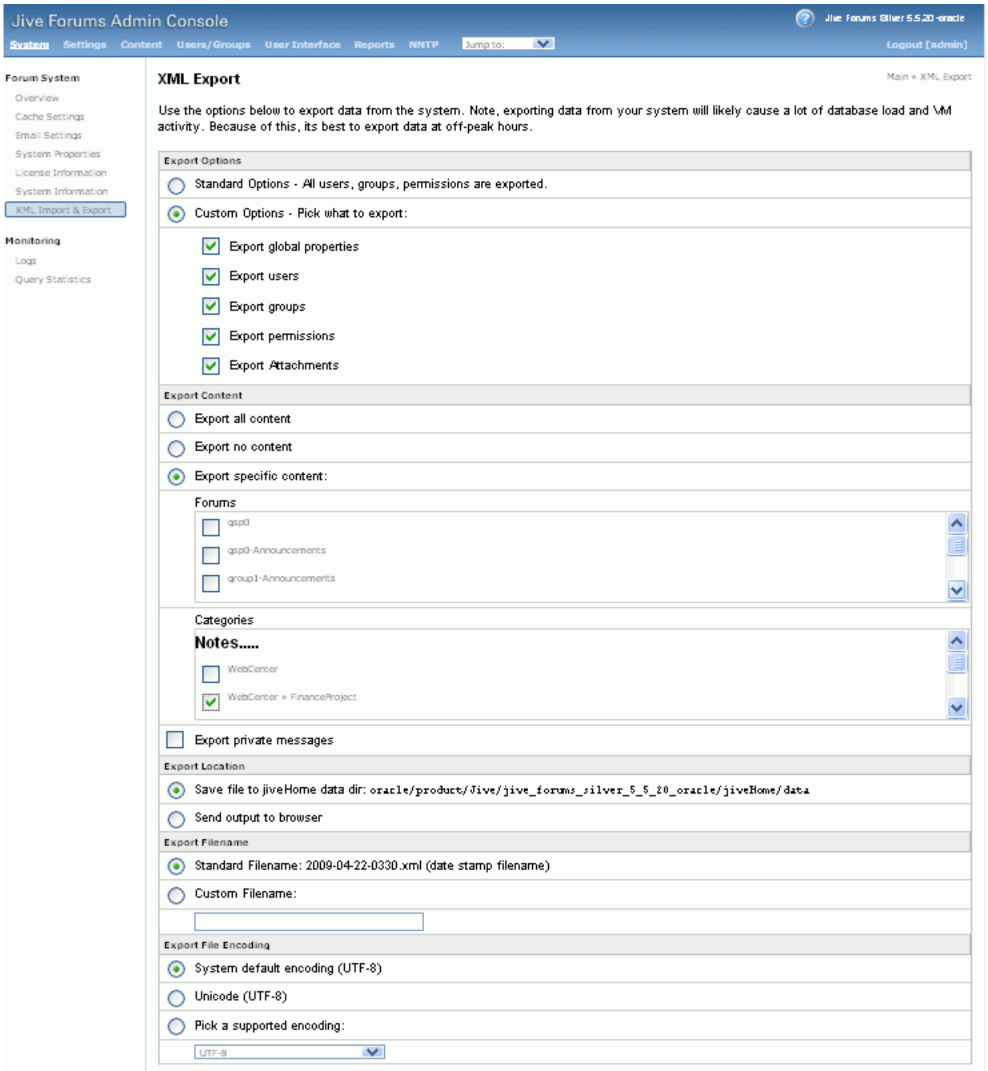
   a. **Export Options** - Select **Custom Options**, and select all the check boxes.

   b. **Export Content** - Select **Export Specific Content**, and select the name of the forum or category required.

      Note: Group spaces that support multiple forums will use a category to store discussions. Other group spaces use a single forum.

   c. **Export location, Export filename, Export file encoding** - Keep the default values.

Figure 31–9 Exporting Group Space Discussions



XML Export

Use the options below to export data from the system. Note, exporting data from your system will likely cause a lot of database load and VM activity. Because of this, its best to export data at off-peak hours.

Export Options

○ Standard Options - All users, groups, permissions are exported.

● Custom Options - Pick what to export:

☑ Export global properties

☑ Export users

☑ Export groups

☑ Export permissions

☑ Export Attachments

Export Content

○ Export all content

○ Export no content

● Export specific content:

Forums

□ qsp0

□ qsp0-Announcements

□ group1-Announcements

Categories

Notes.....

□ WebCenter

☑ WebCenter » FinanceProject

□ Export private messages

Export Location

● Save file to jiveHome data dir: `oracle/product/Jive/jive_forums_silver_5_5_20_oracle/jiveHome/data`

○ Send output to browser

Export Filename

● Standard Filename: 2009-04-22-0330.xml (date stamp filename)

○ Custom Filename:

Export File Encoding

● System default encoding (UTF-8)

○ Unicode (UTF-8)

○ Pick a supported encoding:

UTF-8

5. Click **Start Export**.

6. Once complete, copy the `.zip` file (that contains the export `.xml` file) from the `MW_HOME/user_projects/domains/my_domain/config/fmwconfig/servers/<server_name>/owc_discussions_11.1.1.2.0/data` directory to same location on the target discussions server.

   For example, `MW_HOME/user_projects/domains/my_domain/config/fmwconfig/servers/WLS_Services/owc_discussions_11.1.1.2.0/data`.

Before importing group space discussions on the target system, the group space you are migrating must exist on the target. See Section 31.1.9.1, "Importing Group Spaces Using WebCenter Spaces".

31.1.7.2 Importing Discussions for a Group Space

Use the Oracle WebCenter Discussions Server Admin Console to import group space discussions exported from another WebCenter Spaces application.

Ensure that the associated group space exists on the target before you import the group space discussion data. See Section 31.1.8.1, "Exporting Group Spaces Using WebCenter Spaces".

> **Note:** Oracle WebCenter Discussions Server generates discussion category and forum IDs sequentially. Therefore, when importing discussion data between two targets (or source to target), there is a chance that the same IDs will exist on both systems. When ID clashes occur, the imported forum (or category) is assigned a new, unique ID and therefore you must reconfigure the group space to point to the new ID. See Step 11 below for details.

To import group space discussions:

1. Login to the Oracle WebCenter Discussions Server Admin Console.

   You can login directly if you know the console's URL. For example: `http://example.com:8890/owc_discussions/admin`

   Alternatively, login through WebCenter Spaces as follows:

   a. Login to WebCenter Spaces with administrative privileges.

      See Section 32.1, "Logging into WebCenter Spaces as an Administrator."

   b. Click the **Administration** link at the top of the application.

   c. Click the **Group Spaces** tab.

   d. From the **Actions** menu, choose **Edit Group Space**, for the group space you want to export.

   e. Click the **Service** tab, then **Discussions**.

   f. Click **Forum Administration**, and login to the Admin Console.

2. In the Admin Console, select the **System** menu and then choose **XML Export & Import** in the sidebar.

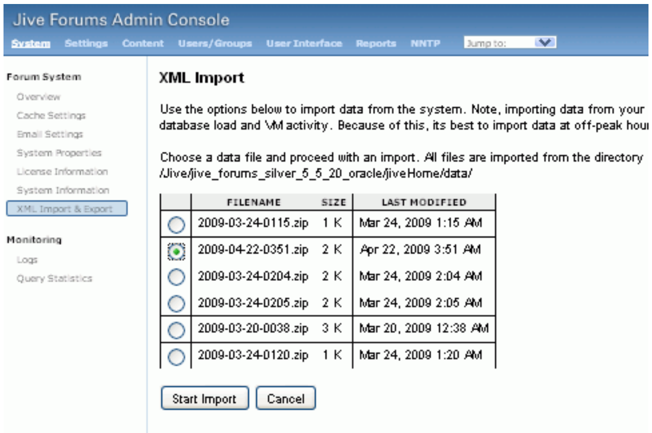
3. Select **Data Import**.

4. Choose the appropriate group space export file from the list available (Figure 31–10).

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_11.1.1.2.0/data/` to same location on this target. See also, Section 31.1.7.1, "Exporting Discussions for a Group Space".

Where `DOMAIN_HOME` is the path to the Oracle WebLogic Server domain. For example, `MW_HOME/user_projects/domains/my_domain/config/fmwconfig/servers/WLS_Services/owc_discussions_11.1.1.2.0/data/`.

Figure 31–10 Importing Group Space Discussions



XML Import

Use the options below to import data from the system. Note, importing data from your database load and VM activity. Because of this, its best to import data at off-peak hou

Choose a data file and proceed with an import. All files are imported from the directory /Jive/jive_forums_silver_5_5_20_oracle/jiveHome/data/

	FILENAME	SIZE	LAST MODIFIED
○	2009-03-24-0115.zip	1 K	Mar 24, 2009 1:15 AM
●	2009-04-22-0351.zip	2 K	Apr 22, 2009 3:51 AM
○	2009-03-24-0204.zip	2 K	Mar 24, 2009 2:04 AM
○	2009-03-24-0205.zip	2 K	Mar 24, 2009 2:05 AM
○	2009-03-20-0038.zip	3 K	Mar 20, 2009 12:38 AM
○	2009-03-24-0120.zip	1 K	Mar 24, 2009 1:20 AM

5. Click **Start Import**.

   On import, the group space discussions data is copied to the discussions server. In the next step you will reassociate the group space you migrated earlier with this newly imported data.

6. Select the **Content** menu, and then choose **Content Summary** in the sidebar.

   All the categories and forums in the system are listed here.

7. Select **WebCenter**, and then click the **Move** button for the newly imported forum or category.

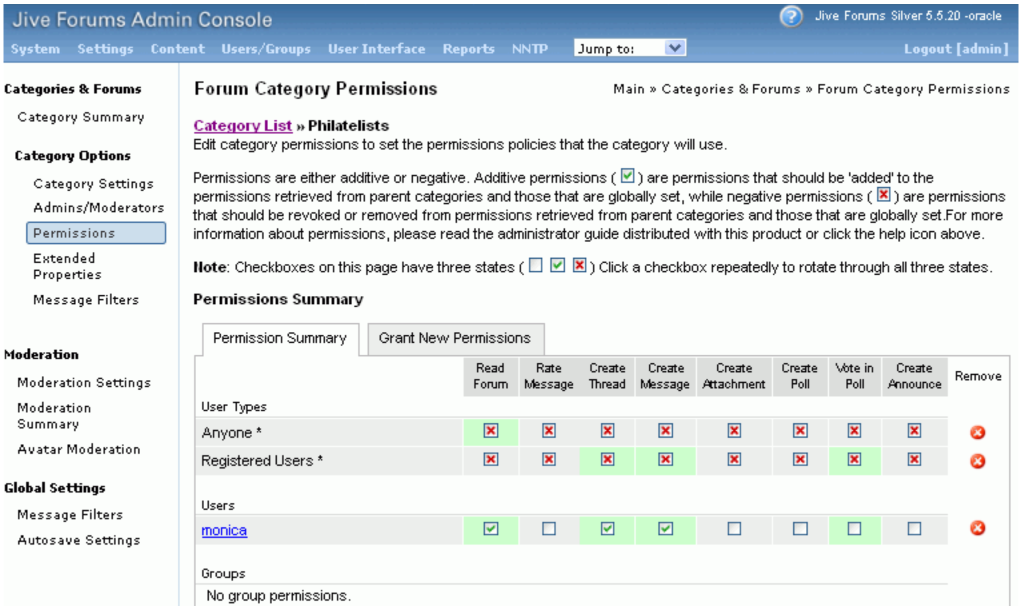
8. Select the root category for the target WebCenter Spaces application, and click **Move Categories**.

   The Category Summary page shows the new location.

9. Click **Permissions** in the sidebar.

10. Deselect all the permissions for the User Types: **Anyone** and **Registered Users**, and click **Save Changes** (Figure 31–11).

Figure 31–11 Editing Forum Permissions



Forum Category Permissions

Category List » **Philatelists**

Edit category permissions to set the permissions policies that the category will use.

Permissions are either additive or negative. Additive permissions (☑) are permissions that should be 'added' to the permissions retrieved from parent categories and those that are globally set, while negative permissions (☒) are permissions that should be revoked or removed from permissions retrieved from parent categories and those that are globally set.For more information about permissions, please read the administrator guide distributed with this product or click the help icon above.

Note: Checkboxes on this page have three states (□ ☑ ☒) Click a checkbox repeatedly to rotate through all three states.

Permissions Summary

Permission Summary | Grant New Permissions

	Read Forum	Rate Message	Create Thread	Create Message	Create Attachment	Create Poll	Vote in Poll	Create Announce	Remove
User Types									
Anyone *	☒	☒	☒	☒	☒	☒	☒	☒	⊗
Registered Users *	☒	☒	☒	☒	☒	☒	☒	☒	⊗
Users									
monica	☑	□	☑	☑	□	□	□	□	⊗
Groups									
No group permissions.									

11. In WebCenter Space, navigate to the group space's Discussions Forum Settings tab, to reassociate the group space with the discussion data that you just imported:

    a. Login to WebCenter Spaces with administrative privileges.

       See Section 32.1, "Logging into WebCenter Spaces as an Administrator."

    b. Click the **Administration** link at the top of the application.

    c. Click the **Group Spaces** tab.

    d. From the **Actions** menu, choose **Edit Group Space**, for the group space you want to export.

    e. Click the **Services** tab, then **Discussions**.

    f. Click the **Search** icon besides Category ID or Forum ID, and choose the imported category (or forum) from the list.

    g. Click **Apply**.

31.1.7.3 Exporting Wikis and Blogs for a Group Space

For Oracle databases, use Oracle Data Pump utilities and the group space export script (`owc_wiki_export.sql`) to export wikis and blogs associated with a particular group space. During the export process, wikis and blogs stored on Oracle WebCenter Wiki schema are exported to the data pump directory (the `WC_PUMP_DIR` directory in the example below.)

Before you start, you must copy the group space export script provided with Oracle WebCenter (`WC_ORACLE_HOME/wikiserver/owc_wiki/WEB-INF/classes/owc_wiki_export.sql`) to the computer where you run SQL. If you ran the script previously, be sure to remove the dump file `WCWIKI_EXPDP.dmp` from the `WC_PUMP_DIR` directory before running the script again.

Note: For non-Oracle databases, refer to the manufacturer's documentation for data migration instructions.

To export group space wikis and blogs:

1. Copy the group space export script from /WC_ORACLE_HOME/wikiserver/owc_wiki/WEB-INF/classes/owc_wiki_export.sql to the computer where you run SQL, for example: /myscripts/
2. Go to *ORACLE_HOME*/bin of your database where the Oracle WebCenter Wiki schema is installed, and connect to the database using sqlplus as the schema owner:

   ```
   DB_ORACLE_HOME/bin/sqlplus "<srcrcuprefix>_WIKI/password@dbhost"
   ```

3. Create the data pump directory (data_pump_dir):

   ```
   SQL> create or replace directory WC_PUMP_DIR as
   '<full_path_to_existing_directory_on_the_file_system>';
   ```

   For example:

   ```
   SQL> create or replace directory WC_PUMP_DIR as '/tmp/wikiData/';
   ```

   For more information, see "Oracle Data Pump" in *Oracle Database Utilities*.
4. Grant the Oracle WebCenter Wiki schema (srcrcuprefix_WIKI) read/write access to the data pump directory.

   For example:

   ```
   SQL> grant read, write on directory WC_PUMP_DIR to srcrcuprefix_WIKI;
   ```

5. Run owc_wiki_export.sql:

   For example, if you copied the script to a directory called /myscripts/:

   ```
   SQL> connect
   srcrcuprefix_WIKI/password@//dbhost:dbport/service
   ```

   ```
   SQL> @/myscripts/owc_wiki_export.sql
   ```

6. When prompted, enter the wiki domain associated with the group space.

WCWIKI_EXPDP.dmp is created in the WC_PUMP_DIR. For example, /tmp/wikiData/.

31.1.7.4 Importing Wikis and Blogs for a Group Space

For Oracle databases, use Oracle Data Pump utilities and the group space import script (owc_wiki_import.sql) to import group space wikis and blogs, exported from another WebCenter Spaces application.

Before you start, you must copy the group space import script provided with Oracle WebCenter (WC_ORACLE_HOME/wikiserver/owc_wiki/WEB-INF/classes/owc_wiki_import.sql) to the computer where you run SQL. If the source and target databases are different, you must edit this script, as described below.

> **Note:** For non-Oracle databases, refer to the manufacturer's documentation for data migration instructions.

The import script will import the data based on the domain name, so make sure the same domain name does not exist in the target schema before running the script. Also ensure that the associated group space exists on the target before you import the group space wikis and blogs. See Section 31.1.8.1, "Exporting Group Spaces Using WebCenter Spaces".

To import group space wikis and blogs:

1. Copy the group space import script from `WC_ORACLE_HOME/wikiserver/owc_wiki/WEB-INF/classes/owc_wiki_import.sql` to the computer where you run SQL, for example, `/myscripts/`.
2. Copy the exported file, for example `WCWIKI_EXPDP.dmp`, to an appropriate directory on the target system.

   For example:

   ```
   SQL> cp /testserver/tmp/wikiData/WCWIKI_EXPDP.dmp
   /productionserver/tmp/wikiDataTarget/WCWIKI_EXPDP.dmp
   ```
3. Go to *`ORACLE_HOME`*`/bin` of your database where Oracle WebCenter Wiki schema is installed, and connect to the database using `sqlplus` as the schema owner:

   ```
   DB_ORACLE_HOME/bin/sqlplus "<tgtrcuprefix>_WIKI/password@dbhost"
   ```
4. Grant the Oracle WebCenter Wiki schema (`tgtrcuprefix_WIKI`) read/write access to the data pump directory.

   For example:

   ```
   SQL> grant read, write on directory WC_PUMP_DIR to tgtrcuprefix_WIKI;
   ```
5. Create the `data_pump_dir`:

   ```
   SQL> create or replace directory WC_PUMP_DIR as
   '<full_path_to_existing_directory_on_the_file_system>';
   ```

   For example:

   ```
   SQL> create or replace directory WC_PUMP_DIR as
   '/tmp/wikiDataTarget/';
   ```

   For more information, see "Oracle Data Pump" in *Oracle Database Utilities*.
6. If the source and target databases are different, edit the import script `/myscripts/owc_wiki_import.sql` as follows:

   ```
   DBMS_DATAPUMP.METADATA_REMAP(dp_handle,'REMAP_SCHEMA','SOURCE
   _WIKI_SCHEMA','TARGET_WIKI_SCHEMA');
   ```

   a. **`SOURCE_WIKI_SCHEMA`** - replace with the source schema where you ran `owc_wiki_export.sql`

   b. **`TARGET_WIKI_SCHEMA`** - replace with the target schema where you will run `owc_wiki_import.sql`
7. Run `owc_wiki_import.sql`:

   For example, if you copied the script to a directory called `/myscripts/`:

   ```
   SQL> connect
   tgtrcuprefix_WIKI/password@//dbhost:dbport/service
   ```

   ```
   SQL> @/myscripts/owc_wiki_import.sql
   ```

31.1.7.5 Exporting Documents for a Group Space

After importing a group space you can use WebDAV to upload group space documents stored in Oracle Content Server to the new target; there is no need to export the content first.

31.1.7.6 Importing Documents for a Group Space

Before migrating group space documents to a new target you must enable the Documents service in the imported group space. Once the service is enabled, you can use WebDAV to upload group space documents onto the target system.

When dragging and dropping content to the target system, **do not** drag the group space folder to the target; you must only drag and drop content that is stored under the group space folder.

WebDAV is enabled on Oracle Content Server out-of-the-box. If you do not know the WebDAV URL for the Oracle Content Server that is used to store group space and personal space documents, contact your Fusion Middleware Administrator. If the base URL for that Oracle Content Server is `http://<host>:<port>/<relative_web_root>`, the WebDAV root URL will be `http://<host>:<port>/<relative_web_root>/idcplg/webdav`.

> **Note:** Depending on the WebDAV client you use, all properties may not be copied over (for example, document descriptions, checkin and checkout status, and versions may not be carried across).

To set up the target group space and import documents from another group space:

1. In WebCenter Spaces, enable the Documents service in the imported group space:
   a. Login to the WebCenter Spaces application that contains the imported group space.

      See Section 32.1, "Logging into WebCenter Spaces as an Administrator."
   b. Click the **Administration** link at the top of the application.
   c. Click the **Group Spaces** tab.
   d. From the **Actions** menu, choose **Edit Group Space**, for the imported group space.
   e. Click the **Services** tab.
   f. Select the check box next to **Documents** to enable this service, and then click **Apply**.
   g. Click **OK** to dismiss the warning about permission configuration requirements.
   h. Click the **Roles** tab, and assign appropriate **Documents** permissions to each group space role.
   i. Click **Apply** to save.
2. Using WebDAV (for Oracle Content Server), drag and drop content from the folder belonging to the source group space to the empty folder assigned to the target group space.

31.1.8 Exporting Group Spaces

Administrators can export one or more group spaces using WebCenter Spaces and WLST commands.

Group space information is exported into a single export archive (`.ear` file). The EAR file contains a metadata archive (`.mar` file) and a single XML file containing the security policy information. You can save export group space archives to your local file system or to a remote server file system.

For more information about what is exported, see Section 31.1.1, "Understanding WebCenter Spaces Export and Import".

The export process does not include data associated with external group space services, such as, Discussions, Announcements, Wiki, Blogs, and Documents. To learn how to move data associated with these services, see Section 31.1.7, "Migrating Back-end Components for Individual Group Spaces".

Groups spaces are locked during an export operation to prevent simultaneous imports/exports of the same group space. If someone else is exporting a particular group space, all subsequent attempts to export (or import) the same group space are blocked.

Note: No icons, skins, images, or personalizations are exported. For information on personalizations, see the section "Personalizing Your Page View" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

This section includes the following:

- Section 31.1.8.1, "Exporting Group Spaces Using WebCenter Spaces"
- Section 31.1.8.2, "Exporting Group Spaces Using WLST"

If you want to export an entire WebCenter Spaces application, see Section 31.1.4, "Exporting an Entire WebCenter Spaces Application".

31.1.8.1 Exporting Group Spaces Using WebCenter Spaces

WebCenter Spaces administrators can export one or more group spaces from WebCenter Spaces administration pages. For details, see Section 38.1, "Exporting Group Spaces".

31.1.8.2 Exporting Group Spaces Using WLST

Use the WLST command `exportGroupSpaces` to export one or more group spaces. For command syntax and examples, see "exportGroupSpaces" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

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

31.1.9 Importing Group Spaces

Administrators can import a group space archive (.EAR) using WebCenter Spaces and WLST commands.

On import, *all* group spaces included in the archive are created or re-created on the target application. Existing group spaces are deleted then replaced, and new group spaces are created.

If you intend to import group spaces with names identical to those available on the target application, ensure that those group spaces are offline in the target application. It is not possible to overwrite a group space, on import, if it is online. For details, see "Taking a Group Space Offline" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

Groups spaces are locked during an import operation to prevent simultaneous imports/exports of the same group space. If someone else is importing a particular group space, all subsequent attempts to import (or export) the same group space are blocked.

All group spaces must have a security policy. When you import a brand new group space you must ensure that the group space's security policy is included in the export archive. Existing group spaces 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 group space (with security), security policy updates do not apply immediately. Any user logged in to WebCenter Spaces must log out and log back in to adopt the new group space security policy.

If data migration is important, group space documents, discussions, and wikis and blogs can be migrated for individual group spaces. For details, see Section 31.1.7, "Migrating Back-end Components for Individual Group Spaces".

This section includes the following:

- Section 31.1.9.1, "Importing Group Spaces Using WebCenter Spaces"
- Section 31.1.9.2, "Importing Group Spaces Using WLST"

After importing one or more group spaces, consider initiating an Oracle Secure Enterprise Search crawl to index the newly imported data.

31.1.9.1 Importing Group Spaces Using WebCenter Spaces

WebCenter Spaces administrators can import a group space archive (.EAR) into another WebCenter Spaces application. For details, see Section 38.2, "Importing Group Spaces".

31.1.9.2 Importing Group Spaces Using WLST

Use the WLST command `importGroupSpaces` to import one or more group spaces. For command syntax and examples, see "importGroupSpaces" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

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

31.1.10 Migrating Back-end Components for Group Space Templates

Group space templates do not contain any *data* so there is no need to migrate back-end component data when exporting and importing group space templates.

You must, however, migrate the group space template's folder (on Oracle Content Server) to the target instance as described below. If you do not, the Documents service is not enabled in any group space that you create, using this template.

Importing the Back-end Folder for a Group Space Template

Use WebDAV (for Oracle Content Server), to drag and drop the folder belonging to the source group space template to the target instance.

WebDAV is enabled on Oracle Content Server out-of-the-box. If you do not know the WebDAV URL for the Oracle Content Server that WebCenter Spaces uses, contact your Fusion Middleware Administrator. If the base URL for that Oracle Content Server is `http://<host>:<port>/<relative_web_root>`, the WebDAV root URL will be `http://<host>:<port>/<relative_web_root>/idcplg/webdav`.

31.1.11 Exporting Group Space Templates

Administrators can export group space templates and import them into other WebCenter Spaces applications. Out-of-the-box templates, such as the Group Project and Community of Interest templates, cannot be exported.

While export and import utilities are primarily used to move information between WebCenter Spaces applications, the group space template export feature is also useful as a backup service, and for sharing and exchanging templates with others.

Group space template information is exported into a single export archive (.EAR file). The EAR file contains a metadata archive (.MAR file) and a single XML file containing group space security policy information.

Group space templates include pages, metadata, security information such as custom roles, and service information only; no data, such as documents, discussion threads, and list data, is stored with the template.

You can save export archives to your local file system or to a remote server file system.

This section includes the following:

- Section 31.1.11.1, "Exporting Group Space Templates Using WebCenter Spaces"
- Section 31.1.11.2, "Exporting Group Space Templates Using WLST"

See also, Section 31.1.8, "Exporting Group Spaces".

31.1.11.1 Exporting Group Space Templates Using WebCenter Spaces

WebCenter Spaces administrators can export one or more group space templates from WebCenter Spaces administration pages. For details, see Section 38.3, "Exporting Group Space Templates".

31.1.11.2 Exporting Group Space Templates Using WLST

Use the WLST command `exportGroupSpaceTemplates` to export one or more group space templates. For command syntax and examples, see "exportGroupSpaceTemplates" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

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

31.1.12 Importing Group Space Templates

Administrators can import a group space template archive (.EAR) into another WebCenter Spaces application.

On import, *all* group space templates included in the archive are re-created on the target application. If a group space template exists on the target, then it is deleted and replaced. If a group space template does not exist, then it is created.

Newly imported group space templates are not immediately available for general use. You must publish the imported templates to make them available to everyone. See Section 37.5.3, "Publishing and Hiding Group Space Templates".

This section includes the following:

- Section 31.1.12.1, "Importing Group Space Templates Using WebCenter Spaces"
- Section 31.1.12.2, "Importing Group Space Templates Using WLST"

See also, Section 31.1.9, "Importing Group Spaces".

31.1.12.1 Importing Group Space Templates Using WebCenter Spaces

WebCenter Spaces administrators can import one or more group space templates from WebCenter Spaces administration pages. For details, see Section 38.4, "Importing Group Space Templates"

31.1.12.2 Importing Group Space Templates Using WLST

Use the WLST command `importGroupSpaces` to import one or more group space templates. For command syntax and examples, see "importGroupSpaces" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

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

31.2 Exporting and Importing Custom WebCenter Applications for Data Migration

This section describes how to export and import metadata and customizations of a custom WebCenter application developed with Oracle WebCenter Framework.

It includes the following sections:

- Understanding Custom WebCenter Application Export and Import
- Prerequisites for Custom WebCenter Application Export and Import
- Exporting Portlet Client Metadata (Custom WebCenter Applications)
- Importing Portlet Client Metadata (Custom WebCenter Applications)
- Exporting WebCenter Services Metadata and Data (Custom WebCenter Applications)
- Importing WebCenter Services Metadata and Data (Custom WebCenter Applications)
- Migrating Security for Custom WebCenter Applications
- Migrating Data (Custom WebCenter Applications)

31.2.1 Understanding Custom WebCenter Application Export and Import

Several migration tools are available to export and import custom WebCenter applications, their connections and customizations (that is, customizations applied to an application, pages, and portlets) between stage and production environments (Figure 31–12).

Figure 31–12 WebCenter Application Export and Import

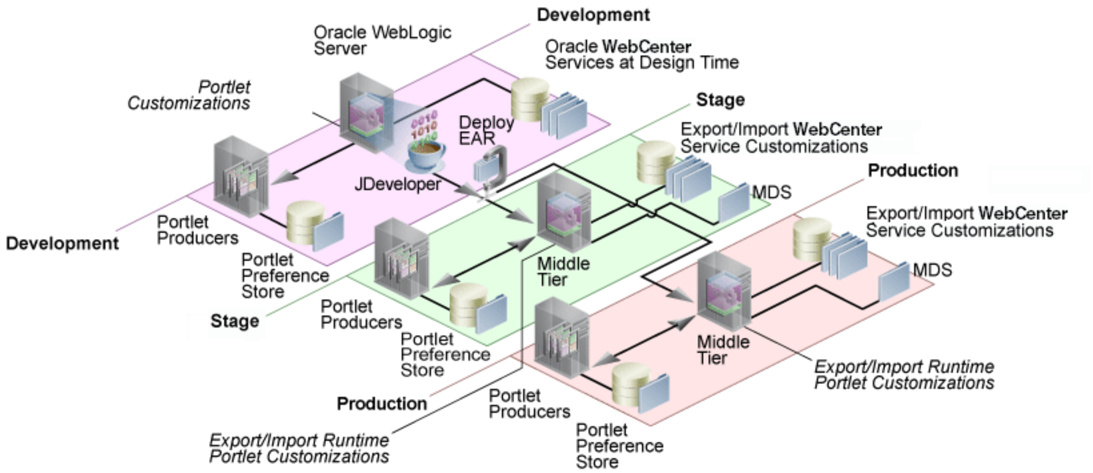


Table 31–2 lists available migration tools and their capabilities. All customizations listed in Table 31–2 are migrated with custom WebCenter applications.

Table 31–2 Custom WebCenter Application Migration Tools

Migration Tools	Capabilities
Portlet Client WLST Commands	Enable export and import of portlet client metadata, and producer customizations and personalizations.
MDS WLST Commands	Enables export and import of: ■ WebCenter application metadata including customizations made to pages and WebCenter services ■ Data stored in the `connections.xml` and `adf-config.xml` 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 WebCenter application data. For information, see the part "Oracle Data Pump" in the *Oracle Database Utilities* guide.
Non-Oracle database utilities	Refer to the database manufacturer's documentation for information about their data migration tools.

31.2.2 Prerequisites for Custom WebCenter Application Export and Import

Before exporting or importing metadata and customizations for a custom WebCenter 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. You should note, however, that pages created on the source instance at runtime will not display on the target instance because no page grants will exist on the target.

31.2.3 Exporting Portlet Client Metadata (Custom WebCenter Applications)

To export portlet client metadata and producer customizations and personalizations, for a custom WebCenter application, use the WLST command `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*.

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 1.12.3.1, "Running Oracle WebLogic Scripting Tool (WLST) Commands"

For information on how to import portlet client metadata associated with all applications, see "Portlet Preference Store Migration Utilities" in *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*.

31.2.4 Importing Portlet Client Metadata (Custom WebCenter Applications)

This section describes how to import portlet client metadata and producer customizations and personalizations, for a custom WebCenter application, using the WLST command `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*.

To import portlet client metadata:

1. Start the WebLogic Scripting Tool (WLST) located at `WC_ORACLE_HOME/common/bin`.

   On UNIX, start WLST using `wlst.sh`.

   On Windows, use `wlst.cmd`.

See also, Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool (WLST) Commands".

2. Run the WLST command `deleteMetadata` to delete the metadata under `/oracle/adf/portlet`.

   ```
   deleteMetadata(application='application', server='server', docs='docs')
   ```

   where:

   - `application`: Name of the WebCenter application (for example, `sampleApp`)
   - `server`: Name of the managed server (for example, `portletConsumer`).
   - `docs`: List of comma separated fully qualified document name(s) or document name patterns (such as * and ** patterns).

   For example:

   ```
   deleteMetadata(application='sampleApp', server='WLS_CustomApp',
   docs='/oracle/adf/portlet/**')
   ```

   For detailed syntax and examples, see "deleteMetadata" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

3. Run the WLST command `importPortletClientMetadata`:

   ```
   importPortletClientMetadata(appName, fileName, server, applicationVersion)
   ```

   where:

   - `appName`: Name of the WebCenter application (for example, `sampleApp).`
   - `fileName`: Name of the exported EAR file containing the portlet client metadata (for example, `export.ear).`
   - `server`: Name of the managed server (for example, `portletConsumer`).
   - `applicationVersion`: Version number of the deployed application, if multiple versions of the application is deployed.

For detailed syntax and examples, see "importPortletClientMetadata" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*. See also the chapter "Metadata Services (MDS) Custom WLST Commands" in Oracle Fusion Middleware WebLogic Scripting Tool Command Reference.

31.2.5 Exporting WebCenter Services Metadata and Data (Custom WebCenter Applications)

The metadata created by WebCenter services is stored in the Oracle metadata store (MDS). This section describes the transfer of the base documents and their customizations using WLST. For detailed information about MDS, see the chapter "Managing the Oracle Metadata Repository" in *Oracle Fusion Middleware Administrator's Guide*.

Customizations listed in Table 31–3 are also exported when WebCenter applications are migrated between stage and production environments.

1. Start the WebLogic Scripting Tool (WLST) located at *`WC_ORACLE_HOME`*`/common/bin`.

   On UNIX, start WLST is called `wlst.sh`.

   On Windows, use `wlst.cmd`.

See also, Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool (WLST) Commands".

2. Run the WLST command `exportMetadata`:

```
exportMetadata(application, server, toLocation, docs, [restrictCustTo],
[excludeAllCust], [excludeBaseDocs], [excludeExtendedMetadata], [fromLabel],
[toLabel], [applicationVersion])
```

   For example:

```
exportMetadata(application='sampleApp', server='WLS_CustomApp',
toLocation='/tmp/myrepos', docs='/oracle/webcenter/**')
```

   For detailed syntax and examples, see "exportMetadata" in Oracle Fusion Middleware WebLogic Scripting Tool Command Reference.

   Note: In this example, "`docs='/oracle/webcenter/**`" will export the required documents for all WebCenter services storing metadata in MDS.

   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`. To export configuration file updates that are stored in MDS, run the WLST command `exportMetadata` with "`docs='META-INF/mdssys/cust/adfshare/adfshare/**`".

Where:

- `application`: Application name for which the metadata is to be exported (for example, `sampleApp).`
- `server`: Target server on which this application is deployed (for example, `WLS_CustomApp).`
- `toLocation`: Target directory to which documents selected from the source partition are to be transferred. The `toLocation` parameter can be used as a temporary file system for transferring metadata from one server to another.
- `docs`: List of comma separated fully qualified document name(s) and/or document name patterns (* and ** patterns).
- `restrictCustTo`: List of customization layer names. This list is used to restrict the export of customization documents that match the specified customization layers. This option is ignored if the `excludeAllCust` option is also specified.
- `excludeAllCust`: Specifies whether to export all customization documents. This option overrides the `restrictCustTo` option.
- `excludeBaseDocs`: Specifies whether to export base documents.
- `excludeExtendedMetadata`: Specifies whether to export the Extended Metadata documents.
- `fromLabel`: If specified, transfers the documents from the source partition that is associated with this label.
- `toLabel`: If specified, works with the `fromLabel` variable to transfers the delta between `fromLabel` to `toLabel` from the source partition.

- applicationVersion: Application version in case multiple versions of the same application are deployed.

The metadata for WebCenter services, which consists of base and customization documents, are stored in the following paths:

- **Announcements**: /oracle/webcenter/collab/announcement/**
- **Documents**: /oracle/webcenter/doclib/** and /oracle/webcenter/doclib/view/jsf/fragments/**
- **Discussions**: /oracle/webcenter/collab/forum/**
- **General Settings**: /oracle/webcenter/generalsettings/**
- **Group Space Events**:/oracle/webcenter/collab/calendar/community/**
- **Lists**: /oracle/webcenter/list/** and /oracle/webcenter/list/view/jsf/regions/**
- **Mail**: /oracle/webcenter/collab/mail/**
- **Notes**: /oracle/webcenter/note/**
- **Page**: /oracle/webcenter/page/** and /pageDefs/**
- **Recent Activity**: /oracle/webcenter/recentactivity/**
- **RSS News Feed**: oracle/webcenter/rss/**
- **Links**: /oracle/webcenter/relationship/**
- **Scope**: /oracle/webcenter/framework/scope/**
- **Search**: /oracle/webcenter/search/**
- **Tags**: /oracle/webcenter/tagging/**
- **adf-config.xml, connections.xml**: /META-INF/mdssys/cust/adfshare/adfshare/**

  Configuration file updates are not stored under the /oracle/webcenter/ directory alongside WebCenter services. To export customizations associated with these files, run exportMetadata again with "docs='META-INF/mdssys/cust/adfshare/adfshare".

31.2.6 Importing WebCenter Services Metadata and Data (Custom WebCenter Applications)

To import custom WebCenter application metadata and customizations:

1. Start the WebLogic Scripting Tool (WLST) located at *WC_ORACLE_HOME*/common/bin.

   On UNIX, start WLST using wlst.sh.

   On Windows, use wlst.cmd.

   See also, Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool (WLST) Commands".

2. Run the WLST command importMetadata:

```
importMetadata( application, server, fromLocation, docs, [restrictCustTo],
[excludeAllCust], [excludeBaseDocs], [excludeExtendedMetadata],
[cancelOnException], [applicationVersion])
```

For example:

```
importMetadata(application='sampleApp', server='WLS_CustomApp',
fromLocation='/tmp/myrepos', docs='/**')
```

Where:

- `application`: Application name for which the metadata is be imported (for example, `sampleApp`).
- `server`: Name of the target server on which this application is deployed (for example, `WLS_CustomApp`).
- `fromLocation`: Source directory from where documents are selected for the transfer. The `fromLocation` parameter can be used as a temporary file system location for transferring metadata from one server to another.
- `docs`: List of comma separated fully qualified document name(s) and/or document name patterns (* and ** patterns).
- `restrictCustTo`: List of customization layer names. This list is used to restrict the import of customization documents that match the specified customization layers. This option is ignored if the `excludeAllCust` option is also specified.
- `excludeAllCust`: Specifies whether to import all customization documents. This option overrides the `restrictCustTo` option.
- `excludeBaseDocs`: Specifies whether to import base documents.
- `excludeExtendedMetadata`: Specifies whether to import the Extended Metadata documents.
- `cancelOnException`: Whether to terminate the import operation when an exception is encountered. On termination, the delete is rolled back if supported by the target store.
- `applicationVersion`: Application version in case multiple versions of the same application are deployed.

For detailed syntax and examples, see "importMetadata" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

31.2.7 Migrating Security for Custom WebCenter Applications

Security migration involves moving the identity store, credential store, and policy store, from one WebCenter application to another. The process is the same for all WebCenter applications so, for custom WebCenter applications, you can follow the same instructions provided for WebCenter Spaces:

- Section 31.1.3.1, "Exporting the LDAP Identity Store"
- Section 31.1.3.2, "Importing the LDAP Identity Store"
- Section 31.1.3.3, "Exporting and Importing the LDAP Credential Store"
- Section 31.1.3.4, "Exporting and Importing the LDAP Policy Store"

31.2.8 Migrating Data (Custom WebCenter Applications)

To export the custom WebCenter application data, use the export and import database utilities. This section includes the following sub sections:

- Section 31.2.8.1, "Exporting Data (Custom WebCenter Applications)"
- Section 31.2.8.2, "Importing Data (Custom WebCenter Applications)"

31.2.8.1 Exporting Data (Custom WebCenter Applications)

To export custom WebCenter 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 31–13.
- For non-Oracle databases, refer to the manufacturer's documentation.

Example 31–13 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 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.

31.2.8.2 Importing Data (Custom WebCenter Applications)

To import custom WebCenter 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 31–14.
- For non-Oracle databases, refer to the manufacturer's documentation.

Example 31–14 Data Pump Utility (Import)

```
DB_ORACLE_HOME/bin/impdp  \"sys/password@serviceid as sysdba\"
FROMUSER=srcrcuprefix_WEBCENTER TOUSER=tgtrcuprefix_WEBCENTER FILE=/tmp/wc.dmp
STATISTICS=none TRANSFORM=oid:n
```

where:

- DB_ORACLE_HOME is the directory in which the database for the Oracle WebCenter schema is installed.
- password is the password for system database user.
- serviceid is the service ID of the database connection.
- FROMUSER is the exported schema.
- TOUSER is the imported schema. This is the RCU suffix that was used during installation, _WEBCENTER, along with the user supplied prefix. For example, DEV_WEBCENTER.
- FILE contains the data to be imported.

For more information, see "Oracle Data Pump" in the *Oracle Database Utilities* guide.

31.3 Backing Up and Recovering WebCenter Applications

To recover data from disasters, such as the loss of database hardware, inadvertent removal of data from file or database, it is important to back up WebCenter applications on a frequent basis. The frequency of backup depends on how often the underlying information stored by WebCenter changes in a particular customer application, and how much time and amount of information could acceptably be lost. Incremental or partial backups may be applied where the data is critical to the business and must be restored due to a failure.

Backup and recovery of WebCenter components can be managed through database export and import utilities, and various other tools. For more information, see "Part IV Advanced Administration: Backup and Recovery" in *Oracle Fusion Middleware Administrator's Guide*.

31.4 Troubleshooting Import and Export Issues for WebCenter Spaces

This section contains the following subsections:

- Section 31.4.1, "ResourceLimitException Issue"
- Section 31.4.3, "Page or Group Space Not Found Messages After Import"
- Section 31.4.4, "Group Space Import Archive Exceeds Maximum Upload File Size"
- Section 31.4.5, "Lists Not Imported Properly"

31.4.1 ResourceLimitException Issue

Problem

The `ResourceLimitException` error displays when you try to export all group spaces or an entire WebCenter 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.

31.4.2 Exporting and Importing Group Spaces in Multibyte Languages

Problem

On Linux, group space export or import fails for one or more group spaces created in multibyte languages due to naming restrictions. Group 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 WebCenter Spaces replaces with "_"(underscore)). If any other characters are used in the group space name, export or import fails.

Solution

Enforce the naming restriction on the server on which Oracle WebCenter is deployed. To do this, set the environment variable `LC_ALL` set to `utf-8`.

31.4.3 Page or Group Space Not Found Messages After Import

Problem

When users first log in to WebCenter Spaces after an import operation they may see a "Page not found" or "Group space not found" message if the page or group space they last visited no longer exists. Such messages display because "last accessed" page information is retained during an import operation.

Solution

No action required. Users will not see the message the next time they log in.

31.4.4 Group Space Import Archive Exceeds Maximum Upload File Size

Problem

There is a file size limitation uploading content to WebCenter Spaces. If your export archive exceeds the maximum upload size then the import operation through WebCenter Spaces administration will fail.

Solution

Import the group space archive using WLST. For details, see Section 31.1.9.2, "Importing Group Spaces Using WLST".

Alternatively, modify the content repository upload parameter in `web.xml`. The default maximum upload size is 2 GB. See also, "Editing web.xml" in Appendix A, "WebCenter Configuration".

31.4.5 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 migrated 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.

31.4.6 Exporting WebCenter Spaces Customizations

When you export WebCenter Spaces you can choose whether certain application customizations are included in the export archive or whether to exclude them, using the option "Include Customizations". Table 31–3 highlights those services and task flows that store customizations, and which are optional on migration. Table 31–4 lists all the application and group space customizations which are optional on export.

