Oracle® Fusion Middleware

Administrator's Guide for Oracle WebCenter Interaction

10*g* Release 4 (10.3.3.0.0)

E14107-05

May 2013

Describes how to perform administration tasks for Oracle WebCenter Interaction.

ORACLE

Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Interaction, 10*g* Release 4 (10.3.3.0.0)

E14107-05

Primary Author: Sarah Bernau

Contents

4 About User Interface Customization

5 Managing Administrative Objects and Portal Utilities

6 Managing Portal Users and Groups

7 Managing Portal Content

8 Extending Portal Services with Portlets

9 Providing Content and Services to Users through Communities

10 Managing Search

11 Automating Administrative Tasks

12 Migrating, Backing-Up, and Restoring Your Portal

A Configuring Portal Settings

F Default Behavior of Search Service

G Oracle WebCenter Console for Microsoft SharePoint

Preface

This guide describes how to perform initial tasks required to prepare Oracle WebCenter Interaction for use and how to perform ongoing portal management tasks.

Audience

This book is written for:

- **Portal administrators**: users who are part of the Administrators group, and therefore have complete access to all objects and utilities available through the Oracle WebCenter Interaction user interface
- **Administrative users**: users who have access to the Administration area of the portal and have limited activity rights to create objects (for example, users, documents, portlets)
- **System administrators**: user who are responsible for maintaining the portal hardware, integrating the portal with back-end systems (for example, single sign-on), and other advanced configuration outside of the Oracle WebCenter Interaction user interface

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

For more information, see the following documents in the Oracle WebCenter Interaction 10*g* Release 4 (10.3.3.0.0) documentation set:

- *Oracle WebCenter Interaction Release Notes*
- *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Interaction for Windows*

- *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Interaction for Unix and Linux*
- *Oracle Fusion Middleware Upgrade Guide for Oracle WebCenter Interaction for Windows*
- *Oracle Fusion Middleware Upgrade Guide for Oracle WebCenter Interaction for Unix and Linux*
- *Oracle Fusion Middleware User's Guide for Oracle WebCenter Interaction*

Conventions

The following text conventions are used in this document:

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

1

Completing Portal Initial Set-Up Tasks

When you first deploy your portal, you must perform several set-up tasks before your portal is ready for your users, such as configuring initial security, populating the portal with documents, and setting automated system maintenance.

1. Change the default Administrator password. To change the password, edit the Administrator user. For information on editing a user, see Section 6.2.4, "Specifying Authentication Settings for a User."

   WARNING: If you change the Administrator password, you must also update the password in the Oracle WebCenter Configuration Manager, on the Tagging Service: WCI Directory page. This value propagates to the Notification Service and the Activity Service. After changing the value in the Configuration Manager, you must restart the Tagging Service, the Notification Service, and the Activity Service.

2. Create administrative roles based on the business user needs in your company. For information on what roles are and how to create them, see Section 6.5.3, "Roles."
3. Configure display, navigation, and branding for the default experience definition and any additional experience definitions. For details, see Chapter 4, "About User Interface Customization."
4. Populate the portal with users, and configure groups, users, user profiles, and Access Control Lists (ACLs) to enable managed access. For details, see Chapter 6, "Managing Portal Users and Groups."
5. Populate the portal with documents, and configure ACLs to manage access. For details, see Chapter 7, "Managing Portal Content."
6. Set up automated system maintenance, such as user synchronization, search updates, document refresh, and housekeeping jobs. For details, see Chapter 11, "Automating Administrative Tasks."

After you have completed your initial portal deployment, you can extend your base portal deployment to include users from new authentication sources, new content types, documents from new content sources, or search among federated portals. You might optionally configure localization, single sign-on (SSO), and advanced configuration file settings.

2

Overview of Oracle WebCenter Interaction

This chapter provides an overview of portal components, the portal user interface, and portal security.

It includes the following sections:

2.1 Components Installed with the Portal

The following table describes the components available in the portal installer. For information on installing these components, refer to the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Interaction for Windows* or the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Interaction for Unix and Linux*.