> **Note:** User personalizations are never migrated during export and import. For more information on customization and personalization and the difference between them, see "Customizing and Personalizing Page Content" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

Table 31–3 WebCenter Spaces - Service Customizations

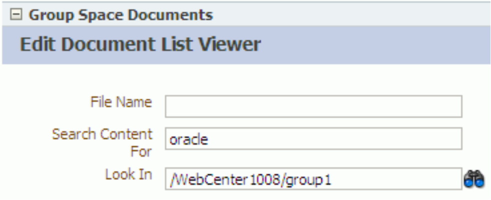
Services in WebCenter Spaces	Customizations	Export
Announcements Service	None	
Announcement Tab	None	
Announcement Task Flow	None	
Discussions Service		
Sidebar	None	
Discussions Tab	None	
Discussion Forum Manager Task Flow	None	
Forum Task Flow	None	
Discussion Task Flows	None	
Documents Service		
Documents Tab	None	
Document Manager Task Flow	■ 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. See also, "Understanding the Document Manager Task Flow" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.	Optional
Document List Viewer Task Flow	 ⊟ Group Space Documents Edit Document List Viewer File Name Search Content For: oracle Look In: /WebCenter1008/group1 Table column settings, such as, visible columns, column sizes, and ordering. In page edit mode, default fields that display document search results can be customized and additional fields can be added. See also, "Understanding the Document List Viewer Task Flow" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.	Optional

Table 31–3 (Cont.) WebCenter Spaces - Service Customizations

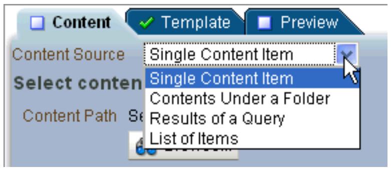
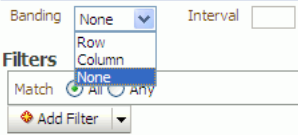
Services in WebCenter Spaces	Customizations	Export
Content Presenter Task Flow	 Content Template Preview Content Source Single Content Item Select conten Single Content Item Contents Under a Folder Content Path Results of a Query List of Items In page edit mode, content and display template settings. See also, "Understanding the Content Presenter Task Flow" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.	Optional
Recent Documents Task Flow	None	
Events Service		
Events Tab	None	
Events Task Flow	Page edit mode: - Task flow customizations: Display Mode, Grid Start Hour, Second Timezone. - Calendars overlay properties: Name, Order, Color and Visibility.	Optional
Instant Messaging and Presence Service		
Buddies Task Flow	None	
Lists Service		
List Tab	None	
List Viewer Task Flow	Page edit mode: ▪ Banding type and interval, and column filter settings  Banding None Interval Row Column Filters None Match All Any Add Filter ▪ Column settings: Sort column and sort direction (ascending, descending), column sizes, and column order See also, "Working with the Lists Service" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.	Optional
List Manager Task Flow	None	
Mail Service		
Sidebar	None	
Mail Task Flow	None	
Notes Service	None	

Table 31–3 (Cont.) WebCenter Spaces - Service Customizations

Services in WebCenter Spaces	Customizations	Export
Pages	Page edit mode: task flow and portlet customizations using Oracle Composer, such as, Maximize, Move, Vertical Height	Always
	Page properties: Page Name, Description, Keywords, Scheme, Scheme Background Color, Page Security, Page Parameters, Page modified date, and so on.	Always
	Component properties: Title, Background Color, and so on.	Always
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	None	
Resource Catalog	None	
RSS News Feed Service	None	
Search Service	None	
Saved Search	Shared/Private option for saved searches. Saved search customizations.	Optional
Tags Service		
Tags	None	
Tags Center	None	
Tag Sidebar	None	
Worklist Service	None	

Table 31–4 WebCenter Spaces - Application and Group Space Customizations

WebCenter Spaces	Customizations	Export
Application Settings		Optional
Administration: General tab	All properties	
Administration: General tab	Language	
Administration: Pages tab	Settings such as, Set Page Defaults, Order, and Show Page	
Administration: Sidebar tab	All properties	
Administration: Services tab	Default settings for Discussions, Mail, and People Connections (Profiles, Message Boards, Feedback, Connections, Activity Streams)	
Application Sidebar	Applications/folder display order, and personalization allowed setting	
Group Space Settings		Optional
Group Spaces Settings: Pages tab	Settings such as, Set Page Defaults, Order, and Show Page	

Table 31–4 (Cont.) WebCenter Spaces - Application and Group Space Customizations

WebCenter Spaces	Customizations	Export
Group Spaces Settings: other tabs	All properties	

Part VI

Application Administration for Oracle WebCenter Spaces

Part VI contains the following chapters:

- Chapter 32, "Accessing WebCenter Spaces Administration Pages"
- Chapter 33, "Customizing WebCenter Spaces"
- Chapter 34, "Managing Users and Roles for WebCenter Spaces"
- Chapter 35, "Managing Pages in WebCenter Spaces"
- Chapter 36, "Making Applications Available in WebCenter Spaces"
- Chapter 37, "Managing Group Spaces in WebCenter Spaces"
- Chapter 38, "Exporting and Importing Group Spaces"

32

Accessing WebCenter Spaces Administration Pages

This chapter describes how to access administration pages in the WebCenter Spaces application. It contains the following subsections:

- Section 32.1, "Logging into WebCenter Spaces as an Administrator"
- Section 32.2, "WebCenter Spaces Administration Pages"

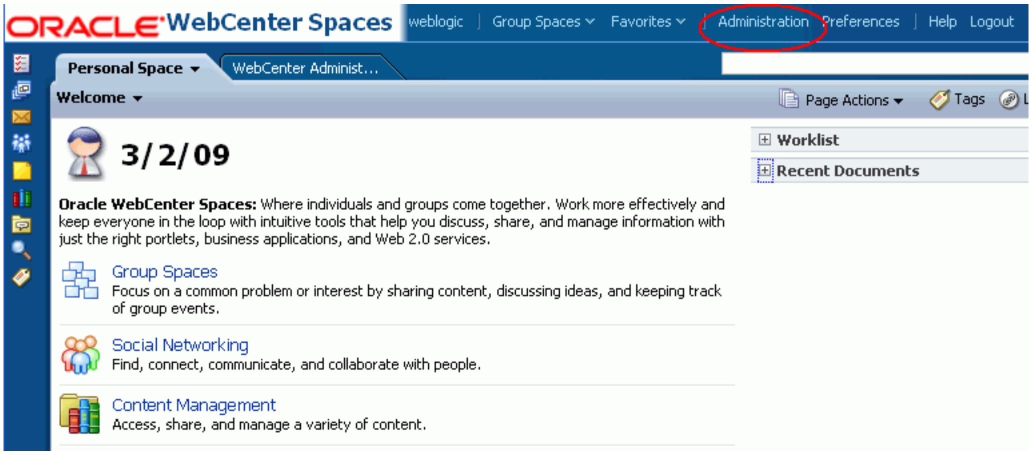
Audience

The content of this chapter is intended for WebCenter Spaces administrators. Users granted the WebCenter Spaces `Administrator` role or a custom role that grants the `Application-Manage` permission).

32.1 Logging into WebCenter Spaces as an Administrator

WebCenter users with administrative privileges will see an **Administration** link at the top of the application when they log in (Figure 32–1).

Figure 32–1 Administration Link



Oracle WebCenter Spaces: Where individuals and groups come together. Work more effectively and keep everyone in the loop with intuitive tools that help you discuss, share, and manage information with just the right portlets, business applications, and Web 2.0 services.

Group Spaces
Focus on a common problem or interest by sharing content, discussing ideas, and keeping track of group events.

Social Networking
Find, connect, communicate, and collaborate with people.

Content Management
Access, share, and manage a variety of content.

The **Administration** link provides access to administration and application settings for WebCenter Spaces. For more detail, see Section 32.2, "WebCenter Spaces Administration Pages".

> **Note:** If you do not see this link, you do not have administrative privileges. Ask your WebCenter Spaces Administrator to check the permissions assigned to your role.

WebCenter Spaces administrators may assign administrative privileges to other users, if required. For more information, see Section 34.2.4, "Giving a User Administrative Privileges".

To log in to WebCenter Spaces.

1. Open WebCenter Spaces using the following URL:

   ```
   http://host:port/webcenter
   ```

   If you do not know which host or port to use, ask your systems administrator. See also, "Managing Ports" in *Oracle Fusion Middleware Administrator's Guide*.

   If you have access to Fusion Middleware Control, this information is available on the WebCenter Space home page. See Section 6.2, "Navigating to the Home Page for WebCenter Spaces".

2. Enter your user name in the **User Name** field and your password in the **Password** field.

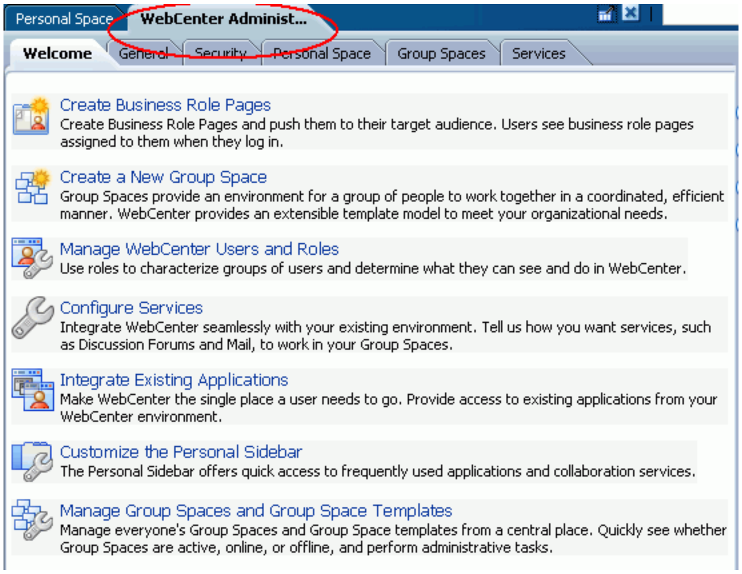
3. Click **Login**.

Check that you can see the **Administration** link at the top of the application (Figure 32–1).

32.2 WebCenter Spaces Administration Pages

There are six WebCenter Administration pages—Welcome, General, Security, Personal Space, Group Spaces, and Services (Figure 32–2):

Figure 32–2 WebCenter Administration Pages



Create Business Role Pages
Create Business Role Pages and push them to their target audience. Users see business role pages assigned to them when they log in.

Create a New Group Space
Group Spaces provide an environment for a group of people to work together in a coordinated, efficient manner. WebCenter provides an extensible template model to meet your organizational needs.

Manage WebCenter Users and Roles
Use roles to characterize groups of users and determine what they can see and do in WebCenter.

Configure Services
Integrate WebCenter seamlessly with your existing environment. Tell us how you want services, such as Discussion Forums and Mail, to work in your Group Spaces.

Integrate Existing Applications
Make WebCenter the single place a user needs to go. Provide access to existing applications from your WebCenter environment.

Customize the Personal Sidebar
The Personal Sidebar offers quick access to frequently used applications and collaboration services.

Manage Group Spaces and Group Space Templates
Manage everyone's Group Spaces and Group Space templates from a central place. Quickly see whether Group Spaces are active, online, or offline, and perform administrative tasks.

Administrators can perform all their administrative duties from here:

Administration Page	Description
Welcome	This page is a convenient launching pad for some common administrative tasks. Click a task link to navigate to the appropriate page.
General	Use this page to customize WebCenter Spaces. For example, you can specify a default language, application name, and so on. For more information, see: Chapter 33, Naming Your WebCenter Chapter 33, Changing the WebCenter Logo Chapter 33, Applying Look and Feel Using Skins Chapter 33, Choosing the Default Display Language Chapter 33, Customizing Copyright and Privacy Statements Chapter 33, Customizing the Online Help Link Chapter 33, Enabling and Disabling Personal Spaces Chapter 34, Allowing Self-Registration Chapter 35, Customizing the Self-Registration Page Chapter 35, Customizing the Login Page
Security	Use this page to manage WebCenter users and roles. For more information, see: Chapter 34, Managing Users and Roles for WebCenter Spaces
Personal Space	Use this page to manage pages for personal spaces and WebCenter Spaces, and to customize everyone's sidebar. For more information, see: Chapter 35, "Managing Pages in WebCenter Spaces" Chapter 33, Customizing the Sidebar
Group Spaces	Use this page to manage group spaces and group space templates. For more information, see: Chapter 37, Managing Group Spaces in WebCenter Spaces Chapter 37, Managing Group Space Templates
Services	Use this page to set application-wide properties for discussion forums, announcements, mail, and people connection components such as activity streams, personal profiles, connections, messages boards, and feeback. For more information, see: Section 12.10, "Setting Discussion Forum Options for WebCenter Spaces" Section 15.9, "Setting Send Mail Notifications for WebCenter Spaces" Section 16.3, "Configuring the People Connections Service for WebCenter Spaces"

33

Customizing WebCenter Spaces

This chapter describes how to customize WebCenter Spaces for your target audience. You must login to WebCenter Spaces with administrative privileges to set any of the application-wide properties described here.

This chapter includes the following sections:

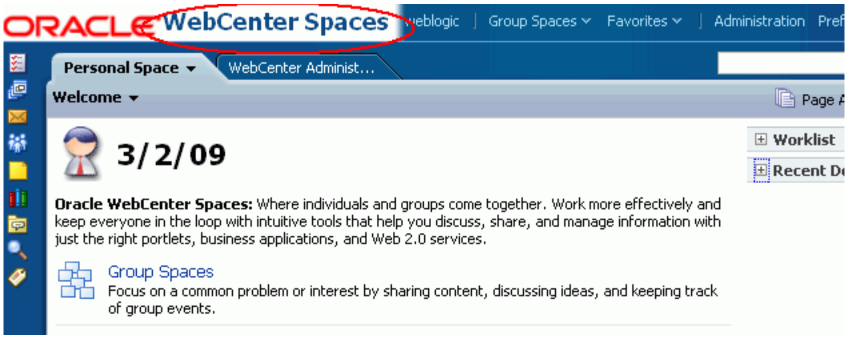
Audience

The content of this chapter is intended for WebCenter Spaces administrators. Users granted the WebCenter Spaces `Administrator` role or a custom role that grants the `Application-Manage` permission).

33.1 Naming Your WebCenter

Out-of-the-box, the application name *WebCenter Spaces* appears in the banner (see Figure 33–1). If you prefer, you can change the name to better suit your target audience. For example, you might want to display your company name here or the name of a department within your company.

Figure 33–1 Naming Your WebCenter



Oracle WebCenter Spaces: Where individuals and groups come together. Work more effectively and keep everyone in the loop with intuitive tools that help you discuss, share, and manage information with just the right portlets, business applications, and Web 2.0 services.

Group Spaces
Focus on a common problem or interest by sharing content, discussing ideas, and keeping track of group events.

Note: You can change the logo that displays next to the application name too. See Section 33.4, "Changing the WebCenter Logo".

To change the name of your WebCenter Spaces application:

1. Login to WebCenter Spaces with administrative privileges.

   See Section 32.1, "Logging into WebCenter Spaces as an Administrator".

2. Click the **Administration** link at the top of the application.

3. Click the **General** tab.

4. In the **Application Name** field, enter the new name.

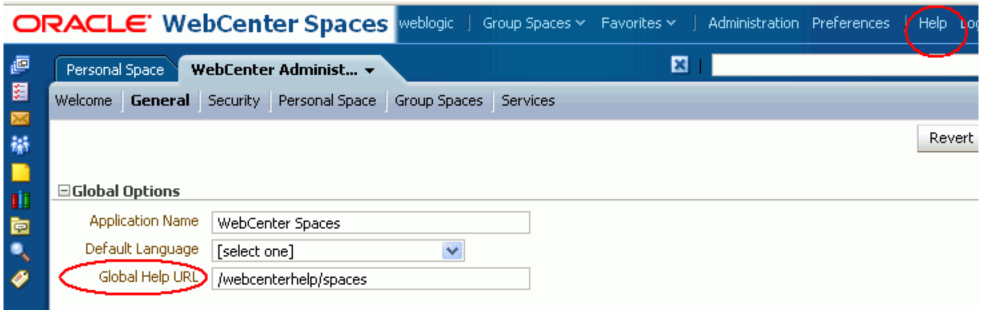
   Alphanumeric characters are allowed and also spaces, underscores (_) and dashes (-). For example, `Finance Department - My Corporation`.

5. Click **Apply**.

33.2 Customizing the Online Help Link

Online help for WebCenter Spaces displays when you click the Help link located at the top of the application (see Figure 33–2). Out-of-the-box, this Help link opens Oracle's built-in help. If you want, you can write online help specifically aimed at your end-users and redirect the Help link to a different help location.

Figure 33–2 Customizing the Help Link



Application Name: WebCenter Spaces
Default Language: [select one]
Global Help URL: /webcenterhelp/spaces

When you customize the Help link, built-in help for WebCenter Spaces is still available through help buttons, help icons, and so on.

To customize the main Help link for WebCenter Spaces:

1. Login to WebCenter Spaces with administrative privileges.

   See Section 32.1, "Logging into WebCenter Spaces as an Administrator".
2. Click the **Administration** link at the top of the application.
3. Click the **General** tab.
4. In the **Global Help URL** field, enter the location of your help (Figure 33–2).

   Ensure that you enter a fully qualified URL in the format:

   ```
   http://host:port/helplocation
   ```

   For example:

   ```
   http://myhost:8888/myhelp
   ```

   The default Global Help URL is `/webcenterhelp/spaces`. This URL opens Oracle Help for the Web (OHW) and displays Oracle's built-in help for WebCenter Spaces.

   > **Note:** If you leave the Global Help URL field blank, the Help link is not displayed.

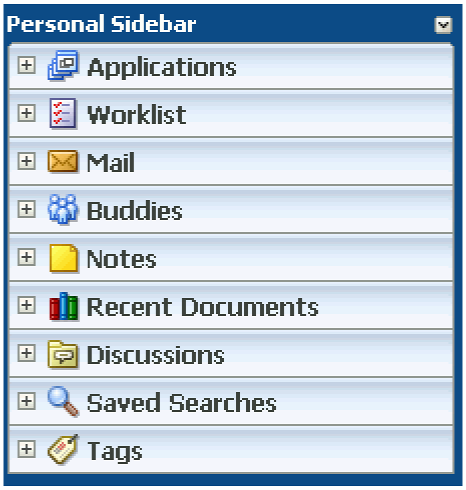
5. Click **Apply**.

Click **Help** at the top of the application to check the custom help opens correctly.

33.3 Customizing the Sidebar

The Sidebar in WebCenter Spaces offers users quick access to personal services such mail, worklist assignments, personal contacts, and more. Out-of-the-box, the Sidebar will offer the full range of WebCenter services that are available and WebCenter users can hide any services they do not use or require.

Figure 33–3 The Sidebar



The Sidebar is configurable. WebCenter Spaces administrators can customize the default sidebar for all users as follows:

- Hiding and Showing Task Flows in the Sidebar

- Locking Sidebar Content

33.3.1 Hiding and Showing Task Flows in the Sidebar

Administrators can choose which services are available through the sidebar and the order they are displayed. If some services are not in use or not yet configured you can hide them.

If you want to hide the entire sidebar, hide all available services.

To hide or show services on the sidebar:

1. Login to WebCenter Spaces with administrative privileges.

   See Section 32.1, "Logging into WebCenter Spaces as an Administrator".

2. Click the **Administration** link at the top of the application.

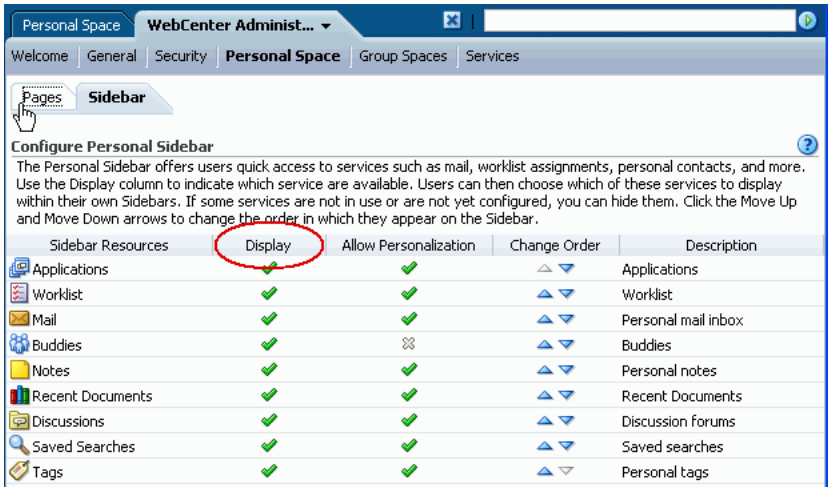
3. Click the **Personal Space** tab.

4. Click the **Sidebar** tab.

5. Set the **Display** option (Figure 33–4):

   - Click the gray cross to show an item on the sidebar (cross changes to check mark).
   - Click the green check mark to hide an item on the sidebar (check mark changes to cross).

Figure 33–4 Customizing the Sidebar



Configure Personal Sidebar

The Personal Sidebar offers users quick access to services such as mail, worklist assignments, personal contacts, and more. Use the Display column to indicate which service are available. Users can then choose which of these services to display within their own Sidebars. If some services are not in use or are not yet configured, you can hide them. Click the Move Up and Move Down arrows to change the order in which they appear on the Sidebar.

Sidebar Resources	Display	Allow Personalization	Change Order	Description
Applications	✓	✓	△ ▽	Applications
Worklist	✓	✓	△ ▽	Worklist
Mail	✓	✓	△ ▽	Personal mail inbox
Buddies	✓	✗	△ ▽	Buddies
Notes	✓	✓	△ ▽	Personal notes
Recent Documents	✓	✓	△ ▽	Recent Documents
Discussions	✓	✓	△ ▽	Discussion forums
Saved Searches	✓	✓	△ ▽	Saved searches
Tags	✓	✓	△ ▽	Personal tags

6. Use the **Move Up** and **Move Down** arrows to change the display order.

Any changes you make immediately impact everyone's personal sidebar.

33.3.2 Locking Sidebar Content

Users can personalize their sidebar, that is, display sidebar panes when they require them and hide sidebar panes that they do not need or use. Sidebar personalization is useful for hiding non-essential services but might prove less desirable for sidebar content that is critical for user productivity. By locking individual panes on the sidebar, WebCenter Spaces administrators can control which resources always display and which resources never display.

To lock sidebar content:

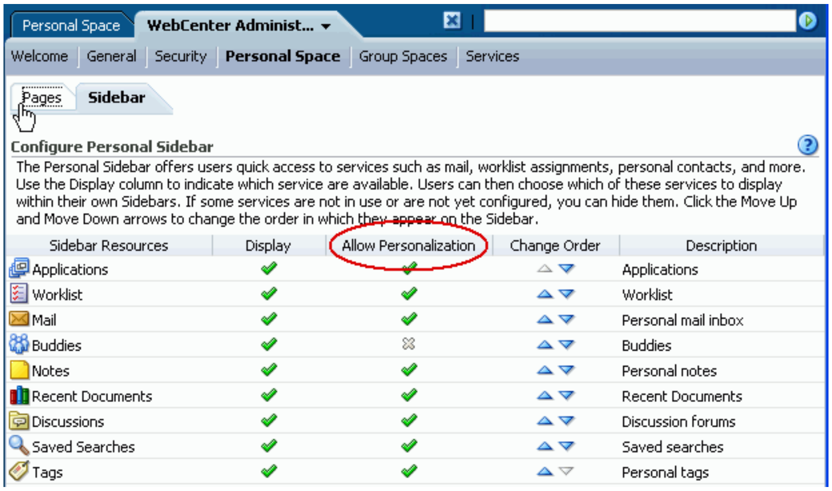
1. Login to WebCenter Spaces with administrative privileges.

   See Section 32.1, "Logging into WebCenter Spaces as an Administrator".

2. Click the **Administration** link at the top of the application.
3. Click the **Personal Space** tab.
4. Click the **Sidebar** tab.
5. Set **Allow Personalization** (Figure 33–5):

   - Click the gray cross to allow user personalization (cross changes to check mark).
   - Click the green check mark to prevent user personalization (check mark changes to cross).

Figure 33–5 Controlling Sidebar Personalization



Configure Personal Sidebar

The Personal Sidebar offers users quick access to services such as mail, worklist assignments, personal contacts, and more. Use the Display column to indicate which service are available. Users can then choose which of these services to display within their own Sidebars. If some services are not in use or are not yet configured, you can hide them. Click the Move Up and Move Down arrows to change the order in which they appear on the Sidebar.

Sidebar Resources	Display	Allow Personalization	Change Order	Description
Applications	✓	✓	△▼	Applications
Worklist	✓	✓	▲▼	Worklist
Mail	✓	✓	▲▼	Personal mail inbox
Buddies	✓	✗	▲▼	Buddies
Notes	✓	✓	▲▼	Personal notes
Recent Documents	✓	✓	▲▼	Recent Documents
Discussions	✓	✓	▲▼	Discussion forums
Saved Searches	✓	✓	▲▼	Saved searches
Tags	✓	✓	▲▽	Personal tags

Any changes you make immediately impact everyone's personal sidebar.

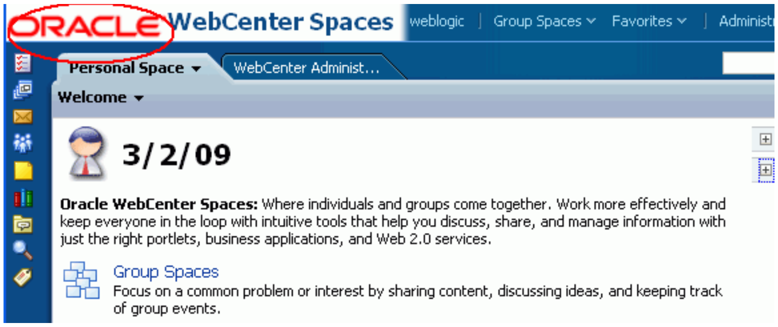
33.4 Changing the WebCenter Logo

One way to apply corporate branding to WebCenter Spaces, is to add your company logo to the top left corner of the application (Figure 33–6). If your company's logo is not suitable, any graphic that brings visual interest can be used.

> **Note:** You can change the application name that displays next to the logo too. See Section 33.1, "Naming Your WebCenter".

The logo you specify will resize automatically, according to the application skin.

Figure 33–6 Changing the WebCenter Logo



Oracle WebCenter Spaces: Where individuals and groups come together. Work more effectively and keep everyone in the loop with intuitive tools that help you discuss, share, and manage information with just the right portlets, business applications, and Web 2.0 services.

Focus on a common problem or interest by sharing content, discussing ideas, and keeping track of group events.

To change the WebCenter logo:

1. Login to WebCenter Spaces with administrative privileges.

   See Section 32.1, "Logging into WebCenter Spaces as an Administrator".
2. Click the **Administration** link at the top of the application.
3. Click the **General** tab.
4. Click **Browse** for the **Application Logo** property.

   The File Upload dialog box opens.
5. Select the logo you want to use.
6. Click **Apply** to save.

The logo is uploaded to the WebCenter Spaces image directory (`/webcenter/images`) and the new logo immediately appears in the top left corner of the application banner.

33.5 Applying Look and Feel Using Skins

As WebCenter Spaces Administrator, you may customize the appearance of WebCenter Spaces for all users by changing its skin. A skin changes the way the user interface appears, but does not change the application's behavior. A selection of built-in skins are provided with WebCenter Spaces. Alternatively, create skins of your own and brand the application according to your corporate image.

This section includes the following subsections:

- Section 33.5.1, "What You Should Know About Application Skins"
- Section 33.5.2, "Selecting a Skin"
- Section 33.5.3, "Making New Skins Available to WebCenter Spaces"

33.5.1 What You Should Know About Application Skins

The look and feel of WebCenter Spaces is driven by an ADF Faces skin. A skin in ADF Faces is a global style sheet for the entire application. Every component in WebCenter Spaces will automatically use the styles described by this skin. ADF Faces skins are based on the Cascading Style Sheet specification, and use CSS 3.0 syntax.

Out-of-the-box, WebCenter Spaces uses the *Deep Sea* skin. In addition, WebCenter Spaces provides several built-in skins, with names such as *Storm* and *Midnight*, so that you can experiment with some different look and feels. For details, see Section 33.5.2, "Selecting a Skin".

If none of the built-in skins suit your requirements or you want to apply a look and feel that reflects your corporate brand, you may provide your own ADF Faces skin and apply it to WebCenter Spaces. For details, see Section 33.5.3, "Making New Skins Available to WebCenter Spaces".

33.5.2 Selecting a Skin

To apply a different skin to your WebCenter Spaces application:

1. Login to WebCenter Spaces with administrative privileges.

   See Section 32.1, "Logging into WebCenter Spaces as an Administrator".

2. Click the **Administration** link at the top of the application.
3. Click the **General** tab.
4. Choose an **Application Skin** from the list provided.

   The skin list provided is generated from a file called `trinidad-skins.xml`. To add skins to this file, read Section 33.5.3, "Making New Skins Available to WebCenter Spaces".

5. Click **Apply**.

The selected skin is immediately applied to WebCenter Spaces.

33.5.3 Making New Skins Available to WebCenter Spaces

If none of the built-in skins suit your requirements or you want to apply a look and feel that reflects your corporate brand, you may provide your own ADF Faces skin and apply it to WebCenter Spaces.

Custom skin deployment typically takes place before the WebCenter Spaces application goes live or during scheduled maintenance periods. As well as providing the skin file (.css) and all supporting images, you must register the skin in a trinidad-skins.xml file, build and deploy a customized WebCenter Spaces .WAR file, and restart WebCenter Spaces. For more information, refer to the white paper "*Extending WebCenter Spaces*" available on the Oracle Technology Network (`http://www.oracle.com/technology/products/webcenter/pdf/owcs_r11_extend_spaces_wp.pdf`).

33.6 Applying Site Templates

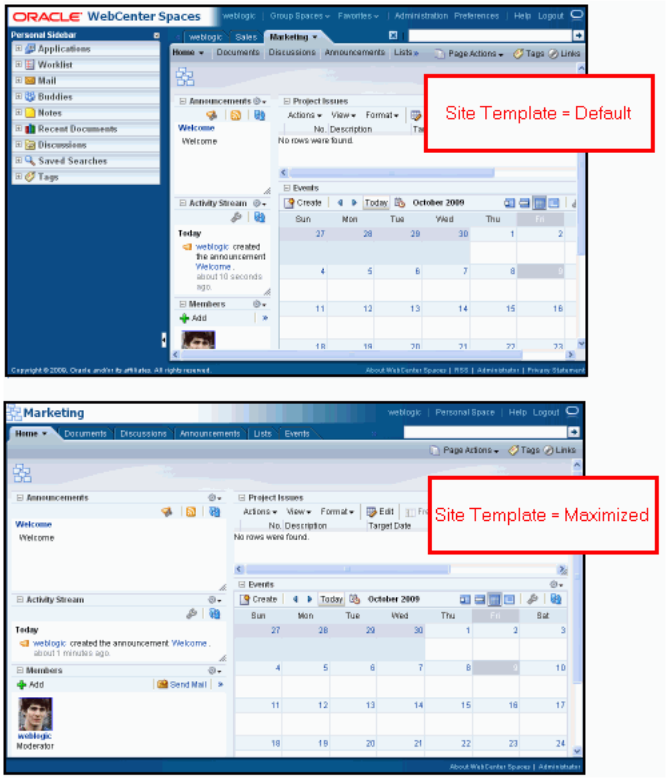
In WebCenter Spaces, site templates define the structure of WebCenter pages, and also the content. Every page, whether displayed in a personal space or a group space, is displayed within a site template.

For example, a typical site template might define areas such as the global tool bar, the sidebar, the footer, and so on (Figure 33–7).

Out-of-the-box site templates include:

- **Default** - Normal WebCenter Spaces view with global tool bar, the sidebar, the footer, and so on.
- **Maximized** - Displays personal spaces and group spaces in full-screen mode to occupy the entire screen; all other WebCenter Spaces components are hidden.

Figure 33–7 Out-of-the-Box Site Templates



Site Template = Default

Site Template = Maximized

Administrators can define the site template that is applied to:

- Everyone's personal space
- New group spaces, by default

Group space moderators can override the default selection in their group space but users cannot override the site template applied to their personal space. See Section 33.6.1, "Choosing the Default Site Templates for Personal Spaces and Group Spaces".

Users can view any page with any one of these site templates by appending a URL parameter called `wc.chromeLevel` to the page's URL.

- **Default Site Template** - `http://host.com/webcenter/spaces/mygroup/page/Contacts?wc.chromeLevel=default`
- **Maximized Site Template** - `http://host.com/webcenter/spaces/mygroup/page/Contacts?wc.chromeLevel=gsDefault`

Site templates are defined in XML files. If you want to exclude certain content or display different content within these template areas you can modify any of the out-of-the-box site templates through JDeveloper or you can create new site templates of your own. You can also customize the site template list, such that your users only see site templates that you want them to use. See Section 33.6.2, "Making New Site Templates Available to WebCenter Spaces".

33.6.1 Choosing the Default Site Templates for Personal Spaces and Group Spaces

To select the site template that is used to display personal spaces and a default site template for group spaces:

1. Login to WebCenter Spaces with administrative privileges.

   See Section 32.1, "Logging into WebCenter Spaces as an Administrator".

2. Click the **Administration** link at the top of the application.
3. Click the **General** tab.
4. Choose a **Site Template for Personal Space** from the list provided.

   The site template you select is applied to everyone's personal space.

   > **Note:** If you choose the **Maximized** option, users will not have access to My Group Spaces, user preference settings, favorites, or the Sidebar.

   To add your own site templates to this list, read Section 33.6.2, "Making New Site Templates Available to WebCenter Spaces".

5. Choose a **Default Site Template for Group Spaces** from the list provided.

   The site template you select is applied to all new group spaces. Group space moderators choose a different site template for their group space if required.

   To add your own site templates to this list, read Section 33.6.2, "Making New Site Templates Available to WebCenter Spaces".

6. Click **Apply**.

33.6.2 Making New Site Templates Available to WebCenter Spaces

If the out-of-the-box site template set does not suit your requirements, you may provide your own template set for WebCenter Spaces. You can modify any of the out-of-the-box site templates through JDeveloper, you can create new site templates of your own, and you can customize the list of templates on offer inside WebCenter Spaces.

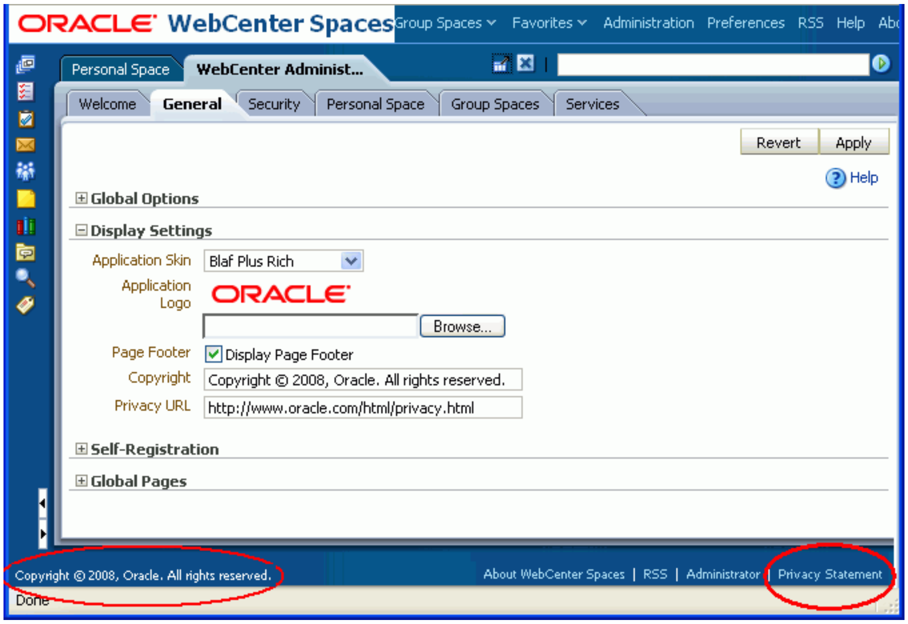
Site template customization typically takes place before the WebCenter Spaces application goes live or during scheduled maintenance periods as you must build and deploy a customized WebCenter Spaces .WAR file that contains your site templates, and restart WebCenter Spaces. For more information, refer to the white paper "*Extending WebCenter Spaces*" available on the Oracle Technology Network (`http://www.oracle.com/technology/products/webcenter/pdf/owcs_r11_extend_spaces_wp.pdf`).

33.7 Customizing Copyright and Privacy Statements

Administrators can customize or hide copyright and privacy statements for WebCenter Spaces. If displayed, the copyright and privacy URL appear in the application's page footer (Figure 33–8):

- Copyright - Displays a copyright statement for the entire application.
- Privacy URL - Links to a document that contains a privacy policy for the entire application.

Figure 33–8 Customizing the Copyright and Privacy URL



Application Skin: Blaf Plus Rich

Application Logo

Page Footer: ☑ Display Page Footer

Copyright: Copyright © 2008, Oracle. All rights reserved.

Privacy URL: http://www.oracle.com/html/privacy.html

Copyright © 2008, Oracle. All rights reserved.

Individual group spaces may provide their own copyright and privacy statements. See "Customizing Copyright and Privacy Statements" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

To customize or hide copyright and privacy statements:

1. Login to WebCenter Spaces with administrative privileges.

   See Section 32.1, "Logging into WebCenter Spaces as an Administrator".

2. Click the **Administration** link at the top of the application.

3. Click the **General** tab.

4. Do one of the following:

   - Select **Display Page Footer** to display copyright and privacy information at the bottom of the application.
   - Deselect **Display Page Footer** to hide the page footer. No legal notices will display.

5. If you have chosen to display legal notices:

   - **Copyright** - Enter a suitable copyright statement for the WebCenter Spaces application. If no copyright information is required, leave this field blank.
   - **Privacy URL** - Specify the location of the application's privacy policy. Enter a fully qualified URL. If no privacy information is required, leave this field blank.

6. Click **Apply** to save.

New settings immediately display in the page footer.

33.8 Choosing the Default Display Language

WebCenter Spaces provides run-time translations for 27 languages and 100 different locales.

Table 33–1 Languages Available for WebCenter 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

Table 33–1 lists all the languages available to WebCenter Spaces out-of-the-box. Your WebCenter Spaces administrator can reduce the number of available languages exposed in WebCenter Spaces by modifying the `supported-languages.xml` file, as described in the white paper "*Extending WebCenter Spaces*" available on the Oracle Technology Network (`http://webcenter.oracle.com`).

When a new language setting is specified, application content is translated, including links, field labels, display text, message text, and dialog boxes. However, information that users add to WebCenter Spaces such as announcements, documents, discussion forum content, and the like, is not translated. All user supplied content displays only in the language used by its author.

It is the administrator's job to choose a default *application display language* for WebCenter Spaces. When picking the default language, consider which language suits the majority of people using the application. The first time a user logs in to WebCenter Space the default language displays but individuals can personalize their display language through user preferences.

The default application display language only applies when users log in to WebCenter Spaces. All public pages, such as the welcome page and login page, display in the *browser language*.

WebCenter Spaces provides a language switcher on the welcome, login, and self registration pages to accommodate anyone whose native language is not the browser language. The language switcher sets the *session language cookie* which overrides the browser language and any default display language you may define for the application. The session language is retained for the life of the session cookie. When a user clears browser cookies—deliberately—the session language is also cleared and the browser language (unauthenticated) and default display language (authenticated) become active again.

To summarize, the order of precedence for WebCenter Spaces display language settings from weakest to strongest is as follows:

- **Browser setting** - your Browser documentation will describe how to change the browser's language.
- **Application setting** - see instructions below.
- **User preference setting** - see "Setting a User Preference Display Language" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

- **Session setting** - see "Setting a Session Display Language" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.
- **Group space setting** - see "Setting a Group Space Display Language" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

To select the default application display language for WebCenter Spaces:

1. Login to WebCenter Spaces with administrative privileges.

   See Section 32.1, "Logging into WebCenter Spaces as an Administrator".
2. Click the **Administration** link at the top of the application.
3. Click the **General** tab.
4. Choose a **Default Language**.
5. Click **Apply**.

The new language is effective immediately.

33.9 Enabling and Disabling WebCenter Services

In WebCenter Spaces, a series of WebCenter services expose social networking and personal productivity features through various task flows (Table 33–2):

Table 33–2 WebCenter Services

Services A to M	Services N to W
Announcements[1]	Notes [2]
Blog [1]	Page [2]
Discussion [1]	People Connections [2]
Documents [1]	RSS [2]
Events [1]	Recent Activities [2]
Instant Messaging and Presence (IMP) [1]	Search [1]
Links[2]	Tags [2]
Lists [2]	Wiki [1]
Mail [1]	Worklist [1]

[1] Service requires a connection to external back-end server.

[2] Services, such as notes, links, pages, tags, and so on, use the same WebCenter repository and MDS repository as WebCenter Spaces to store their data.

Some WebCenter services[1], such as Mail, require an *external* back-end server. The Fusion Middleware Administrator is responsible for managing connections to all external servers and also maintains the WebCenter and MDS repositories where application data, specific to WebCenter Spaces[2], is stored. See also Chapter 3, "Maintaining WebCenter Spaces".

When a service, such as Mail, is available in WebCenter Spaces:

[1] Service requires a connection to an external back-end server.

[2] Services, such as notes, links, lists, pages, tags, and so on, use the same WebCenter repository and MDS repository as WebCenter Spaces to store their data.

- Associated task flows display in the resource catalog.
- Existing task flows function as expected.
- (Group space services only) Moderators choose whether to enable or disable the service in their group spaces—using the *Group Space Settings - Services* page.

When a back-end server is not configured, intentionally or otherwise, WebCenter Spaces cannot offer features or functionality related to that service:

- Associated task flows are not available in the resource catalog.
- Existing task flows display a message indicating that the service is currently unavailable.
- (Group space services only) Service is not listed, as available, to group space moderators —on *Group Space Settings - Services* page.

Reporting Temporary Issues with WebCenter Services

When a service is temporarily unavailable, report the issue to the Fusion Middleware Administrator. The Fusion Middleware Administrator can use Fusion Middleware Control to investigate, diagnose, and solve issues with WebCenter services. See also, Section 30.2.1, "Monitoring WebCenter Spaces".

Hiding Task Flows Belonging to Disabled Services

Most WebCenter Services are optional. If you decide not to offer a particular service in WebCenter Spaces, temporarily or permanently, consider removing any associated task flows that display, by default, out-of-the-box.

Oracle recommends that you hide disabled services in the sidebar too. See, Section 33.3, "Customizing the Sidebar".

Enabling and Disabling Services for a Single Group Space

Group space moderators can enable or disable available WebCenter services within their group spaces. See, "Enabling and Disabling Services Available to a Group Space" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

33.10 Enabling and Disabling Personal Spaces

Personal spaces are optional in WebCenter Spaces—it is not mandatory to provide users with a private work area where they can store personal content and perform personal tasks. Users can fully participate in group space collaboration projects without a personal space.

Users who do not have a personal space are presented with My Group Spaces when they login. No personal productivity tools are available (such as the personal sidebar, favorites links, and so on) and users cannot create personal pages or see personal pages that other users might share.

The `Application-View` permission controls which users have their own personal space. Administrators can disable personal spaces for everyone using WebCenter Spaces or specific users only. Use the table in step 5 to determine which permission settings you require.

To enable or disable user access to personal spaces:

1. Login to WebCenter Spaces with administrative privileges.

   See Section 32.1, "Logging into WebCenter Spaces as an Administrator".

2. Click the **Administration** link at the top of the application.
3. Click the **Security** tab.
4. Click the **Roles** tab.
5. Select or clear the **Application-View** check box as follows:

Role	Select Application-View	Clear Application-View
Spaces-User	Everyone has a personal space.	Users do not have a personal space unless you grant them another role that specifies otherwise.
Any Custom Role	Users assigned any custom role have a personal space.	Users with this role do not have a personal space. [1]
Administrator	Users assigned this role have a personal space.	Users with this role do not have a personal space. [1]
Public-User	Unauthenticated users can see personal pages/content marked public.	Unauthenticated users only see the login page.

[1] Assumes the Application-View permission is disabled for the Spaces-User and the Public-User.

6. Click **Apply** to save.

New permissions are effective immediately.

33.11 Publishing the WebDAV URL

WebCenter Spaces uses an Oracle Content Server to store group space and personal space documents. WebDAV (Web-Based Distributed Authoring and Versioning), which allows users to look at their content repository using their Windows Explorer, can be used with Oracle Content Server and hence with WebCenter Spaces content.

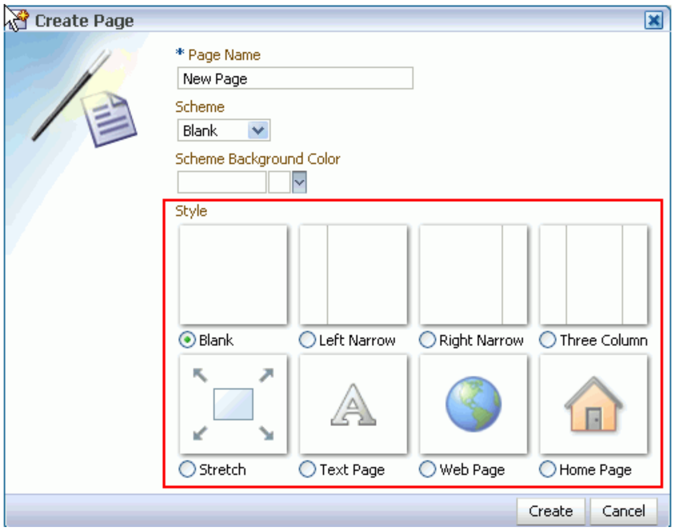
Using WebDAV, WebCenter users can seamlessly drag and drop content, files, and folders back and forth between their desktop and their personal and group spaces. Users will not know the WebCenter Spaces WebDAV URL unless you publish this information—maybe in a document or on a business role page that everyone can access.

Contact your Fusion Middleware Administrator to find out the URL for the Oracle Content Server that WebCenter Spaces is using to store group space and personal space documents. If the base URL for that Oracle Content Server is `http://<host>:<port>/<relative_web_root>`, the WebDAV root URL will be `http://<host>:<port>/<relative_web_root>/idcplg/webdav`.

33.12 Making New Page Styles Available

WebCenter Spaces offers eight page styles out-of-the-box (Figure 33–9).

Figure 33–9 Standard Page Styles



Create Page

* Page Name: New Page

Scheme: Blank

Scheme Background Color:

Style

● Blank ○ Left Narrow ○ Right Narrow ○ Three Column

○ Stretch ○ Text Page ○ Web Page ○ Home Page

Some page styles come prepopulated with a selection of useful task flows. Others include properties that suggest a particular use for the page. For example, the Web page style includes a configurable property for specifying a URL. See "WebCenter Seeded Page Styles" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

If the built-in page styles do not suit your requirements or you want to offer a different set of page styles, you may create page styles of your own (defined in .jspx files) and deploy them to WebCenter Spaces.

Custom page style deployment typically takes place before the WebCenter Spaces application goes live or during scheduled maintenance periods as you must build and deploy a customized WebCenter Spaces .WAR file that contains your new page style files (.jspx), and restart WebCenter Spaces. For more information, refer to the white paper "*Extending WebCenter Spaces*" available on the Oracle Technology Network (`http://www.oracle.com/technology/products/webcenter/pdf/owcs_r11_extend_spaces_wp.pdf`).

33.13 Customizing the Oracle Composer Catalog and Deploying New Task Flows

In WebCenter Spaces, the Oracle Composer's catalog provides access to page content, such as task flows and portlets, and page layout components, such as images, content boxes, hyperlinks, and the like. The catalog presents available resources in a series of folders and subfolders and the content on offer changes dynamically depending on which services are currently available. For example, in a particular group space, mail-related task flows will display in the group space catalog when mail services are available but will not display if the back-end mail server is not yet configured or the Mail service has been disabled by the group space moderator.

WebCenter Spaces provides two catalogs out-of-the-box—a personal space catalog and a group space catalog. Each catalog contains a default set of task flows. Should you need to add new task flows, remove task flows, or reorganize the folder hierarchy to better suit your audience you can make a copy, and customize each catalog through JDeveloper.

Catalog customizations and new task flow deployment typically take place before the WebCenter Spaces application goes live or during scheduled maintenance periods as you must build and deploy a customized WebCenter Spaces .WAR file that includes your custom catalogs and custom task flows, and restart WebCenter Spaces. For more information, refer to the white paper "*Extending WebCenter Spaces*" available on the Oracle Technology Network (`http://www.oracle.com/technology/products/webcenter/pdf/owcs_r11_extend_spaces_wp.pdf`.

34

Managing Users and Roles for WebCenter Spaces

This chapter describes how to manage users, roles, and permissions in WebCenter Spaces. It includes the following sections:

- Section 34.1, "Understanding Users, Roles, and Permissions"
- Section 34.2, "Managing Users"
- Section 34.3, "Managing Application Roles and Permissions"
- Section 34.4, "Allowing Self-Registration"
- Section 34.5, "Troubleshooting Issues with Users and Roles"

Audience

The content of this chapter is intended for WebCenter Spaces administrators. Users granted the WebCenter Spaces `Administrator` role or a custom role that grants the `Application-Manage` permission).

Refer to Section 24.3, "Adding Users to the Embedded LDAP Identity Store" if you are a Fusion Middleware Administrator responsible for security-sensitive administrative duties that require configuration through Fusion Middleware Control or WLST.

34.1 Understanding Users, Roles, and Permissions

Read this section to understand more about WebCenter users, application roles, and permissions granted to WebCenter users working in their personal space. It includes the following subsections:

- Section 34.1.1, "Understanding Users"
- Section 34.1.2, "Understanding Application Roles"
- Section 34.1.3, "Understanding Application Permissions"
- Section 34.1.4, "Understanding Discussions Server Role and Permission Mapping"
- Section 34.1.5, "Understanding Group Space Roles and Permissions"

When a WebCenter user becomes a member of a group space, a different set of roles and responsibilities apply. See "What You Should Know About Group Space Roles and Permissions" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

34.1.1 Understanding Users

A WebCenter user is an member of WebCenter Spaces—provisioned directly from an existing identity store. See also, Section 24.3, "Adding Users to the Embedded LDAP Identity Store."

All users in the identity store are assigned minimal WebCenter Spaces privileges through the `Spaces-User` role. The only exception is the Fusion Middleware Administrator (`weblogic`). Out-of-the-box, the Fusion Middleware Administrator is the only user assigned full administrative privileges through the `Administrator` role. For more information, read the next section Section 34.1.2.1, "Default Application Roles".

It is the Fusion Middleware Administrator's job to assign each WebCenter user an appropriate application role. Alternatively, the Fusion Middleware Administrator may choose to assign the `Administrator` role to another user and delegate this responsibility.

Table 34–1 Default Administrator in WebCenter Spaces

User	Description
Fusion Middleware Administrator (weblogic)	Administrator for the entire application server, sometimes referred to as the super administrator. This user can manage any application on the server, including WebCenter Spaces.

WebCenter Spaces supports self-registration. When new WebCenter users self-register, they create their own login and password and a new user account is created in the identity store. See also, Section 34.4, "Allowing Self-Registration".

34.1.2 Understanding Application Roles

Application roles control the level of access a user has to information and services in WebCenter Spaces. Specifically, application roles determine what a user can see and do in their *personal space.*

Application role assignment is the responsibility of the WebCenter Spaces administrator. Administrators can assign users a default application role or create additional, custom roles specific to their WebCenter Spaces application. For more detail, see:

- Default Application Roles
- Custom Application Roles

Application roles only apply while a user is working within their personal space. Within a particular group space a different set of roles and permissions apply and it is the group space moderator's responsibility to determine suitable role assignments for each of its members. See also "Managing Group Space Roles and Permissions" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

> **Note:** Application roles and permissions defined within WebCenter Spaces are stored in its *policy store* and, consequently, apply to this WebCenter Spaces application only. Enterprise roles are different; enterprise roles are stored within the application's *identity store* and do not imply any permissions within WebCenter Spaces.

34.1.2.1 Default Application Roles

WebCenter Spaces provides several default application roles that cannot be deleted (Table 34–2).

Table 34–2 Default Application Roles for WebCenter Spaces

Application Role	Description	Modify?
Administrator	Users with the `Administrator` role can set application-wide properties for WebCenter Spaces, create business role pages, configure defaults for discussion forums, mail, and people connection services, and perform other administrative duties such as editing the login page and the self-registration page. Administrators can also manage users and roles for WebCenter Spaces, delegate or revoke privileges to/from other users, manage group spaces and group space templates, and also import and export group space information. Out-of-the-box, the Fusion Middleware Administrator is the only user assigned full WebCenter Spaces administrative privileges through the `Administrator` role.	Yes* *Except for Application permissions which are read-only
Spaces-User	Authenticated users of WebCenter Spaces are granted the `Spaces-User` role. After logging in, users assigned with this role have access to their own personal space, pages that they create, and public pages. These users can also view public group spaces, create group spaces, and create group space templates. This role inherits permissions from the `Public_User` role. In WebCenter Spaces, the `Spaces-User` role is equivalent to the `authenticated-user` role.	Yes
Public-User	Anyone with access to WebCenter Spaces who is not logged in, is granted the `Public_User` role. Such users are anonymous, unidentified, and can see public content only. In WebCenter Spaces, the `Public-User` role is equivalent to the `anonymous-role`.	Yes

34.1.2.2 Custom Application Roles

Custom application roles (sometimes known as user-defined roles) are specific to your WebCenter Spaces application. When setting up WebCenter Spaces, it is the WebCenter Spaces administrator's job to identify which application roles are required, choose suitable role names, and define the responsibilities of each role.

For example, an education environment might require roles such as Teacher, Student, and Guest. While roles such as Finance, Sales, Human Resources, and Support would be more appropriate for a corporate environment.

To learn how to set up applications roles for WebCenter users, see Section 34.3.2, "Defining Application Roles."

34.1.3 Understanding Application Permissions

Every application role has specific, defined capabilities known as permissions. These permissions allow individuals to perform specific actions in their personal space.

Permissions are categorized as follows and listed individually in the subsequent tables:

- Application
- Group Spaces
- Group Space Templates
- Pages
- Discussions
- Links
- People Connections

With a particular category, the `Manage` permission (such as `Group Spaces-Manage`) contains all other permissions (for example, `Group Spaces-Configure` and `Group Spaces-View`). No permission, except `Manage`, inherits privileges from other permissions.

Table 34–3 Application Permissions in WebCenter Spaces

Category	Application Permissions
Application	**Manage** - Enables access to all *WebCenter Spaces Administration* pages: General, Security, Personal Space, Group Spaces, and Services. Through these pages, users can manage application security (users/roles), set application-wide properties, create business role pages, manage everyone's personal pages, view group spaces accessible to them, as well as export/import group spaces and group space templates. Some administrative tasks are exclusive to the out-of-the-box `Administrator` role and cannot be performed by granting the `Application-Manage` permission. These tasks include editing the login page, the self-registration page, and profile gallery pages, as well as the ability to manage *all* group spaces and group space templates. **Configure** - Same as the `Application-Manage` permission but excludes security privileges. Users with this permission cannot access the Security page. **View** - Enables users to view the WebCenter Spaces application.
Group Spaces)	**Manage** - Enables access to the group space *Settings* page (General, Roles, Members, Pages, Services, Custom Attributes). Through these pages users can manage group space membership, assign permissions and roles, manage, delete, and export group spaces, set group space properties, and manage service availability. **Configure** - Same as the `Group Spaces-Manage` permission but excludes security privileges. Users with this permission cannot access the Roles and Members pages unless they are a group space moderator. **View** - View group spaces. **Create** -Create group spaces.

Table 34–3 (Cont.) Application Permissions in WebCenter Spaces

Category	Application Permissions
Group Space Templates	**Manage** - Enables users to manage and delete any group space templates that is accessible to them. **View** - Enables user to view group space template information and create group spaces based on a template. **Create** - Users can create group space templates.
Pages	**Manage** - Edit properties of a personal page, set personal page permissions, and all other page actions. **Delete** - Delete a personal page. **Edit** - Add or edit personal page content, rearrange content, and set page parameters and properties. **Personalize** - Personalize your view of a personal page by adding, editing, or removing content. **View** - View a personal page. **Create** - Create or design a new personal page. These permissions do not apply to group space pages. Group space page permissions are granted on a per group space-basis by the group space moderator.
Discussions	**Manage** - Manage categories, forums, and topics on the back-end discussions server. Set discussion forum properties for all group spaces. See also, Section 34.1.4, "Understanding Discussions Server Role and Permission Mapping".
Links	**Manage** - Create and delete links between objects, and manage link permissions. **Delete** - Delete a link between two objects. **Create** - Create links between objects.
People Connections	**Manage** -Manage application-wide settings for People Connection services. **Edit** -Edit content associated with People Connection services. **Share** -Share content associated with People Connection services with others.

34.1.4 Understanding Discussions Server Role and Permission Mapping

WebCenter Spaces uses *application roles* to manage user permissions in personal spaces and *group space roles* to manage user permissions with a group space. On the Oracle WebCenter Discussions server, a different set of roles and permissions apply.

Users who are working with discussions and announcements in WebCenter Spaces automatically map to the appropriate Oracle WebCenter Discussions server role, see Table 34–4 and Table 34–5.

Table 34–4 Discussions Server Roles and Permissions - Application

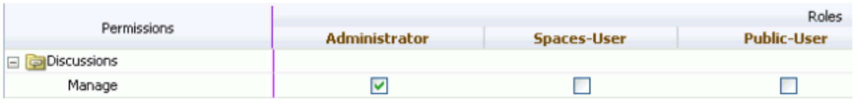
Discussion Server Role	Discussion Server Permissions	WebCenter Spaces Equivalent Application Permission
Administrator	Category Admin	`Discussions-Manage` Create, read, update and delete sub categories, forums and topics inside the category for which permissions are granted.

Table 34–5 Discussions Server Roles and Permissions - For Group Spaces

Discussion Server Role	Discussion Server Permissions	WebCenter Spaces Equivalent Group Space Permissions
Moderator	Category Admin Forum Admin	▪ `Discussions-Manage` Create, read, update and delete forums and topics. ▪ `Announcements-Manage` Create, read, update and delete announcements.
	Read Forum Create Thread Create Message Create Announcement	▪ `Discussions-Edit` Create and reply to topics. ▪ `Announcements-Edit` Create and edit announcements.
	Read Forum	▪ `Discussions-View` View forums and topics. ▪ `Announcements-View` View announcements.

Any user assigned the `Application-Discussions-Manage` permission in WebCenter Spaces is automatically added to Oracle WebCenter Discussions and assigned the `Administrator` role with the `Category Admin` permission. Out-of-the box, WebCenter Spaces assigns the `Application-Discussions-Manage` permission to the `Administrator` role only, as shown in Figure 34–1.

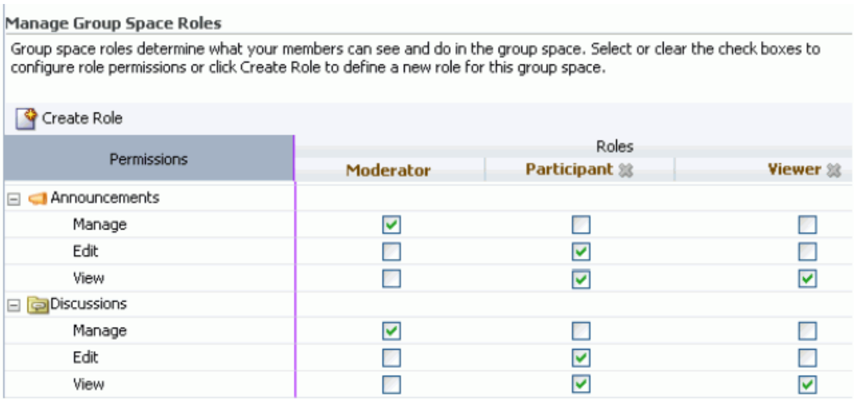
Figure 34–1 Application Roles - Default Discussion Permissions



Permissions	Administrator	Spaces-User	Public-User
	Roles		
⊟ Discussions			
Manage	☑	□	□

Similarly, in group spaces, any member assigned the `Discussions-Manage`, `Discussions-Edit`, or `Discussion-View` permission is granted the corresponding permissions on the Oracle WebCenter Discussions server. Out-of-the box, discussion and announcement permissions for the default group space roles `Moderator`, `Participant`, and `Viewer`, are as shown in Figure 34–2.

Figure 34–2 Group Space Roles - Default Discussion Permissions



Manage Group Space Roles

Group space roles determine what your members can see and do in the group space. Select or clear the check boxes to configure role permissions or click Create Role to define a new role for this group space.

Permissions	Roles		
	Moderator	Participant	Viewer
⊟ Announcements			
Manage	☑	☐	☐
Edit	☐	☑	☐
View	☐	☑	☑
⊟ Discussions			
Manage	☑	☐	☐
Edit	☐	☑	☐
View	☐	☑	☑

34.1.5 Understanding Group Space Roles and Permissions

Application roles and permissions only apply when users are working in their personal space. Within a particular group space, a different set of roles and permissions apply and it is the group space moderator's responsibility to determine suitable role assignments for each of its members. For details, see "Managing Group Space Roles and Permissions" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

34.2 Managing Users

Administrators must ensure that all WebCenter users have appropriate permissions. To get permissions, users must be assigned to an appropriate application role.

This section tells you how to assign roles and contains the following subsections:

- Section 34.2.1, "What You Need to Know About Managing Users"
- Section 34.2.2, "Assigning Users (and Groups) to Roles"
- Section 34.2.3, "Assigning a User to a Different Role"
- Section 34.2.4, "Giving a User Administrative Privileges"
- Section 34.2.5, "Revoking Application Roles"
- Section 34.2.6, "Adding or Removing Users"

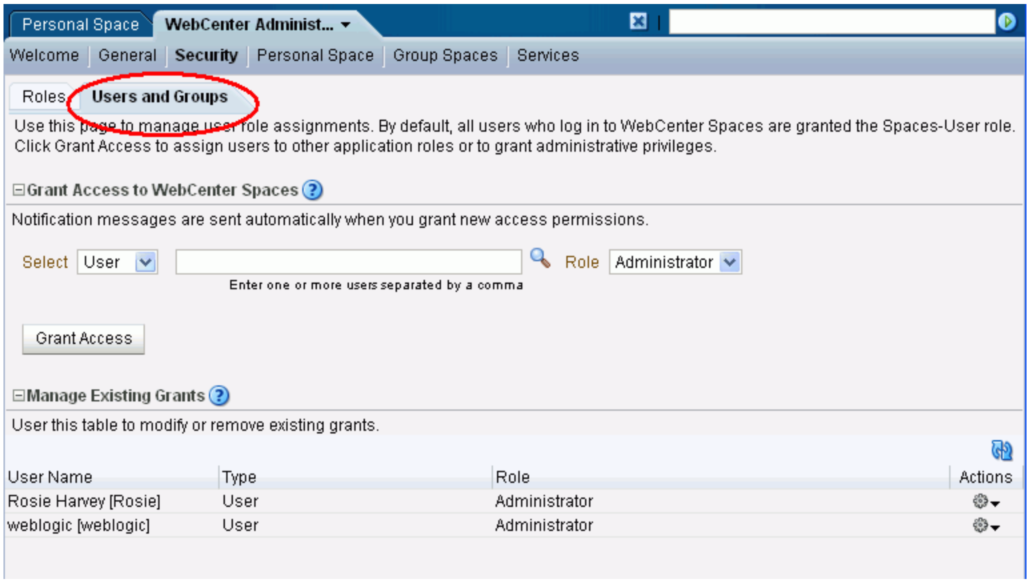
34.2.1 What You Need to Know About Managing Users

From the *Users and Groups* page (Figure 34–3), administrators can manage application roles for all the users who have access to WebCenter Spaces, that is, all users defined in the identity store. From here, you can change user role assignments, grant administrative privileges, and revoke user permissions.

Only users granted special (nondefault) application privileges appear in this table. Initially, all users in the WebCenter Spaces identity store are assigned minimal privileges through the `Spaces-User` role. Users with the default `Spaces-User` role are not listed here.

See also, Section 24.3, "Adding Users to the Embedded LDAP Identity Store."

Figure 34–3 WebCenter Administration - Users Page



Use this page to manage user role assignments. By default, all users who log in to WebCenter Spaces are granted the Spaces-User role. Click Grant Access to assign users to other application roles or to grant administrative privileges.

⊟Grant Access to WebCenter Spaces

Notification messages are sent automatically when you grant new access permissions.

Select: User   Role: Administrator

Enter one or more users separated by a comma

Grant Access

⊟Manage Existing Grants

User this table to modify or remove existing grants.

User Name	Type	Role	Actions
Rosie Harvey [Rosie]	User	Administrator	⚙▾
weblogic [weblogic]	User	Administrator	⚙▾

34.2.2 Assigning Users (and Groups) to Roles

Initially, all users in the WebCenter Spaces identity store are assigned minimal privileges through the `Spaces-User` role. You can assign individual users (or multiple users in the same enterprise group) to a different application role through WebCenter Spaces Administration.

Updates in your back-end identity store, such as new users or someone leaving an enterprise group, are automatically reflected in WebCenter Spaces. Initially, when you assign an enterprise group to a WebCenter Spaces 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.

> **Note:** For WebCenter Spaces to properly maintain enterprise group-to-role mappings, the back-end discussions server and content server must support enterprise groups. If either back-end server does not support enterprise groups, users belonging to enterprise groups are individually added to WebCenter Spaces roles and subsequent group updates in the identity store are not reflected in WebCenter Spaces. This can quickly become a maintenance issue, especially when enterprise groups contain large number of users. Oracle WebCenter Discussion Server and Oracle Universal Content Management versions provided with Oracle WebCenter 11.1.1.2.0 support enterprise groups but previous versions may not.

To assign a user (or a group of users) to a different application role:

1. Login to WebCenter Spaces with administrative privileges.

   See Section 32.1, "Logging into WebCenter Spaces as an Administrator".

2. Click the **Administration** link at the top of the application.

3. Click the **Security** tab.

4. Click the **Users and Groups** tab (Figure 34–3).

This page lists WebCenter users to which additional roles are defined.

5. Choose **User** or **Group** from the drop down.

   Select **User** to grant permissions to one or more users defined in the identity store. Select **Group** to grant permissions to groups of users.

6. If you know the exact name of the user or group, enter the name in the box provided, separating multiple names with a comma.

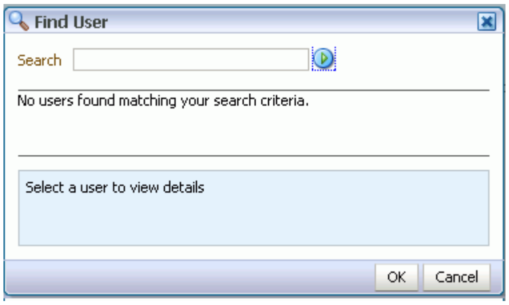
   If you are not sure of the name you can search your identity store:

   a. Click the **Find** icon (Figure 34–4).

Figure 34–4 Find Icon

The Find User (or Find Group) dialog box opens (Figure 34–5).

Figure 34–5 Finding Users and Groups in the identity store



No users found matching your search criteria.

Select a user to view details

   b. Enter two or more characters that appear in the name you are looking for.

   c. Click the **Search** icon.

   Users (or groups) matching your search criteria display in the **Select User** dialog box. The search is case-sensitive.

   d. Select one or more names from the list.

   To assign roles to multiple users or groups, multi-select all the names required. **Ctrl-Click** rows to select multiple names.

   Note: Nested enterprise groups must be added explicitly. Groups that are nested within a group hierarchy do not automatically inherit the same permissions as the parent group.

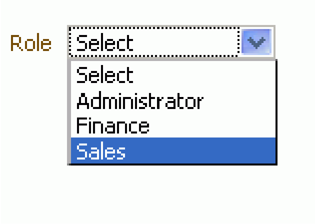
   ---

   e. Click **OK**.

   The names that you select are display on the **User and Groups** tab.

7. To assign a role, select a **Role** from the drop down (Figure 34–6).

Figure 34–6 Assigning a User Role



Select an appropriate role for the selected users (or groups). Only choose **Administrator** to assign full, administrative privileges for WebCenter Spaces.

If the role you want is not listed, create a new role that meets your requirements (see Section 34.3.2, "Defining Application Roles").

When no role is selected, the user assumes the `Spaces-User` role. See Section 34.1.2.1, "Default Application Roles".

8. Click **Grant Access**.

User's names and new role assignment display in the table.

34.2.3 Assigning a User to a Different Role

From time to time, a user's role in WebCenter Spaces may change. For example, a user may move out of sales into the finance department and in this instance, the user's role assignment may change from *Sales* to *Finance*.

Note: You cannot modify your own role or the Fusion Middleware Administrator's role. See Section 34.1.2, "Understanding Application Roles".

To assign a user to a different role:

1. Login to WebCenter Spaces with administrative privileges.

   See Section 32.1, "Logging into WebCenter Spaces as an Administrator".

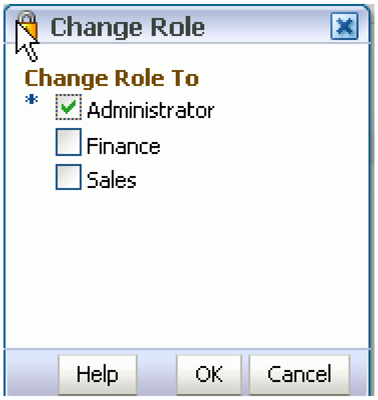
2. Click the **Administration** link at the top of the application.
3. Click the **Security** tab.
4. Click the **Users and Groups** tab.
5. In the **Manage Existing Grants** table, scroll down to the user you want.

   Only users with nondefault role assignments are listed in the table. If the user you want is not listed, grant the role required as described in Section 34.2.2, "Assigning Users (and Groups) to Roles".

6. Click the **Actions** icon, then choose **Change Role** from the drop down list.

   The Change Role dialog box opens (Figure 34–7).

Figure 34–7 Changing a User's Application Role



Change Role To

* ☑ Administrator

□ Finance

□ Sales

7. Select roles as follows:

   - Select **Administrator** to assign full, administrative privileges for WebCenter Spaces.
   - Select select one or more roles from the list available.

     If the role you want is not listed, create a new role that meets your requirements (see Section 34.3.2, "Defining Application Roles").

     At least one role must be selected. To revoke all role assignments, reverting user permissions to the default `Spaces-User` role, see Section 34.2.5, "Revoking Application Roles".

8. Click **OK**.

New role assignments display in the table.

34.2.4 Giving a User Administrative Privileges

It is easy to give a user full, administrative privileges for WebCenter Spaces through the `Administrator` role. Administrators have the highest privilege level and can view and modify anything in WebCenter Spaces so take care when assigning the `Administrator` role.

Some administrative tasks are exclusive to the `Administrator` role and cannot be performed by granting the `Application-Manage` permission. These tasks include editing the login page, the self-registration page, and profile gallery pages.

To give a user administrative privileges:

1. Login to WebCenter Spaces with administrative privileges.

   See Section 32.1, "Logging into WebCenter Spaces as an Administrator".

2. Click the **Administration** link at the top of the application.
3. Click the **Security** tab.
4. Click the **Users and Groups** tab.

   The Role column indicates which users already have full administrative privileges through the `Administrator` role.

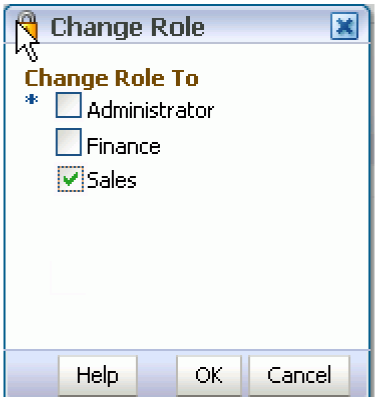
5. In the **Manage Existing Grants** table, scroll down to the user you want.

Only users with nondefault role assignments are listed in the table. If the user you want is not listed, follow steps in Section 34.2.2, "Assigning Users (and Groups) to Roles" to grant the `Administrator` role.

6. Click the **Actions** icon, then choose **Change Role** from the drop down list.

   The Change Role dialog box opens (Figure 34–7).

Figure 34–8 Changing a User's Application Role



Change Role

Change Role To

* ☐ Administrator

☐ Finance

☑ Sales

7. Select **Administrator** to assign full, administrative privileges for WebCenter Spaces.
8. Select **OK**.

The new role assignment displays in the table.

34.2.5 Revoking Application Roles

It is easy to revoke application role assignments that no longer apply. You can revoke roles individually or revoke all application roles assigned to a particular user at once.

Revoking all a user's application roles does not remove that user from the identity store and the user still has access to WebCenter Spaces through the default `Spaces-User` role.

> **Note:** You cannot revoke your own role assignments or the Fusion Middleware Administrator's role. See Section 34.1.2, "Understanding Application Roles".

To revoke application roles:

1. Login to WebCenter Spaces with administrative privileges.

   See Section 32.1, "Logging into WebCenter Spaces as an Administrator".
2. Click the **Administration** link at the top of the application.
3. Click the **Security** tab.
4. Click the **Users and Groups** tab.
5. In the **Manage Existing Grants** table, scroll down to the user you want.
6. Click the **Actions** icon:

- Choose **Change Role** icon to revoke one or more, specific application roles. See also Section 34.2.3, "Assigning a User to a Different Role".
- Choose **Delete Role Assignments** to revoke all roles assigned to that user, and then click **Delete** when asked for confirmation.

Access for that user is revoked immediately.

When you delete all the roles assigned to a particular user, the user is no longer listed on the Users page. The user remains in the identity store and still has access to WebCenter Spaces through the `Spaces-User` role. See Section 34.1.2.1, "Default Application Roles".

34.2.6 Adding or Removing Users

WebCenter Spaces administrators cannot add new user data directly to the WebCenter Spaces identity store or remove user credentials. Identity store management is the responsibility of the systems administrator and takes place through the WLS Administration Console or directly into embedded LDAP identity stores using LDAP commands. See also, Section 24.3, "Adding Users to the Embedded LDAP Identity Store."

WebCenter Spaces administrators can, however, enable self-registration for the application. Through self-registration, invited and uninvited users can create their own login and password for WebCenter Spaces. A user who self registers is immediately and automatically granted access to WebCenter Spaces and a new user account is created in the identity store. See also, Chapter 34.4, "Allowing Self-Registration".

34.3 Managing Application Roles and Permissions

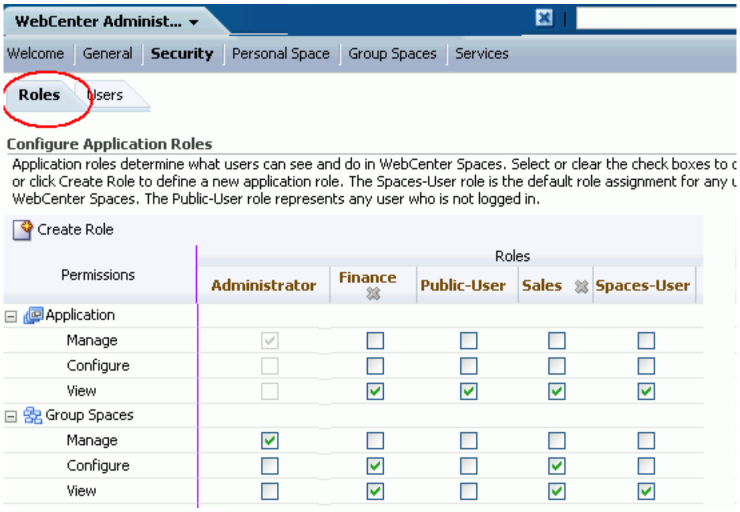
WebCenter Spaces uses application roles to manage permissions for users working in their *personal space*. This section tells you how to manage application roles, and their permissions from WebCenter Administration pages. It contains the following subsections:

- Section 34.3.1, "What You Need to Know About Application Roles and Permissions"
- Section 34.3.2, "Defining Application Roles"
- Section 34.3.3, "Modifying Application Role Permissions"
- Section 34.3.4, "Granting Permissions to the Public-User"
- Section 34.3.5, "Granting Permissions to the Spaces-User"
- Section 34.3.6, "Deleting Application Roles"

34.3.1 What You Need to Know About Application Roles and Permissions

From the Roles page (Figure 34–9), administrators can manage application roles and permissions. From here, you can edit the permissions assigned to an application role, create new application roles, or delete unused roles.

Figure 34–9 WebCenter Administration - Roles Page



Configure Application Roles

Application roles determine what users can see and do in WebCenter Spaces. Select or clear the check boxes to c or click Create Role to define a new application role. The Spaces-User role is the default role assignment for any u WebCenter Spaces. The Public-User role represents any user who is not logged in.

Create Role

Permissions	Roles				
	Administrator	Finance	Public-User	Sales	Spaces-User
Application					
Manage	☑	□	□	□	□
Configure	□	□	□	□	□
View	□	☑	☑	☑	☑
Group Spaces					
Manage	☑	□	□	□	□
Configure	□	☑	□	☑	□
View	□	☑	□	☑	☑

Application roles apply when a user is working within their personal space. A different set of roles and permissions apply when a user is working within a particular group space. It is the group space moderator's responsibility to determine suitable role assignments for each of its group space members. See also "Managing Group Space Roles and Permissions" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

WebCenter Spaces provides several default application roles. You cannot delete default application roles but you can modify the default permission assignments for each role. For more information, see Section 34.1, "Understanding Users, Roles, and Permissions".

34.3.2 Defining Application Roles

Use roles to characterize groups of WebCenter users and determine what they can see and do in their personal spaces.

When defining application roles, use self-descriptive role names and try to keep the role policy as simple as possible. Choose as few roles as you can, while maintaining an effective policy.

Take care to assign appropriate access rights when assigning permissions for new roles. Do not allow users to perform more actions than are necessary for the role but at the same time, try not to inadvertently restrict them from activities they must perform. In some cases, users might fall into multiple roles.

To define a new application role:

1. Login to WebCenter Spaces with administrative privileges.

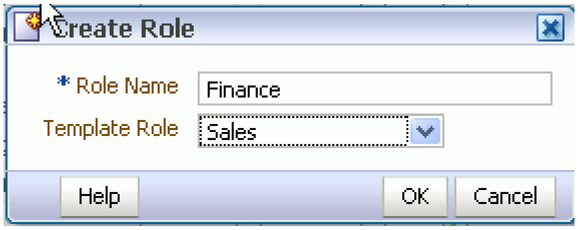
   See Section 32.1, "Logging into WebCenter Spaces as an Administrator".

2. Click the **Administration** link at the top of the application.
3. Click the **Security** tab.
4. Click the **Roles** tab.

   Current application roles for WebCenter Spaces display as columns in the table.

5. Click **Create Role** to define a new role for WebCenter users.

Figure 34–10 Creating a New Role



* Role Name: Finance

Template Role: Sales

6. Enter a suitable name for the role.

   Ensure the role names that are self-descriptive. Make it as obvious as possible which users should belong to which roles. Role names cannot include special characters or whitespace.

7. (Optional) Choose a **Template Role**.

   The new role inherits permissions from the template role. You can modify these permissions in the next step.

   Choose **Administrator** to create a role that inherits full, administrative privileges. Conversely, choose `Public-User` to create a role that *typically* provides minimal privileges. Alternatively, choose a custom application role to be your template.

8. Click **OK**.

   The new role appears as a column in the table. The permissions list shows which actions users with this role can perform.

9. To modify user permissions for the role, select or clear each permission check box.

10. Click **Apply** to save any changes that you make to the role's permissions.

34.3.3 Modifying Application Role Permissions

Administrators can modify the permissions associated with application roles at any time. Application permissions are described in Section 34.1.3, "Understanding Application Permissions".

Application role permissions allow individuals to perform specific actions in their personal space. With a particular category, the `Manage` permission (such as `Group Spaces-Manage`) contains all other permissions (for example, `Group Spaces-Configure` and `Group Spaces-View`).

> **Note:** Application permissions cannot be modified for the `Administrator` role. See also Section 34.1.2.1, "Default Application Roles".

To change the permissions assigned to a role:

1. Login to WebCenter Spaces with administrative privileges.

   See Section 32.1, "Logging into WebCenter Spaces as an Administrator".

2. Click the **Administration** link at the top of the application.

3. Click the **Security** tab.

4. Click the **Roles** tab.

5. Select or clear **Permissions** check boxes to enable or disable permissions for a role.

6. Click **Apply** to save.

The new permissions are effective immediately.

34.3.4 Granting Permissions to the Public-User

Anyone who is not logged in to WebCenter Spaces assumes the `Public-User` role. Out-of-the-box, the `Public-User` role is granted minimal privileges, that is, the `Application-View` permissions only.

> **Caution:** Take care when granting permissions to the `Public-User` role. Avoid granting administrative permissions such as `Application-Manage`, `Application-Configure`, other `Manage` permissions, or any permission that might be considered unnecessary.

Granting the Application-View Permission

The `Application-View` permission allows unauthenticated users to see public WebCenter Spaces application pages, such as the welcome page, and also content that individual WebCenter users choose to make public.

When `Application-View` permissions are granted to the `Public-User` role:

- Ensure that your WebCenter users understand that any personal page or personal content they choose to make public will become accessible to unauthenticated users outside of the WebCenter Spaces community, that is, anyone with Web access.
- Consider customizing the default welcome page that displays to public users before they login. See Section 35.3.1, "Customizing the Public Welcome Page".

If you do not want unauthenticated users to see WebCenter Spaces content that is marked 'public', do not grant the `Application-View` permission to the `Public-User` role. When public access is disabled, public content cannot be seen by unauthenticated users. Also, the welcome page for WebCenter Spaces is not displayed; public users are directed straight to a login page. Administrators may customize the default login page, if required. See Section 35.3.2, "Customizing the Login Page".

Granting Other Permissions

Be careful when assigning permissions to the `Public-User` role. For security reasons, Oracle recommend that you limit what anonymous users can see and do in WebCenter Spaces.

34.3.5 Granting Permissions to the Spaces-User

Anyone who is logged in to WebCenter Spaces assumes the `Spaces-User` role. Out-of-the-box, the `Spaces-User` role is granted minimal privileges, that is, the `Application-View`, `Group Space-Create`, `Group Space Templates-Create`, `Pages-Create`, `Profiles-Edit` permissions only.

Note that the `Spaces-User` role always inherits permissions from the `Public-User` role.

34.3.6 Deleting Application Roles

When an application role is no longer required you should remove it from WebCenter Spaces. This helps maintain a valid role list, and prevents inappropriate role assignment.

Application roles are deleted even when users are still assigned to the them. As you cannot delete any default roles, WebCenter users will always have the `Spaces-User` role.

> **Note:** Default roles cannot be deleted (`Administrator`, `Spaces-User`, `Public-User`). See Section 34.1.2.1, "Default Application Roles".

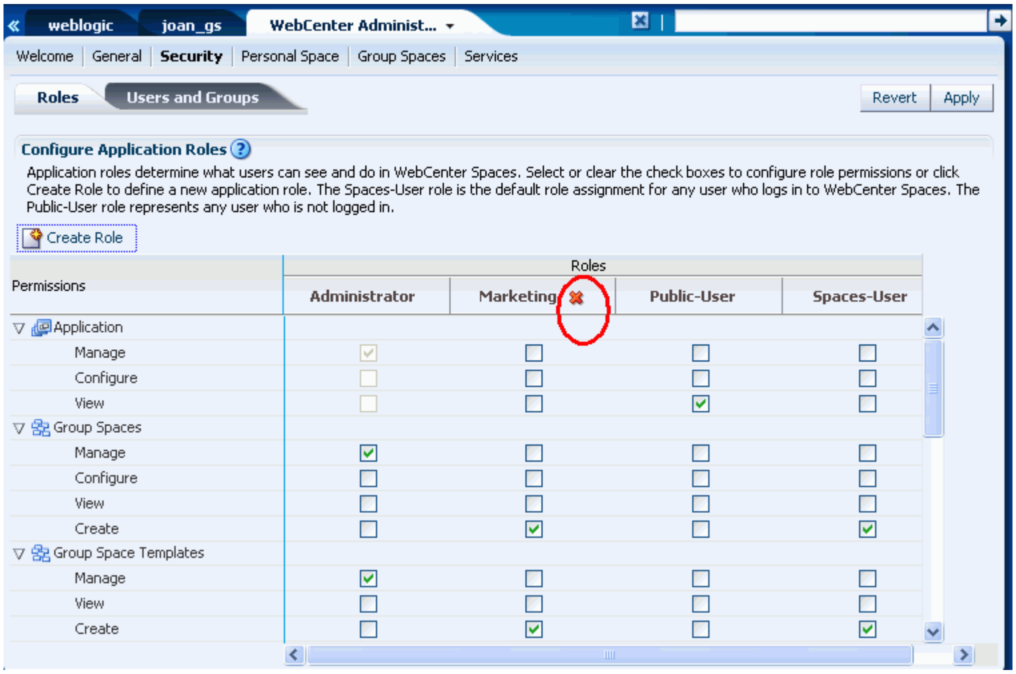
To delete an application role:

1. Login to WebCenter Spaces with administrative privileges.

   See Section 32.1, "Logging into WebCenter Spaces as an Administrator".

2. Click the **Administration** link at the top of the application.
3. Click the **Security** tab.
4. Click the **Roles** tab.
5. Select the Delete Role icon next to the role you want to delete (Figure 34–11).

Figure 34–11 Deleting an Application Role



Application roles determine what users can see and do in WebCenter Spaces. Select or clear the check boxes to configure role permissions or click Create Role to define a new application role. The Spaces-User role is the default role assignment for any user who logs in to WebCenter Spaces. The Public-User role represents any user who is not logged in.

Permissions	Roles			
	Administrator	Marketing ✖	Public-User	Spaces-User
▽ Application				
Manage	☑	□	□	□
Configure	□	□	□	□
View	□	□	☑	□
▽ Group Spaces				
Manage	☑	□	□	□
Configure	□	□	□	□
View	□	□	□	□
Create	□	☑	□	☑
▽ Group Space Templates				
Manage	☑	□	□	□
View	□	□	□	□
Create	□	☑	□	☑

6. Click **OK** to confirm that you want to delete the role.

   The role is removed from the table. Any users assigned to this role only, assume the default `Spaces-User` role and do not display on the Users tab.

34.4 Allowing Self-Registration

Self-registration allows users to create their own login and password for WebCenter Spaces. A user who self registers is immediately and automatically granted access to WebCenter Spaces and a new user account is created in the application's identity store.

When *anyone* is allowed to self-register, that is any public user, a Register link or Register button displays below the WebCenter Spaces login form. To enable this feature, see Section 34.4.2, "Enabling Anyone to Self-Register".

Self-registration by invitation is allowed too. This feature allows group space moderators to send out membership invitations to people who are not currently registered with WebCenter Spaces but might be interested in their group space. Before accessing the group space, invitees must create an account with WebCenter Spaces and their account details are added to the application's identity store. When the group space moderator approves their subscription request they will gain access to the group space. See Section 34.4.1, "Enabling Self-Registration By Invitation-Only".

Note: If self-registration is not enabled in WebCenter Spaces, identity store management takes place through the WLS Administration Console (or directly into embedded LDAP identity stores using LDAP commands) and is the responsibility of your systems administrator. See also, Section 24.3, "Adding Users to the Embedded LDAP Identity Store."

A self-registration page is supplied out-of-the-box. Users with the `Administrator` role can add new components to the page and change the page layout if required. See Section 35.3.3, "Customizing the Self-Registration Page".

The self-registration page provided with WebCenter Spaces offers to send a "user name reminder email" to anyone who tries to register using an existing email address. This feature only works if public credentials are defined for the external application that is providing authentication for the Mail service. If users experience issues with this feature, ask your Fusion Middleware Administrator to check the mail server connection and its associated external application connection are configured correctly and that public credentials are defined. See also, Section 15.3, "Registering Mail Servers".

34.4.1 Enabling Self-Registration By Invitation-Only

Out-of-the-box, only existing WebCenter users are candidates for group space membership. While this might meet the needs of most WebCenter Spaces applications it is likely that some group spaces will want to recruit members outside of the WebCenter Spaces community.

The WebCenter Spaces administrator can extend group space membership to users outside of WebCenter Spaces by allowing them to self-register on an *invitation-only* basis. When this facility is enabled, group space moderators can invite anyone to join their group space by sending them a customizable invitation by mail. The invitation includes a secure, self-registration URL which the invited party clicks to accept group space membership.

New members recruited in this way must create an account with WebCenter Spaces before gaining access to the group space. Users who self-register by invitation are added to the identity store, and to the group space member list.

Note: Users who self-register by invitation will be assigned the default application role too—`Spaces-User`. Out-of-the box, users with the `Spaces-User` role have access to their own personal space, pages that they create, and public pages. They are also allowed to view public group spaces, join any group space that allows self-subscription, and create group spaces of their own. When you enable self-registration, consider modifying `Spaces-User` permissions to suit your exact requirements. See also, Section 34.3.3, "Modifying Application Role Permissions".

To allow external users to join group spaces:

1. Login to WebCenter Spaces with administrative privileges.

   See Section 32.1, "Logging into WebCenter Spaces as an Administrator".

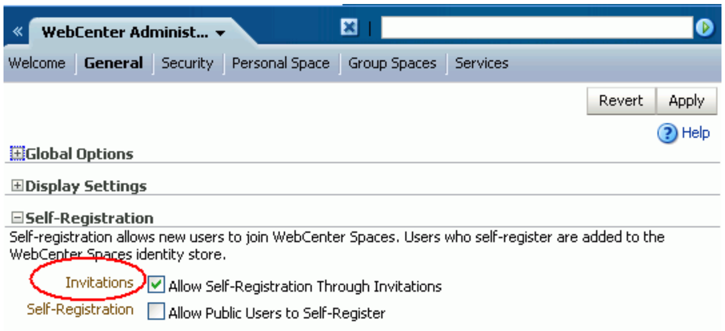
2. Click the **Administration** link at the top of the application.

3. Click the **General** tab.

4. Select **Allow Self-Registration Through Invitations** (Figure 34–12).

   When you deselect this option, only existing WebCenter users are candidates for group space membership.

Figure 34–12 Allowing Self-Registration Through Invitations



Self-registration allows new users to join WebCenter Spaces. Users who self-register are added to the WebCenter Spaces identity store.

Invitations ☑ Allow Self-Registration Through Invitations

Self-Registration □ Allow Public Users to Self-Register

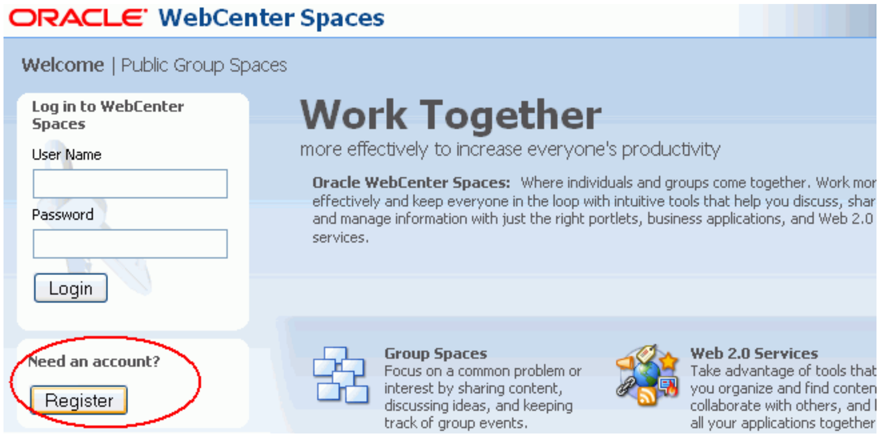
5. Click **Apply**.

Group space moderators may invite non-WebCenter users to become members of their group space. See "Inviting a Non-WebCenter Spaces User" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

34.4.2 Enabling Anyone to Self-Register

When *anyone* is allowed to self-register, that is any public user, a Register link displays in the top right corner of the application or a Register button displays below the WebCenter Spaces login form (Figure 34–13).

Figure 34–13 Self-Registration Available on Login Form



more effectively to increase everyone's productivity

Oracle WebCenter Spaces: Where individuals and groups come together. Work mor effectively and keep everyone in the loop with intuitive tools that help you discuss, shar and manage information with just the right portlets, business applications, and Web 2.0 services.

Focus on a common problem or interest by sharing content, discussing ideas, and keeping track of group events.

Take advantage of tools that you organize and find conten collaborate with others, and l all your applications together

New users must create an account before gaining access to the WebCenter Spaces application.

Users who self-register are added directly to the WebCenter Spaces identity store and assigned the `Spaces-User` application role. Out-of-the-box, users with `Spaces-User` role have access to their own personal space, pages that they create, and public pages. They are also allowed to view public group spaces, join any group space that allows self-subscription, and create group spaces of their own. If you enable self-registration, consider modifying `Spaces-User` permissions to suit your exact requirements. See Section 34.3.3, "Modifying Application Role Permissions".

To allow anyone to self-register with WebCenter Spaces:

1. Login to WebCenter Spaces with administrative privileges.

   See Section 32.1, "Logging into WebCenter Spaces as an Administrator".

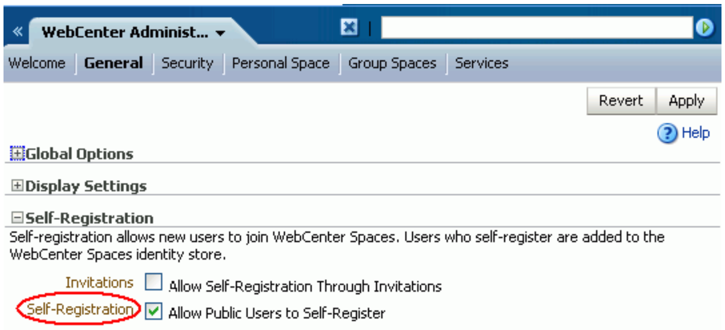
2. Click the **Administration** link at the top of the application.

3. Click the **General** tab.

4. Select **Allow Public Users to Self-Register** (Figure 34–14).

   When you deselect this option, public users cannot self-register with WebCenter Spaces. You still enable self-registration on an invitation-only basis if you want. See Section 34.4.1, "Enabling Self-Registration By Invitation-Only".

Figure 34–14 Allowing Self-Registration Through Invitations



Self-registration allows new users to join WebCenter Spaces. Users who self-register are added to the WebCenter Spaces identity store.

Invitations ☐ Allow Self-Registration Through Invitations

Self-Registration ☑ Allow Public Users to Self-Register

5. Click **Apply**.

See also, "Registering Yourself with WebCenter Spaces" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

34.5 Troubleshooting Issues with Users and Roles

For WebCenter Spaces to properly maintain enterprise group-to-role mappings, the back-end discussions server and content server must support enterprise groups. Oracle WebCenter Discussion Server and Oracle Universal Content Management versions provided with Oracle WebCenter 11.1.1.2.0 support enterprise groups but previous versions may not.

If a back-end server does not support enterprise groups, users belonging to enterprise groups are individually added to WebCenter Spaces roles and subsequent group updates in the identity store are not reflected in WebCenter Spaces. This can quickly become a maintenance issue, especially when enterprise groups contain large number of users.

An error message displays if a new back-end server that does not support enterprise groups is enabled in WebCenter Spaces where enterprise group-to-role assignments exist. In this instance, delete all the enterprise group-to-role assignments and reassign roles to individual users instead.

35 Managing Pages in WebCenter Spaces

This chapter describes how to manage personal pages and business role pages, and how to set up WebCenter Spaces for the public user. It includes the following sections:

- Section 35.1, "Managing Business Role Pages"
- Section 35.2, "Managing Personal Pages"
- Section 35.3, "Setting Up the Public User Experience"

Audience

The contents of this chapter is intended for WebCenter Spaces application administrators. Application administrators are users who are granted the WebCenter Spaces `Administrator` role or a custom role that grants the `Application-Manage` permission.

35.1 Managing Business Role Pages

- Section 35.1.1, "What You Should Know About Business Role Pages"
- Section 35.1.2, "Creating a Business Role Page"
- Section 35.1.3, "Specifying the Target Audience for Business Role Pages"
- Section 35.1.4, "Choosing a Default Display Order for Business Role Pages"
- Section 35.1.5, "Editing a Business Role Page"
- Section 35.1.6, "Copying a Business Role Page"
- Section 35.1.7, "Deleting a Business Role Page"

35.1.1 What You Should Know About Business Role Pages

One way a business role page differs from a shared personal page is that a business role page is *pushed* to all the users to whom it is assigned. When users log in, they see their assigned business role pages as tabs in their personal spaces.

In contrast, when users share a personal page, the shared page is not presented automatically in the views of those users with whom it is shared. Instead, users discover shared personal pages through the Manage Pages dialog.

> **See Also:** For information about sharing pages, see "Setting and Revoking Page Access Permissions" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

Business role pages provide an efficient way to roll out pages to a common audience. For example, if everyone in the HR department must access a Hiring Status page, the administrator can assign the Hiring Status business role page to the department's role (HR_ORG). In an instant, the business role page is pushed to every user assigned to the HR_ORG role.