Component	Description
Administrative Portal	The administrative portal handles portal setup, configuration, and content. It enables administrative functions, such as creating and managing portlets and other Web services.
Portal	The portal serves end user portal pages and content. It enables end users to access portal content through My Pages, community pages, the Knowledge Directory, and search. The portal also enables some administrative actions, such as setting preferences on portlets or managing communities.
Portal Database (scripts)	The scripts used to configure the database are included in the portal installer. The portal database stores portal objects, such as user and group configurations, document records, and administrative objects. The portal database does not store the documents available through your portal. Source documents are left in their original locations.
Automation Service	The Automation Service runs jobs and other automated portal tasks. You run jobs to perform tasks such as crawling documents into the Knowledge Directory, synchronizing groups and users with external authentication sources, and maintaining the search collection.
API Service	The API Service provides access to the SOAP API.

Component	Description
Image Service	The Image Service serves static content used or created by portal components. It serves images and other static content for use by the Oracle WebCenter Interaction system. Whenever you extend the base portal deployment to include additional components, such as portal servers or integration products, you may have to install additional Image Service files. For information on installing the Image Service files for those components, refer to the documentation included with the component software.
Search	The Search component indexes portal content such as documents, portlets, communities, and users as well as many other Oracle WebCenter objects.
Document Repository Service	The Document Repository Service stores content uploaded into the portal and Oracle WebCenter Collaboration.
Content Upload Service	The Content Upload Service lets you add files to the portal's Knowledge Directory by uploading them to the Document Repository Service, rather than leaving them in their original locations. This is useful if users must access documents located in an internal network from outside your network.
Directory Service	The Directory Service enables Oracle WebCenter Interaction to act as an LDAP server, exposing the user, group, and profile data in the portal database through an LDAP interface, enabling other Oracle WebCenter products (and other third-party applications) to authenticate users against the portal database.
Remote Portlet Service	The Remote Portlet Service includes the following components: ■ Activity Service The Activity Service includes the User Status portlet, which lets users post their current status; the User Activities portlet, which displays a user's status history and any other recent activities that are submitted by other applications; and a REST-based API for submitting activities into a user's activity stream. **Note**: If you use the REST-based API to submit other activities into the activity stream, those activities will also be displayed in the User Activities portlet. ■ Remote Portlets There are several portlets included with the Remote Portlet Service: Enterprise Poke, KD Browser, Last 5 Profile Viewers, My Picture, Online Now, Posted Links, Total Profile Views, RSS Reader, and Submit to KD.
Notification Service	The Notification Service enables the portal to send e-mail notifications to users upon specified events. There are no portal events that trigger notifications, but other Oracle WebCenter events do trigger notifications. For example, Oracle WebCenter Collaboration can be configured to send notifications to users when documents are uploaded.

Component	Description
Tagging Engine Service	The Tagging Engine is a collaborative information discovery and recovery system that provides personal and collective management of enterprise content, helping you more effectively locate, organize, and share information. You organize content by using tags, which are meaningful keywords that you and other people create and apply to items and people. If your administrator has enabled the auto-tagging feature, the system automatically tags items and people that fit the auto-tagging criteria. You can search for items and people by creating search queries that can include a combination of text, tags, and properties. Included with the Tagging Engine are several portlets to access tagging features: Tagging Engine Items, Tagging Engine People, Tagging Engine Search, Tagging Engine Tag Cloud, and Tagging Engine Results.
Search Service	The Search Service communicates tagging information between the portal, the Tagging Engine, and Oracle WebCenter Collaboration. It performs search queries and returns content to the requesting component (the Tagging Engine or Oracle WebCenter Collaboration).
Content Services	Content Services scan third-party systems/applications for new content, categorizing links to this content in the organized, searchable structure of the portal's Knowledge Directory. Users can then access this content through the portal user interface. ■ Documentum Content Service ■ UCM Content Service ■ Lotus Notes Content Service (Windows deployments) ■ Windows File Content Service (Windows deployments) ■ Exchange Content Service (Windows deployments)
Identity Services	Identity Services let you import users, groups, and user profile information from third-party user repositories into the portal. Identity Services also enable the portal to authenticate users through the third-party user repositories. ■ Microsoft's Active Directory (AD) ■ LDAP (Lightweight Directory Protocol)
Development Tools	■ Interaction Development Kit (IDK) The IDK enables Java and .NET developers to rapidly build, deliver, and enhance user-centric composite applications through Oracle WebCenter Interaction. It provides interfaces for Integration Web Services—authentication, profile, crawler, and search—that integrate enterprise systems into Oracle WebCenter Interaction. It provides SOAP-based remote APIs to expose portal, search, and Oracle WebCenter Collaboration features. In addition, the IDK has an extensive portlet API to assist in portlet development. ■ JSR 168 Container The Oracle WebCenter JSR-168 Container lets you deploy portlets in Oracle WebCenter Interaction that conform to the JSR-168 portlet standard. ■ Logging Utilities The Logging Utilities consist of a set of three tools to receive, display, and store logging messages sent from Oracle WebCenter Interaction products.