If an individual user, who is not part of the HR_ORG role, wants to see the page, the application administrator can grant access to this user.

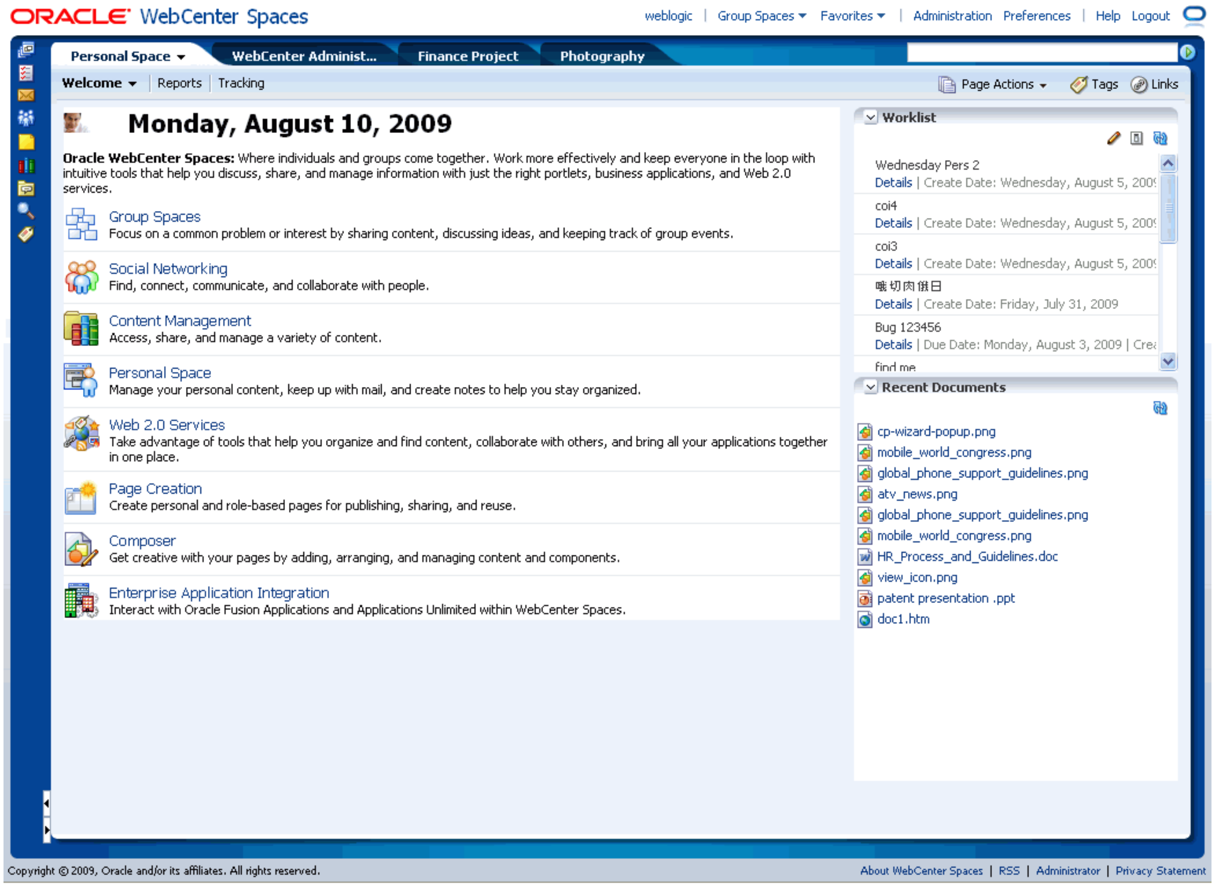
Only a WebCenter Spaces administrator can create a business role page (for more information, see Section 35.1.2, "Creating a Business Role Page"). From the WebCenter Administration page, administrators can view and edit business role pages, set up page defaults, copy pages, delete pages, manage page security, and manage group spaces.

Other users can edit, copy, and delete business role pages, and change page permissions, but only if a WebCenter Spaces administrator grants them the privilege to do so (for more information, see Section 35.1.3, "Specifying the Target Audience for Business Role Pages").

Default Welcome Page

Out-of-the-box, WebCenter Spaces provides a business role page named *Welcome* (Figure 35–1).

Figure 35–1 The Out-of-the-Box Business Role Page "Welcome"


ORACLE WebCenter Spaces
weblogic | Group Spaces ▾ Favorites ▾ | Administration Preferences | Help Logout
Personal Space ▾
WebCenter Administ...
Finance Project
Photography
Welcome ▾ | Reports | Tracking
Page Actions ▾
Tags
Links

Monday, August 10, 2009

Oracle WebCenter Spaces: Where individuals and groups come together. Work more effectively and keep everyone in the loop with intuitive tools that help you discuss, share, and manage information with just the right portlets, business applications, and Web 2.0 services.

Group Spaces
Focus on a common problem or interest by sharing content, discussing ideas, and keeping track of group events.

Social Networking
Find, connect, communicate, and collaborate with people.

Content Management
Access, share, and manage a variety of content.

Personal Space
Manage your personal content, keep up with mail, and create notes to help you stay organized.

Web 2.0 Services
Take advantage of tools that help you organize and find content, collaborate with others, and bring all your applications together in one place.

Page Creation
Create personal and role-based pages for publishing, sharing, and reuse.

Composer
Get creative with your pages by adding, arranging, and managing content and components.

Enterprise Application Integration
Interact with Oracle Fusion Applications and Applications Unlimited within WebCenter Spaces.

Worklist

Wednesday Pers 2
Details | Create Date: Wednesday, August 5, 200

coi4
Details | Create Date: Wednesday, August 5, 200

coi3
Details | Create Date: Wednesday, August 5, 200

哦切肉俄日
Details | Create Date: Friday, July 31, 2009

Bug 123456
Details | Due Date: Monday, August 3, 2009 | Cre

find me

Recent Documents

cp-wizard-popup.png
mobile_world_congress.png
global_phone_support_guidelines.png
atv_news.png
global_phone_support_guidelines.png
mobile_world_congress.png
HR_Process_and_Guidelines.doc
view_icon.png
patent presentation .ppt
doc1.htm

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

About WebCenter Spaces | RSS | Administrator | Privacy Statement

All users, including the application administrator, see this page in their application view. By default, it appears as the first page in everyone's personal space. As the application administrator, you can edit page content, change the page position, hide the page from everyone, or grant custom permissions as described in this chapter; however, you cannot delete the default Welcome page.

Contact your systems administrator if you would like the default Welcome page (or some other business role page) to display when users log in, rather than the page they accessed last. See also, Section 9.1.3, "Choosing the First Page Displayed in WebCenter Spaces."

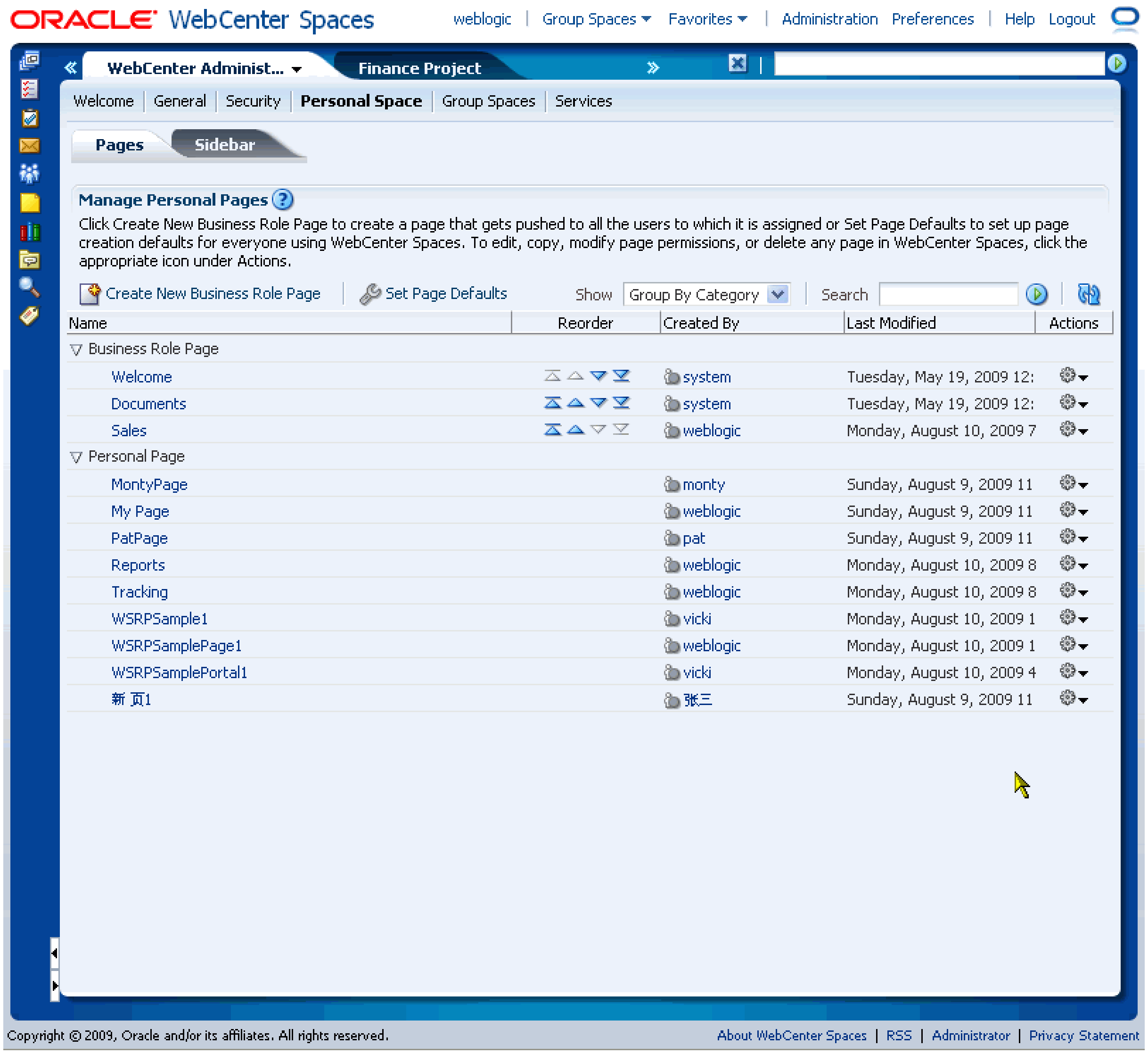
35.1.2 Creating a Business Role Page

To create a new business role page and push it out to a target audience:

1. Log in to WebCenter Spaces with administrative privileges as described in Section 32.1, and click the **Administration** link at the top of the application.
2. Click the **Personal Space** tab to bring it forward.
3. Click the **Pages** tab to bring it forward.

   All WebCenter Spaces pages are listed here, including existing business role pages (Figure 35–2).

Figure 35–2 Viewing Business Role Pages


ORACLE WebCenter Spaces
weblogic | Group Spaces ▾ Favorites ▾ | Administration Preferences | Help Logout
WebCenter Administ... ▾
Finance Project
Welcome | General | Security | Personal Space | Group Spaces | Services
Pages
Sidebar

Manage Personal Pages

Click Create New Business Role Page to create a page that gets pushed to all the users to which it is assigned or Set Page Defaults to set up page creation defaults for everyone using WebCenter Spaces. To edit, copy, modify page permissions, or delete any page in WebCenter Spaces, click the appropriate icon under Actions.

Create New Business Role Page
Set Page Defaults
Show Group By Category
Search

Name	Reorder	Created By	Last Modified	Actions
▽ Business Role Page				
Welcome		system	Tuesday, May 19, 2009 12:	
Documents		system	Tuesday, May 19, 2009 12:	
Sales		weblogic	Monday, August 10, 2009 7	
▽ Personal Page				
MontyPage		monty	Sunday, August 9, 2009 11	
My Page		weblogic	Sunday, August 9, 2009 11	
PatPage		pat	Sunday, August 9, 2009 11	
Reports		weblogic	Monday, August 10, 2009 8	
Tracking		weblogic	Monday, August 10, 2009 8	
WSRPSample1		vicki	Monday, August 10, 2009 1	
WSRPSamplePage1		weblogic	Monday, August 10, 2009 1	
WSRPSamplePortal1		vicki	Monday, August 10, 2009 4	
新 页1		张三	Sunday, August 9, 2009 11	

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

About WebCenter Spaces | RSS | Administrator | Privacy Statement

4. Click **Create New Business Role Page**.

5. Enter a name for the page (**Page Name**), and then choose a **Scheme**, **Background Color**, and **Style**.

   The page creation options that you see in this dialog are the same as the page creation options you set for personal pages.

   > **See Also:** For information about page creation options, see "Creating Pages" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.
   >
   > For information about setting up page creation defaults, see Section 35.2.2, "Setting Up a Default Look and Feel for Personal Pages."

6. Click **Create**.

   An empty page opens with your chosen look and feel.

Later, you can add content to the page (see "Working with Page Content" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*). The next section (Section 35.1.3) steps you through setting access permissions for the business role page.

7. Next steps:

   - Add content to the page, for details, see "Working with Page Content" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.
   - Define the page audience, see Section 35.1.3, "Specifying the Target Audience for Business Role Pages."
   - Choose the page display order, see Section 35.1.4, "Choosing a Default Display Order for Business Role Pages."

35.1.3 Specifying the Target Audience for Business Role Pages

The target audience for business role pages may change from time to time. For example, you may want the whole sales team to see a page originally designed for a product development team. Or you may want to provide access to the Marketing department's page to a sales team member. Or you may want to provide additional access privileges, such as the *Edit Page* privilege, to a selected department member.

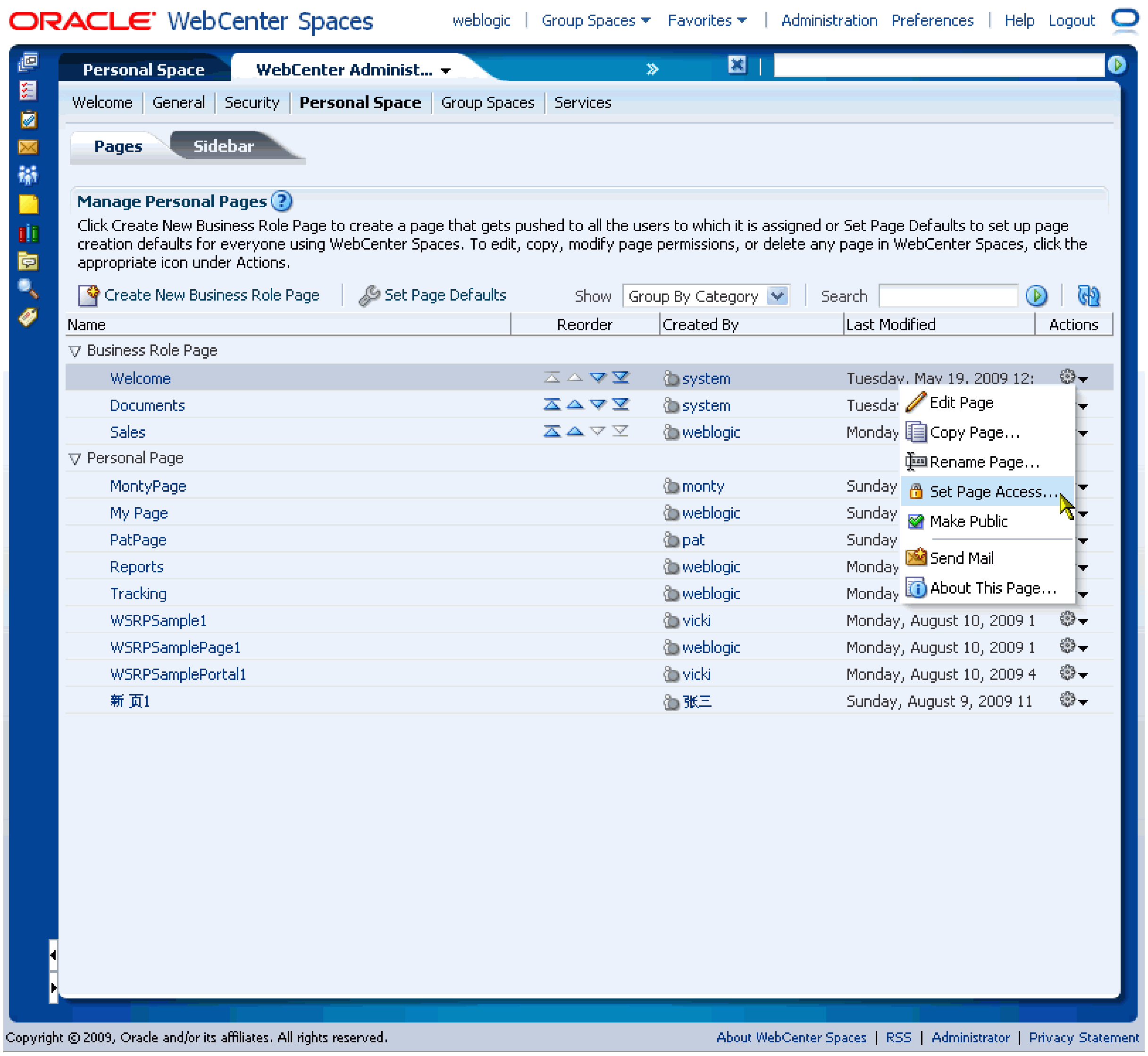
Administrators can configure page permissions in two places—through WebCenter Administration pages (described below) or through the Manage Pages dialog (see "Setting and Revoking Page Access Permissions" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*).

To add or change user permissions for a business role page:

1. Log in to WebCenter Spaces with administrative privileges as described in Section 32.1, and click the **Administration** link at the top of the application.
2. Click the **Personal Space** tab to bring it forward.
3. Click the **Pages** tab to bring it forward.
4. Optionally, from the **Show** drop-down menu, choose **Group By Category**.

   The **Business Role Page** section lists every business role page in WebCenter Spaces.
5. Click the **Actions** icon for the business role page for which you are setting access, and select **Set Page Access** from the resulting context menu (Figure 35–3).

Figure 35–3 Setting Access Permissions for a Business Role Pages



Manage Personal Pages

Click Create New Business Role Page to create a page that gets pushed to all the users to which it is assigned or Set Page Defaults to set up page creation defaults for everyone using WebCenter Spaces. To edit, copy, modify page permissions, or delete any page in WebCenter Spaces, click the appropriate icon under Actions.

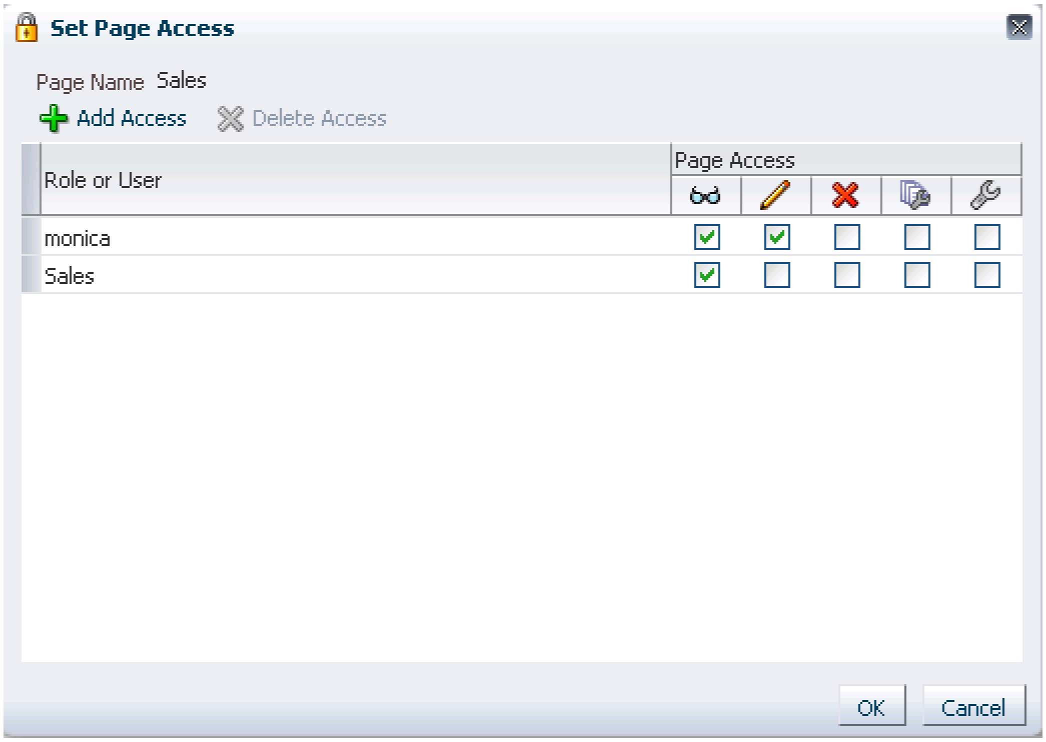
Name	Reorder	Created By	Last Modified	Actions
▽ Business Role Page				
Welcome		system	Tuesday, May 19, 2009 12:	▾
Documents		system	Tuesda	▾
Sales		weblogic	Monday	▾
▽ Personal Page				
MontyPage		monty	Sunday	▾
My Page		weblogic	Sunday	▾
PatPage		pat	Sunday	▾
Reports		weblogic	Monday	▾
Tracking		weblogic	Monday	▾
WSRPSample1		vicki	Monday, August 10, 2009 1	▾
WSRPSamplePage1		weblogic	Monday, August 10, 2009 1	▾
WSRPSamplePortal1		vicki	Monday, August 10, 2009 4	▾
新 页1		张三	Sunday, August 9, 2009 11	▾

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

About WebCenter Spaces | RSS | Administrator | Privacy Statement

The Set Page Access dialog opens (Figure 35–4).

Figure 35–4 Setting Page Access



Set Page Access

Page Name Sales

Add Access Delete Access

Role or User	Page Access				
monica	☑	☑	□	□	□
Sales	☑	□	□	□	□

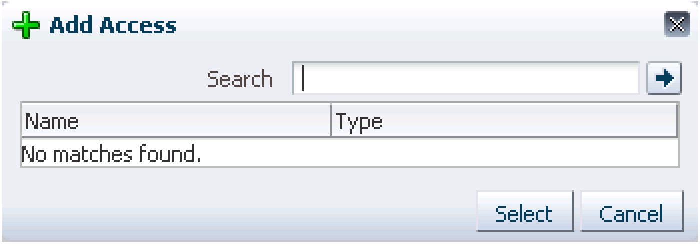
6. Set access permissions:

   - To grant access to additional users and roles, click **Add Access**, and then make your selections. Follow steps 7 and 8.
   - To modify the permissions assigned to a current user or role, select or deselect the appropriate permission checkboxes. For details, see step 9.
   - To revoke access to the pages, highlight the user or the role, and then click **Delete Access**.

7. Click **Add Access**.

   The Add Access dialog opens (Figure 35–5).

Figure 35–5 The Add Access Dialog



Add Access

Search

Name	Type
No matches found.	

8. Identify the users who should see this business role page in their personal space.

   > **Note:** To provide access to public users, search for and select `anonymous-role`.

Choose from all available users, enterprise groups, enterprise roles, and application roles. Use the Search feature to search your identity store:

a. In the **Search** field, enter two or more characters.

   The search is not case-sensitive.

b. Click the **Search** icon.

   Users, groups, and roles matching your search criteria appear in the **Add User** dialog.

c. Select one or multiple names from the list.

   Ctrl-Click to select multiple users.

d. Click **Select**.

   The results of your selection appear in the Set Page Access dialog. By default, selected users have the *View Page* permission.

9. For each user name, group, or application role, select one or more checkboxes to grant page privileges:

   - **View Page—**Users can view the page but cannot perform any actions on the page.
   - **Edit Page—**Users can edit the page. This includes adding, rearranging, and deleting content, and changing the page scheme.
   - **Delete Page—**Users can delete the page.
   - **Manage Page—**Users have full access rights to the page. These users can edit the page, revise the page layout, set additional access privileges for other users, and all other page privileges.
   - **Personalize Page—**Users can change their personal view of the page. Such changes do not affect any other user's view of the page.

   Note: To revoke a privilege, deselect the checkbox.

   For more information, see Section 34.1.3, "Understanding Application Permissions."

10. Click **OK** to save your changes.

    The page is pushed to its target audience, who sees it in their personal space the next time they log in to WebCenter Spaces.

35.1.4 Choosing a Default Display Order for Business Role Pages

If you present business role pages in a logical order, the page content is more accessible and easier for users to navigate. As administrator, you can determine the initial order in which business role pages are presented to their intended audience.

Individual users can change the initial display order you specify through the Manage Pages dialog. Additionally, they can hide the business role pages they do not use.

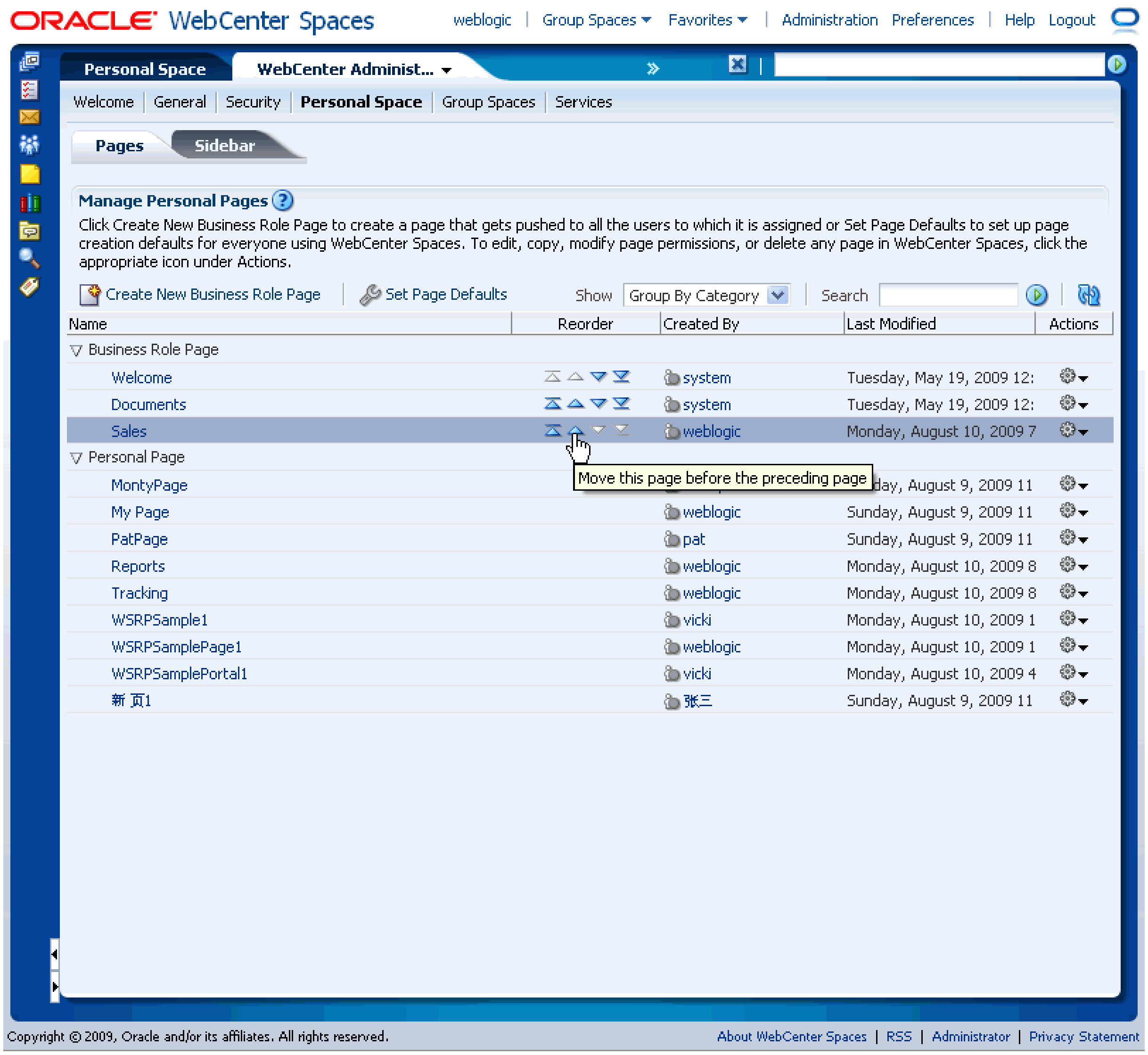
See Also: For information about changing the display order of pages, see "Changing the Order of Pages Through the Manage Pages Dialog." For information about hiding pages, see "Hiding, Showing, Opening, and Closing Pages." You can find this information in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

To change the display order of all business role pages:

1. Log in to WebCenter Spaces with administrative privileges as described in Section 32.1, and click the **Administration** link at the top of the application.
2. Click the **Personal Space** tab to bring it forward.
3. Click the **Pages** tab to bring it forward.
4. Optionally, from the **Show** drop-down menu, choose **Group By Category**.

   The **Business Role Page** section lists every business role page in WebCenter Spaces.
5. Click the arrows in the **Reorder** column to change the default display order (Figure 35–6).

Figure 35–6 Choosing a Default Display Order for Business Role Pages


ORACLE WebCenter Spaces
weblogic | Group Spaces ▾ | Favorites ▾ | Administration | Preferences | Help | Logout
Personal Space
WebCenter Administ... ▾
Welcome | General | Security | Personal Space | Group Spaces | Services
Pages
Sidebar
Create New Business Role Page
Set Page Defaults
Show
Group By Category
Search

Manage Personal Pages

Click Create New Business Role Page to create a page that gets pushed to all the users to which it is assigned or Set Page Defaults to set up page creation defaults for everyone using WebCenter Spaces. To edit, copy, modify page permissions, or delete any page in WebCenter Spaces, click the appropriate icon under Actions.

Name	Reorder	Created By	Last Modified	Actions
▽ Business Role Page				
Welcome		system	Tuesday, May 19, 2009 12:	
Documents		system	Tuesday, May 19, 2009 12:	
Sales		weblogic	Monday, August 10, 2009 7	
▽ Personal Page				
MontyPage			day, August 9, 2009 11	
My Page		weblogic	Sunday, August 9, 2009 11	
PatPage		pat	Sunday, August 9, 2009 11	
Reports		weblogic	Monday, August 10, 2009 8	
Tracking		weblogic	Monday, August 10, 2009 8	
WSRPSample1		vicki	Monday, August 10, 2009 1	
WSRPSamplePage1		weblogic	Monday, August 10, 2009 1	
WSRPSamplePortal1		vicki	Monday, August 10, 2009 4	
新 页1		张三	Sunday, August 9, 2009 11	

Move this page before the preceding page

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

About WebCenter Spaces | RSS | Administrator | Privacy Statement

Alternatively, drag and drop pages into the correct position.

35.1.5 Editing a Business Role Page

Anyone granted the `Edit Page` permission on a business role page can edit that page. For these users, the editing process is the same as for regular pages (for more information, see "Editing Pages" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*).

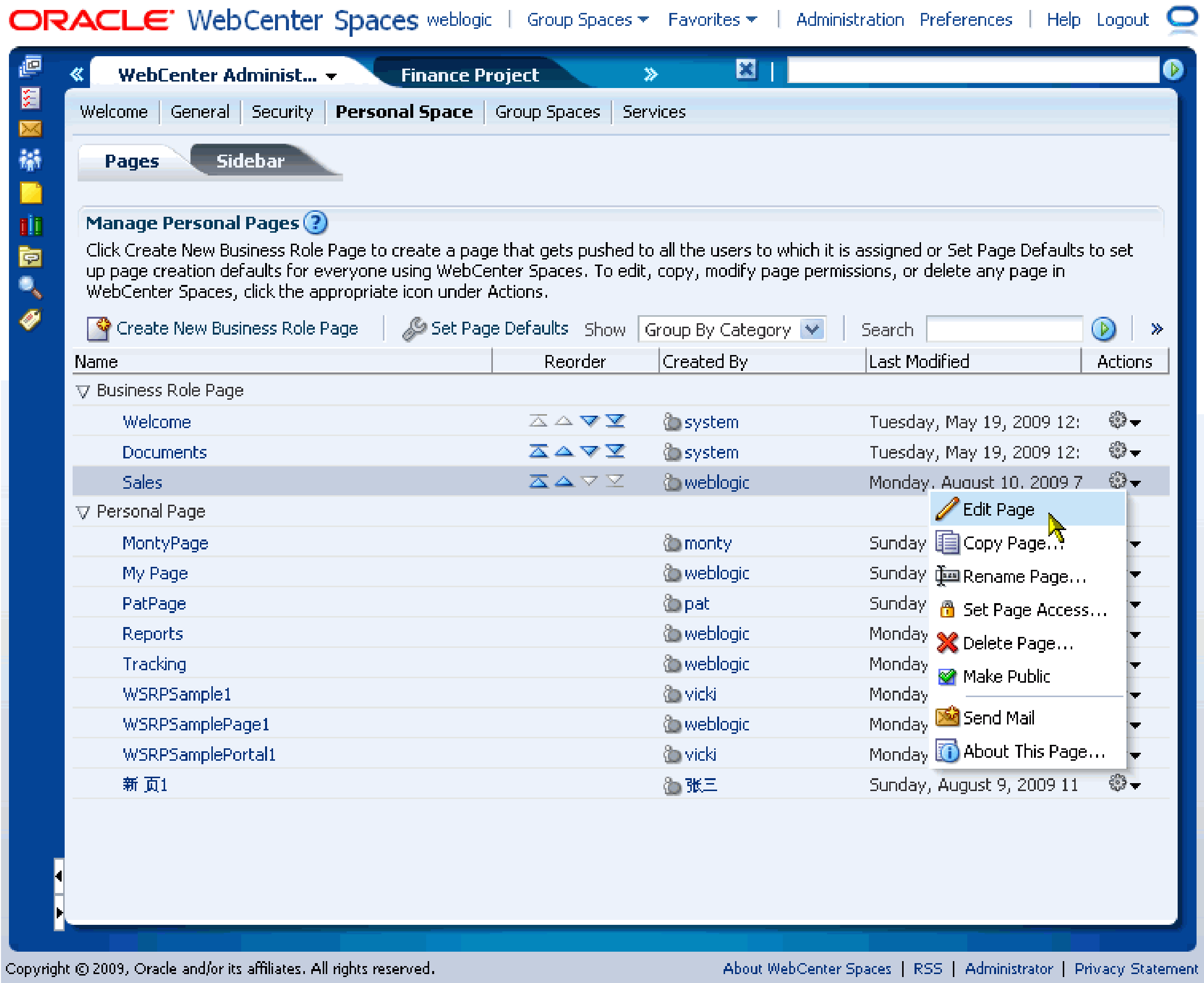
Administrators also have the option of initiating an edit of a business role page from WebCenter Administration pages.

To edit a business role page through WebCenter Administration:

1. Log in to WebCenter Spaces with administrative privileges as described in Section 32.1, and click the **Administration** link at the top of the application.
2. Click the **Personal Space** tab to bring it forward.
3. Click the **Pages** tab to bring it forward.
4. Optionally, from the **Show** drop-down menu, choose **Group By Category**.

   The **Business Role Page** section lists every business role page in WebCenter Spaces.
5. Click the **Actions** icon for the page you want to edit, and select **Edit Page** from the resulting context menu (Figure 35–7).

Figure 35–7 Editing Business Role Pages



Manage Personal Pages

Click Create New Business Role Page to create a page that gets pushed to all the users to which it is assigned or Set Page Defaults to set up page creation defaults for everyone using WebCenter Spaces. To edit, copy, modify page permissions, or delete any page in WebCenter Spaces, click the appropriate icon under Actions.

Show: Group By Category

Name	Reorder	Created By	Last Modified	Actions
▽ Business Role Page				
Welcome		system	Tuesday, May 19, 2009 12:	
Documents		system	Tuesday, May 19, 2009 12:	
Sales		weblogic	Monday, August 10, 2009 7	
▽ Personal Page				
MontyPage		monty	Sunday	
My Page		weblogic	Sunday	
PatPage		pat	Sunday	
Reports		weblogic	Monday	
Tracking		weblogic	Monday	
WSRPSample1		vicki	Monday	
WSRPSamplePage1		weblogic	Monday	
WSRPSamplePortal1		vicki	Monday	
新 页1		张三	Sunday, August 9, 2009 11	

The page opens in edit mode in Oracle Composer (for more information, see "Editing Pages" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*).

6. Edit the page, and click **Save** and then **Close** when you have finished.

35.1.6 Copying a Business Role Page

When you copy a business role page, you can save it as another business role page or as a personal page. If you create another business role page, you must set access on the new page because access permissions from the original page are not copied (for more information, see Section 35.1.3, "Specifying the Target Audience for Business Role Pages").

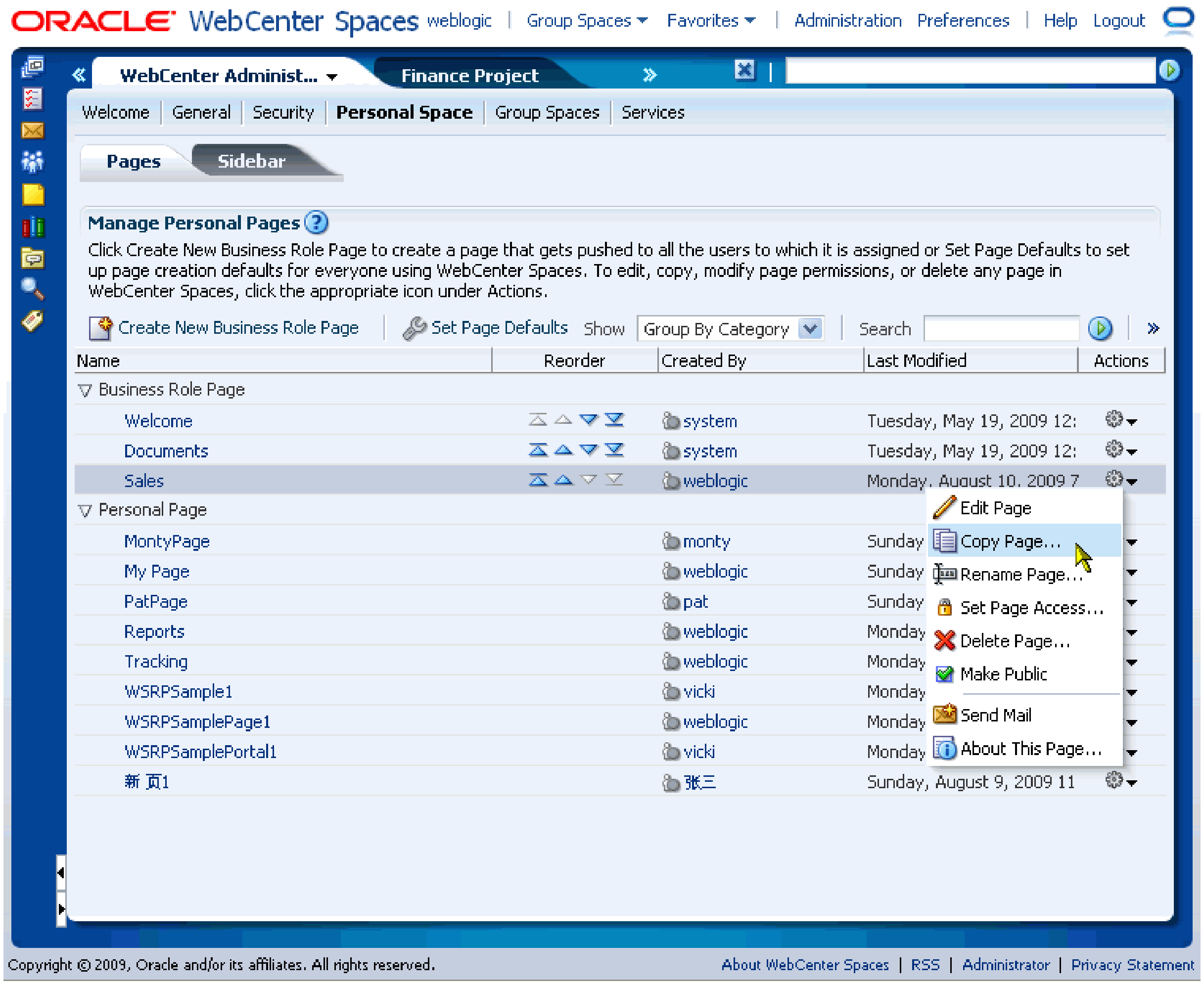
To copy a business role page:

1. Log in to WebCenter Spaces with administrative privileges as described in Section 32.1, and click the **Administration** link at the top of the application.
2. Click the **Personal Space** tab to bring it forward.
3. Click the **Pages** tab to bring it forward.
4. Optionally, from the **Show** drop-down menu, choose **Group By Category**.

The **Business Role Page** section lists every business role page in WebCenter Spaces.

5. Click the **Actions** icon for the page you want to copy, and select **Copy Page** from the resulting context menu (Figure 35–8).

Figure 35–8 Copying a Business Role Page


ORACLE WebCenter Spaces
weblogic | Group Spaces ▾ Favorites ▾ | Administration Preferences | Help Logout
WebCenter Administ... ▾
Finance Project
Welcome | General | Security | Personal Space | Group Spaces | Services
Pages
Sidebar
Create New Business Role Page
Set Page Defaults
Show
Search
Edit Page
Copy Page...
Rename Page...
Set Page Access...
Delete Page...
Make Public
Send Mail
About This Page...
About WebCenter Spaces | RSS | Administrator | Privacy Statement

Manage Personal Pages

Click Create New Business Role Page to create a page that gets pushed to all the users to which it is assigned or Set Page Defaults to set up page creation defaults for everyone using WebCenter Spaces. To edit, copy, modify page permissions, or delete any page in WebCenter Spaces, click the appropriate icon under Actions.

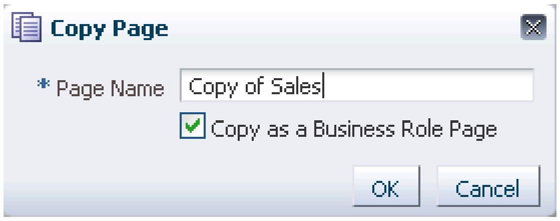
Show: Group By Category

Name	Reorder	Created By	Last Modified	Actions
▽ Business Role Page				
Welcome		system	Tuesday, May 19, 2009 12:	⚙▾
Documents		system	Tuesday, May 19, 2009 12:	⚙▾
Sales		weblogic	Monday, August 10, 2009 7	⚙▾
▽ Personal Page				
MontyPage		monty	Sunday	
My Page		weblogic	Sunday	
PatPage		pat	Sunday	
Reports		weblogic	Monday	
Tracking		weblogic	Monday	
WSRPSample1		vicki	Monday	
WSRPSamplePage1		weblogic	Monday	
WSRPSamplePortal1		vicki	Monday	
新 页1		张三	Sunday, August 9, 2009 11	⚙▾

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

6. Enter a name for the new page (Figure 35–9).

Figure 35–9 Naming the New Page



* Page Name: Copy of Sales

☑ Copy as a Business Role Page

7. Do one of the following:

- Select **Copy as a Business Role Page** if you intend to push the copy out to a group of people with a similar job role.
- Deselect **Copy as a Business Role Page** if you intend to expose the copy only in your own application view.

8. Click **OK**.

The new page opens in edit mode in Oracle Composer (for more information, see "Editing Pages" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*).

35.1.7 Deleting a Business Role Page

Once a business role page is removed from WebCenter Spaces, it cannot be recovered. Deleted pages are permanently removed, and users previously assigned that page no longer see it in their view.

Anyone granted the `Delete Page` permission on a business role page can delete it. For these users, the process is the same as deleting regular pages (for more information, see "Deleting Pages" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*).

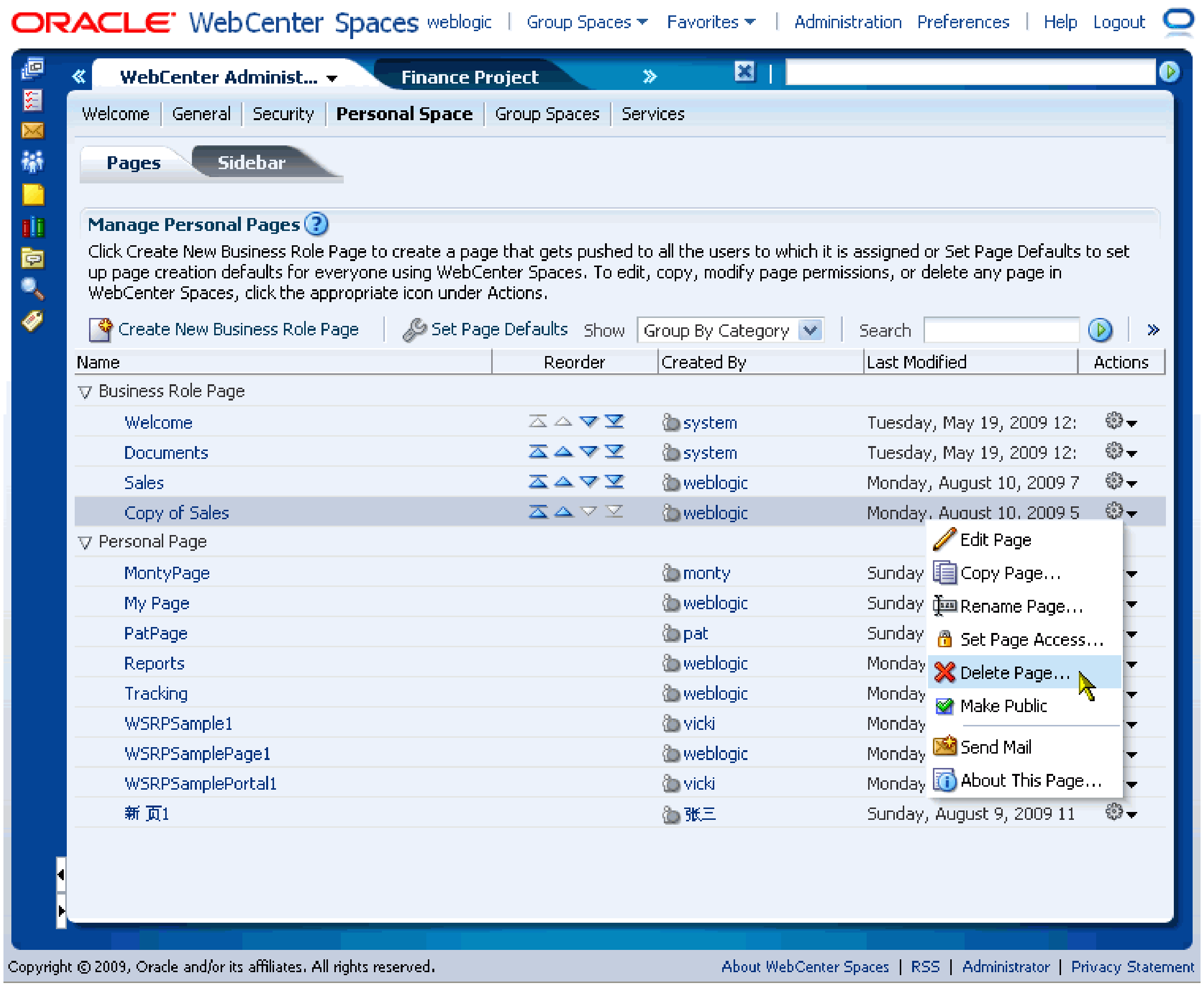
Administrators have the option of deleting business role pages from the WebCenter Administration page.