Component	Description
.NET Integration Services	Console for SharePoint (Windows deployments) Oracle WebCenter Console for Microsoft SharePoint imports, indexes, and returns Microsoft Windows Sharepoint Services resources through Oracle WebCenter Interaction Search.

2.2 Additional Oracle WebCenter Interaction Components

The following table describes components that provide additional functionality for the portal. For more information on these components or to download the components, visit the Oracle Support site at http://www.oracle.com/support/index.html.

Component	Description
Activity Services	Activity Services extend portal functionality to enable analysis, collaboration, publishing, and simple portlet creation. ■ Oracle WebCenter Analytics Oracle WebCenter Analytics Analytics delivers comprehensive reporting on activity and content usage within portals and composite applications, allowing you to know and meet user information needs. ■ Oracle WebCenter Collaboration Oracle WebCenter Collaboration helps people to work together through the web, supporting tasks, projects, communities, calendars, discussions, and document sharing with version control.
Enterprise Social Computing Products	Enterprise Social Computing Products provide tools that enable users to freely contribute and actively work together. ■ Oracle WebCenter Pagelet Producer Oracle WebCenter Pagelet Producer is an enterprise system that lets developers create reusable widgets for mashup applications and allows IT to easily manage a diverse set of Web resources.
Developer Tools	The following developer tools help you rapidly build applications through Oracle WebCenter Interaction: ■ Oracle WebCenter Portlet Toolkit for Microsoft .NET The Oracle WebCenter Portlet Toolkit for Microsoft .NET is used to speed the development of ASP.NET portlets for use with Oracle WebCenter Interaction. This product includes the .NET Portlet API and the .NET Web Control Consumer. The .NET Web Control Consumer enables you to create portlets using Microsoft .NET Web Controls, part of Oracle WebCenter Application Accelerator for Microsoft .NET. ■ Oracle WebCenter WSRP Producer for .NET If you want to deploy portlets in Oracle WebCenter Interaction that conform to the WSRP portlet standard, you need the Oracle WSRP Consumer and the Oracle WebCenter WSRP Producer. The Oracle WSRP Consumer is available as a standalone product. The Oracle WebCenter WSRP Producer is available as part of the Oracle WebCenter Application Accelerator for Microsoft .NET. ■ UI Customization Installer The User Interface Customization Installer (UICI) automates most of the steps required to set up a development environment for the portal. Minimal Eclipse and Ant configuration is still necessary. The UICI is for advanced applications, most UI customizations can be accomplished through adaptive functionality available with Oracle WebCenter Interaction.

2.3 Overview of the Browsing User Interface

This section provides an overview of the features available to browsing users. For details on these features, see the *Oracle Fusion Middleware User's Guide for Oracle WebCenter Interaction*.

This section includes the following topics:

2.3.1 Portal Banner

There are several features available at the top of your portal that provide access to some basic portal functions (such as help and search).

Feature	Description
Greeting	Lets you know that you are logged in as the correct user. By default your greeting is `Welcome, user name` where *user name* is the name of the user by which you are logged in.
Administration	Provides access to the Administrative Objects Directory, where you can create and manage portal objects and access portal utilities. **Note**: **Administration** appears only if you have the Access Administration activity right.
My Account	Lets you edit your user profile, display options, locale settings, and search preferences, as well as view your user profile and change your password. **Note**: You must have the Edit Own Profile activity right to be able to edit your user profile.
Help	Opens the help associated with the displayed page.
Log Off	Logs you out of your portal.
Search box and button	Let you search for documents, document folders, communities, community pages, portlets, and users in your portal.
Top Best Bet icon	Takes you directly to the top best bet result for the term you enter in the search box. If no top best bet has been set for the term, you will see the regular search results. **Note**: appears next to the search box only if enabled by portal developers.
Advanced Search	Lets you perform an advanced search by searching the portal for text or specific document properties.
Federated Search	Lets you perform a federated search (if any federated search resources have been configured by an administrative user) to search other content, portals, and Web search engines. **Note**: **Federated Search** appears only if enabled by portal developers.

2.3.2 Portal Menus

There are several menus available in the portal that provide access to information in your portal (such as communities and documents). Administrative users with the Create Experience Definition activity right and your portal developer control which menus appear, including custom menus.

Menu	Description
My Profile	Lets you view your user profile. User profiles provide information about users, such as address and position.
My Pages	Provides access to your My Pages. My Pages are your personalized view of the portal. You choose the applications, tools, and services (in the form of portlets) to display on each My Page. For example, you might create a My Page that includes a search tool for all the employees in your company and a portlet that displays the most recent news about your company.
My Communities	Lets you view and manage the communities to which you belong. Communities are sites within a portal designed for a specific audience or task, such as collaborative projects. You might have communities based on departments in your company. For example, the Marketing department might have a community containing press information, leads volumes, a trade show calendar, and so on. The Engineering department might have a separate community containing project milestones, regulatory compliance requirements, and technical specifications.
Directory	Provides access to the Knowledge Directory. The Knowledge Directory is similar to a file system tree in that documents are organized in folders and subfolders. A folder can contain documents uploaded by users or imported by content crawlers, as well as links to people, portlets, and communities. If your administrator has given you permission, you might also be allowed to add documents to the Knowledge Directory, or submit yourself as an expert on a particular topic.

2.3.3 Directing Users to Portal Areas with Friendly URLs

You can direct users to one of their My Pages, to a community, to a user profile, to a Knowledge Directory folder, to a document, or to search results with a simple URL, referred to as a friendly URL.

- To direct users to one of their My Pages, to a community, to a user profile, to a Knowledge Directory folder, or to a document, create a link in the following format: *http://portal.company.com/portal/server.pt/object_token/object_name/object_id*
  - Replace *http://portal.company.com/portal/server.pt* with the URL to your portal.
  - Replace *object_token* with the token for the type of object to which you are linking.

    The default values are: `mypage`, `community`, `user`, `directory`, and `document`, but you can customize them. For example, "directory" could instead be "folder."
  - Replace *object_name* with the name of the object. Replace any spaces in My Page, community, user, or Knowledge Directory folder names with underscores (_); replace any spaces in document names with plus signs (+).
  - Replace *object_id* with the ID of the object.

Note:

- Users must have at least Read access to the object to which you are directing them.
- If an object cannot be found, the user will receive an error message.
- If more than one object has the name specified in the link and an ID is not specified, the portal displays a list of objects with the same name and the user can select which one to view.

- To direct users to search results, create a link in the following format: *http://portal.company.com/portal/server.pt*/search?q=*search+term*[&num=*items*]
  - Replace *http://portal.company.com/portal/server.pt* with the URL to your portal.
  - Replace *search+term* with the term you want to search for, replacing any spaces with plus signs (+).
  - You can optionally specify the number of results to display per page. To do so, include the `num` element and replace *items* with the number of results you want to display per page.

2.4 Overview of the Administrative User Interface, Features, and Tools

The administrative user interface enables you to create and manage administrative objects and enables you to access portal utilities.