To delete a business role page through WebCenter Administration:

1. Log in to WebCenter Spaces with administrative privileges as described in Section 32.1, and click the **Administration** link at the top of the application.
2. Click the **Personal Space** tab to bring it forward.
3. Click the **Pages** tab to bring it forward.
4. Optionally, from the **Show** drop-down menu, choose **Group By Category**.

   The **Business Role Page** section lists every business role page in WebCenter Spaces.
5. Click the **Actions** icon for the page you want to delete, and select **Delete Page** from the resulting context menu (Figure 35–10).

Figure 35–10 Deleting Business Role Pages


ORACLE WebCenter Spaces weblogic | Group Spaces ▾ Favorites ▾ | Administration Preferences | Help Logout
WebCenter Administ... ▾
Finance Project
Welcome | General | Security | Personal Space | Group Spaces | Services
Pages
Sidebar
Create New Business Role Page
Set Page Defaults
Show Group By Category
Search
Edit Page
Copy Page...
Rename Page...
Set Page Access...
Delete Page...
Make Public
Send Mail
About This Page...
About WebCenter Spaces | RSS | Administrator | Privacy Statement

Manage Personal Pages

Click Create New Business Role Page to create a page that gets pushed to all the users to which it is assigned or Set Page Defaults to set up page creation defaults for everyone using WebCenter Spaces. To edit, copy, modify page permissions, or delete any page in WebCenter Spaces, click the appropriate icon under Actions.

Name	Reorder	Created By	Last Modified	Actions
▽ Business Role Page				
Welcome		system	Tuesday, May 19, 2009 12:	
Documents		system	Tuesday, May 19, 2009 12:	
Sales		weblogic	Monday, August 10, 2009 7	
Copy of Sales		weblogic	Monday, August 10, 2009 5	
▽ Personal Page				
MontyPage		monty	Sunday	
My Page		weblogic	Sunday	
PatPage		pat	Sunday	
Reports		weblogic	Monday	
Tracking		weblogic	Monday	
WSRPSample1		vicki	Monday	
WSRPSamplePage1		weblogic	Monday	
WSRPSamplePortal1		vicki	Monday	
新 页1		张三	Sunday, August 9, 2009 11	

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

6. In the resulting dialog, click **Delete** to confirm your intention to delete the page.

35.2 Managing Personal Pages

This section describes how to manage personal pages in WebCenter Spaces. It includes the following sections:

- Section 35.2.1, "What You Should Know About Personal Page Management"
- Section 35.2.2, "Setting Up a Default Look and Feel for Personal Pages"
- Section 35.2.3, "Editing Personal Pages with Administrative Privileges"
- Section 35.2.4, "Changing Access Permissions for a Personal Page"
- Section 35.2.5, "Copying a Personal Page"
- Section 35.2.6, "Deleting a Personal Page"

35.2.1 What You Should Know About Personal Page Management

In WebCenter Spaces, application administrators can access everyone's personal pages from one, central place: the **WebCenter Administration** page. From here, administrators can view and edit personal pages, set up personal page creation defaults, and copy and delete personal pages. Administrators can also manage page security and modify public page settings.

While individuals are primarily responsible for managing content and pages in their own personal space, it is important that administrators also have access. Administrators may be required to clean up or manage personal data when owners experience difficulties with their personal pages or leave the organization.

35.2.2 Setting Up a Default Look and Feel for Personal Pages

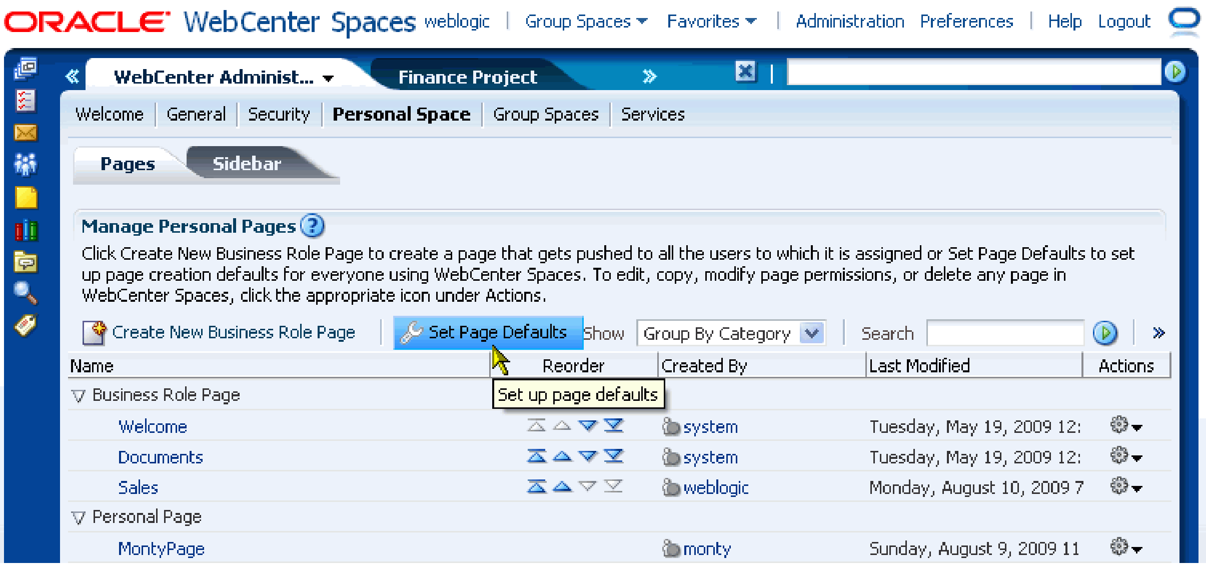
Administrators can use WebCenter Spaces to set up a default look and feel for personal and business role pages. Use this feature to simplify page creation for first-time users or to steer users toward a particular page scheme and style. Individuals may override these settings through the Manage Pages dialog associated with their personal space. For more information, see "Setting Page Creation Defaults for Your Personal Pages" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

Page defaults apply to personal pages and business role pages only. Defaults for pages created within the context of a group space are controlled by the group space moderator. For more information, see "Managing Group Space Pages" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

To set up a default look and feel for personal pages (including business role pages):

1. Log in to WebCenter Spaces with administrative privileges as described in Section 32.1, and click the **Administration** link at the top of the application.
2. Click the **Personal Space** tab to bring it forward.
3. Click the **Pages** tab to bring it forward.
4. Click **Set Page Defaults** (Figure 35–11).

Figure 35–11 Setting Page Defaults For Everyone



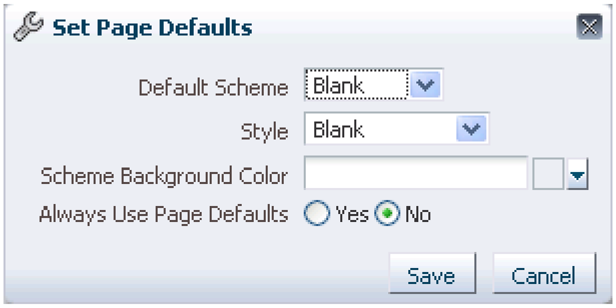
Manage Personal Pages

Click Create New Business Role Page to create a page that gets pushed to all the users to which it is assigned or Set Page Defaults to set up page creation defaults for everyone using WebCenter Spaces. To edit, copy, modify page permissions, or delete any page in WebCenter Spaces, click the appropriate icon under Actions.

Name	Reorder	Created By	Last Modified	Actions
▽ Business Role Page				
Welcome		system	Tuesday, May 19, 2009 12:	
Documents		system	Tuesday, May 19, 2009 12:	
Sales		weblogic	Monday, August 10, 2009 7	
▽ Personal Page				
MontyPage		monty	Sunday, August 9, 2009 11	

The **Set Page Defaults** dialog opens (Figure 35–12):

Figure 35–12 Set Page Defaults Dialog



Set Page Defaults

Default Scheme: Blank

Style: Blank

Scheme Background Color:

Always Use Page Defaults ○ Yes ● No

5. In the **Set Page Defaults** dialog, select a default scheme for all new personal pages and business role pages from the **Default Scheme** drop-down menu.

   The Default Scheme drop-down menu provides a selection of background color and images. For illustrations of listed schemes, see "Introducing Default Page Schemes and Styles" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

6. Select a layout for the page structure from the **Style** drop-down menu.

   For illustrations of listed styles, see "Introducing Default Page Schemes and Styles" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

7. Select an **Always Use Page Defaults** option to specify when to apply these page defaults:

   Choose from:

   - **Yes** - Personal pages and business role pages are automatically created with the defaults that you select here. The Create Page dialog does not open when users create personal pages. Instead, the page is created immediately. If page owners want to use different schemes or layouts, they can edit page properties through Oracle Composer.

     See Also: For information about Oracle Composer, see "Introducing Oracle Composer" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*; for information about changing a page scheme or style through Oracle Composer, see "Changing the Page Scheme and Scheme Background Color" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*

   - **No** - The scheme and style defaults you specify here are presented as default selections when a user creates a personal page or an administrator creates a business role page. Page owners can override your selections before they create the page.

   Experienced users may decide to override the defaults that you pick here by setting up page defaults of their own. For more information, see "Setting Page Creation Defaults for Your Personal Pages" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

8. Click **Save**.

35.2.3 Editing Personal Pages with Administrative Privileges

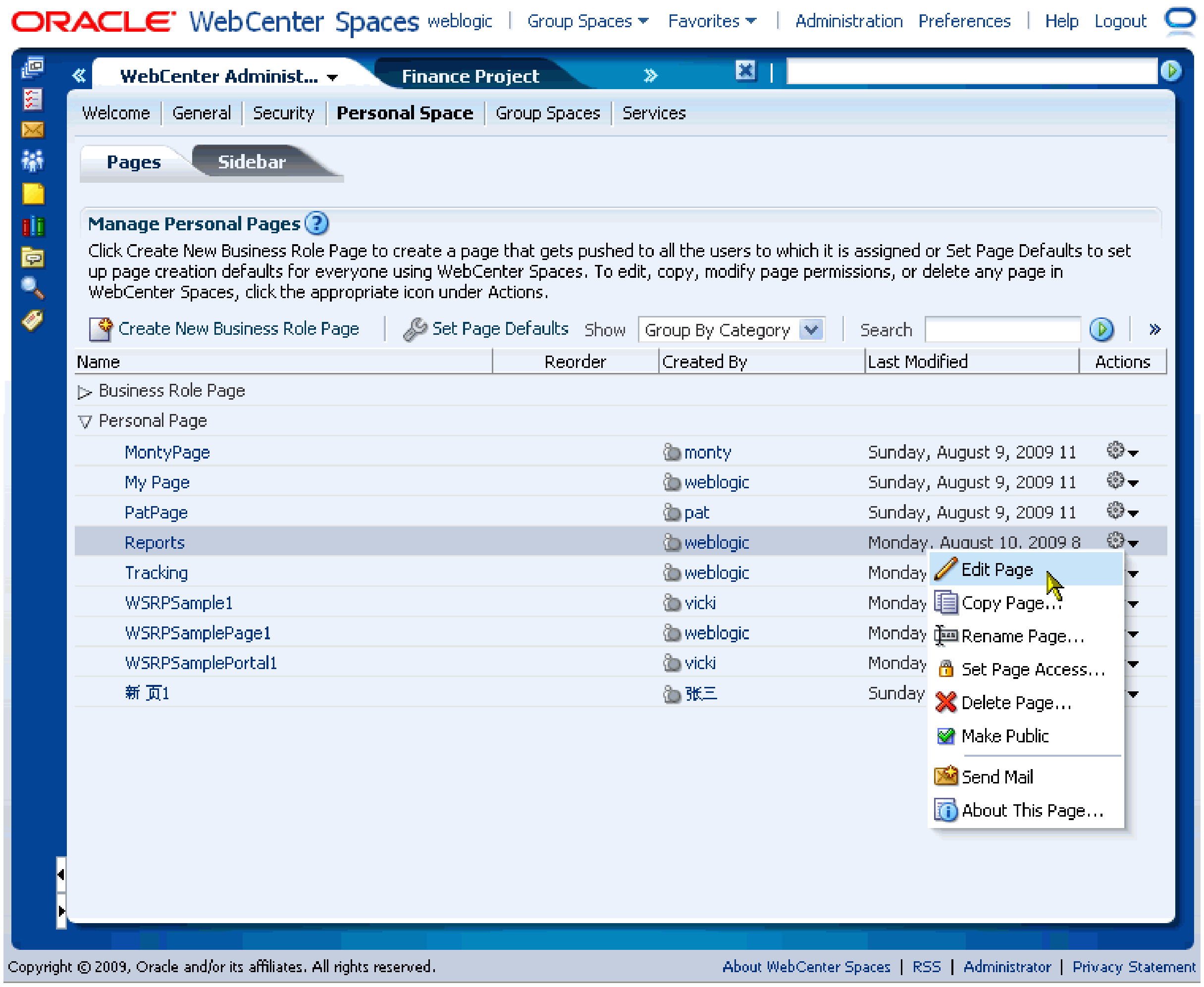
Administrators are authorized to view and modify any page in a personal space, including other people's personal pages. Individuals are primarily responsible for editing content and pages in their own personal spaces, but, occasionally, administrators may be required to clean up or edit personal data.

To edit a personal page as the WebCenter Spaces administrator:

1. Log in to WebCenter Spaces with administrative privileges as described in Section 32.1, and click the **Administration** link at the top of the application.
2. Click the **Personal Space** tab to bring it forward.
3. Click the **Pages** tab to bring it forward.
4. Optionally, from the **Show** drop-down menu, select **Group By Category**.

   The **Personal Page** section lists every personal page in WebCenter Spaces.
5. Click the **Actions** icon for the page you want to edit, and select **Edit Page** from the resulting context menu (Figure 35–13).

Figure 35–13 Editing Personal Pages



Manage Personal Pages

Click Create New Business Role Page to create a page that gets pushed to all the users to which it is assigned or Set Page Defaults to set up page creation defaults for everyone using WebCenter Spaces. To edit, copy, modify page permissions, or delete any page in WebCenter Spaces, click the appropriate icon under Actions.

Name	Reorder	Created By	Last Modified	Actions
▷ Business Role Page				
▽ Personal Page				
MontyPage		monty	Sunday, August 9, 2009 11	
My Page		weblogic	Sunday, August 9, 2009 11	
PatPage		pat	Sunday, August 9, 2009 11	
Reports		weblogic	Monday, August 10, 2009 8	
Tracking		weblogic	Monday	
WSRPSample1		vicki	Monday	
WSRPSamplePage1		weblogic	Monday	
WSRPSamplePortal1		vicki	Monday	
新 页1		张三	Sunday	

The page opens in Oracle Composer.

> **See Also:** To find out more about editing a page through Oracle Composer, see the following chapters in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*:
>
> - "Introducing Oracle Composer"
> - "Creating, Editing, and Deleting Pages"
> - "Working with Page Content"

6. Update the page, and click **Save** and then **Close** when you have finished.

35.2.4 Changing Access Permissions for a Personal Page

Administrators are authorized to view and manage security for any page in WebCenter Spaces. This includes personal pages. Page owners normally determine who can see their pages, but, occasionally, when a page owner is not available, the administrator may be required to make changes.

Administrators can configure page permissions in two places: through WebCenter Administration pages, as described here, or through their Manage Pages dialog in the same way as regular users.

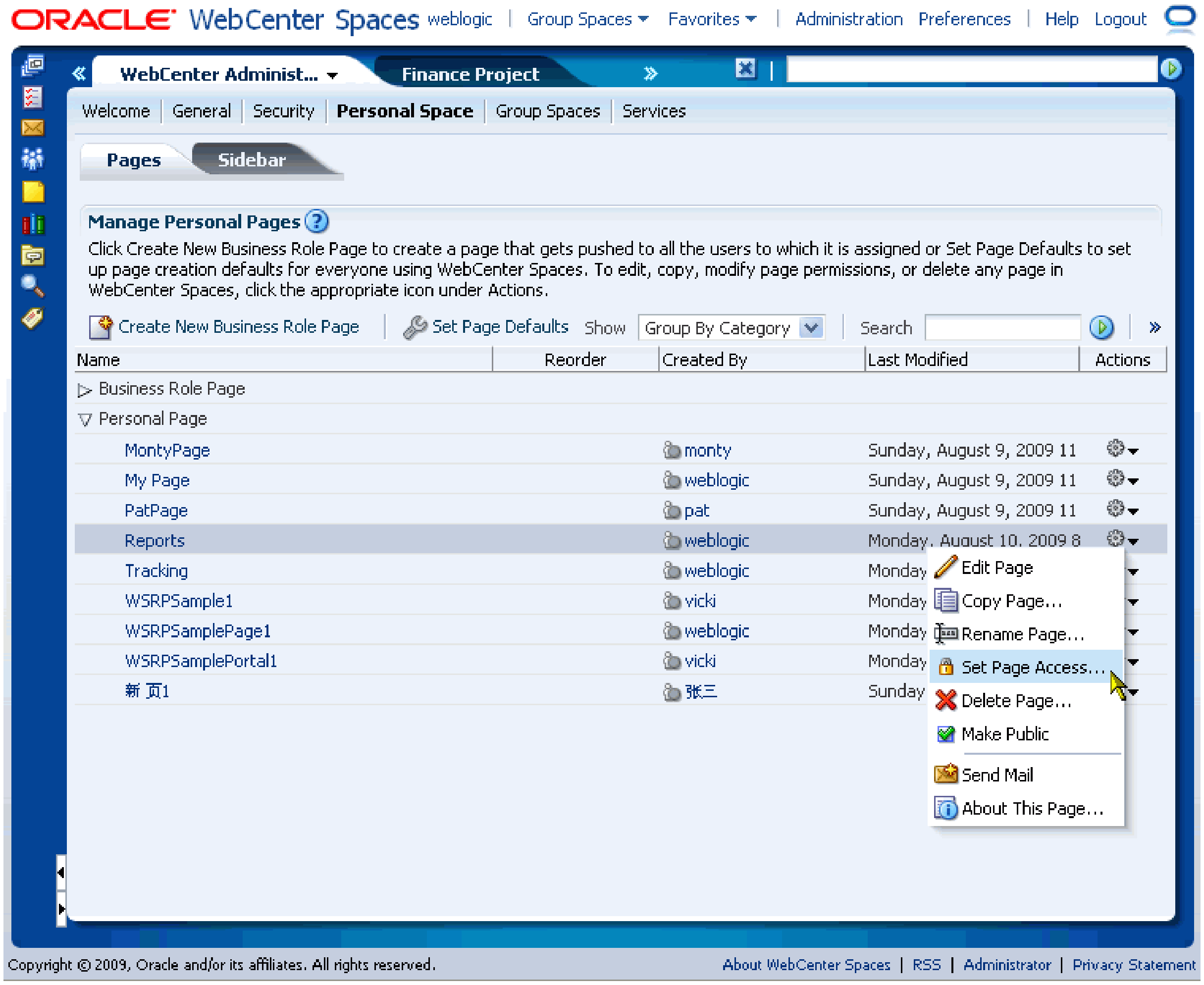
> **See Also:** For information about changing page access permissions through the Manage Pages dialog, see "Setting and Revoking Page Access Permissions" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

To change access permissions for a personal page as the WebCenter Spaces administrator:

1. Log in to WebCenter Spaces with administrative privileges as described in Section 32.1, and click the **Administration** link at the top of the application.
2. Click the **Personal Space** tab to bring it forward.
3. Click the **Pages** tab to bring it forward.
4. Optionally, from the **Show** drop-down menu, choose **Group By Category**.

   The **Personal Page** section lists every personal page in WebCenter Spaces.
5. Click the **Actions** icon for the page on which to set access, and select **Set Page Access** from the resulting context menu (Figure 35–14).

Figure 35–14 Editing Page Access



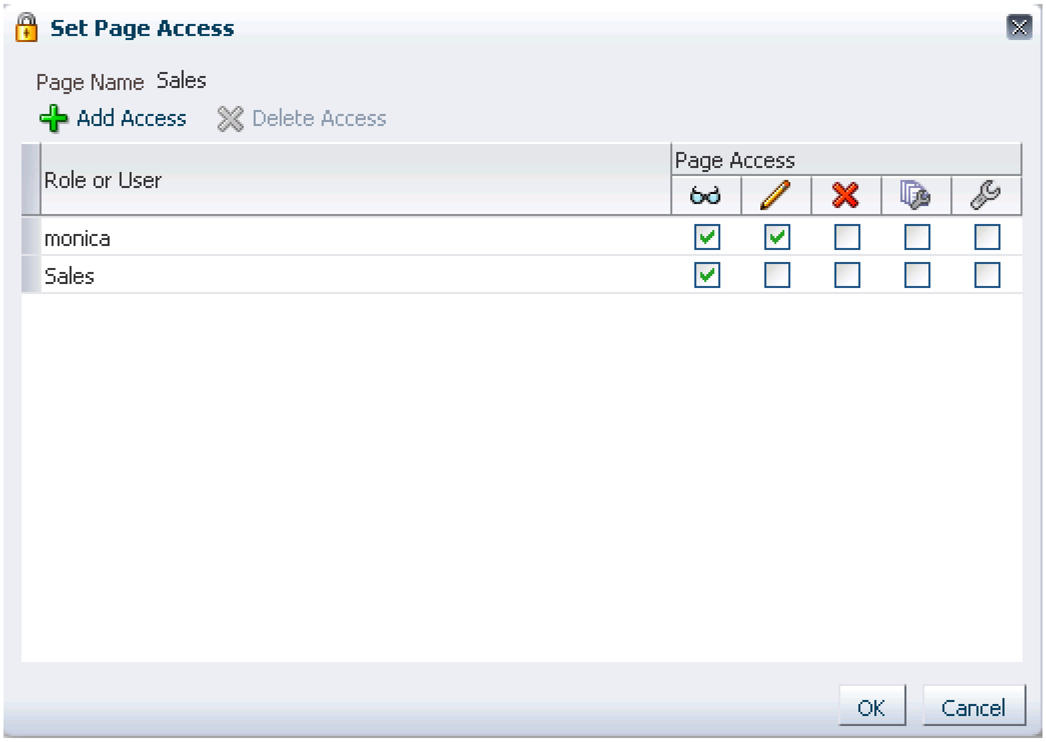
Manage Personal Pages

Click Create New Business Role Page to create a page that gets pushed to all the users to which it is assigned or Set Page Defaults to set up page creation defaults for everyone using WebCenter Spaces. To edit, copy, modify page permissions, or delete any page in WebCenter Spaces, click the appropriate icon under Actions.

Name	Reorder	Created By	Last Modified	Actions
▷ Business Role Page				
▽ Personal Page				
MontyPage		monty	Sunday, August 9, 2009 11	⚙▾
My Page		weblogic	Sunday, August 9, 2009 11	⚙▾
PatPage		pat	Sunday, August 9, 2009 11	⚙▾
Reports		weblogic	Monday, August 10, 2009 8	⚙▾
Tracking		weblogic	Monday	▾
WSRPSample1		vicki	Monday	▾
WSRPSamplePage1		weblogic	Monday	▾
WSRPSamplePortal1		vicki	Monday	▾
新 页1		张三	Sunday	▾

The Set Page Access dialog opens (Figure 35–15).

Figure 35–15 Set Page Access Dialog



Set Page Access

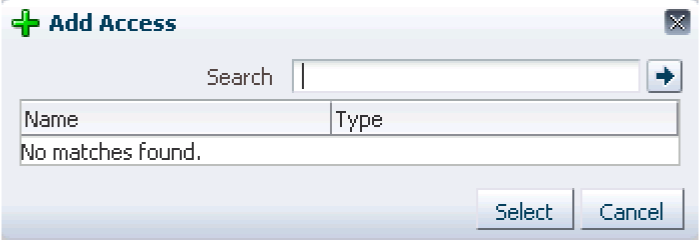
Page Name Sales

Role or User	Page Access				
	👓	✎	✗	⧉	🔧
monica	☑	☑	□	□	□
Sales	☑	□	□	□	□

6. To grant access to users and roles, click **Add Access**.

   The Add Access dialog opens (Figure 35–5).

Figure 35–16 Add Access Dialog



Add Access

Search

Name	Type
No matches found.	

7. Identify the users to enable to access this page in their personal space.

   Choose from all available users, enterprise groups, enterprise roles, and application roles. Use the Search feature to search your identity store:

   a. In the **Search** field, enter two or more characters.

      The search is not case sensitive.

   b. Click the **Search** icon.

      Users, groups, and roles matching your search criteria appear in the **Add Access** dialog.

   c. Select one or more names from the list.

      Ctrl-Click to select multiple users.

d. Click **Select**.

   The results of your selection appear in the Set Page Access dialog. By default, users have the *View Page* permission on the page.

8. To modify the permissions assigned to a current user or role, select or deselect the appropriate permission checkboxes:

   - **View Page—**The selected user or role can access the page for viewing, but cannot perform any actions on the page.
   - **Delete Page—**The selected user or role can delete the page.
   - **Manage Page—**The selected user or role has full access rights to the page. The user can edit the page, revise the page layout, set additional access privileges for other users, and all other page privileges.
   - **Edit Page—**The selected user or role can edit the page. This includes adding, rearranging, and deleting content.
   - **Personalize—**The selected user or role can personalize the page. Personalizations are changes made to a page in view mode. Such changes do not affect any other user's view of the page.

     Note: You can revoke privileges by taking the same steps and deselecting one or multiple privileges for a listed user or role.

     For more information, see Section 34.1.3, "Understanding Application Permissions."

   - To revoke access to the page, select the user or role and click **Delete Access**.

9. Click **OK**.

35.2.5 Copying a Personal Page

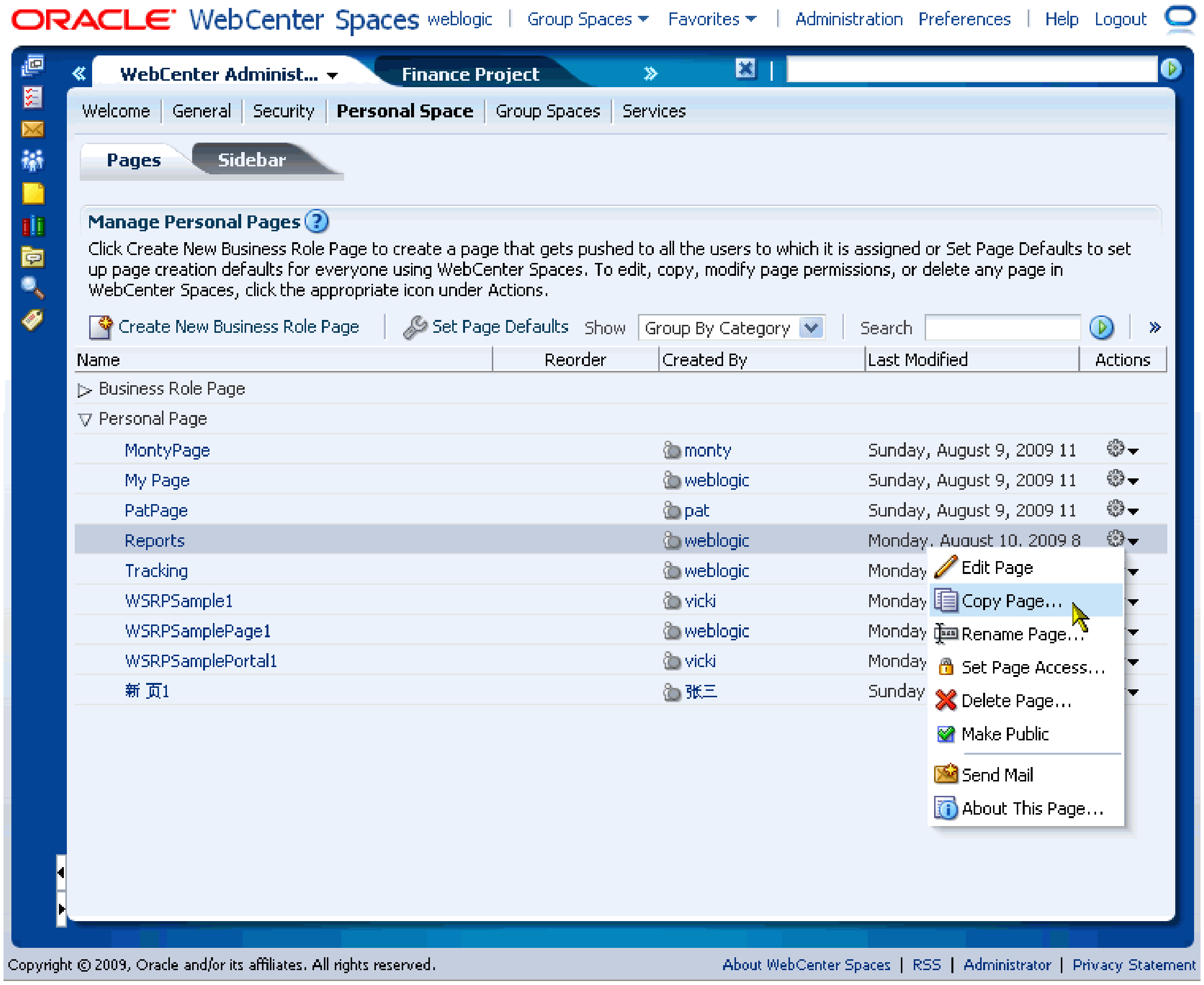
Administrators are authorized to copy any page in WebCenter Spaces. This includes other users' personal pages. When you copy a personal page as an administrator, you can save it as a business role page to be pushed to other users or as a personal page in your own personal space. If you create another business role page, you must set access on the new page because access permissions from the original page are not copied. For more information, see Section 35.1.1, "What You Should Know About Business Role Pages."

To copy a personal page as an administrator:

1. Log in to WebCenter Spaces with administrative privileges as described in Section 32.1, and click the **Administration** link at the top of the application.
2. Click the **Personal Space** tab to bring it forward.
3. Click the **Pages** tab to bring it forward.
4. Optionally, from the **Show** drop-down menu, choose **Group By Category**.

   The **Personal Page** section lists every personal page in WebCenter Spaces.
5. Click the **Actions** icon for the page you want to copy, and select **Copy Page** from the resulting context menu (Figure 35–17).

Figure 35–17 Copy Page Option on an Actions Menu


ORACLE WebCenter Spaces
weblogic | Group Spaces ▾ Favorites ▾ | Administration Preferences | Help Logout
WebCenter Administ... ▾
Finance Project
Welcome | General | Security | Personal Space | Group Spaces | Services
Pages
Sidebar

Manage Personal Pages

Click Create New Business Role Page to create a page that gets pushed to all the users to which it is assigned or Set Page Defaults to set up page creation defaults for everyone using WebCenter Spaces. To edit, copy, modify page permissions, or delete any page in WebCenter Spaces, click the appropriate icon under Actions.

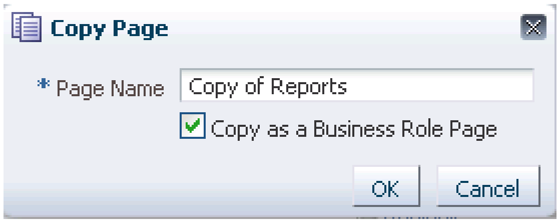
Create New Business Role Page
Set Page Defaults
Show Group By Category
Search

Name	Reorder	Created By	Last Modified	Actions
▷ Business Role Page				
▽ Personal Page				
MontyPage		monty	Sunday, August 9, 2009 11	⚙▾
My Page		weblogic	Sunday, August 9, 2009 11	⚙▾
PatPage		pat	Sunday, August 9, 2009 11	⚙▾
Reports		weblogic	Monday, August 10, 2009 8	⚙▾
Tracking		weblogic	Monday	▾
WSRPSample1		vicki	Monday	▾
WSRPSamplePage1		weblogic	Monday	▾
WSRPSamplePortal1		vicki	Monday	▾
新 页1		张三	Sunday	▾

Edit Page
Copy Page...
Rename Page...
Set Page Access...
Delete Page...
Make Public
Send Mail
About This Page...
Copyright © 2009, Oracle and/or its affiliates. All rights reserved.
About WebCenter Spaces | RSS | Administrator | Privacy Statement

6. Enter a name for the new page (Figure 35–18).

Figure 35–18 Copy Page Dialog



* Page Name: Copy of Reports

☑ Copy as a Business Role Page

7. Do one of the following:

   - Select **Copy as a Business Role Page** if you intend to push the page out to a group of people with a similar job role.
   - Deselect **Copy as a Business Role Page** if you intend to expose the copy only in your own application view.

8. Click **OK**.

The new page opens in edit mode in Oracle Composer (for more information, see "Editing Pages" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*).

35.2.6 Deleting a Personal Page

Once a personal page is removed from WebCenter Spaces it cannot be recovered. Deleted pages are permanently removed. Administrators are authorized to delete any page in WebCenter Spaces, including personal pages.

Anyone granted the `Delete Page` permission on a personal page can delete it. For these users, the process is the same as deleting regular pages (see "Deleting Pages" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*).

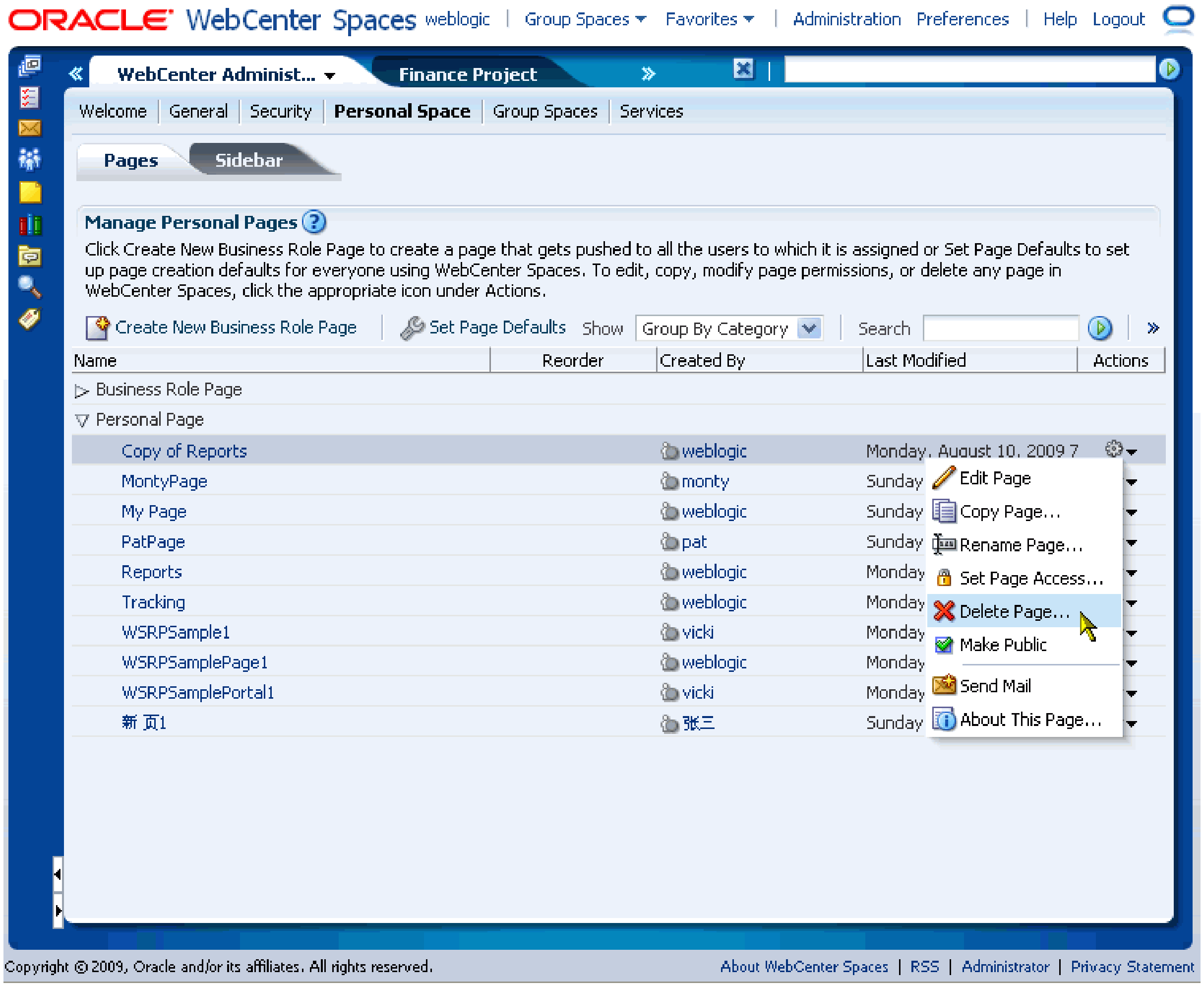
Administrators also have the option of deleting personal pages from the WebCenter Administration page.

To delete a personal page through WebCenter Administration:

1. Log in to WebCenter Spaces with administrative privileges as described in Section 32.1, and click the **Administration** link at the top of the application.
2. Click the **Personal Space** tab to bring it forward.
3. Click the **Pages** tab to bring it forward.
4. Optionally, from the **Show** drop-down menu, choose **Group By Category**.

   The **Personal Page** section lists every personal page in WebCenter Spaces.
5. Click the **Actions** icon for the page you want to delete, and select **Delete Page** from the resulting context menu (Figure 35–19).

Figure 35–19 Delete Page Option on an Actions Menu


ORACLE WebCenter Spaces
weblogic | Group Spaces | Favorites | Administration Preferences | Help Logout
WebCenter Administ...
Finance Project
Welcome | General | Security | Personal Space | Group Spaces | Services
Pages
Sidebar
Create New Business Role Page
Set Page Defaults
Show Group By Category
Search
Edit Page
Copy Page...
Rename Page...
Set Page Access...
Delete Page...
Make Public
Send Mail
About This Page...
About WebCenter Spaces | RSS | Administrator | Privacy Statement

Manage Personal Pages

Click Create New Business Role Page to create a page that gets pushed to all the users to which it is assigned or Set Page Defaults to set up page creation defaults for everyone using WebCenter Spaces. To edit, copy, modify page permissions, or delete any page in WebCenter Spaces, click the appropriate icon under Actions.

Name	Reorder	Created By	Last Modified	Actions
▷ Business Role Page				
▽ Personal Page				
Copy of Reports		weblogic	Monday, August 10, 2009 7	
MontyPage		monty	Sunday	
My Page		weblogic	Sunday	
PatPage		pat	Sunday	
Reports		weblogic	Monday	
Tracking		weblogic	Monday	
WSRPSample1		vicki	Monday	
WSRPSamplePage1		weblogic	Monday	
WSRPSamplePortal1		vicki	Monday	
新 页1		张三	Sunday	

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

6. In the resulting dialog, click **Delete** to confirm your intention to delete the page.

Deleted pages are permanently removed. You cannot recover a deleted page.

35.3 Setting Up the Public User Experience

By default, when users who are not logged in (also called *unauthenticated* or *public* users) access the WebCenter Spaces home page they see the public Welcome page. The Welcome page appears because it is a business role page assigned to the *anonymous-role*—that is, it is a public page. Other public pages provided out-of-the-box include the Login page and the Self-Registration page.

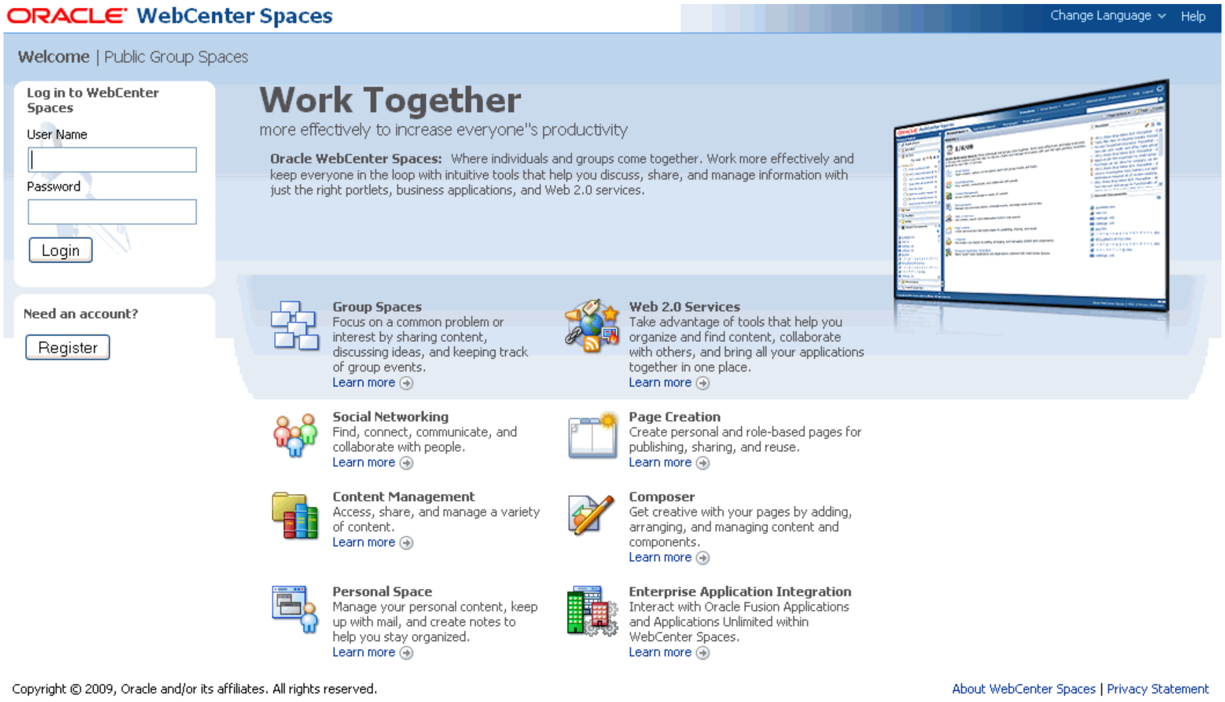
Administrators can customize default public pages and disable public access. This section provides information about performing these actions. It includes the following subsections:

- Section 35.3.1, "Customizing the Public Welcome Page"
- Section 35.3.2, "Customizing the Login Page"
- Section 35.3.3, "Customizing the Self-Registration Page"
- Section 35.3.4, "Preventing Public Users From Seeing Personal or Business Role Pages"

35.3.1 Customizing the Public Welcome Page

The *public* Welcome page (Figure 35–20) is shown when public users access the WebCenter Spaces home page. The purpose of the public Welcome page is to provide information and enable user login. If you decide to disable public access to all application pages, the public Welcome page is not shown and users are directed to the Login page. For more information, see Section 34.3.4, "Granting Permissions to the Public-User."

Figure 35–20 Public Welcome Page



ORACLE WebCenter Spaces

Change Language | Help

Welcome | Public Group Spaces

Log in to WebCenter Spaces

User Name

Password

Login

Need an account?

Register

Work Together

more effectively to increase everyone"s productivity

Oracle WebCenter Spaces: Where individuals and groups come together. Work more effectively and keep everyone in the loop with intuitive tools that help you discuss, share, and manage information with just the right portlets, business applications, and Web 2.0 services.

Group Spaces
Focus on a common problem or interest by sharing content, discussing ideas, and keeping track of group events.
Learn more

Web 2.0 Services
Take advantage of tools that help you organize and find content, collaborate with others, and bring all your applications together in one place.
Learn more

Social Networking
Find, connect, communicate, and collaborate with people.
Learn more

Page Creation
Create personal and role-based pages for publishing, sharing, and reuse.
Learn more

Content Management
Access, share, and manage a variety of content.
Learn more

Composer
Get creative with your pages by adding, arranging, and managing content and components.
Learn more

Personal Space
Manage your personal content, keep up with mail, and create notes to help you stay organized.
Learn more

Enterprise Application Integration
Interact with Oracle Fusion Applications and Applications Unlimited within WebCenter Spaces.
Learn more

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

About WebCenter Spaces | Privacy Statement

Administrators cannot change security settings for the public Welcome page provided with WebCenter Spaces.

If you want to exclude or change content on the public Welcome page, you must customize the default page through Oracle JDeveloper, deploy a customized WebCenter Spaces .WAR file containing your page, and restart WebCenter Spaces. Therefore, custom page deployment typically takes place *before* the WebCenter Spaces application goes live or during scheduled maintenance periods. For more information, refer to the white paper "*Extending WebCenter Spaces*" available on the Oracle Technology Network (`http://www.oracle.com/technology/products/webcenter/pdf/owcs_r11_extend_spaces_wp.pdf`).

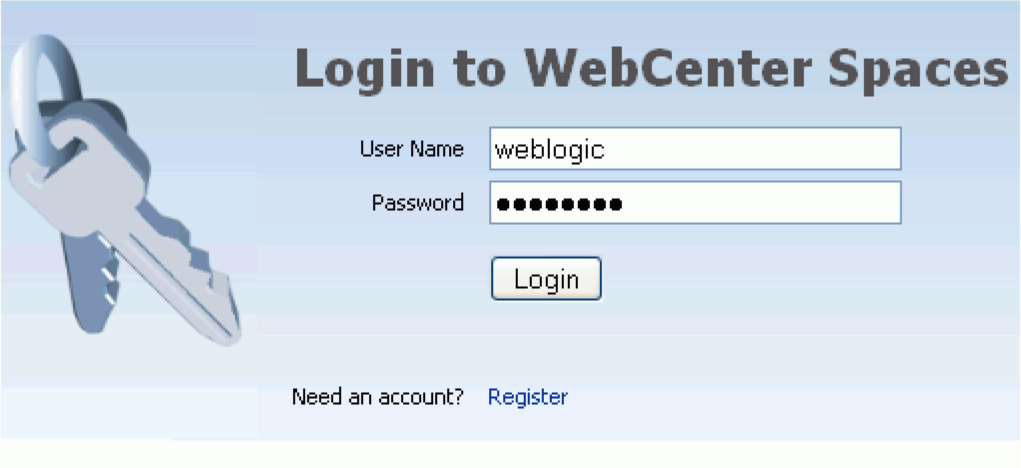
> **Note:** The public Welcome page differs from the out-of-the-box business role page, also called *Welcome*, that everyone sees in their personal space when they are logged in to WebCenter Spaces. Unlike the public Welcome page, you can modify the business role Welcome page using Oracle Composer. For more information, see Section 35.1.1, "What You Should Know About Business Role Pages."

35.3.2 Customizing the Login Page

Users with the `Administrator` role can customize certain aspects of the default Login page through Oracle Composer. Administrators cannot edit or delete input fields and buttons on the page, but they can add new components and change the page layout.

Figure 35–21 shows the Login page that is supplied out-of-the-box.

Figure 35–21 Default Login Page



Login to WebCenter Spaces

User Name: weblogic

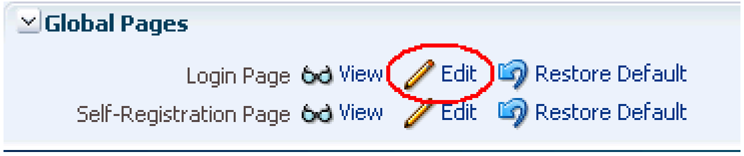
Password: ●●●●●●●●

Need an account? Register

To view and customize the Login page through WebCenter Administration:

1. Log in to WebCenter Spaces with administrative privileges as described in Section 32.1, and click the **Administration** link at the top of the application.
2. Click the **General** tab to bring it forward.
3. In the **Global Pages** section, click the **Edit** icon associated with the Login page (Figure 35–22) to open the page in Oracle Composer.

Figure 35–22 Edit Icon for Login Page

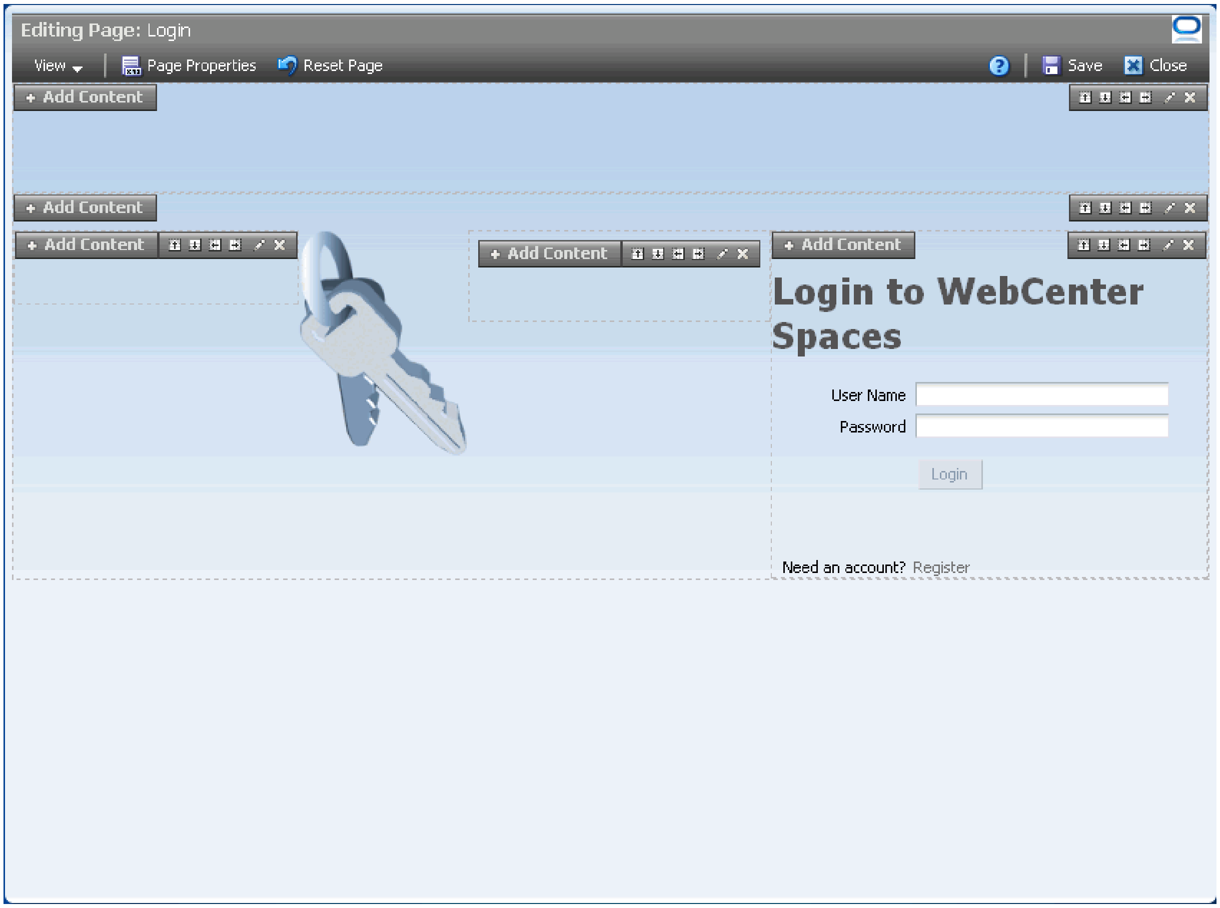


Global Pages
Login Page View Edit Restore Default
Self-Registration Page View Edit Restore Default

   Alternatively, click **View** to see how the current page appears.

4. In Oracle Composer, add new components and change the page layout as required (Figure 35–23).

Figure 35–23 Customizing the Login Page



5. Click **Save** to save your changes, and then click **Close** to exit Oracle Composer.

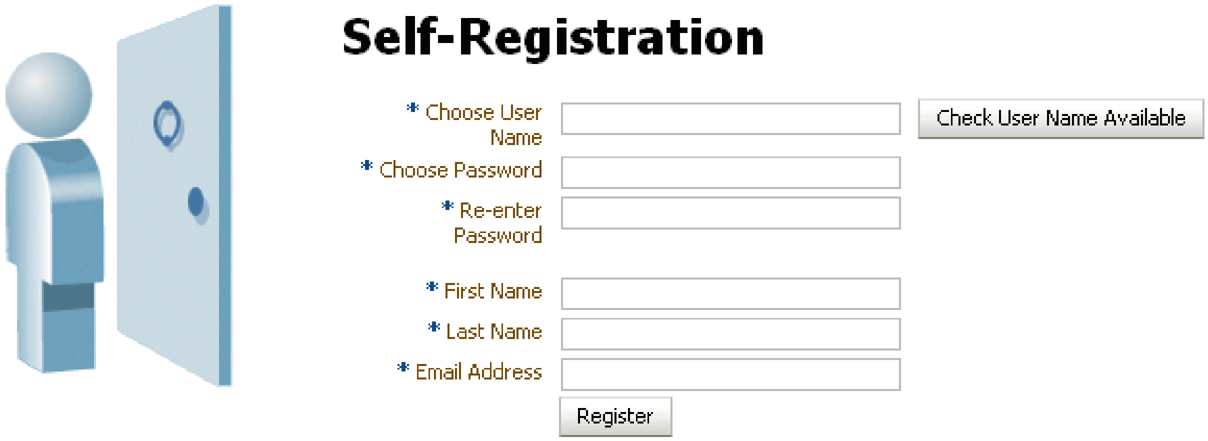
   Tip: To remove all of your customizations and revert back to the default Login page, follow steps 1 and 2 in this section, and then click **Restore Default** next to **Login Page** (Figure 35–22).

35.3.3 Customizing the Self-Registration Page

The Self-Registration page enables anyone with web access to register with WebCenter Spaces. For more information about self-registration, see Section 34.4, "Allowing Self-Registration."

Figure 35–24 shows the default Self-Registration page that is supplied out-of-the-box.

Figure 35–24 Default Self-Registration Page

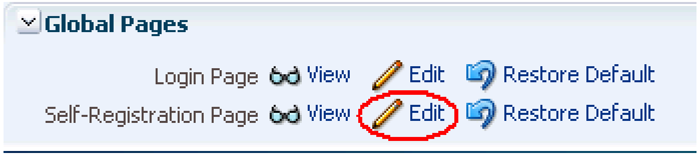


Users with the `Administrator` role can customize certain aspects of this page through Oracle Composer. Administrators cannot edit or delete input fields and buttons on the page, but they can add new components and change the page layout. For example, as the administrator, you might want to add some text to the page to describe your password policy.

To view and customize the Self-Registration page through WebCenter Administration:

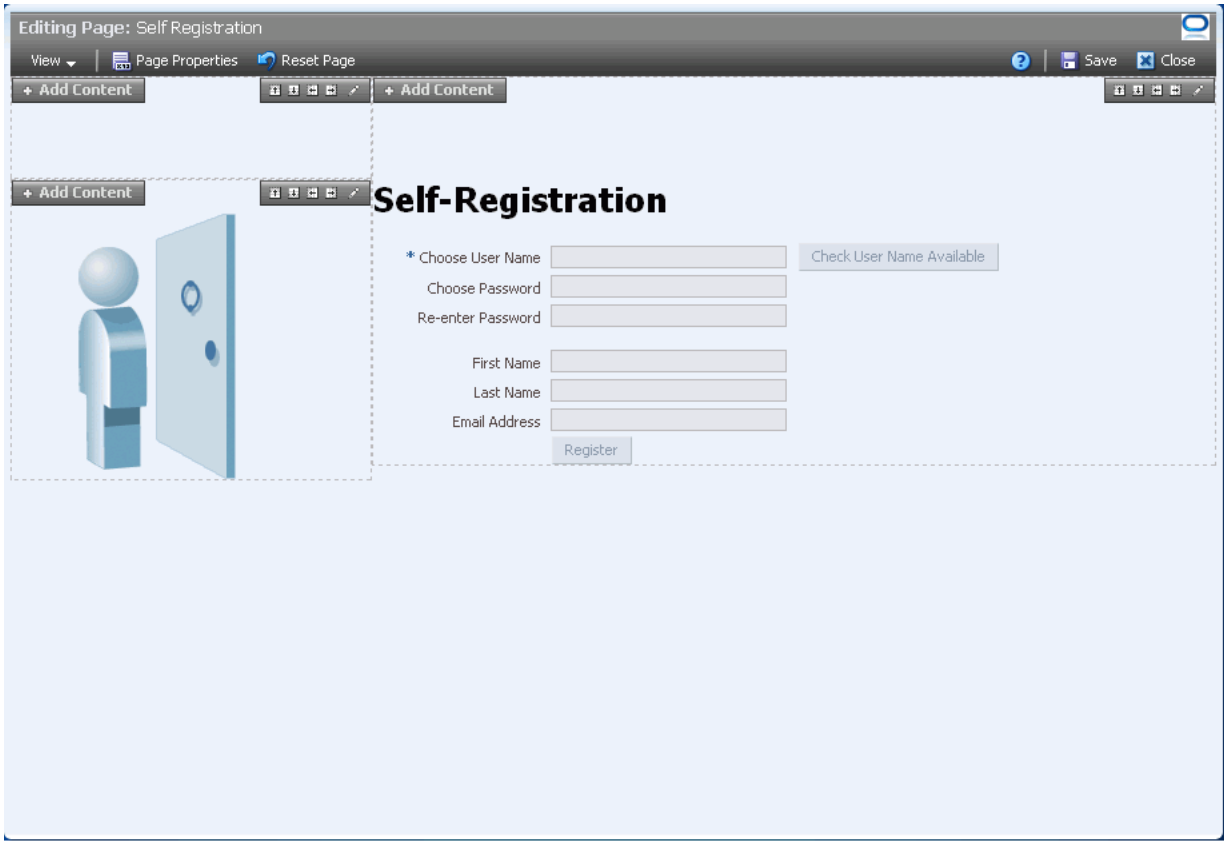
1. Log in to WebCenter Spaces with administrative privileges as described in Section 32.1, and click the **Administration** link at the top of the application.
2. Click the **General** tab to bring it forward.
3. In the **Global Pages** section, click the **Edit** icon associated with the Self-Registration page to open it in Oracle Composer(Figure 35–25).

   Figure 35–25 Edit Icon for Self-Registration Page

   Alternatively, click **View** to see how the current page appears.
4. Add new components and change the page layout as required (Figure 35–26).

Figure 35–26 Customizing the Self-Registration Page



5. Click **Save** to save your changes, and then click **Close** to exit Oracle Composer.

> **Tip:** To remove all of your customizations and revert back to the default page, follow steps 1 and 2 in this section, and then click **Restore Default** next to **Self-Registration Page** (Figure 35–25).

35.3.4 Preventing Public Users From Seeing Personal or Business Role Pages

For security reasons, you may not want WebCenter Spaces users to share their personal pages with public users. You can restrict public access by disabling the `Application-View` permission for all public users. For more information, see Section 34.3.4, "Granting Permissions to the Public-User."

36

Making Applications Available in WebCenter Spaces

The Applications pane in the Sidebar provides offers WebCenter users quick access to applications they use the most. It is the WebCenter Spaces administrator's job to manage the content of the Applications pane. You control the range of applications available, the way they are presented, and how they are launched.

This section includes the following subsections:

- Section 36.1, "What You Should Know About the Applications Pane"
- Section 36.2, "Making an Application Available to WebCenter Users"
- Section 36.3, "Editing Links in the Applications Pane"
- Section 36.4, "Arranging the Applications List"
- Section 36.5, "Locking Applications Displayed in the Applications Pane"
- Section 36.6, "Removing Links from the Applications Pane"

Providing they are not locked, individual WebCenter users may hide links to applications if they do not need them. See "Hiding and Showing Task Flows in the Sidebar" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter.*

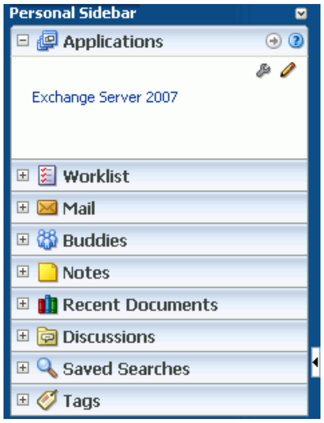
Audience

The content of this chapter is intended for WebCenter Spaces administrators. Users granted the WebCenter Spaces `Administrator` role or a custom role that grants the `Application-Manage` permission).

36.1 What You Should Know About the Applications Pane

WebCenter Spaces offers users centralized access to frequently-used Web applications from the Sidebar. The WebCenter Spaces administrator manages the range of applications available, the way they are presented, and how they are launched from the Applications pane (Figure 36–1).

Figure 36–1 Sidebar - Applications Pane



Personal Sidebar

Applications

Exchange Server 2007

WebCenter users need not know nor care about where the information comes from, they simply click a link to launch their day-to-day applications, and if necessary, supply their user name and password information. WebCenter users may hide links that they do not use but they cannot add links of their own.

The Applications pane can launch different types of application:

- **External Applications** - Web-based, external applications that perform their own user authentication. WebCenter administrators must register external applications through the Oracle Enterprise Manager Fusion Middleware Control Console before exposing them in WebCenter Spaces. For more information, see Section 22.2.1, "Registering External Applications Using Fusion Middleware Control".
- **WebCenter Task Flows** - Built-in task flows specific to WebCenter Spaces. A range of WebCenter task flows are available out-of-the-box including Document Library Viewer, Discussions Viewer, and more. Any of these can be launched directly from the Applications pane.

For more information, see Section 36.2, "Making an Application Available to WebCenter Users".

36.2 Making an Application Available to WebCenter Users

The Applications pane can display links to external applications registered through Fusion Middleware Control Console and also links to any of the built-in WebCenter task flows. When you expose an application through this pane, the application becomes available to every WebCenter user.

Some WebCenter users may not want to see all the applications offered through the Applications pane. If this is the case, individuals may personalize their view to show only those applications they must access.

To make an application available to WebCenter users:

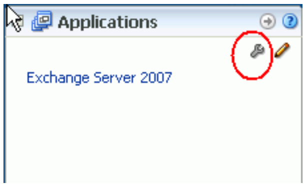
1. Login to WebCenter Spaces with administrative privileges.

   See Section 32.1, "Logging into WebCenter Spaces as an Administrator".

2. In the Sidebar, click the Edit icon for the Applications pane (Figure 36–2).

   If you do not have administrative privileges you will not see this icon.

Figure 36–2 Applications Pane - Edit Icon



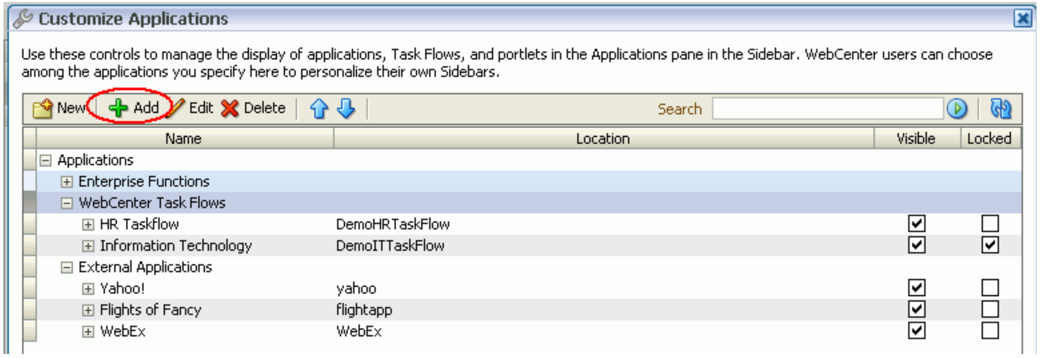
When you edit the Applications pane, every WebCenter user will see your changes.

> **Note:** For information about the Sidebar, see "Working with the WebCenter Spaces Sidebar" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

3. To add a link to an application, select the folder where you want the link to appear, and then click the green Add icon (Figure 36–3).

   To add a new folder, click the New icon. To create a subfolder, expand the parent folder first. Section 22.2, "Registering External Applications"

Figure 36–3 Editing the Applications Pane



Use these controls to manage the display of applications, Task Flows, and portlets in the Applications pane in the Sidebar. WebCenter users can choose among the applications you specify here to personalize their own Sidebars.

Name	Location	Visible	Locked
Applications			
Enterprise Functions			
WebCenter Task Flows			
HR Taskflow	DemoHRTaskFlow	☑	□
Information Technology	DemoITTaskFlow	☑	☑
External Applications			
Yahoo!	yahoo	☑	□
Flights of Fancy	flightapp	☑	□
WebEx	WebEx	☑	□

4. Navigate to the external application or task flow you require, and click its associated **Add** link (Figure 36–4).

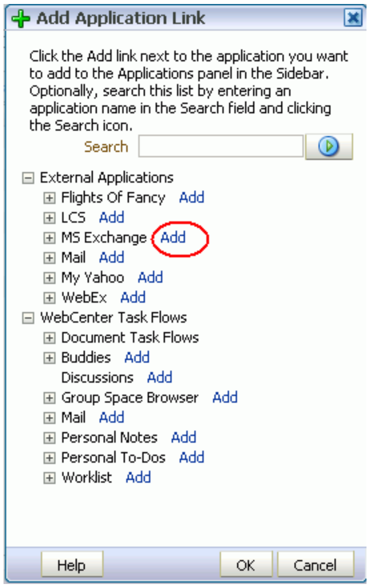
   - To navigate to a previously registered external application, expand the **External Applications** node, and then expand the required application.

     Only registered external applications which have a *Login URL* defined appear in this list. If the application you want is not listed, ask your WebCenter administrator to register the application for you. See also Section 22.2, "Registering External Applications".

   - To navigate to a task flow, expand the **WebCenter Task Flows** node. If necessary, expand one or more subfolders to access the required task flow.

   If you are not sure of the exact name, enter a full or partial search term in the **Search** box, and then click **Find** to search for the application. Application names matching your search criteria are displayed.

Figure 36–4 Choosing an Application



Add Application Link

Click the Add link next to the application you want to add to the Applications panel in the Sidebar. Optionally, search this list by entering an application name in the Search field and clicking the Search icon.

Search

- External Applications
  - Flights Of Fancy Add
  - LCS Add
  - MS Exchange Add
  - Mail Add
  - My Yahoo Add
  - WebEx Add
- WebCenter Task Flows
  - Document Task Flows
  - Buddies Add
  - Discussions Add
  - Group Space Browser Add
  - Mail Add
  - Personal Notes Add
  - Personal To-Dos Add
  - Worklist Add

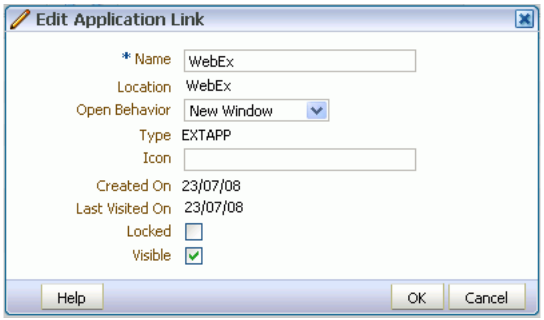
An information message displays indicating whether the application link was successful.

5. Click **OK** to dismiss the message box.
6. To add another application, repeat steps 4 and 5.
7. Click **OK** to return to the Edit Applications dialog box.

   The selected application(s) appears within your chosen folder. From here, you can change the display name for the application link and set other display-related properties.
8. To edit link details for an application, highlight the row in the table and then click the Edit icon.

   The Edit Application Link dialog box opens (Figure 36–5).

Figure 36–5 Editing Application Links



Edit Application Link

* Name	WebEx
Location	WebEx
Open Behavior	New Window
Type	EXTAPP
Icon	
Created On	23/07/08
Last Visited On	23/07/08
Locked	□
Visible	☑

9. Edit the link display properties, as required.

   For details, see Table 36–1, " Application Link Properties":

Table 36–1 Application Link Properties

Property	Description
Name	Enter the link text that WebCenter users will click to launch the application.
Location	(Read-only) Displays the internal name for the application or task flow.
Open Behavior	Choose how the application displays when users click the link: - **WebCenter Tab** - Application displays as a tab in WebCenter Spaces, and the application displays there. The current WebCenter Spaces context is maintained. - **New Window** - Application opens in a new browser window. The current WebCenter Spaces context is maintained. This is the default selection. - **Current Window** - Application opens in the current browser window (in place of WebCenter Spaces).
Type	(Read-only) Displays the link type: EXTAPP - External application or TASKFLOW - WebCenter task flow
Icon	Associate an icon with the application. Enter a full qualified URL or a relative URL that specifies the location of a valid icon. The icon displays alongside the link in the Sidebar. For best results, choose an icon that is 16 x 16 pixels.
Created On	Shows when the link was created.
Last Visited On	Shows the last time a user clicked the link. If a link is not used very often or at all, you might consider removing it from the Applications pane.
Locked	Indicate whether WebCenter users are allowed to show/hide the link. Select **Locked** to prevent users from showing/hiding the link. Deselect **Locked** to let the user decide whether the link displays in their personal view. Individuals users can show or hide the link depending of whether they need access to the application from the Sidebar.
Visible	Indicate whether WebCenter users see a link to this application in the Applications pane. Select **Visible** to show the link. Deselect **Visible** to hide the link.

10. Click **OK** to save.
11. Click **Close** to dismiss the Edit Application Link dialog box.

New or updated links appear in the Applications pane. Click the link to test that it works correctly.

36.3 Editing Links in the Applications Pane

To edit a link displayed in the Applications pane:

1. Login to WebCenter Spaces with administrative privileges.

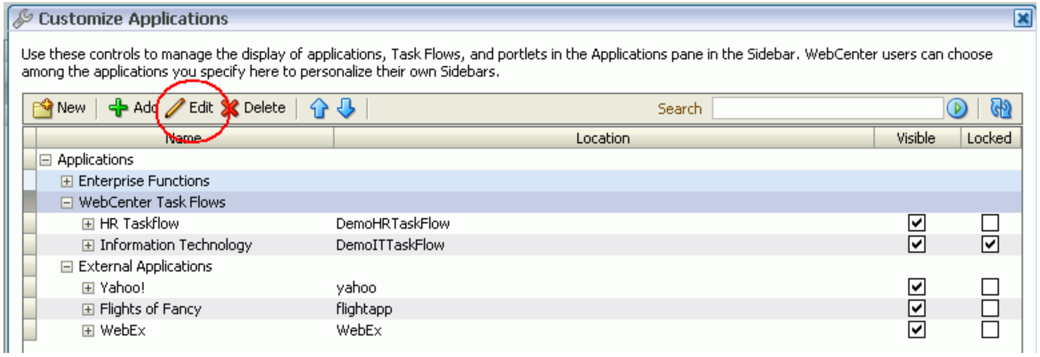
   See Section 32.1, "Logging into WebCenter Spaces as an Administrator".

2. In the Sidebar, click the Edit icon for the Applications pane.

> **Note:** When you edit the Applications pane, every WebCenter user sees your changes.

3. Select an application link by highlighting the row in the table.
4. Click the Edit icon (Figure 36–6).

Figure 36–6 Editing Application Links



Customize Applications

Use these controls to manage the display of applications, Task Flows, and portlets in the Applications pane in the Sidebar. WebCenter users can choose among the applications you specify here to personalize their own Sidebars.

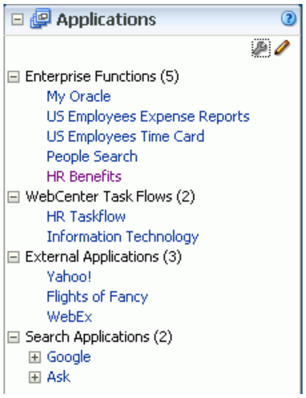
Name	Location	Visible	Locked
⊟ Applications			
⊞ Enterprise Functions			
⊟ WebCenter Task Flows			
⊞ HR Taskflow	DemoHRTaskFlow	☑	□
⊞ Information Technology	DemoITTaskFlow	☑	☑
⊟ External Applications			
⊞ Yahoo!	yahoo	☑	□
⊞ Flights of Fancy	flightapp	☑	□
⊞ WebEx	WebEx	☑	□

5. Edit the link properties, as required. For details, see Table 36–1, " Application Link Properties".
6. Click **OK** to save.
7. Click **Close** to dismiss the Edit Applications dialog box.

36.4 Arranging the Applications List

As WebCenter Spaces administrator, you choose the display order of links in the Applications pane. You can also organize your application links into a hierarchy by creating sub folders. These sub folders, which can represent topic areas, can be nested into other sub folders (Figure 36–7).

Figure 36–7 Arranging the Applications List



Applications

- ⊟ Enterprise Functions (5)
  - My Oracle
  - US Employees Expense Reports
  - US Employees Time Card
  - People Search
  - HR Benefits
- ⊟ WebCenter Task Flows (2)
  - HR Taskflow
  - Information Technology
- ⊟ External Applications (3)
  - Yahoo!
  - Flights of Fancy
  - WebEx
- ⊟ Search Applications (2)
  - ⊞ Google
  - ⊞ Ask

1. Login to WebCenter Spaces with administrative privileges.

   See Section 32.1, "Logging into WebCenter Spaces as an Administrator".
2. In the Sidebar, click the Edit icon for the Applications pane.

> **Note:** When you edit the Applications pane, every WebCenter user sees your changes.

3. Reorganize your applications. For example:

   - **Rearrange the display order.** Select an application or a folder, and then click the Move Up and Move Down icons until it appears in the correct place. When you move a folder, everything under the folder moves with it.

     Alternatively, drag and drop an application to the correct position.

   - **Create a new folder or sub folder.** Select a parent folder (if required), click the New Folder icon, enter a suitable **Name**, and then click **Create.**

   - **Rename a folder.** Click the **Display Name** and edit the folder name in place.

4. Click **Close** to save.

36.5 Locking Applications Displayed in the Applications Pane

WebCenter Spaces administrators can lock links displayed in the Applications pane. When you lock a link, WebCenter users are not allowed to show/hide the link.

Unlock links to let the user decide whether the link displays in their personal view. Individuals users can show or hide the link depending of whether they need access to the application from the Sidebar.

To lock an application link:

1. Login to WebCenter Spaces with administrative privileges.

   See Section 32.1, "Logging into WebCenter Spaces as an Administrator".

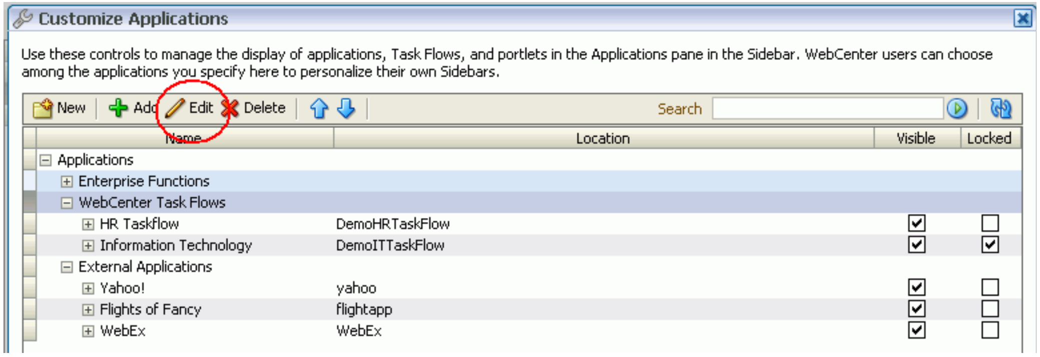
2. In the Sidebar, click the Edit icon for the Applications pane.

> **Note:** When you edit the Applications pane, every WebCenter user will see your changes.

3. Select the required application by highlighting the row in the table.

4. Click the Edit icon (Figure 36–8).

Figure 36–8 Editing Application Links



Use these controls to manage the display of applications, Task Flows, and portlets in the Applications pane in the Sidebar. WebCenter users can choose among the applications you specify here to personalize their own Sidebars.

Name	Location	Visible	Locked
⊟ Applications			
⊞ Enterprise Functions			
⊟ WebCenter Task Flows			
⊞ HR Taskflow	DemoHRTaskFlow	☑	□
⊞ Information Technology	DemoITTaskFlow	☑	☑
⊟ External Applications			
⊞ Yahoo!	yahoo	☑	□
⊞ Flights of Fancy	flightapp	☑	□
⊞ WebEx	WebEx	☑	□

5. To lock the application, select **Locked**.

6. Click **OK** to save.
7. Click **Close** to dismiss the Edit Applications dialog box.

36.6 Removing Links from the Applications Pane

When application links are no longer required, WebCenter Spaces administrators can remove them from the Applications pane.

Removing links is permanent. If a link might be useful in the future, consider hiding the link instead (by deselecting the **Visible** property). For details, see Section 36.3, "Editing Links in the Applications Pane".

To permanently remove an application link:

1. Login to WebCenter Spaces with administrative privileges.

   See Section 32.1, "Logging into WebCenter Spaces as an Administrator".

2. In the Sidebar, click the Edit icon for the Applications pane.

   > **Note:** When you edit the Applications pane, every WebCenter user will see your changes.

3. Select the required application (or application folder) by highlighting the row in the table.
4. To remove the application link, click the Delete icon.

   When you delete a folder, you delete the folder and all the applications displayed in the folder.

5. Click **Delete** to confirm.
6. Click **Close** to dismiss the Edit Applications dialog box.

37

Managing Group Spaces in WebCenter Spaces

This chapter describes how a WebCenter Spaces administrator with `Group Spaces-Manage` or `Group Space Templates-Manage` permissions can manage everyone's group spaces and group space templates in WebCenter Spaces. It includes the following sections:

- Section 37.1, "What You Should Know About Group Space Management"
- Section 37.2, "Viewing Group Space Information"
- Section 37.3, "Changing the Status of a Group Space"
- Section 37.4, "Enabling and Disabling Services"
- Section 37.5, "Managing Group Space Templates"
- Section 37.6, "Troubleshooting"

For more information about exporting and importing group space information, see Chapter 38, "Exporting and Importing Group Spaces".

Audience

This chapter is intended for WebCenter Spaces administrators (users granted the WebCenter Spaces `Administrator` role or a custom role that grants the `Application-Manage` permission).

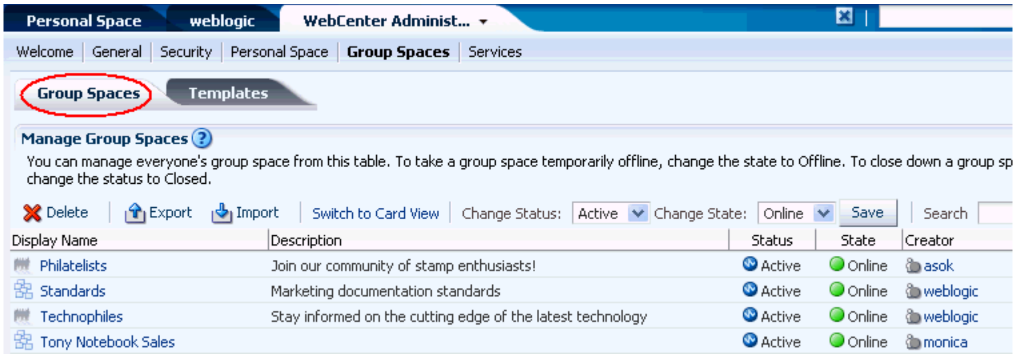
37.1 What You Should Know About Group Space Management

WebCenter Spaces administrators with `Group Spaces-Manage` or `Group Space Templates-Manage` permissions can manage any group space or group space template on the **WebCenter Administration** > **Group Spaces** page (Figure 37–1). From here, you can take any group space temporarily offline and close down any group spaces deemed inactive. Administrators can rename and edit any group space, as well as delete group spaces when they are no longer required.

Group space moderators do not have access to this page. While group space moderators may perform *some* of these tasks for group spaces that they own through group space administration, the WebCenter Spaces administrator can manage all of them.

The **Group Spaces** administration page offers import and export services, too. For more information, see Chapter 38, "Exporting and Importing Group Spaces".

Figure 37–1 WebCenter Administration - Group Spaces



Manage Group Spaces

You can manage everyone's group space from this table. To take a group space temporarily offline, change the state to Offline. To close down a group sp change the status to Closed.

Change Status: Active Change State: Online

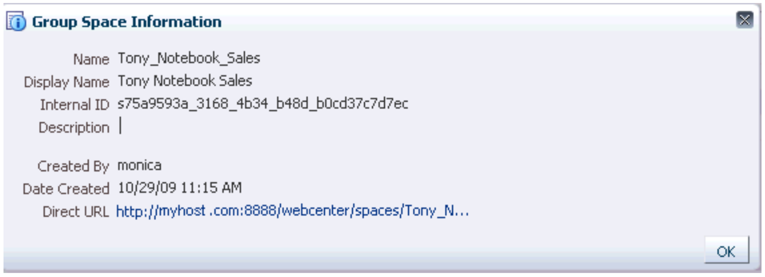
Display Name	Description	Status	State	Creator
Philatelists	Join our community of stamp enthusiasts!	Active	Online	asok
Standards	Marketing documentation standards	Active	Online	weblogic
Technophiles	Stay informed on the cutting edge of the latest technology	Active	Online	weblogic
Tony Notebook Sales		Active	Online	monica

37.2 Viewing Group Space Information

WebCenter Spaces administrators can view and manage any group space on the **WebCenter Administration** > **Group Spaces** page. From here, you can quickly see whether group spaces are active, online, offline, who created the group space (the group space moderator), and the date on which group spaces were created.

The **Actions** icon menu offers additional options for editing, renaming, and deleting group spaces, and if you select **About Group Space** you can access useful information such as the group's space direct URL and internal ID (Figure 37–2).

Figure 37–2 About Group Space



Name Tony_Notebook_Sales
Display Name Tony Notebook Sales
Internal ID s75a9593a_3168_4b34_b48d_b0cd37c7d7ec
Description
Created By monica
Date Created 10/29/09 11:15 AM
Direct URL http://myhost .com:8888/webcenter/spaces/Tony_N...

By default, group spaces are listed alphabetically. To view the information sorted by a different column, click the sort icon for the column. Sort icons appear when you hover the mouse cursor over the column header.

To display the group space administration page:

1. Log in to WebCenter Spaces with administrative privileges.

   See Section 32.1, "Logging into WebCenter Spaces as an Administrator".

2. Click the **Administration** link at the top of the application.
3. Click the **Group Spaces** tab.
4. Click the **Group Spaces** subtab.

37.3 Changing the Status of a Group Space

WebCenter Spaces administrators can change the status of any group space. This section describes the steps to perform the following tasks:

- Section 37.3.1, "Taking Any Group Space Offline"

- Section 37.3.2, "Bringing Any Group Space Back Online"
- Section 37.3.3, "Closing Any Group Space"
- Section 37.3.4, "Reactivating Any Group Space"
- Section 37.3.5, "Deleting a Group Space"

37.3.1 Taking Any Group Space Offline

When a group space is offline, members of the group space who do not have `Group Spaces-Manage` permission are unable to access the group space. If members try to access the group space, they will see the *Group Space Unavailable* page. See also "Customizing the Group Space Unavailable Page" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

Administrators and group space members with `Group Spaces-Manage` permission can access a group space that is offline. So if, for example, an administrator who notices inappropriate content can take a group space offline, fix the content, and bring it back online later.

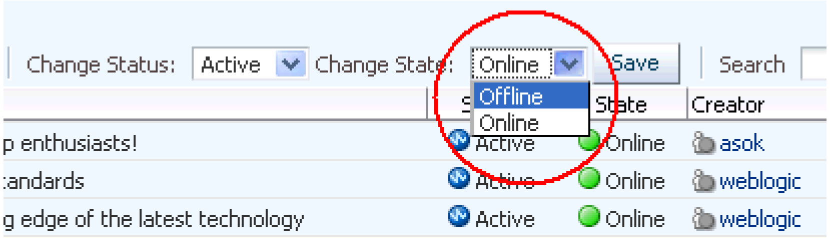
To permanently close down a group space that is not being used any more, see Section 37.3.3, "Closing Any Group Space".

To take a group space offline:

1. Log in to WebCenter Spaces with administrative privileges.

   See Section 32.1, "Logging into WebCenter Spaces as an Administrator".
2. Click the **Administration** link at the top of the application.
3. Click the **Group Spaces** tab.
4. Click the **Group Spaces** subtab.
5. On the **Group Spaces** page, select the group space you require by highlighting the row in the table.
6. From the **Change State** dropdown list, select **Offline** (Figure 37–3).

Figure 37–3 Taking a Group Space Offline



	S	State	Creator
p enthusiasts!	Active	Online	asok
:andards	Active	Online	weblogic
g edge of the latest technology	Active	Online	weblogic

7. Click **Save**.

37.3.2 Bringing Any Group Space Back Online

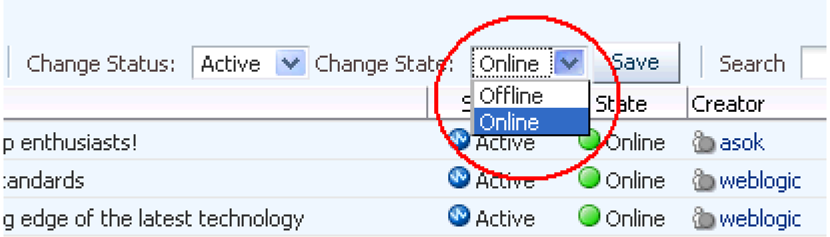
To bring any group space back online:

1. Log in to WebCenter Spaces with administrative privileges.

   See Section 32.1, "Logging into WebCenter Spaces as an Administrator".
2. Click the **Administration** link at the top of the application.

3. Click the **Group Spaces** tab.
4. Click the **Group Spaces** subtab.
5. On the **Group Spaces** page, select the required group space by highlighting the row in the table.
6. From the **Change State** dropdown list, select **Online** (Figure 37–4).

Figure 37–4 Bringing a Group Space Online



	S	State	Creator
p enthusiasts!	Active	Online	asok
:andards	Active	Online	weblogic
g edge of the latest technology	Active	Online	weblogic

7. Click **Save**.

37.3.3 Closing Any Group Space

A WebCenter Spaces administrator can close any group space that is no longer being used. When you close a group space, the content is archived. The group space is removed from everyone's **Group Spaces** menu to avoid clutter, but its content remains accessible and searchable to those who may want to reference it.

Current members may still access the group space through My Group Spaces. See "Viewing Available Group Spaces" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

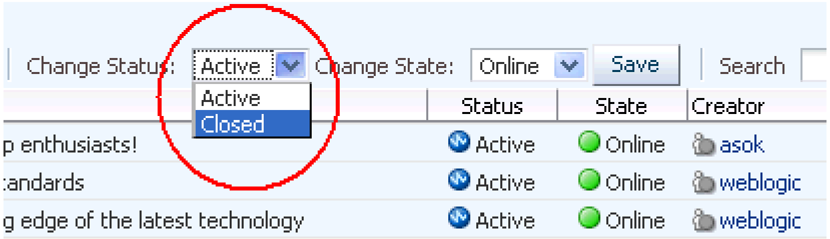
If you want to close down a group space temporarily, take the group space offline instead. See Section 37.3.1, "Taking Any Group Space Offline".

To close a group space:

1. Log in to WebCenter Spaces with administrative privileges.

   See Section 32.1, "Logging into WebCenter Spaces as an Administrator".
2. Click the **Administration** link at the top of the application.
3. Click the **Group Spaces** tab.
4. Click the **Group Spaces** subtab.
5. On the **Group Spaces** page, select the required group space by highlighting the row in the table.
6. From the **Change Status** dropdown list, select **Closed** (Figure 37–5).

Figure 37–5 Closing a Group Space



	Status	State	Creator
p enthusiasts!	Active	Online	asok
:andards	Active	Online	weblogic
g edge of the latest technology	Active	Online	weblogic

7. Click **Save**.

37.3.4 Reactivating Any Group Space

WebCenter Spaces administrators and group space moderators may close a group space if it is no longer being used. If you want to reopen a group space, you can do so.

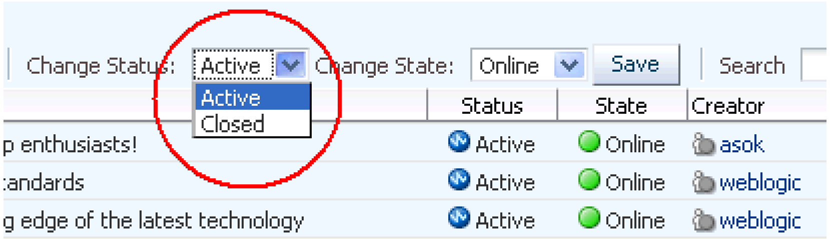
To reactivate a group space:

1. Log in to WebCenter Spaces with administrative privileges.

   See Section 32.1, "Logging into WebCenter Spaces as an Administrator".

2. Click the **Administration** link at the top of the application.
3. Click the **Group Spaces** tab.
4. Click the **Group Spaces** subtab.
5. On the **Group Spaces** page, select the required group space by highlighting the row in the table.
6. From the **Change Status** dropdown list, select **Active** (Figure 37–6).

Figure 37–6 Activating a Group Space



Change Status: Active | Change State: Online | Save | Search

	Status	State	Creator
p enthusiasts!	Active	Online	asok
:andards	Active	Online	weblogic
g edge of the latest technology	Active	Online	weblogic

7. Click **Save**.

37.3.5 Deleting a Group Space

WebCenter Spaces administrators with the `Group Spaces-Manage` permission can delete any group space. Once a group space is removed from WebCenter Spaces, it cannot be recovered. Group spaces are permanently removed and current members will no longer see the group space in their view.

Most group space data is deleted too; the exceptions are group space discussions, announcements, wikis, and blogs, which remain on the associated back-end servers.

You cannot delete a group space while the moderator is editing group space settings, but there are no other restrictions.

To delete a group space that is no longer required:

1. Log in to WebCenter Spaces with administrative privileges.

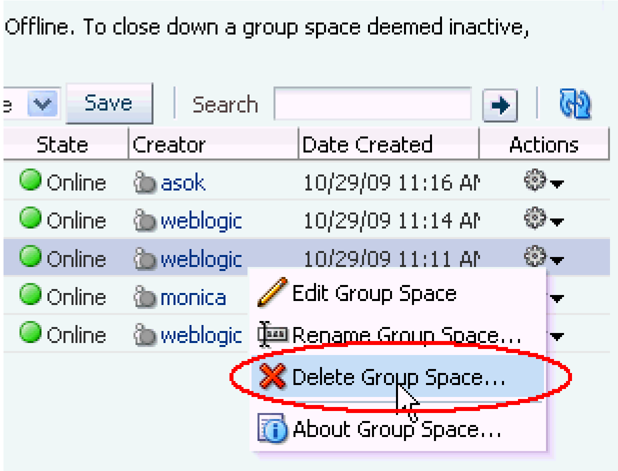
   See Section 32.1, "Logging into WebCenter Spaces as an Administrator".

2. Click the **Administration** link at the top of the application.
3. Click the **Group Spaces** tab.
4. Click the **Group Spaces** subtab.
5. On the **Group Spaces** page, select the required group space by highlighting the row in the table.

Ctrl-Click rows to select more than one.

6. Click the **Actions** icon for the page, and choose **Delete** (Figure 37–7).

Figure 37–7 Deleting a Group Space



Offline. To close down a group space deemed inactive,

State	Creator	Date Created	Actions
Online	asok	10/29/09 11:16 AI	
Online	weblogic	10/29/09 11:14 AI	
Online	weblogic	10/29/09 11:11 AI	
Online	monica		
Online	weblogic		

7. Click **Delete** to confirm that you want to delete the group space(s).

If the delete process fails for any reason, the group space is not removed from the administrator's **Group Spaces** tab; this sometimes happens when a back-end server cannot be contacted. If the administrator clicks **Delete** again from here, the group space will be removed.

37.4 Enabling and Disabling Services

WebCenter Spaces services, such as Discussions and Mail, are configured by your Fusion Middleware Administrator through Fusion Middleware Control or using the WLST command-line tool. New services automatically become available in WebCenter Spaces when the application starts up—no additional configuration is required inside WebCenter Spaces. Likewise, there is no facility to disable services for the entire application as the Fusion Middleware Administrator takes care of this through Fusion Middleware Control. See Section 2, "Getting WebCenter Spaces Up and Running".

You can enable and disable services for individual group spaces inside the WebCenter Spaces application: Announcements, Discussions, Documents, Group Space Events, Instant Messaging and Presence, Lists, and Mail. In most cases, the group space moderator will manage service requirements for their own group space, but WebCenter Spaces administrators can also perform this task if required to do so. For details, see "Enabling and Disabling Services Available to a Group Space" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

37.5 Managing Group Space Templates

WebCenter Spaces administrators with the `Group Space Templates-Manage` permission can review, publish, hide, and delete any group space template. This section describes how to perform these tasks:

- Section 37.5.1, "What You Should Know About Managing Group Space Templates"
- Section 37.5.2, "Viewing Group Space Templates"
- Section 37.5.3, "Publishing and Hiding Group Space Templates"

- Section 37.5.4, "Deleting a Group Space Template"

37.5.1 What You Should Know About Managing Group Space Templates

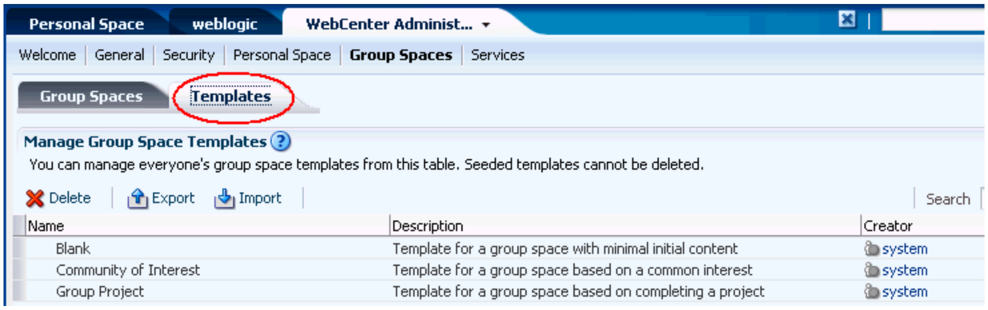
Several group space templates are provided out-of-the-box: Group Project, Community of Interest, and Blank. In addition to these, users with the `Group Spaces-Create` permission can create customized templates from group spaces and share them with other users. For more information, see "What You Should Know About Group Space Templates" and "Creating Your Own Group Space Templates" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

WebCenter administrators with the `Group Space Templates-Manage` permission can manage *every* group space template from the **WebCenter Administration** > **Templates** page (Figure 37–8). You can see which group space templates are currently available and delete group space templates when they are no longer required. You can also publish templates—making them available to everyone—or restrict them to private use only.