This section covers the following topics:

2.4.1 Portal Objects

The following table describes the portal objects you can create through the **Create Object** list in the Administrative Objects Directory.

Object	Description
Administrative Folder	Administrative folders provide a hierarchical structure that make it easy to organize portal objects and manage security.
Authentication Source - Remote	Authentication sources enable you to import users, groups, and group memberships that are already defined in your enterprise in existing user repositories, such as Active Directory or LDAP servers. After users are imported, you can authenticate them with the credentials from those user repositories.
Community	Communities are sites within a portal designed for a specific audience or task, such as collaborative projects.
Community Template	Community templates define the basic structure for the resulting communities, such as which page templates to include and, optionally, a header or footer for the community.

Object	Description
Content Crawler - Remote	Remote content crawlers enable you to import content from external content repositories such as a Windows NT file system, Documentum, Microsoft Exchange, or Lotus Notes.
Content Crawler - WWW	Web content crawlers enable you to import content from Web sites.
Content Source - Remote	Remote content sources provide access to external content repositories, such as a Windows NT file system, Documentum, Microsoft Exchange, or Lotus Notes.
Content Source - WWW	Web content sources provide access to Web sites.
Content Type	Content types specify several options — the source content format (such as Microsoft Office, Web page, or Lotus Notes document), whether the text of the content should be indexed for searching, and how to populate values for document properties.
Experience Definition	Experience definitions provide multiple user experiences within a single portal. An experience definition defines certain elements of a user experience, such as adaptive page layout settings, branding style, and navigation.
External Operation	An external operation enables you to run shell scripts (for example, .sh or .bat files) through the portal and schedule these actions through portal jobs. For example, you might want to create a script that queries documents, pings portal servers, e-mails snapshot query results to users, or runs some other custom job, then create an external operation that points to the script, and use a job to run the script on a specified schedule.
Federated Search - Incoming	An incoming federated search allows other Oracle WebCenter Interaction portals to search your portal.
Federated Search - Outgoing	An outgoing federated search enables users of your portal to search other Oracle WebCenter Interaction portals or other external repositories.
Filter	Filters control what content goes into which folder when crawling in documents or using Smart Sort to filter content into new folders. A filter sets conditions that document links must pass to be sorted into associated folders in the Knowledge Directory.
Group	Groups are sets of users, sets of other groups, or both. Groups enable you to more easily control security because you assign each group different activity rights and access privileges.
Invitation	Invitations allow you to direct potential users to your portal, making it easy for them to create their own user accounts and letting you customize their initial portal experiences with content that is of particular interest to them.
Job	Jobs allow you to schedule portal management operations. A job is a collection of related operations. Each operation is one task, such as a crawl for documents, an import of users, or one of the system maintenance tasks.
Page (Only displays when in a community folder)	Community pages let you categorize information for your community audience.
Page Template	Page templates define the basic structure for the resulting community pages, such as the column layout and which portlets to include.

Object	Description
Portlet	Portlets provide portal users customized tools and services as well as information. Portlets let you to integrate applications, tools, and services into your portal, while taking advantage of portal security, caching, and customization.
Portlet Bundle	Portlet bundles are groups of related portlets, packaged together for easy inclusion on My Pages or community pages.
Portlet Template	Portlet templates allow you to create multiple instances of a portlet, each displaying slightly different information.
Profile Source - Remote	Profile sources allow you to import user information (such as name, address, or phone number) that is already defined in your enterprise in existing user repositories, such as Active Directory or LDAP servers. The imported user information can be used to populate user profiles or can be passed to content crawlers, remote portlets, or federated searches as user information.
Property	Properties provide information about, as well as a way to search for, documents and objects in your portal. For example, you might want to create an Author property so users can find all the documents or objects created by a particular user.
Remote Server	Remote servers group together Web services that are installed on the same computer and require the same type of authentication. With a remote server, you enter the base URL and authentication settings just once for multiple Web services, and, if you must move the Web services, you just must change the remote server settings.
Snapshot Query	Snapshot portlets enable you to display the results of a search in a portlet or e-mail the results to users. You can select which repositories to search (including Oracle WebCenter Collaboration), and limit your search by language, object type, folder, property, and text conditions.
User	Portal users enable you to authenticate the people who access your portal and assign appropriate security for the documents and objects in your portal. Users can be imported from external user repositories, created through the portal, created through invitations, self-registered, or just guests (unauthenticated users).
Web Service - Authentication	Authentication Web services enable you to specify general settings for your external user repository, leaving the more detailed settings (like domain specification) to be set in the associated remote authentication sources, enabling you to create different authentication sources to import each domain without having to repeatedly specify all the settings.
Web Service - Content	Content Web services enable you to specify general settings for your external user repository, leaving the target and security settings to be set in the associated remote content source and remote content crawler, enabling you to crawl multiple locations of the same content repository without having to repeatedly specify all the settings.
Web Service - Intrinsic Portlet	Portlet Web services allow you to specify functional settings for your portlets, leaving the display settings to be set in each associated portlet. An intrinsic portlet Web service references one or more sets of code that are located on the portal computer.