It is important to keep the template list up to date and valid. Anyone who creates a group space will see public templates as well as their own private templates.

The **Templates** page provides import and export services, too. For more information, see Chapter 38, "Exporting and Importing Group Spaces".

Figure 37–8 WebCenter Administration - Templates Page



You can manage everyone's group space templates from this table. Seeded templates cannot be deleted.

Name	Description	Creator
Blank	Template for a group space with minimal initial content	system
Community of Interest	Template for a group space based on a common interest	system
Group Project	Template for a group space based on completing a project	system

37.5.2 Viewing Group Space Templates

WebCenter Spaces administrators with the `Group Space Templates-Manage` permission can view and manage any group space through the **WebCenter Administration** > **Templates** page. From here, you can quickly see who created each group space template (the group space moderator), and the date on which it was created. The **Actions** menu offers additional options for deleting group space templates, and you can publish and hide templates from here, too.

By default, group space templates are listed alphabetically. To view the information sorted by a different column, click the sort icon for the column. Sort icons appear when you hover the mouse cursor over the column header.

To see a list of every group space template in WebCenter Spaces, together with their description, creator, and other useful information:

1. Log in to WebCenter Spaces with administrative privileges.

   See Section 32.1, "Logging into WebCenter Spaces as an Administrator".

2. Click the **Administration** link at the top of the application.

3. Click the **Group Spaces** tab.

4. Click the **Templates** subtab.

37.5.3 Publishing and Hiding Group Space Templates

While WebCenter Spaces can accommodate any number of templates, a limited number of templates is sometimes more effective. The WebCenter Spaces administrator or users granted the `Group Space Templates - Manage` permission can maintain the template list on the **WebCenter Administration > Group Spaces > Templates** page. To view the **WebCenter Administration > Group Spaces > Templates** page, a user must additionally be granted `Application-Configure` permission by the WebCenter Spaces administrator.

To publish or hide a group space template:

1. Log in to WebCenter Spaces with administrative privileges.

   See Section 32.1, "Logging into WebCenter Spaces as an Administrator".

2. Click the **Administration** link at the top of the application.
3. Click the **Group Spaces** tab.
4. Click the **Templates** subtab.
5. On the **Templates** page, from the **Actions** menu, choose:
   - **Publish Group Space Template** to share the template with everyone.
   - **Make Group Space Template Private** to remove the template from the group space template list. The template owner can use the template, but nobody else will see it.
6. Confirm your selection.

> **Note:** The seeded (out-of-the-box) templates can be made private and published by the WebCenter Spaces administrator or users granted the `Group Space Templates - Manage` permission. If made private, they cannot be seen on the **My Group Spaces > Templates** page; they can only be seen on the **WebCenter Administration > Group Spaces > Templates** page.

37.5.4 Deleting a Group Space Template

WebCenter Spaces administrators with the `Group Space Templates-Manage` permission can delete any group space template except the seeded (out-of-the-box) templates: Blank, Community of Interest, Group Project.

To delete a group space template that is no longer required:

1. Log in to WebCenter Spaces with administrative privileges.

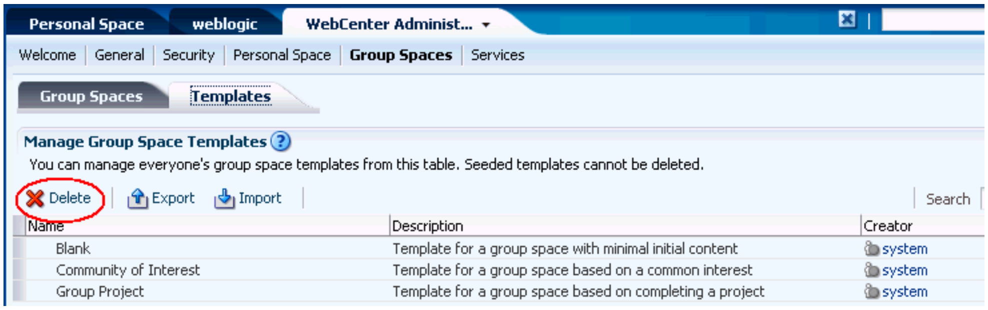
   See Section 32.1, "Logging into WebCenter Spaces as an Administrator".

2. Click the **Administration** link at the top of the application.
3. Click the **Group Spaces** tab.
4. Click the **Templates** subtab.
5. On the **Templates** page, select the required template by highlighting the row in the table.

   Ctrl-Click rows to select more than one template.

6. Click the **Delete** icon (Figure 37–9) or choose **Delete Group Space Template** from the **Actions** menu.

Figure 37–9 Deleting a Group Space Template



Manage Group Space Templates

You can manage everyone's group space templates from this table. Seeded templates cannot be deleted.

Name	Description	Creator
Blank	Template for a group space with minimal initial content	system
Community of Interest	Template for a group space based on a common interest	system
Group Project	Template for a group space based on completing a project	system

7. Click **Yes** to confirm that you want to delete the selected template(s).

37.6 Troubleshooting

This section includes troubleshooting information in the following sections:

- Section 37.6.1, "Troubleshooting WebCenter Spaces Workflows"
- Section 37.6.2, "Troubleshooting Service Provisioning Issues"

37.6.1 Troubleshooting WebCenter Spaces Workflows

If you experience issues with WebCenter Spaces workflows, review the following sections:

- Section 37.6.1.1, "Validating the WebCenter Workflow Configuration"
- Section 37.6.1.2, "Troubleshooting Issues with WebCenter Spaces Workflows"

37.6.1.1 Validating the WebCenter Workflow Configuration

The *Oracle Fusion Middleware Installation Guide for Oracle WebCenter* describes how to install and configure WebCenter Spaces workflows. For details, see "Back-End Requirements for WebCenter Spaces Workflows". You can validate the workflow configuration as follows:

1. Log in to WebCenter Spaces.
2. Create a group space and then navigate to the **Members** tab (group space settings).
3. Invite a new member with any role (say `User2`).
4. Log out, and then log in to WebCenter Spaces as `User2`.
5. Expand **Worklist** in the sidebar.
6. Open the invite notification and click the **Accept** button.
7. Open **My Group Spaces**.

If the WebCenter Spaces workflows are working properly, the newly created group space appears in **My Group Spaces** for `User2`. If the group space is not listed, there is some issue with the configuration.

37.6.1.2 Troubleshooting Issues with WebCenter Spaces Workflows

If WebCenter Spaces workflows are not working properly, follow these steps to help troubleshoot the issue:

1. Check that WebCenter Spaces workflows are deployed on the Oracle SOA server:

   a. Log in to Fusion Middleware Control.

   b. Check that **WebCenterWorklistDetailApp.ear** is deployed.

   c. Verify that **sca_CommunityWorkflows_rev1.0.jar** is deployed.

   See "Oracle SOA Server - Workflow Deployment" in *Oracle Fusion Middleware Installation Guide for Oracle WebCenter*.

2. Ensure the Web Service connection between the Oracle SOA server and WebCenter Spaces is secure:

   a. Check the alias in the keystore file on the Oracle SOA server.

   For example, use the following command to list the content of the keystore file on the Oracle SOA server:

   `keytool -list -v -keystore bpel.jks -storepass <password>`

   There should be an entry with:

   ```
   Alias name: webcenter_spaces_ws
   ```

   See "Oracle SOA and Oracle WebCenter - WS-Security Configuration" in *Oracle Fusion Middleware Installation Guide for Oracle WebCenter*.

   b. Verify that the credential stores for both WebCenter Spaces and Oracle SOA server are configured correctly.

   See "Updating the Credential Stores" in the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter*.

   c. Check that keystores exist at both ends of the connection, for example:

   - `webcenter.jks` (copied to WebCenter Spaces end)

   - `bpel.jks` (copied to Oracle SOA server end)

   For example, the following commands generate `webcenter.jks` and `bpel.jks`:

   ```
   keytool -genkeypair -keyalg RSA -dname
   "cn=webcenter,dc=us,dc=oracle,dc=com" -alias webcenter -keypass mypassword
   -keystore webcenter.jks -storepass mypassword -validity 360
   keytool -exportcert -v -alias webcenter -keystore webcenter.jks -storepass
   mypassword -rfc -file webcenter.cer
   keytool -importcert -alias webcenter_spaces_ws  -file webcenter.cer
   -keystore bpel.jks -storepass mypassword
   keytool -genkeypair -keyalg RSA -dname "cn=bpel,dc=us,dc=oracle,dc=com"
   -alias bpel -keypass mypassword -keystore bpel.jks -storepass mypassword
   -validity 360
   keytool -exportcert -v -alias bpel -keystore bpel.jks -storepass mypassword
   -rfc -file bpel.cer
   keytool -importcert -alias bpel -file bpel.cer -keystore webcenter.jks
   -storepass mypassword
   ```

   See "Generating the Keystores" in the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter*.

d. Configure role members for the `BPMWorkflowAdmin` application role in Oracle SOA server (`soa-infra`).

   When associating the domain with an identity store that does not contain the user `weblogic`, you must assign some other valid user to the application role `BPMWorkflowAdmin`. Use WLST commands to do this from the SOA Oracle home, for example, to assign a user named "monty" that exists in LDAP:

   ```
   cd $SOA_ORACLE_HOME/common/bin/
   wlst.sh

   connect('<admin username>','<admin password>',
   'mysoahost.us.oracle.com:7001')
   revokeAppRole(appStripe="soa-infra", appRoleName="BPMWorkflowAdmin",
   principalClass="oracle.security.jps.service.policystore.ApplicationRole",
   principalName="SOAAdmin")
   grantAppRole(appStripe="soa-infra", appRoleName="BPMWorkflowAdmin",
   principalClass="weblogic.security.principal.WLSUserImpl",
   principalName="monty")
   ```

   See "Security Commands" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

37.6.2 Troubleshooting Service Provisioning Issues

When you create a group space, an error similar to the following may display if provisioning a service exceeds the time allowed:

```
Group space created with the following warning(s) : Issues were faced while
provisioning the service(s) - List Service. Check the group space services
settings page if these services have been provisioned.
```

When a group space is created, services are provisioned in parallel in multiple threads. If provisioning a service exceeds the specified timeout, the thread is interrupted. The timeout may be exceeded due to time needed to copy the metadata when the latency between the midtier and the database is too high, network issues, database performance issues, and so on.

To check if the issue is due to exceeding the timeout, search the log file for a message similar to the following:

```
[2009-10-19T08:43:22.659+00:00] [WLS_Spaces] [WARNING] []
[oracle.webcenter.webcenterapp] [tid: [ACTIVE].ExecuteThread: '0' for queue:
'weblogic.kernel.Default (self-tuning)'] [userId: weblogic] [ecid:
0000IHfxTHMDScX_TtCCyc1Ar22000002f,0] [APP: webcenter] Concurr: The thread is
timed out in 5000 milisec. for oracle.webcenter.list:Execution timedout[[
    queued :   13 ms
    suspended :    0 ms
    running : 5787 ms
    timeout : 5000 ms
    service : oracle.webcenter.community
    resource : oracle.webcenter.list
    source : oracle.webcenter.concurrent.RunnableTask@43c4d1
             (oracle.webcenter.concurrent.RunnableTask)
    submission : 3
]]
```

In this case, the running time of 5787 ms exceeded the timeout of 5000 ms.

If possible, the root cause of the timeout should be addressed; for example, resolve networking or database performance issues. Once this is done, the group space can be created again and the error should not be encountered. If the performance cannot be improved and the error persists, the timeout value may be increased for the service encountering the error. Refer to Section A.4, "Tuning Oracle WebCenter Performance." and chapter "Oracle WebCenter Performance Tuning" in the *Oracle Fusion Middleware Performance and Tuning Guide* for more information on setting concurrency management parameters in `adf-config.xml`.

38 Exporting and Importing Group Spaces

Oracle WebCenter provides a set of export and import utilities that enable you to back up or move group space information between WebCenter applications, and stage or production environments. This chapter describes how to export and import group spaces and group space templates through WebCenter Spaces administration page. It includes the following sections:

- Section 38.1, "Exporting Group Spaces"
- Section 38.2, "Importing Group Spaces"
- Section 38.3, "Exporting Group Space Templates"
- Section 38.4, "Importing Group Space Templates"
- Section 38.5, "Troubleshooting Issues with Group Space Import and Export"

Fusion Middleware Administrators can also export/import group spaces and group space templates using WLST commands. To find out more about these WLST commands, how to migrate the back-end data associated with group spaces, and also how to export an entire WebCenter Spaces application, see Section 31.1, "Exporting and Importing WebCenter Spaces for Data Migration".

Audience

The content of this chapter is intended for WebCenter Spaces administrators. Users granted the WebCenter Spaces `Administrator` role or a custom role that grants the `Application-Manage` permission).

38.1 Exporting Group Spaces

WebCenter Spaces administrators can export group spaces and import them into other WebCenter Spaces applications. Group spaces must be taken offline, even if only temporarily, to prevent data conflicts during the export process. See, Section 37.3.1, "Taking Any Group Space Offline".

Group space information is exported into a single export archive (`.ear` file). The EAR file contains a metadata archive (`.mar` file) and, optionally, a single XML file containing group space security policy information. You can save export archives to your local file system or to a remote server file system.

For more information about what is exported, read Section 31.1.1, "Understanding WebCenter Spaces Export and Import"

The export process does not include data associated with external services such as Mail, Discussions, Announcements, Wikis, Blogs, Instant Messaging and Presence, Personal Event, and Documents, as all this data is stored on external servers. To learn how to move data associated with these services, refer to documentation for that product. See also, Section 31.1.7, "Migrating Back-end Components for Individual Group Spaces".

> **Note:** No icons, skins, images, out-of-the-box templates, or personalizations are exported. Personalizations are changes that individuals make to their personal view of a group space. See also, "Personalizing Your Page View" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

WebCenter Spaces administrators can export group spaces through WebCenter Spaces Administration as described here. Fusion Middleware administrators can also export group spaces using WLST commands. For details, see Section 31.1.9.2, "Importing Group Spaces Using WLST".

You can also export group space templates but this is a separate process. You cannot export group spaces and group space templates into a single archive. For details, see Section 38.3, "Exporting Group Space Templates".

To export one or more group spaces using WebCenter Spaces:

1. Login to WebCenter Spaces with administrative privileges.

   See Section 32.1, "Logging into WebCenter Spaces as an Administrator".

2. Click the **Administration** link at the top of the application.
3. Click the **Group Spaces** tab.
4. Click the **Group Spaces** subtab.
5. Select the group space required by highlighting the row in the table.

   To select multiple group spaces, **Ctrl-click** or **Shft-click** multiple rows.

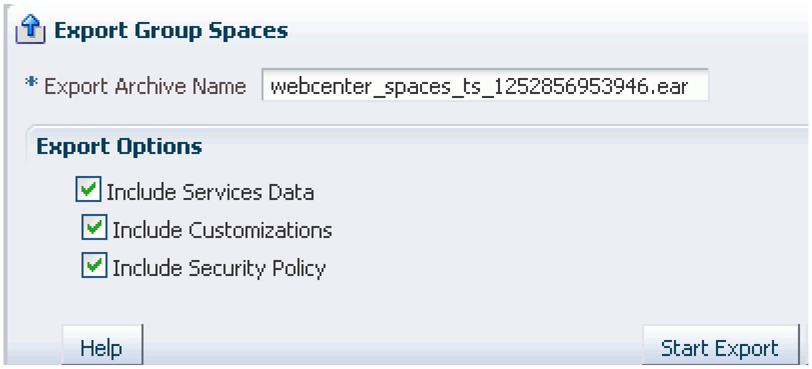
   Ensure that all the group spaces you select are *offline*. Group spaces must be taken offline, even if only temporarily, to prevent data conflicts during the export process. Unsaved changes are not exported. See also Section 37.3.1, "Taking Any Group Space Offline".

   > **Note:** Members with the `Group Space-Manage` permission should avoid editing group spaces that are taken offline during the export process.

6. Click **Export** in the toolbar.

   The Export Group Spaces dialog box opens (Figure 38–1).

Figure 38–1 Exporting Group Spaces



Export Group Spaces

* Export Archive Name: webcenter_spaces_ts_1252856953946.ear

Export Options

☑ Include Services Data

☑ Include Customizations

☑ Include Security Policy

7. Change the **Export Archive Name** or accept the default name.

   To ensure uniqueness, the default .ear filename contains a timestamp: `webcenter_spaces_ts_<timestamp>.ear`

8. Set export options as required. For details, see Table 38–1:

Table 38–1 Group Space Export Options

Field	Description

Include Services Data	Select to export the following
	■ Data stored in the WebCenter repository for the following services: Group Space Events, Lists, Links, Tags, People Connections
	■ Default settings for Profiles, Message Boards, Feedback, Connections, Activity Streams
	■ Activity Stream Task Flow Customizations
	If the group spaces selected for export contain a large amount of data, consider using the database export utilities to move the WebCenter schema data instead. For example:
	`DB_ORACLE_HOME/bin/expdp \"sys/password@serviceid as sysdba\" OWNER=srcrcuprefix_WEBCENTER FILE=/tmp/WCS.dmp STATISTICS=none`
	`DB_ORACLE_HOME/bin/impdp \"sys/password@serviceid as sysdba\" FROMUSER=srcrcuprefix_WEBCENTER TOUSER=tgtrcuprefix_WEBCENTER FILE=/tmp/WCS.dmp STATISTICS=none TRANSFORM=oid:n`
	For details, refer to the *Oracle Database Utilities* guide.
	Deselect this option if you do not want to export any data associated with lists, events, tags, links, and people connection services. For example, when moving a group space from a test environment to a stage or production environment where test data is not required.

Include Customizations	Select to export group space customizations. For information about which customizations are optional on export, see Table 31–3 and Table 31–4. If you deselect this option, WebCenter Spaces is exported without these group space customizations. Portlet and page customizations are always exported. See also Figure 31–1, "Information Exported with WebCenter Spaces".

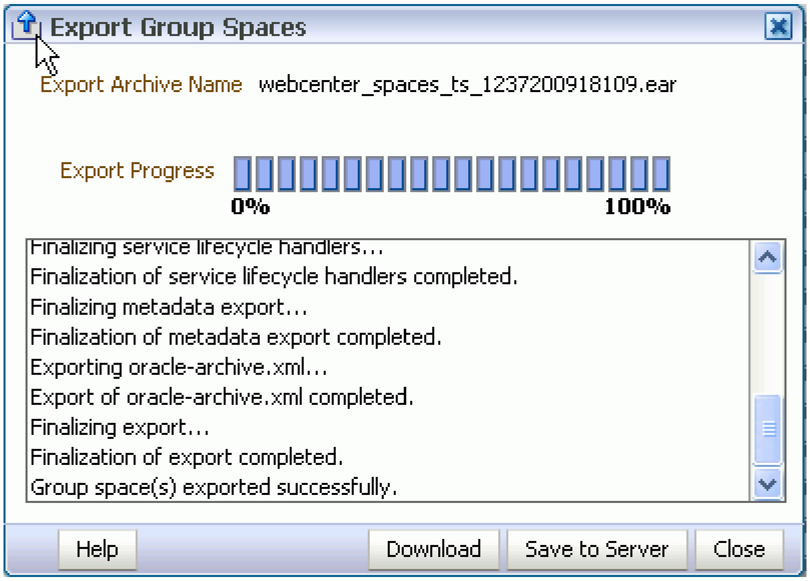
Table 38–1 (Cont.) Group Space Export Options

Field	Description
Include Security Policy	Select to migrate security information with the group space. When selected, an XML file is generated (`policy-store.xml`) containing the following security related information: ■ Group space roles (and permissions assigned to each role). ■ Group space members (and member role assignments). Deselect this option if you do not want to export group space security information. This option is useful when exporting group spaces between a stage and production environments, where: ■ Members used during testing are not required in the production environment. ■ The group space exists on the production instance and you do not want to overwrite the security information. **Note:** When exporting a brand new group space, always select (check) this option as you cannot import a new group space without a security policy.

9. Click **Start Export**.

   Progress information is displayed during the export process (Figure 38–2).

Figure 38–2 Exporting Group Spaces In Progress



Export Archive Name webcenter_spaces_ts_1237200918109.ear

```
Finalizing service lifecycle handlers...
Finalization of service lifecycle handlers completed.
Finalizing metadata export...
Finalization of metadata export completed.
Exporting oracle-archive.xml...
Export of oracle-archive.xml completed.
Finalizing export...
Finalization of export completed.
Group space(s) exported successfully.
```

10. When the export process is complete, specify a location for the export archive (.ear). Select one of:

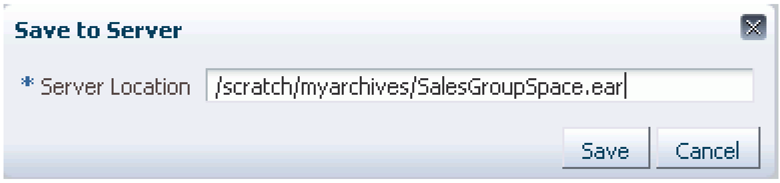
    - **Download** - Saves the export EAR file to your local file system.

      Your Browser downloads and save the archive locally. The actual download location depends on your Browser set up.

    - **Save to Server** - Saves the export .ear file to a server location.

When the Save to Server dialog box displays (Figure 38–3), enter a suitable path in **Server Location**, for example, `/tmp`, and then click **Save**. Ensure that the server directory you specify has `write` permissions.

Figure 38–3 Saving Group Space Export Archives to a Server Location



Save to Server

* Server Location: /scratch/myarchives/SalesGroupSpace.ear

11. Click **Close** to dismiss the Export Group Spaces window.

The export archive (.ear) is saved to the specified location.

38.2 Importing Group Spaces

WebCenter Spaces administrators can import a group space archive (.ear) into another WebCenter Spaces application.

On import, *all* group spaces included in the archive are created or re-created on the target application. Existing group spaces are deleted then replaced, and new group spaces are created.

All group spaces need a security policy to work properly so, when you import a brand new group space for the first time, you must ensure that the group space's security policy is included in the export archive. Existing group 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.

If data migration is important, group space documents, discussions, and wikis and blogs can be migrated for individual group spaces. For details, see Section 31.1.7, "Migrating Back-end Components for Individual Group Spaces".

WebCenter Spaces administrators can import group spaces through WebCenter Spaces Administration as described here. Fusion Middleware administrators can also import group spaces using WLST commands. For details, see Section 31.1.9.2, "Importing Group Spaces Using WLST"

To import one or more group spaces:

1. Login to WebCenter Spaces with administrative privileges.

   See Section 32.1, "Logging into WebCenter Spaces as an Administrator".

2. Click the **Administration** link at the top of the application.

3. Click the **Group Spaces** tab.

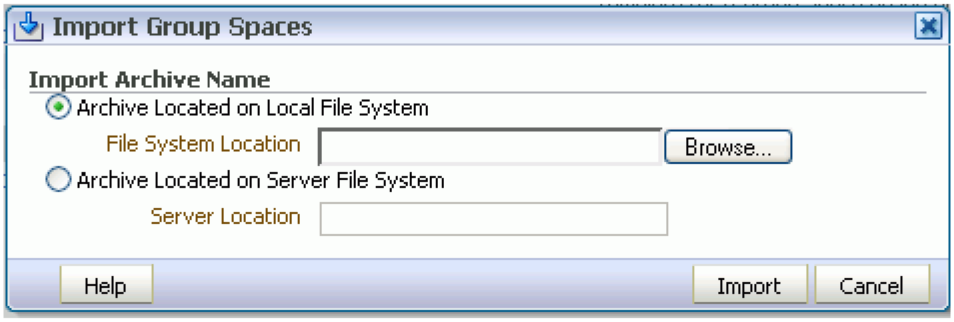
4. Click the **Group Spaces** subtab.

   Remember to take existing group spaces offline, before attempting to import a new version. For details, see Section 37.3.1, "Taking Any Group Space Offline".

5. Click **Import** in the toolbar.

   The Import Group Spaces dialog box opens (Figure 38–4).

Figure 38–4 Importing Group Spaces



Import Group Spaces

Import Archive Name

● Archive Located on Local File System

File System Location

○ Archive Located on Server File System

Server Location

6. Specify the location of your group space archive (.ear). Select one of:

   - **Archive Located on Local File System** - Enter the **File System Location**. Alternatively, click **Browse** to locate the directory on the local file system where the .ear file is stored.

   - **Archive Located on Server File System** - Enter the path, including the archive filename, in **Server Location**. For example, `/tmp/MyGroupSpaceExport.ear`. You can specify any shared location accessible from this WebCenter Spaces application.

7. Click **Import**.

   If you try to import group spaces that exist in the target WebCenter Space application, you must confirm whether you want to overwrite them. To delete existing group spaces and replace them with imported versions, answer **Yes**. Answer **No** to cancel the import process.

   If the import process detects a conflict between the group spaces you are trying to import and those which exist on the target, a message displays to help you resolve the issue. For example, conflict messages display if a group space on the target application has the same name but a different GUID to a group space you are trying to import. In this instance you could change the name of the source group space and create a new export archive, or rename the conflicting group space in the target application and import the same archive.

   An information message displays when all group spaces import successfully.

8. Click **Close** to dismiss the Import Group Space window.

Imported group spaces are *offline* initially because, mostly, some additional work is required before they are ready for general use. For example, you may want to migrate data associated with back-end components. For details, see:

Section 31.1.7.2, "Importing Discussions for a Group Space"

Section 31.1.7.4, "Importing Wikis and Blogs for a Group Space"

Section 31.1.7.5, "Exporting Documents for a Group Space"

Once content and membership details are finalized you may bring the group space online, see Section 37–4, "Bringing a Group Space Online".

38.3 Exporting Group Space Templates

WebCenter Spaces administrators can export group space templates and import them into other WebCenter Spaces applications. Out-of-the-box templates, such as the Group Project and Community of Interest templates, cannot be exported.

While export and import utilities are primarily used to move information between WebCenter Spaces applications, the group space template export feature is also useful as a backup service, and for sharing and exchanging templates with others.

Group space template information is exported into a single export archive (.ear file). The EAR file contains a metadata archive (.MAR file) and a single XML file containing group space security policy information.

Group space templates include pages, metadata, security information such as custom roles, and service information only; no data, such as documents, discussion threads, and list data, is stored with the template.

You can save export archives to your local file system or to a remote server file system.

WebCenter Spaces administrators can export group space templates through WebCenter Spaces Administration as described here. Fusion Middleware administrators can also export group space templates using WLST commands. For details, see Section 31.1.11.2, "Exporting Group Space Templates Using WLST",

> **Note:** You can also export group space information but this is a separate process. For details, see Section 38.1, "Exporting Group Spaces". You cannot export group spaces and group space templates into a single archive.

To export one or more group spaces templates using WebCenter Spaces:

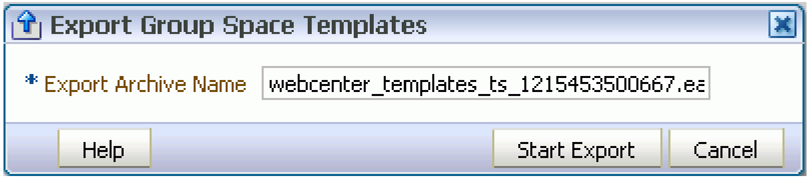
1. Login to WebCenter Spaces with administrative privileges.

   See Section 32.1, "Logging into WebCenter Spaces as an Administrator".
2. Click the **Administration** link at the top of the application.
3. Click the **Group Spaces** tab.
4. Click the **Templates** subtab.
5. Select the group space templates required by highlighting the row in the table.

   To select multiple group space templates, **Ctrl-click** the document rows.
6. Click **Export** on the toolbar.

   The Export Group Space Template dialog box opens (Figure 38–5).

Figure 38–5 Exporting Group Space Templates



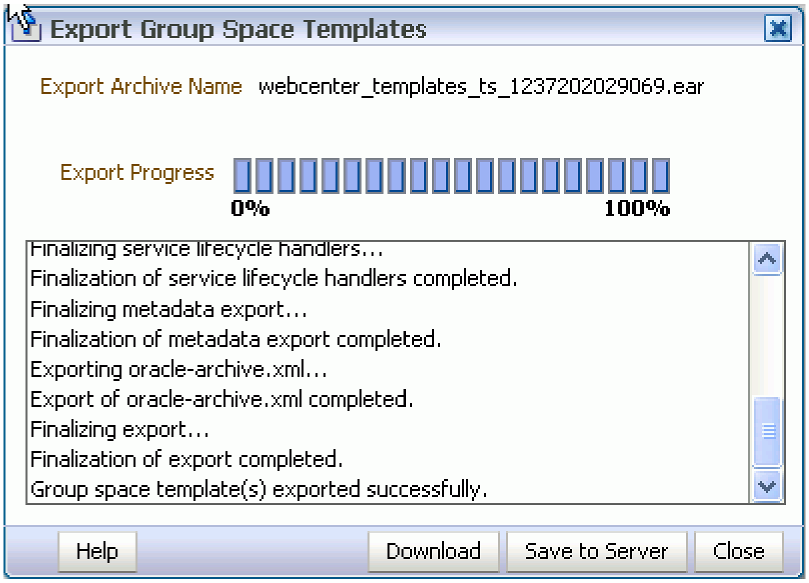
* Export Archive Name: webcenter_templates_ts_1215453500667.ea

7. Change the **Export Archive Name** or accept the default name.

   To ensure uniqueness, the default .ear filename contains a timestamp: `webcenter_templates_ts_<timestamp>.ear`
8. Click **Start Export**.

   Progress information is displayed during the export process (Figure 38–6).

Figure 38–6 Exporting Group Space Templates In Progress



Export Archive Name webcenter_templates_ts_1237202029069.ear

```
Finalizing service lifecycle handlers...
Finalization of service lifecycle handlers completed.
Finalizing metadata export...
Finalization of metadata export completed.
Exporting oracle-archive.xml...
Export of oracle-archive.xml completed.
Finalizing export...
Finalization of export completed.
Group space template(s) exported successfully.
```

9. When the export process is complete, specify a location for the export archive (.ear). Select one of:

   - **Download** - Saves the export EAR file to your local file system.

     Your Browser downloads and save the archive locally. The actual download location depends on your Browser set up.

   - **Save to Server** - Saves the export .ear file to a server location. For example, `/tmp`. Ensure that there are write permissions on the server directory that you specify.

     After clicking **Save to Server**, enter the **Server Location** and then click **Save**.

10. Click **Close** to dismiss the Export Group Space Templates window.

The export archive (.ear) is saved to the specified location.

38.4 Importing Group Space Templates

WebCenter Spaces administrators can import a group space template archive (.ear) into another WebCenter Spaces application.

On import, *all* group space templates included in the archive are re-created on the target application. If a group space template exists on the target, then it is deleted and replaced. If a group space template does not exist, then it is created.

Newly imported group space templates are not immediately available for general use. You must publish the imported templates to make them available to everyone. See Section 37.5.3, "Publishing and Hiding Group Space Templates".

WebCenter Spaces administrators can import group space templates through WebCenter Spaces Administration as described here. Fusion Middleware administrators can also import group space templates using WLST commands. For details, see Section 31.1.11.2, "Exporting Group Space Templates Using WLST".

To import one or more group space templates using WebCenter Spaces:

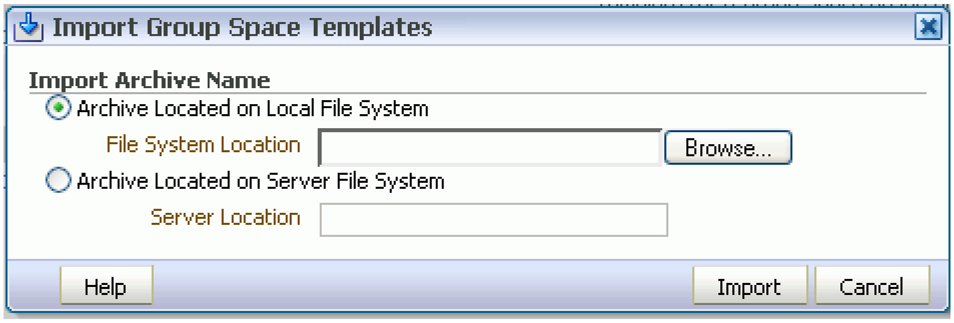
1. Login to WebCenter Spaces with administrative privileges.

See Section 32.1, "Logging into WebCenter Spaces as an Administrator".

2. Click the **Administration** link at the top of the application.
3. Click the **Group Spaces** tab.
4. Click the **Templates** subtab.
5. Click **Import** on the toolbar.

   The Import Group Space Templates dialog box opens (Figure 38–7).

Figure 38–7 Importing Group Space Templates



Import Group Space Templates

Import Archive Name

● Archive Located on Local File System

File System Location

○ Archive Located on Server File System

Server Location

6. Specify the location of your group space template archive (.ear). Select one of:
   - **Archive Located on Local File System** - Enter the **File System Location**. Alternatively, click **Browse** to locate the directory on the local file system where the .EAR file is stored.
   - **Archive Located on Server File System** - Enter the **Server Location**. Any shared location accessible from this WebCenter Spaces application.
7. Click **Import**.

   If you try to import a group space template that exists in the WebCenter Spaces application, you must confirm whether you want to continue. To delete existing group space templates and replace them with imported versions, answer **Yes**. Answer **No** to cancel the import process.

   An information message displays when all templates import successfully.
8. Click **Close** to dismiss the Import Group Space Templates window.

Newly imported group space templates are not immediately available for general use. You must publish the imported templates to make them available to everyone. See Section 37.5.3, "Publishing and Hiding Group Space Templates".

38.5 Troubleshooting Issues with Group Space Import and Export

This section contains the following subsections:

- Section 38.5.1, "ResourceLimitException Issue"
- Section 38.5.2, "Group Space Blocked After Unsuccessful Export or Import"
- Section 38.5.3, "Page or Group Space Not Found Message After Import"
- Section 38.5.4, "Group Space Import Archive Exceeds Maximum Upload File Size"
- Section 38.5.5, "Maximum Number of Group Spaces Exceeded on Export"
- Section 38.5.6, "Lists Not Imported Properly"

38.5.1 ResourceLimitException Issue

This section provides the solution to resolve the `ResourceLimitException` issue which occurs during export.

Problem

In WebCenter Spaces, you try to export all group spaces or entire application and the following error displays:

```
Weblogic.common.resourcepool.ResourceLimitException
```

Solution

You must increase the maximum capacity in the JDBC connection pool. To reconfigure the connection pool, log in to the WLS Administration Console. From **Services**, select **Data Sources**, **JDBC**, and then the **Connection Pool** tab.

38.5.2 Group Space Blocked After Unsuccessful Export or Import

If an error occurs during a group space export/import operation, some group space(s) may appear blocked. To unblock a group space, bring the group space back online temporarily, and then take the group space offline again to complete the export/import operation. Switching between the online and offline modes will unblock the group space

38.5.3 Page or Group Space Not Found Message After Import

When users first login to WebCenter Spaces after an import operation they may see a "Page not found" or "Group space not found" message if the page or group space they last visited no longer exists. Last accessed page information is retained during import operations which is why these messages display sometimes.

38.5.4 Group Space Import Archive Exceeds Maximum Upload File Size

Problem

There is a file size limitation uploading content to WebCenter Spaces. If your export archive exceeds the maximum upload size then the import operation through WebCenter Spaces administration will fail.

Solution

Import the group space archive using WLST. See Section 31.1.9.2, "Importing Group Spaces Using WLST".

Alternatively, modify the content repository upload parameter in `web.xml`. The default maximum upload size is 20 MB. See also, Editing web.xml.

38.5.5 Maximum Number of Group Spaces Exceeded on Export

Problem

The maximum number of group spaces that you can export must be less than or equal to 80% of the connection pool size specified for the MDS Data Source.

Solution

Export fewer group spaces or modify the connection pool setting. See also, the *JDBC Data Source* setting in Section A.4, "Tuning Oracle WebCenter Performance".

38.5.6 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 migrated 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.

Part VII

Appendix

Part VII contains the following appendix:

A
WebCenter Configuration

The main configuration files for Oracle WebCenter applications are `adf-config.xml` and `connections.xml`. This appendix describes both these files, how to locate them in a WebCenter application deployment, and also when to configure these files and which tools to use. Other configuration files, such as `web.xml`, are described here too. See also, Section 1.3.5, "Oracle WebCenter Configuration Considerations."

This appendix also outlines how to tune configuration properties for the operating system on which WebCenter applications are installed, WebCenter applications, and their back-end components.

This appendix includes the following sections:

- Section A.1, "Configuration Files"
  - Section A.1.1, "adf-config.xml and connections.xml"
  - Section A.1.2, "web.xml"
- Section A.2, "Cluster Configuration"
- Section A.3, "Configuration Tools"
- Section A.4, "Tuning Oracle WebCenter Performance"
- Section A.5, "Troubleshooting WebCenter 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 WebCenter applications and their back-end services. This section describes how WebCenter applications use each file and the location of these files post deployment. This section includes the following sub sections:

- adf-config.xml and connections.xml
- web.xml

A.1.1 adf-config.xml and connections.xml

`adf-config.xml` and `connections.xml` both store design time configuration information, such as the discussions server, mail server, or Oracle Content Server that is used by the WebCenter application in the development environment:

- **adf-config.xml** - Stores application-level settings, such as the which discussions server or mail server the WebCenter application is currently using.

See also, *Oracle Fusion Middleware Fusion Developer's Guide for Oracle Application Development Framework*.

- **connections.xml** - Stores connection details for WebCenter services.

  See also, *Oracle Fusion Middleware Fusion Developer's Guide for Oracle Application Development Framework*.

After you deploy a WebCenter application to a production environment, you can use Fusion Middleware Control or WLST commands to reconfigure some properties to meet your production requirements. For example, you can modify connection details to point to production server instances.

Any configuration changes that you make, post deployment, are stored as *customizations* in the WebCenter application's Oracle Metadata Services (MDS) repository. MDS uses the original deployed versions of `adf-config.xml` and `connections.xml` as base documents and stores all subsequent customizations separately into MDS using a single customization layer.

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

For information on MDS customizations, see "Understanding the MDS Repository" in *Oracle Fusion Middleware Administrator's Guide*.

Locating Base Documents

`adf-config.xml` and `connections.xml` are both located in the `/META-INF` folder for your application. In a WebCenter application deployment (.ear), you will find the base documents of these files under:

`DOMAIN_HOME``/servers/`*`server_name`*

For example, if the DOMAIN_HOME is *`MW_HOME`*`/wlshome/ /domains/wc_domain/`, both configuration files are located under *`MW_HOME`*`/wlshome/user_projects/domains/wc_domain/servers/WLS_Spaces`.

To determine the exact location, search for the configuration file under this folder. For example, enter the following at a command prompt:

```
> cd
MW_HOME/wlshome/user_projects/domains/wc_domain/servers/WLS_Spac
es
```

```
> find . -name adf-config.xml
```

A sample response, for this particular example, is as follows: `./tmp/_WL_user/webcenter/8gco54/adf/META-INF/adf-config.xml`

You can locate `connections.xml` in a similar way.

Reviewing Post Deployment Customizations in MDS

Post deployment, always use Fusion Middleware Control or WLST commands to review the latest configuration or make configuration changes. In Fusion Middleware Control you will mostly use WebCenter application configuration screens but a useful Systems MBean Browser is also available for reviewing configuration settings. These tools always show you the current configuration so, typically, there is no need for you to examine or change the content of base documents or MDS customization data for files such as `adf-config.xml` and `connections.xml`.

At times it might be useful to 'see' the information in MDS. If for any reason you must extract or examine configuration file customizations that are stored in MDS, use the WLST command `exportMetadata`.

> **See also:** For detailed syntax and examples, see "exportMetadata" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For example, to determine MDS customizations for `connections.xml` in WebCenter Spaces, where application name is always `webcenter`, the managed server is always `WLS_Spaces`, and the file name and location is always `/META-INF/mdssys/cust/adfshare/adfshare/connections.xml.xml`, you might specify:

```
exportMetadata(application='webcenter', server='WLS_Spaces',
toLocation='/tmp/mydata',
docs='/META-INF/mdssys/cust/adfshare/adfshare/connections.xml.xm
l')
```

And similarly, to determine MDS customizations for `adf-config.xml`:

```
exportMetadata(application='webcenter', server='WLS_Spaces',
toLocation='/tmp/mydata',
docs='/META-INF/mdssys/cust/adfshare/adfshare/adf-config.xml.xml
')
```

You choose where to save file customizations by specifying `toLocation`. If, for example, `toLocation` is set to `/tmp/mydata`, then the requested file is saved to `/tmp/mydata/META-INF/mdssys/cust/adfshare/adfshare`.

If no customizations exist for the requested file, then nothing is saved to the specified location—previously extracted customizations at the same location are not overwritten.

Handling Configuration Conflicts

MDS customizations use references to elements in the base document to call out which elements must be inserted/deleted/replaced, and at what location. If an element is inadvertently removed from a future redeployment and MDS contains a reference to that element, then the WebCenter application's configuration appears corrupt. You are unlikely to face this problem but should a previously deployed application appear corrupt after making changes to `adf-config.xml` or `connections.xml` you have the following options:

- Delete MDS customizations for `adf-config.xml` or `connections.xml`, deploy the new EAR file, and reconfigure your application from scratch using Fusion Middleware Control or WLST.

  See below for detailed steps, "Deleting MDS Customizations for adf-config.xml or connections.xml".

- Redeploy the EAR file on a new partition or a partition where older customizations are deleted. In either case, all data previously stored in MDS for the application is lost, including any customizations for `adf-config.xml` or `connections.xml`, and all user personalizations. You must reconfigure your application from scratch too, using Fusion Middleware Control or WLST.

  See also, "deleteMetadata" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

Deleting MDS Customizations for adf-config.xml or connections.xml

1. Delete customizations for `connections.xml`, using WLST. For example:

   ```
   deleteMetadata(application='webcenter', server='WLS_Spaces',
   docs='/META-INF/mdssys/cust/adfshare/adfshare/connections.xml.xml')
   ```

2. Delete customizations for `adf-config.xml`, using WLST. For example:

   ```
   deleteMetadata (application='webcenter', server='WLS_Spaces',
   docs='/META-INF/mdssys/cust/adfshare/adfshare/adf-config.xml.xml')
   ```

3. Restart the WebCenter application.
4. Reconfigure your application from scratch using Fusion Middleware Control or WLST.

A.1.2 web.xml

`web.xml` is a standard J2EE application deployment descriptor file and it is located in the `/META-INF` directory for your application. Typical run-time settings in `web.xml` include initialization parameters, custom tag library locations, and security settings.

Unlike `connections.xml` and `adf-config.xml`, `web.xml` does *not* store post deployment customizations in MDS.

Locating web.xml

To determine the exact location of `web.xml` in a particular WebCenter application deployment, search for the configuration file under:

`DOMAIN_HOME``/servers/`*`server_name`*

For example, if the DOMAIN_HOME is *`MW_HOME`*`/wlshome/user_projects/domains/wc_domain/`, web.xml is located under *`MW_HOME`*`/wlshome/user_projects/domains/wc_domain/servers/WLS_Spaces`.

For example, enter the following at a command prompt:

```
> cd
MW_HOME/wlshome/user_projects/domains/wc_domain/servers/WLS_Spac
es
```

```
> find . -name web.xml
```

A sample response, for this particular example, is as follows:

```
./tmp/_WL_user/webcenter/8gco54/adf/META-INF/web.xml
```

Editing web.xml

You cannot use Fusion Middleware Control or WLST to modify `web.xml` in an existing WebCenter application deployment. If you must modify settings in `web.xml` you will have to do so manually, as described in Appendix A.3.2, "Editing Configuration Files Manually".

The are several instance 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 11.9, "Changing the Maximum File Upload Size".

- **Time after which HTTP sessions expire**. For details, see Tuning Oracle WebCenter Performance.
- **JSP page timeout value**. For details, see Tuning Oracle WebCenter Performance.

A.2 Cluster Configuration

All post deployment configuration through Fusion Middleware Control, WLST, or the Systems MBean Browser is stored as customizations in the MDS repository. In a cluster environment, all configuration changes are visible to all nodes in the cluster. To effect configuration changes that are not dynamic, all nodes in the cluster must be restarted. See also Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments".

In WebCenter applications most configuration changes that you make, through Fusion Middleware Control or using WLST, are not dynamic. For example, when you add or modify connection details for Web services (Announcements, Discussions, Documents, Mail, Instant Messaging and Presence, Search, Worklists) you must restart the application's managed server.

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

If you edit configuration file manually in a cluster environment, then you must ensure that identical changes are made in each cluster member so that the overall cluster configuration remains synchronized.

A.3 Configuration Tools

Oracle offers a range of tools for configuring WebCenter application deployments. This section outline which tools are available and in case you cannot use these tools, describes how to edit configuration files manually.

> **Note:** Most of the WebCenter configuration parameters are immutable and cannot be changed at run time unless otherwise specified.

This section includes the following sub sections:

- Section A.3.1, "Configuration Through Fusion Middleware Control, WLST Commands, and System MBeans Browser"
- Section A.3.2, "Editing Configuration Files Manually"

A.3.1 Configuration Through Fusion Middleware Control, WLST Commands, and System MBeans Browser

Post deployment, always use Fusion Middleware Control or WLST commands to review the latest configuration or make configuration changes. In Fusion Middleware Control you will mostly use WebCenter application configuration screens but a useful Systems MBean Browser is also available for reviewing and modifying configuration settings.

For more information about these tools, read:

- Oracle Enterprise Manager Fusion Middleware Control Console
- Oracle WebLogic Scripting Tool (WLST)
- Oracle System MBean Browser

These tools always show you the current configuration so, typically, there is no need for you to examine or manually change the content of configuration files or MDS customization data for files such as `adf-config.xml` or `connections.xml`.

If you must edit these files directly, to set concurrency options for example, follow instructions in Appendix A.3.2, "Editing Configuration Files Manually" carefully.

A.3.2 Editing Configuration Files Manually

A few configuration settings, such as those stored in `web.xml`, are not exposed through MBeans, and therefore, you cannot use Fusion Middleware Control, WLST commands, or the System MBeans Browser for post deployment configuration.

If you must modify these settings, Oracle recommends that you re-create the WebCenter application deployment `.ear` file with the desired configuration, and redeploy the application. Sometimes this is not feasible or desirable—maybe you do not have access to the `.ear` file, or perhaps you must configure properties uniquely based on where the file is deployed—in this case, follow the manual steps below, using WLST:

1. Prevent the Weblogic Server from re-staging the WebCenter application, except at deployment time. From the WLST shell, type:

```
connect()
edit()
startEdit()
cd("DeploymentConfiguration/<domain_name>")
cmo.setRestageOnlyOnRedeploy(true)
activate()
```

2. Open the configuration file in a text editor and modify configuration properties manually, as required.

   Read Locating Base Documents to find out how to determine the exact location of `adf-config.xml`, `connections.xml`, or `web.xml`.

3. Restart the managed server on which the WebCenter application is deployed.

   See, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

> **Caution:** If you redeploy the WebCenter application in the future you must edit the configuration file again.

A.4 Tuning Oracle WebCenter Performance

Refer to the chapter "Oracle WebCenter 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 Performance Tuning

Performance Tuning	Parameters	File
Environment	System Limit	

Table A–1 (Cont.) WebCenter Performance Tuning

Performance Tuning	Parameters	File
	JDBC Data Source (settings for `MDSDS` and `WebCenterDS`)	
	JRockit virtual machine (JVM) arguments	`setDomainEnv.sh`
WebCenter Application	HTTP Session Timeout	`web.xml`
	JSP Page Timeout	`web.xml`
	ADF Client State Token	`web.xml`
	MDS Cache Size and Purge Rate	`adf-config.xml`
	Concurrency Management	`adf-config.xml`
	CRUD APIs (Create, Read, Update and Delete)	`adf-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 Content Server, and so on, should be tuned as described in guidelines for those back-ends.

A.5 Troubleshooting WebCenter Application Configuration Issues

This section includes the following sub sections:

- Section A.5.1, "WebCenter 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, "WebCenter Spaces Logs Indicate Too Many Open Files"

A.5.1 WebCenter Does Not Display in the Application Deployment Menu in Fusion Middleware Control

Problem

After logging into Fusion Middleware Control, you cannot find the **WebCenter** option in the **Application Deployment** menu.

Solution

Ensure the following:

- Deployed application is an ADF application.

  The **WebCenter** option does not display for applications that are not developed using ADF.

- Deployed application is up and running.

- Deployed application contains accurate information about 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>
  ```

  – `MDSBackingStore` is configured in the application's `adf-config.xml` file. This is provisioned at design time. This section can exist anywhere in the upper `adf-config` element, for instance, after the end tag of `adf-mds-config`. For example, see the text in **bold** in the following snippet:

  ```
  <jndiC:adf-jndi-config>
     <jndiC:ConnectionsJndiContext
  initialContextFactoryClass="oracle.adf.share.jndi.InitialContextFactoryImpl
  "
          backingStoreURL="META-INF/connections.xml"
  backingStoreClass="oracle.adf.share.jndi.MDSBackingStore">
     <jndiC:contextEnv value="true" name="cache_application_scope"/>
     </jndiC:ConnectionsJndiContext>
  </jndiC:adf-jndi-config>
  ```

  – Appropriate listeners exist in the `web.xml` file to register the MBeans. This is provisioned at design time. For example, see the text in **bold** in the following snippet of the `web.xml` file:

  ```
  <listener>
     <description>ADF Config MBeans</description>
     <display-name>ADF Config MBeans</display-name>
  ```

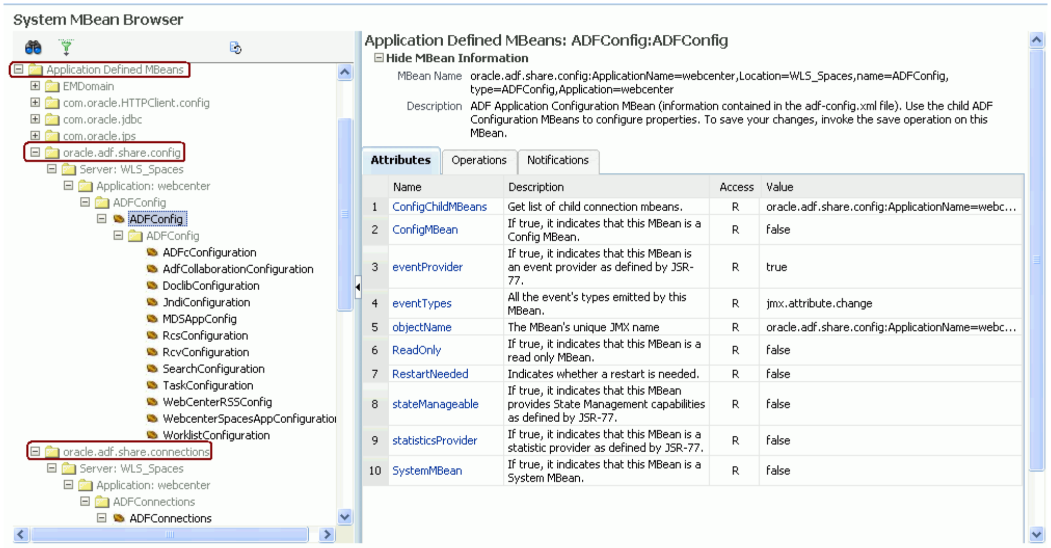
```
<listener-class>oracle.adf.mbean.share.config.ADFConfigLifeCycleCallBack</l
istener-class>
</listener>
<listener>
    <description>ADF Connection MBeans</description>
    <display-name>ADF Connection MBeans</display-name>

<listener-class>oracle.adf.mbean.share.connection.ADFConnectionLifeCycleCal
lBack</listener-class>
</listener>
```

- MBeans are registered for the WebCenter application. To verify this:

  1. In Fusion Middleware Control, from the **Application Deployment** menu, select **System MBean Browser**.
  2. Locate connection MBeans for your application under **Application Defined MBeans** > **oracle.adf.mbean.share.connection**.
  3. Similarly, locate `adf-config` MBeans for your application under **Application Defined MBeans** > **oracle.adf.mbean.share.config**. Figure 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



Application Defined MBeans: ADFConfig:ADFConfig

MBean Name oracle.adf.share.config:ApplicationName=webcenter,Location=WLS_Spaces,name=ADFConfig, type=ADFConfig,Application=webcenter

Description ADF Application Configuration MBean (information contained in the adf-config.xml file). Use the child ADF Configuration MBeans to configure properties. To save your changes, invoke the save operation on this MBean.

	Name	Description	Access	Value
1	ConfigChildMBeans	Get list of child connection mbeans.	R	oracle.adf.share.config:ApplicationName=webc...
2	ConfigMBean	If true, it indicates that this MBean is a Config MBean.	R	false
3	eventProvider	If true, it indicates that this MBean is an event provider as defined by JSR-77.	R	true
4	eventTypes	All the event's types emitted by this MBean.	R	jmx.attribute.change
5	objectName	The MBean's unique JMX name	R	oracle.adf.share.config:ApplicationName=webc...
6	ReadOnly	If true, it indicates that this MBean is a read only MBean.	R	false
7	RestartNeeded	Indicates whether a restart is needed.	R	false
8	stateManageable	If true, it indicates that this MBean provides State Management capabilities as defined by JSR-77.	R	false
9	statisticsProvider	If true, it indicates that this MBean is a statistic provider as defined by JSR-77.	R	false
10	SystemMBean	If true, it indicates that this MBean is a System MBean.	R	false

- 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 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 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 application, but those configurations also show in another application.

Solution

This happens when multiple applications share the MDS partition in the same schema. To resolve this problem, deploy these applications again and ensure that each application uses its own MDS schema and partition combination. For information about creating a MDS repository or configuring an existing WebCenter application to use a different MDS repository or partition, see section "Managing the Oracle Metadata Repository" in *Oracle Fusion Middleware Administrator's Guide*.

A.5.4 WebCenter Spaces Logs Indicate Too Many Open Files

Problem

WebCenter 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 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"

A.6.1 None of the WLST Commands Work

Problem

You are unable to run any WLST commands.

Solution

Ensure the following:

- No files other than Python are stored in the WLST source directory: *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 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 WLST Commands Work."

If generic commands work, then run test commands to check WebCenter-specific commands for syntax errors. Run the appropriate WSLT check command (see Table A–2).

See also, Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool (WLST) Commands."

Table A–2 File Names and WLST Commands for WebCenter Service

Service Name	File Name	WLST Command
Discussions and Announcements	`ForumWLST.py`	`fcpCheck()`
Documents	`DoclibWLST.py`	`doclibCheck()`
External Applications	`ExtAppWLST.py`	`extCheck()`
Group Space Events	`CommunityWLST.py`	`ceCheck()`
Instant Messaging and Presence	`ImpWLST.py`	`rtcCheck()`
Mail	`MailWLST.py`	`mailCheck()`
Producer Help	`ProducerHelperWLST.py`	`producerHelperCheck()`
WSRP Producers	`WsrpWLST.py`	`wsrpCheck()`
PDK Producers	`PdkWLST.py`	`pdkCheck()`

Table A–2 (Cont.) File Names and WLST Commands for WebCenter Service

Service Name	File Name	WLST Command
RSS News Feed	`RSSWLST.py`	`rssCheck()`
Search	`SesWLST.py`	`sesCheck()`
Worklist	`BpelWLST.py`	`bpelCheck()`
WebCenter Spaces and SOA	`WebCenterSpacesSOAWLST.py`	`spaceCheck()`
Export/Import - WebCenter application	`LifecycleWLST.py`	`lifecycleCheck()`
Export/Import - Group Spaces and Template	`ExtImpWLST.py`	`expimpCheck()`
WebCenter Help	`WebCenterWLSTHelper.py`	`basicCheck()`

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 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 1.12.3.1, "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 1.12.3.1, "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 1.12.3.1, "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.

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.

ADF

Application Development Framework. A range of technologies aimed at making **Java EE** application development faster and simpler for developers while at the same time taking advantage of proven software patterns to ensure that the developed application is scalable, performant, and the like.

administrator

In WebCenter Spaces there are two types of administrator:

- Fusion Middleware administrator: Also referred to as systems administrator. A user with complete administrative capabilities. This administrator can perform the complete range of security-sensitive administrative duties, and all installation, configuration, and audit tasks.
- WebCenter Spaces administrator: A WebCenter Spaces user who is responsible for customizing WebCenter Spaces out of the box, managing and granting application roles, and maintaining the application when it is in use.

Ajax

A combination of asynchronous JavaScript, dynamic HTML (DHTML), XML, and XmlHttpRequest communication channel that 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.

Announcements service

A WebCenter service that offers a quick, convenient way to create and widely distribute messages instantly or at a specific time.

API

Application Programming Interface. A set of exposed data structures and functions that an application can use to invoke services on an application object, such as a **portlet**.

Application Development Framework

See **ADF**.

application lifecycle

The process of creating and testing an application in a design time environment, deploying it to a production system, and then performing routine maintenance, such as monitoring performance and migrating customization data. The lifecycle of an application also includes performing further enhancements, restaging, and then redeploying the application to the production system.

Application Programming Interface

See **API**.

application role

Roles that are specific to a particular application and are stored in an application-specific stripe of the policy store.

application skin

Specifies the WebCenter Spaces application background color, screen fonts, and, with some skins, the shapes and images used for application buttons and icons. The WebCenter Spaces administrator chooses the default application skin. WebCenter users may change the application skin on the General tab of the Preferences dialog.

Applications pane

An area of the WebCenter Spaces Sidebar that provides convenient access to your frequently used applications. See **Sidebar**.

authenticated user

A user who is logged into a **custom WebCenter 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 **portlet**s, this user must be authorized through the policy and credential store.

Contrast with **public user**s, who are not logged in, and can access public content only.

authentication

Identification of a user through an identity management system. You can require ADF authentication to enforce credentials for users to access the WebCenter application only (all ADF resources in the application remain accessible), or authentication *and* authorization to enforce credentials for users to access the WebCenter application and any ADF resources that have been secured in the application.

authorization

The policies that define the access rights of an individual or group to a secured resource. This resource may be a page or component within a page.

authorized user

An individual who has access to a secured resource. For non-public resources, this individual is also an **authenticated user**.

Blog service

A WebCenter service for integrating blogs into WebCenter applications.

blog page

A page that provides a personal record of an individual user's experience and opinions. There are two kinds of blog: personal blogs are written by an individual; group blogs are written by several users.

Box layout component

An Oracle Composer layout component. A container that enables the placement of content on a WebCenter Spaces page. In Oracle Composer, a Box is rendered as a rectangle comprised of dashed lines. For designers of custom WebCenter applications, this is the runtime equivalent of a Panel Customizable component.

BPEL

Business Process Execution Language. An XML-based markup language for composing a set of discrete web services into an end-to-end process flow.

business role page

A page, created by the WebCenter Spaces administrator, specifically provided for a given role in an organization. Business role pages provide a targeted environment for users of a particular role by delivering information that is timely and relevant to individual roles without the noise of irrelevant information from other lines of business. Business role pages appear in the personal spaces of users classified under the specified role.

caching

The act of storing frequently accessed information, typically web pages, in a location where it can be accessed quickly to avoid frequent content generation.

See also **expiry-based caching** and **validation-based caching**.

calendar overlay

The ability to display multiple calendars in a single Events task flow.

Change Mode Button component

A component provided in the Oracle 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 Oracle 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.

Community of Interest group space

A **group space** created using the Community of Interest template. This type of group space provides an optimal structure for supporting communities of people, joining together to learn more about a subject area through the sharing of expertise, ideas, and content.

component

An individual piece of an application, for example, a task flow, portlet, page, or layout element such as a box or image.

Component Catalog

A dialog, accessed from Oracle Composer, that provides access to all the content you can add to a WebCenter application page.

component developer

The developer who builds components (such as portlets, **JavaServer Faces** components, and web services).

Component Properties

A dialog, accessed from Oracle Composer, that provides access to a component's parameters, display options, child components, style settings, and associated events.

Connections

In the **People Connections service**, a feature for establishing a social network with other application users.

container

An application program or subsystem in which the program building block, known as a **component**, is run.

content integration services

Services provided by **Oracle WebCenter** to enable developers to display content from a **content repository**, such as by creating **data control**s.

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 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 **custom WebCenter 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 though a content repository. In a **custom WebCenter application**, you can create content repository data controls for the following content repositories: **Oracle Portal**, **Oracle Universal Content Management**, 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

Specifies group space information in addition to that provided by the built-in attributes. Custom attributes can be used to determine the content of the components in a group space based on the parameter passed in. For example, a component can display data for a specific customer by passing in the customer ID. A custom attribute is simply a name value pair, for example customerId=400, orderId=11, userName=Smith, and so on. Custom attributes are stored within the group space template.

custom page

Any page created by a user rather than one provided out of the box.

custom resource catalog

A resource catalog that has been customized to control the components that are visible to specific users.

Contrast with **default resource catalog**.

custom role

A user role created by an administrator or a group space moderator to meet a specific personal space or group space requirement.

custom WebCenter application

A custom WebCenter application is built on top of the ADF using the **WebCenter 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 custom WebCenter application based on their roles and skill levels in the organization. See **WebCenter application**.

Customize mode

A **portlet mode** that enables users to set the default values for portlet preferences for all users.

customizable component

A WebCenter component that can be added to a page at runtime to enable end users to perform personalizations such as move, minimize, restore, or remove on content within those components. Customizable components are the **Panel Customizable component** and the **Show Detail Frame component**.

customization

An update that affects all users.

Contrast with **personalization**.

data control

A mechanism that provides an abstraction of the business service's data model. The ADF data controls provide a consistent mechanism for clients and web application controllers to access data objects, collections, methods, and operations.

See also **content repository data control**.

default language (application-level)

A display language specified by the WebCenter Spaces administrator that is used when users log in to WebCenter Spaces. The WebCenter 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 WebCenter Spaces. 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**.

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

WebCenter services provides a special deployment profile, the **custom WebCenter application** WAR deployment profile, that includes an option to export project metadata.

Design view (JDeveloper)

A view, in **Oracle JDeveloper**, that provides a WYSIWYG representation of a file.

See also **Source view (JDeveloper)**.

Design view (WebCenter Spaces)

A view, in **Oracle Composer**, that provides a WYSIWYG representation of a page and its components.

See also **Source view (WebCenter Spaces)**.

discoverable group space

A group space that can be found by anyone logged into WebCenter Spaces, for example through a search. A group space is made discoverable when the group space moderator enables the Discoverable setting. Discoverable group spaces are listed in My Group Spaces. Users wishing to join the group space can request membership through self-subscription (if enabled) or by contacting the group space moderator.

Discussions service

A WebCenter service that provides a means of creating and participating in text-based discussions with members of a particular group space.

display language

Controls the language in which application user interface elements, such as buttons, field labels, and screen text, are rendered in the browser. The order of precedence for WebCenter application display language settings from weakest to strongest is: browser setting, application setting, user preference setting, session setting, group space setting.

Document List Viewer task flow

A Documents service task flow that exposes a list of documents and, optionally, folders. The list is comprised of the contents of a specific folder or the results of a document search.

Document Manager task flow

A Documents service task flow that exposes all the folders and files available from the default content repository connection and default folder. Use to create, upload, and manage library content; to manage file versions; and to check files out and in.

Documents page

A predefined page provided in every WebCenter Spaces group and personal space that includes the **Document Manager task flow** for managing content.

Documents service

A WebCenter service that provides features for accessing, adding, and managing files; creating and managing file folders; configuring file and folder properties; and searching file and folder content.

The Documents service provides four task flows: Content Presenter, Document List Viewer, Document Manager, and Recent Documents.

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. **custom WebCenter applications** are deployed using both a generic EAR file, which contains the applicaiton 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 168** portlets only.) A **portlet mode** that enables personalization of a JSR 168 portlet. Edit Defaults mode is a display mode for the JSR 168 portlet's properties. In a **custom WebCenter application**, the Edit Defaults mode displays on the portlet's Actions menu as the Customize command.

See also **Edit mode**.

Edit mode

A **portlet mode** that enables personalization of the portlet for each user, for each instance.

See also **Edit Defaults mode**.

edit mode

A view mode that enables users to modify the content, style, and layout of a page. Access edit mode by choosing Edit Page from the Page Actions menu.

EL

Expression Language. Provides a 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 **custom WebCenter application**, EL expressions are encapsulated in the characters "#{" and "}" and typically come in the form #{object.data} where *object* represents any Java object or **ADF** component placed in the **Java EE** web container's page, request, session, or application's scope.

Enterprise Archive file

See **EAR**.

enterprise mashup

An application that enables users to bring all sorts of content and services together in a single place.

Events service

A WebCenter service that provides group calendars, which you can use to schedule meetings, appointments, and so on. You can integrate the Events service with a Microsoft Exchange Server to provide personal calendars for individual users. This service is available only in WebCenter Spaces, and not in custom WebCenter applications.

expiry-based caching

A **caching** method that uses a retention period to specify how long the item is valid in the cache before a refresh is required. When there is a request for the item beyond the retention period, it is refreshed in the cache.

See also **validation-based caching**.

Expression Language

See **EL**.

external application

Applications that do not delegate authentication to the single sign-on server. Instead, they display HTML login forms that ask for application user names and passwords. At the first login, users can choose to have the single sign-on server retrieve these credentials for them. Thereafter, they are logged in to these applications transparently.

farm

A collection of components managed by Fusion Middleware Control. A farm can contain a Managed Server domain and other Oracle Fusion Middleware system components that are installed, configured, and running on the domain.

favorites

A personal list of links to favorite WebCenter Spaces pages and external web sites.

Federated Portal Adapter

See **FPA**.

Feedback

In the **People Connections service**, a feature for posting informal appraisals for and receiving informal appraisals from other application users.

FOD

Fusion Order Demo. An enterprise application built using Oracle Fusion Middleware, including Oracle WebCenter, used to provide examples of WebCenter functionality.

FPA

Federated Portal Adapter. A component of **Oracle Portal** that enables Oracle Portal instances to share their database portlets through the web portlet interface. Using the FPA, Oracle Portal database portlets, including PL/SQL portlets, Portlet Builder portlets, and page portlets can be made available for use in WebCenter applications.

Full Screen Mode (WebCenter Spaces)

A view mode that opens the group space to occupy the entire screen, thus maximizing the display space. The Sidebar is not displayed in Full Screen Mode.

Full Screen mode (Portlets)

(**PDK-Java** portlets only.) A **portlet mode** that provides more content than can be shown in the portlet when it is sharing a page with other portlets.

Fusion Middleware Control

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

Fusion Order Demo (FOD)

See **FOD**.

Group Project group space

A group space created using the Group Project template. This type of group space provides an optimal structure for supporting a core project team where each member might come from a different department but all members contribute toward meeting a common goal.

group space

A work area within WebCenter Spaces that supports a group of people of any size that is organized around an area of interest or a common goal.

group space icon

An image displayed alongside group space names on the Group Spaces page in My Group Spaces to help other users with identification and location.

group space logo

An image displayed on the group space Home page to provide a visual identity for the group space. Group space logos also display alongside the group space name at the top of the page in Full Screen Mode.

group space member

A user who is participating in a group space. Members can be added or invited to a group space, or they can subscribe to a group space themselves if self-registration is enabled.

group space owner

A user who initially created a group space. The group space owner is automatically also a moderator of the group space.

group space template

A starting point for group space creation. WebCenter Spaces includes three templates to get you started: Group Project, Community of Interest, and Blank, but you can turn any group space into a template to use it as the starting point for other similar group spaces.

Group Space Unavailable page

A predefined page that displays when a group space member tries to open a group space that is temporarily offline. Moderators can customize this page.

HA

High Availability. A collection of solutions to ensure that your applications meet the required availability to achieve your business goals, eliminating single points of failure with no or minimal outage in service.

Help mode

A **portlet mode** that displays usage information about the functionality of the portlet.

High Availability

See **HA**.

HTML Markup layout component

An Oracle Composer layout component. A simple HTML component that renders raw HTML and JavaScript mark-up inline on the page.

Hyperlink layout component

An Oracle Composer layout component. A link to an internal or external web page. For designers of custom WebCenter applications, this is the runtime equivalent of a Go Link component.

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 custom WebCenter 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

An Oracle Composer layout component. An illustration that can include a hyperlink. For designers of custom WebCenter applications, this is the runtime equivalent of an Image Link component.

IMP service

See **Instant Messaging and Presence service**.

initialization parameters

The parameters initialized upon the start-up of a standard JSR 168 portlet. Initialization parameters provide an alternative to JNDI (Java Naming and Directory Interface) variables. Use initialization parameters instead of JNDI to configure the behavior of all of the different components of the portlet—for example, servlets and other portlets—in a compatible way. In **Oracle WebCenter**, initialization parameters are entered into the `portlet.xml` file.

Instant Messaging and Presence service

A WebCenter service that enables users to observe the presence status of other authenticated users and provides instant access to interaction options, such as instant messages, emails, and phone calls.

Integrated Development Environment

See **IDE**.

Integrated WLS

Integrated WebLogic Server. A WLS instance used as a platform for pretesting WebCenter application deployments on a local computer. Integrated WLS also contains preconfigured portlet producers and several useful prebuilt portlets.

JAAS

Java Authentication and Authorization Service (JAAS) is a Java package that enables applications to authenticate and enforce access controls upon users. JAAS is designed to complement Java 2 security and implements a Java version of the standard Pluggable Authentication Module (PAM) framework. This enables an application to remain independent from the authentication service, and supports the use of custom authentication modules.

JAAS extends the access control architecture of the Java 2 Security Model to support subject-based authorization. It also supports declarative security settings in deployment descriptors instead of being limited to code-based security settings.

Java Authentication and Authorization Service

See **JAAS**.

Java Content Repository

See **JCR 1.0**.

Java EE

Also known as Java EE 5. Java Enterprise Edition 5 Platform. A platform that enables application developers to develop, deploy, and manage multitier, server-centric, enterprise-level applications. The Java EE platform offers a multitiered distributed application model, integrated XML-based data interchange, a unified security model, and flexible transaction control. You can build your own Java EE portlets and expose them through web producers.

Java Enterprise Edition 5 Platform

See **Java EE**.

Java Portlet Specification

Standardizes how components for portal servers are to be developed. This specification defines a common portlet **API** and infrastructure that provides facilities for personalization, presentation, and security. Portlets using this **API** and adhering to the specification are product-agnostic, and can be deployed to any portal product that conforms to the specification. See also **JSR 168**.

Java Specification Request

See **JSR 168**.

JavaServer Faces

See **JSF**.

JavaServer Page

See **JSP**.

JCR 1.0

Java Content Repository 1.0. Also known as JSR 170. It proposes a standard access and interaction **API** for content repositories, much like JDBC does for databases.

JDeveloper

See **Oracle JDeveloper**.

JSF

JavaServer Faces. A standard Java framework for building web applications. It simplifies development by providing a component-centric approach to developing Java web user interfaces. JSF offers rich and robust **API**s that provide programming flexibility and ensures that applications are well designed with greater maintainability by integrating the Model-View-Controller (**MVC**) design pattern into its architecture. As JSF is a Java standard developed through Java Community Process, development tools like **Oracle JDeveloper** are fully empowered to provide easy to use, visual, and productive development environments for JSF.

JSF JSP

JavaServer Faces JavaServer Page. JSF JSPs differ from plain JSPs through their support of **Oracle ADF Faces** components for the user interface and JSF technology for page navigation. JSF JSP pages leverage the advantages of the Oracle **Application Development Framework** (Oracle ADF) by using the ADF Model binding capabilities for the components in the pages.

JSP

JavaServer Page. An extension to servlet functionality that provides a simple programmatic interface to web pages. JSPs are HTML pages with special tags and embedded Java code that is executed on the web or application server. JSPs provide dynamic functionality to HTML pages. They are actually compiled into servlets when first requested and run in the servlet container.

See also **JSP tags**.

JSP tags

Tags that can be embedded in **JSP**s to enclose Java code. These tags use the `<jsp:` syntax and enclose action elements in the JSP with `begin` and `end` tags similar to XML elements.

JSR 168

Java Specification Request (JSR) 168. Defines a set of **API**s for building standards-based portlets using Java. Portlets built to this specification can be rendered to a portal locally or deployed to a WSRP container for rendering portlets remotely. For more information, see `http://jcp.org/en/jsr/detail?id=168`.

JSR 170

See **JCR 1.0**

JSR 301

See **Oracle JSF Portlet Bridge**.

keystore

A file that provides information about available public and private keys that are used for authentication and data integrity. User certificates and the trust points needed to validate the certificates of peers are also stored securely in the keystore.

layout box

A container that enables placement of content on a WebCenter Spaces page.

layout component

An object for enhancing the usefulness and appearance of a given page. Layout components include layout boxes, a rich text editor, images, hyperlinks, and so on.

Layout Customizable component

A component provided in the Oracle Composer tag library that enables users to select from a set of predefined layouts (for example, two column, three column, two row, and so on) and apply it to the page. Users can apply these layouts to a particular area of the page or to the entire page.

LDAP

Lightweight Directory Access Protocol. A standard, extensible directory access protocol. It is a common language that LDAP clients and servers use to communicate. The framework of design conventions supporting industry-standard directory products, such as the Oracle Internet Directory.

lifecycle

See **application lifecycle**.

Lightweight Directory Access Protocol (LDAP)

See **LDAP**.

Links service

A WebCenter service that provides a means of creating a bidirectional association between two objects, thus setting up easy access between those objects.

List Manager

A task flow of the Lists service that provides access to all the tools for creating and revising lists and list content and to all of a group space's current lists.

Lists page

A predefined page that displays the group space's current lists.

Lists Viewer

A task flow of the Lists service that provides a means of placing a particular list on a group space page.

Mail service

A WebCenter service for exposing familiar email functionality in WebCenter applications.

Managed Server

In a production environment, a Managed Server hosts applications and the resources needed by those applications. A domain, which is a logically related group of Oracle WebLogic Server resources, can have any number of Managed Servers. An Administration Server manages these servers.

mashup

A web application that enables end users to pull information from different sources to create a personalized application that exactly meets their individual requirements.

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.

Model-View-Controller

See **MVC**.

moderator

A WebCenter Spaces user who is responsible for managing a particular group space. A group space moderator can add and remove members, invite new members, enable self registration, provide and update group space metadata, and manage the services available to the group space.

Movable Box layout component

An Oracle Composer layout component. A container that enables the placement of content on a WebCenter Spaces page. Movable Boxes, along with their content, can be moved around on the page. For designers of custom WebCenter 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 Group Spaces page

A predefined page that displays a list of all the group spaces and group space templates available to the currently logged in user. This includes group spaces of which the user is a member, group spaces marked as discoverable, and group spaces that are public and available to everyone.

navigation parameter

Parameters in a **WSRP** container that map to the render parameters with the same name in **JSR 168** portlet code. Navigation parameters are exposed by the portlet to the consumer. The consumer stores and manages parameter values and sends them on every invocation to the portlet. Navigation parameters are a WSRP version 2 feature.

Notes service

A WebCenter service that provides useful features for writing personal notes and reminders. This service is available only in WebCenter Spaces, and not in custom WebCenter applications.

OAM

See **Oracle Access Manager (OAM)**.

OHS

See **Oracle HTTP Server (OHS)**.

OmniPortlet

A component of **Oracle WebCenter** that enables you to inject portal-like capabilities, such as portlets, content integration, and customization, into your **Oracle ADF Faces** applications.

Oracle Access Manager (OAM)

Part of Oracle's enterprise class suite of products for identity management and security, Oracle Access Manager provides a wide range of identity administration and security functions, including several single sign-on options for WebCenter Spaces and WebCenter custom applications. OAM is the recommended single sign-on solution for Oracle WebCenter 11g installations.

Oracle ADF Faces

Oracle **ADF** Faces is a rich set of user interface components based on the new **JavaServer Faces** JSR (JSR 127). Oracle ADF Faces provide various user interface components with built-in functionality, such as data tables, hierarchical tables, and color and date pickers, that can be customized and reused in an application.

Oracle Composer

A seamlessly integrated environment for populating, revising, and configuring WebCenter application pages. It enables users to easily build or revise page layout and content. It also provides the means of adding different components, such as task flows, portlets, content, and other objects, onto a page and then linking those components for a more relevant or personalized view of the information.

Oracle Content Server

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 Content Server is a component of Oracle Universal Content Management.

Oracle WebCenter Discussions Server

Enables integration of discussion forums and announcements into WebCenter application.

Oracle Enterprise Manager

A component that enables administrators to manage Oracle Fusion Middleware services through a single environment. The Fusion Middleware administrator uses Enterprise Manager to configure, manage, and monitor WebCenter applications.

Oracle HTTP Server (OHS)

Software that processes web transactions that use the Hypertext Transfer Protocol (HTTP). Oracle uses HTTP software developed by the Apache Group.

Oracle Internet Directory

Oracle's LDAP V3 compliant LDAP server. It is used as 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 301, the Oracle JSF Portlet Bridge enables application developers to expose a JSF application or task flow as a JSR 168 portlet for consumption in another application.

Oracle Metadata Services

See **MDS**.

Oracle Portal

A component used for the development, deployment, administration, and configuration of enterprise class **portal**s. Oracle Portal incorporates a portal building framework with self-service publishing features to enable you to create and manage information accessed within your portal.

Oracle SES

Oracle Secure Enterprise Search (SES) provides easy-to-use search for public and secure data. It is included with **Oracle WebCenter**. You can override the default search adapters in WebCenter Spaces and use Oracle SES, which provides unified ranking results. The results are listed together, instead of being clustered into separate sections for Documents, Discussions, and so on, with the most relevant items appearing first.

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 SOA Suite

A middleware component of Oracle Fusion Middleware. Oracle SOA Suite enables services to be created, managed, and orchestrated into SOA composite applications. Composites enable you to easily assemble multiple technology components into one SOA composite application. Oracle SOA Suite plugs into heterogeneous infrastructures and enables enterprises to incrementally adopt SOA.

Oracle Technology Network

See **OTN**.

Oracle Universal Content Management

A consolidated content management application that provides multisite web content management, document management, digital asset management and records management.

Oracle WebCenter

A suite of services that enables you to build custom WebCenter applications. Oracle WebCenter reduces the front-end labor historically required to bring necessary business components to the user by capitalizing on the notion of Service Oriented Architecture (SOA). The suite includes a wide range of plug-and-play products, tools, and services that make it easy to build the applications your users need. Oracle WebCenter includes:

- **WebCenter services**
- **Oracle WebCenter Framework**
- **content integration services**
- **ADF**
- **Oracle SES**
- **Oracle WebCenter Discussions Server**
- Mobile Services
- Portlet Pack

Oracle WebCenter Framework

A set of features provided by **Oracle WebCenter** that augments the Java Server Faces (JSF) environment by providing additional integration and runtime customization options It is the basis of Oracle WebCenter and supports the creation and execution of context-rich applications, which can come in the form of human interaction, files and documents, or a clear representation of where the user is within a complex work process. It includes such features as:

- Portlet support
- **content integration services**
- **Oracle JSF Portlet Bridge**
- Search framework
- Customizable components

Oracle WebLogic Server Administration Console

A browser-based, graphical user interface to manage a WebLogic Server domain. Use to:

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

Oracle WebCenter Wiki and Blog Server

Supports integration of wikis and blogs into WebCenter applications. It also supports features that enable application users to create their own wikis and blogs.

OTN

Oracle Technology Network. The online Oracle technical community that provides a variety of technical resources for building Oracle-based applications. You can access OTN at `http://www.oracle.com/technology/`.

Page Customizable component

A component provided in the Oracle Composer tag library that defines the editable area of a page at runtime. Within this area, users can edit properties for a component, add content to the page, arrange content, and so on.

page parameter

A parameter 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 variable**s.

Page Properties

A dialog, accessed from Oracle Composer, that provides access to a page's display options, security settings, and parameters.

page scheme

Determines the background image used in the page. WebCenter Spaces provides several default page schemes and an option for specifying a custom page scheme.

Page service

A service for creating new pages and task flows in your application at runtime.

page style

Determines the initial page structure, for example one column or two column. Some default page styles also include the task flows, components, and page properties useful for a particular purpose. For example, a page created using the Text page style includes a Text layout component.

page variable

A variable that binds your public portlet parameter to the page. Page variables are defined within the `<variableIterator>` of your `PageDef.xml`. One page variable can be bound to multiple public portlet parameters.

Panel Customizable component

A component provided in the Oracle Composer tag library that provides a container region for a group of Oracle ADF components and portlets that are customizable at runtime. Any Show Detail Frame components and portlets added as child components to a Panel Customizable component can be moved or maximized with the Panel Customizable component.

parameter

A variable that controls the default behavior of task flow content and facilitates the wiring of a task flow to page parameters and page definition variables.

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 WebCenter Spaces user who can manipulate the content of a group space. A participant can upload and share documents, initiate and take part in chats with other members, create discussion topics, create new or view existing lists.

PDK-Java

Java Portlet Developer Kit. The development framework used to build and integrate web content and applications with **Oracle WebCenter**. It includes toolkits, samples, and technical articles that help make portal development simple. You can take existing Java **servlet**s, **JSP**s, URL-accessible content and web services and turn them into **portlet**s. It is typically used by external developers and vendors to create portlets and services.

People Connections service

A WebCenter 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

An update that affects only the user who made it.

personal page

A page created by a user in his or her personal space. Personal pages are viewable by other users only if specifically granted access by the user who created the page.

personal profile

A page that displays a user's personal information such as email address, phone number, office location, department, manager, direct reports, and so on.

See also, **Profile**.

personal space

A work area within WebCenter Spaces that provides individual users with a private space for storing personal content, keeping notes, viewing and responding to assignments, maintaining a list of online buddies, and performing many other tasks relevant to their unique working day. Users can also extend this environment by creating additional personal pages and custom content.

portal

A common interface (that is, a web page) that provides a personalized, single point of interaction with web-based applications and information relevant to individual users or class of users.

Portal Developer Kit

See **PDK-Java**.

portlet

A reusable web component that can draw content from many different sources. Portlets can display excerpts of other web sites, generate summaries of key information, perform searches, and access assembled collections of information from a variety of data sources. Because different portlets can be placed on a common page, the user receives a single-source experience, even though the content may be derived from multiple sources. Portlet resources include the many prebuilt portlets availble out of the box and programmatic portlets built through WebCenter's JSR 168, PDK-Java Portlet wizards, and other portlet building tools.

portlet mode

The ways by which a **portlet** can be called to display information. These methods include:

- **Shared Screen mode** or **View mode**
- **Edit mode** or **Edit Defaults mode**
- **Customize mode**
- **Help mode**
- **About mode**

- **Full Screen mode (Portlets)** or **Show Details Page mode**

Portlet Producer Application template

An application template, provided by JDeveloper, for creating an application with the recommended projects and technology scopes required for developing portlets. The Portlet Producer Application template consists of a single project scoped for portlet creation (Portlets).

See also **WebCenter Application template**.

predefined page

A page created by WebCenter Spaces to perform a specific function. Examples of predefined pages include, Welcome pages, Search pages, and Documents pages.

Predeployment Tool

A utility for **custom WebCenter application**s 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 **custom WebCenter application** or a **portal**). When a consumer application renders a portlet, it calls the producer of that portlet, which in turn executes the portlet and returns the results in the form of portlet content. A producer can contain one or more portlets. A portlet can be contained by only one producer.

Oracle WebCenter supports two types of producers:

- Oracle **PDK-Java** producers: Deployed to a **Java EE** application server, which is often remote and communicates through Simple Object Access Protocol (SOAP) over HTTP.
- **Web Services for Remote Portlets** (WSRP): A web services standard that enables the plug-and-play of visual, user-facing web services with portals or other intermediary web applications. Being a standard, WSRP enables interoperability between a standards-enabled container based on a particular language (such as **JSR 168**, .NET, Perl) and any WSRP portal. A portlet (regardless of language) deployed to a WSRP-enabled container can be rendered in any application that supports this standard.

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.

programmatic portlets

Portlets constructed in a non-declarative manner using **APIs**. Also referred to as *hand-* or *manually-coded* portlets.

public group space

A group space that is available to all users, even those who are not logged in to WebCenter Spaces.

public page

A page within WebCenter Spaces that is available to all users, even those who are not logged in to WebCenter Spaces.

public parameter

A portlet parameter that is known to the page and bound to it by way of a page variable.

Contrast with **private parameter**.

public user

A user who can access, but is not logged into, a **WebCenter application**. A public user can view any page that has been marked as public, but cannot personalize or edit any content, or view pages that have any form of access control.

Contrast with **authenticated user**.

Recent Activities service

A WebCenter service that provides a means of tracking recent activities in a WebCenter application.

Recent Documents task flow

A Documents service task flow that exposes the files most recently modified in some way.

resize handle

A user interface element in a task flow chrome increasing or decreasing the height of the task flow.

Resource Action Handling framework

Enables services that expose custom resources to be viewed, searched, and tagged.

Resource Catalog

A catalog that provides a federated view of one or more otherwise unrelated repositories in a unified search and browse user interface. Resources are created and published in their source repository and are then exposed to the developer in JDeveloper's Resource Palette and to the end user in the Resource Catalog Viewer. Resource catalogs can contain layout components, Oracle ADF components, portlets, service task flows, and documents.

Resource Index

The starting point for accessing WebCenter REST APIs. Sending a GET request to the Resource Index URI returns a list of links to entry points for all available services.

resource type

Defines the type of resource that a WebCenter 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 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 **WebCenter 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.

Rich Text portlet

A portlet, based on the **WSRP** standard, offering browser-based rich text editing at runtime on a deployed Oracle ADF **JavaServer Faces** JSP.

RSS service

A WebCenter service that provides a means of publishing content from other services as news feeds. The RSS service supports both RSS 2.0 and Atom 1.0 formats.

Search page

A predefined page for running searches, creating and managing saved searches, and viewing and refining search results.

Search service

A WebCenter service that enables the discovery of information and people in a WebCenter application, returning only the results users are authorized to see

Secure Enterprise Search

See **Oracle SES**.

secured application page

A page created by a user that has not been made available to public users.

Self-Registration page

A predefined page where users can register with WebCenter Spaces, thus creating themselves an 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 group 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 WebCenter 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 Oracle Composer tag library that renders a border or chrome around the child component. It provides a header with an Actions menu and thereby providers 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 mode**s encompassing **Show Page mode** and **Show Details Page mode**.

Show Page mode

A **portlet mode** that provides a smaller portlet display to allow space for additional portlets and other objects in the browser window. For example, a portlet in Show Page mode could be limited to displaying only the ten most recently submitted expense reports, while the same portlet in Show Details Page mode could show all submissions.

Contrast with **Show Details Page mode**.

Sidebar

A panel in WebCenter Spaces that provides quick access to tools and information essential to personal productivity, including mail, personal contacts, and so on.

skin

A style sheet based on the CSS 3.0 syntax specified in one place for an entire application. Instead of providing a style sheet for each component, or inserting a style sheet on each page, you can create one skin for the entire application.

SOA

Service Oriented Architecture. A design methodology aimed at maximizing the reuse of application services.

Source view (JDeveloper)

A view, in **Oracle JDeveloper**, that provides a way to directly edit the source code of a file.

Source view (WebCenter Spaces)

A view, in Oracle Composer, that provides a selectable structural representation of a page and its components.

See also Design view (WebCenter Spaces).

struts

A development framework for Java servlet applications based upon the **MVC** design paradigm.

style properties

Used to override the style information from the skin CSS to set specific instances of component display.

Tags service

A WebCenter service that enables users to apply their own terms to application objects, making it possible to search for those objects using personally meaningful terms.

task flow

A set of ADF Controller activities, control flow rules, and managed beans that interact to allow a user to complete a task. Task flows provide a modular approach for defining control flow in an application. Instead of representing an application as a single JSF page flow, developers can break it up into a collection of reusable task flows.

task flow header

An area at the top of a task flow that displays the task flow name and various tools for interacting with the task flow.

template

See group space template.

Text layout component

An Oracle Composer layout component. A rich text editor for providing static page text. For designers of custom WebCenter applications, this is the runtime equivalent of a Rich Text Editor component.

Unauthorized Access page

A predefined page that is shown when someone without access permission tries to open a page.

URL parameter

See **private parameter**.

validation-based caching

A **caching** method that uses a validation check to determine if the cached item is still valid.

Contrast with **expiry-based caching**.

viewer

WebCenter Spaces users who can look at the information in a group space but cannot contribute any of their own.

View mode

(**JSR 168** portlets only.) A **portlet mode** that enables you to display a JSR 168 portlet on a page that can contain other portlets. It is the only required mode for JSR 168 portlets.

See also **Shared Screen mode**.

WAR

Web application archive file. This file is used in deploying applications on a **Java EE** application server. WAR files encapsulate in a single module all of the components necessary to run an application. WAR files typically contain an application's **servlet**, **JSP**, and **JSF JSP** components.

See also **EAR**.

Web 2.0

Technologies, such as wiki, RSS, and blogs, that enable the construction of highly interactive web applications.

See also **WebCenter services**.

Web Application Archive file

See **WAR**.

Web Clipping

A browser based declarative tool that enables developers and page designers to integrate any Web content with a WebCenter application. It is designed to provide quick integration by leveraging the existing user interface.

Web Clipping portlet

A browser-based declarative tool that enables you to integrate any web application with your **custom WebCenter application**. It is designed to give you quick integration by leveraging the web application's existing user interface. You can drag and drop Web Clipping portlets onto a `*.jspx` page.

Web Page layout component

An Oracle Composer layout component. A means of embedding another web site, wiki, or blog within the context of a WebCenter Spaces page. For designers of custom WebCenter applications, this is the equivalent of an Inline Frame component.

Web server

A program that delivers web pages.

Web Services for Remote Portlets

See **WSRP**.

WebCenter

See **Oracle WebCenter**.

WebCenter application

WebCenter applications encompass both **custom WebCenter application**s and **WebCenter Spaces**.

WebCenter application administrator

The administrator responsible for maintaining the **WebCenter application**. For example, in WebCenter Spaces, the administrator performs tasks such as implementing the branding for the WebCenter application, making new content available, modifying pages, and granting and revoking privileges.

Contrast with 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 WebCenter application, and performing on-going administrative tasks for the WebCenter application and other WebCenter components through Fusion Middleware Control.

WebCenter application developer

The developer who plans, builds, and maintains a **custom WebCenter application** using the Oracle Application Development Framework, **Oracle JDeveloper**, and **Oracle WebCenter**.

WebCenter application end user

The WebCenter application end user is the runtime user of the **WebCenter application**, who accesses pages, portlets, and content, and personalizes portlets (assuming the appropriate privileges).

WebCenter Application template

An application template, provided by JDeveloper, for creating an application with the recommended projects and technology scopes required for developing a WebCenter application. The WebCenter Application template consists of a project for the data model (Model) and a project for consuming portlets, components, and data controllers (ViewController).

See also **Portlet Producer Application template**.

WebCenter Extension for Oracle JDeveloper

An extension available through the Oracle JDeveloper Update Wizard that installs the necessary libraries, templates, wizards, and dialogs needed to build and deploy **custom WebCenter application**s in **Oracle JDeveloper**.

WebCenter Framework

See **Oracle WebCenter Framework**.

WebCenter services

A collection of Web 2.0 services that expose social networking and personal productivity features through various services.

- Announcements service
- Blog service
- Discussions service
- Documents service
- Events service
- Instant Messaging and Presence service
- Links service
- Mail service
- Notes service
- People Connections service
- Recent Activities service
- RSS service
- Search service
- Tags service
- Wiki service
- Worklist service

WebCenter Spaces

A web-based application that offers the very latest technology for social networking, communication, collaboration, and personal productivity. WebCenter Spaces uses services and applications to bring everything together that users require to exchange ideas with others, keep track of personal and work-related tasks, interact with critical applications, and zero in on projects and interests; all within a single integrated environment.

WebCenter Spaces is a **WebCenter application**.

WebCenter Spaces application administrator

See administrator.

WebCenter Spaces RSS reader

An RSS reader provided with WebCenter Spaces that incorporates public news feeds from external sources onto application pages. This RSS reader is available only in WebCenter Spaces, and not in custom WebCenter applications.

WebCenter systems administrator

See administrator.

WebLogic Server

See **WLS**.

Welcome page

There are two types of Welcome page:

- Public Welcome page: A predefined page that users encounter before logging in to WebCenter Spaces.
- Personal Welcome page: A predefined page that introduces users to their personal space.

wiki page

A page that provides in-place editing using HTML or a simple mark-up language. Any user with sufficient privileges can add, revise, and remove wiki content.

Wiki service

A WebCenter service for integrating wiki pages in WebCenter applications.

WLS

WebLogic Server. A scalable, enterprise-ready Java Platform, Enterprise Edition (Java EE) application server. The WebLogic Server infrastructure supports the deployment of many types of distributed applications and is an ideal foundation for building applications based on Service Oriented Architectures (SOA).

See also **Integrated WLS**

WLST

WebLogic Scripting Tool. A command line tool for managing Oracle Fusion Middleware components, such as Oracle WebCenter.

Worklist service

A WebCenter service that provides access to notifications, alerts, and BPEL tasks assigned to the current user.

WSRP

Web Services for Remote Portlets (WSRP) is a web services standard that allows the plug-and-play of visual, user-facing web services with portals or other intermediary web applications. Being a standard, WSRP enables interoperability between a standards-enabled container based on a particular language (such as JSR 168, .NET, Perl) and any WSRP portal. A portlet (regardless of language) deployed to a WSRP-enabled container can be rendered on any portal that supports this standard.

XSL

Extensible Stylesheet Language (XSL) is the language used within style sheets to transform or render XML documents.

Index