Object	Description
Web Service - Profile	Profile Web services enable you to specify general settings for your external user repository, leaving the more detailed settings (like domain specification) to be set in the associated remote profile sources, enabling you to create different profile sources to import information each domain without having to repeatedly specify all the settings.
Web Service - Remote Pagelet	Pagelet Web services allow you to make pagelets created in Oracle WebCenter Pagelet Producer available through the portal.
Web Service - Remote Portlet	Portlet Web services allow you to specify functional settings for your portlets, leaving the display settings to be set in each associated portlet. A remote portlet Web service references services hosted by a separate remote server.
Web Service - Search	Search Web services allow you to specify general settings for your remote search repository, leaving the security settings to be set in the associated outgoing federated searches, enabling you to segregate access to your search repository through multiple outgoing federated searches.

2.4.2 Portal Objects Created Upon Installation

The default portal installation includes several portal objects that are created upon installation.

Object	Description
Administrative Resources (folder)	This folder contains the following objects created at installation: users, groups, the Oracle WebCenter Interaction Authentication Source, the World Wide Web content source, properties, content types, and federated search objects.
Intrinsic Operations (folder)	This folder contains external operations and intrinsic jobs, such as Search Update, Document Refresh, and Weekly Housekeeping. The folder is registered with the primary Automation Service.
Portal Resources (folder)	This folder contains intrinsic portlets and Web services, as well as page, community, and portlet templates.
Default Experience Definition (folder)	This folder contains the users associated with the default experience definition. Upon installation, one user is associated with the default experience definition—Administrator.
Audit Log Management (job)	This job archives old audit messages into files and deletes old audit files.
Bulk Subscriptions (job)	This job subscribes users to communities and portlets when you use bulk add.
Document Refresh (job)	This job performs background maintenance on your search index such as refreshing document links and properties and deleting expired documents.
Dynamic Membership Update Agent (job)	This job updates dynamic group memberships as defined on the Dynamic Membership Rules page of the Group Editor.
Search Update (job)	This job makes sure the search collection is synchronized with the database. You can run multiple instances of this job.
Weekly Housekeeping (job)	This job performs weekly housekeeping on your system, such as deleting expired invitation codes and deleting uploaded files for which links have been deleted.

Object	Description
Navigation Tags Header Portlet (portlet)	This portlet is provided as an example of a custom header that includes navigation tags; you can customize it and use it in communities or experience definitions. This portlet is stored in the Portal Resources folder.
Classic Footer Portlet (portlet)	This portlet is provided as an example of a custom footer that you can customize and use in communities or experience definitions.
Classic Header Portlet (portlet)	This portlet is provided as an example of a custom header that you can customize and use in communities or experience definitions.
Layout Footer Portlet (portlet)	This portlet is provided as an example of a custom footer that uses adaptive tags; you can customize it and use it in communities or experience definitions.
Layout Footer Portlet (portlet)	This portlet is provided as an example of a custom header that uses adaptive tags; you can customize it and use it in communities or experience definitions.
Portal Login (portlet)	This portlet allows users to log in to the portal. You probably want to add this to all your guest users' home pages so that users can log in from the default page displayed when they navigate to your portal.
Tag Login Portlet (portlet)	This portlet is provided as an example of a custom login portlet that uses adaptive tags; you can customize it and add it to your guest users' home pages so that users can log in from the default page displayed when they navigate to your portal. This portlet is stored in the Portal Resources folder. For information on adaptive tags, see the Adaptive Page Layouts section of the *Oracle Fusion Middleware User Interface Customization Guide for Oracle WebCenter Framework Interaction*.
Folder Expertise (portlet)	This portlet displays the folders for which the user is an expert. Administrative users can add users to a folder as an expert through the Related Resources page of the Folder Editor (if they have at least Edit access to the folder and as least Select access to the user), or, if users have the Self-Selected Experts activity right, they can add themselves as experts when they are browsing folders in the Knowledge Directory. This portlet is stored in the Portal Resources folder.
General Information (portlet)	This portlet displays user profile information such as name and address, but an administrative user with at least Edit access to the portlet can configure it to display any information. If your portal displays a legacy layout (rather than adaptive layouts), this portlet is displayed on the user profile page by default. This portlet is stored in the Portal Resources folder.
Managed Communities (portlet)	This portlet displays the communities to which the user has Edit or Admin access. If your portal displays a legacy layout (rather than adaptive layouts), this portlet is displayed on the user profile page by default. This portlet is stored in the Portal Resources folder.
Enterprise Poke	Available only if the Remote Portlet Service is installed. This portlet enables users to "poke" the user whose profile they are viewing. The poke displays in the User Activities stream for the user that was poked and the user that initiated the poke. This portlet is stored in the Enterprise Poke folder.
Last 5 Profile Viewers	Available only if the Remote Portlet Service is installed. This portlet displays the last five users that have viewed the profile the user is viewing. This portlet is stored in the Profile Portlets folder.
Online Now	Available only if the Remote Portlet Service is installed. This portlet shows whether the user has logged in to the portal within the last ten minutes. This portlet is stored in the Profile Portlets folder.

Object	Description
Total Profile Views	Available only if the Remote Portlet Service is installed. This portlet displays the total number of times the profile has been viewed within a specified time (specified in the administrative preferences for the portlet). This portlet is stored in the Profile Portlets folder.
My Picture	Available only if the Remote Portlet Service is installed. This portlet enables a user to upload an image to display as the profile picture. This portlet is stored in the Profile Portlets folder.
Tag Me	Installed with the portal, but requires the Tagging Engine to be installed. This portlet enables users to add a tag to the user whose profile they are viewing. This portlet is stored in the Portal Resources folder.
Job Histories Intrinsic Portlet (portlet)	This portlet displays the same job history information that is displayed on the Job History page of the Automation Service Manager. This portlet is stored in the Portal Resources folder.
Knowledge Directory Portlet	This portlet enables you to browse the Knowledge Directory. You can add this portlet to a My Page or community page. The portlet can display the entire Knowledge Directory or it can be configured to display only selected folders. This portlet is stored in the Knowledge Directory Portlet folder.
Last 5 Profile Viewers	Available only if the Remote Portlet Service is installed. If added to a My Page, this portlet displays the last five users that have viewed your profile. This portlet is stored in the Profile Portlets folder.
Portal Search (portlet)	This portlet lets users search your portal and access their saved searches. Users might want to add this to their home page for easy access to their saved searches. This portlet is stored in the Portal Resources folder.
Posted Links Portlet	Available only if the Remote Portlet Service is installed. This portlet enables you to add links to useful or interesting web pages. When you add a link, the link displays in the portlet and the action displays in your User Activities stream. This portlet is stored in the Posted Links folder.
RSS Reader Portlet (portlet)	This portlet lets users specify an RSS or ATOM feed to display on a My Page. This portlet is stored in the Portal Resources/RSS Reader folder, but is available only if you installed the Remote Portlet Service and imported the RSS Reader migration package.
RSS Community Reader Portlet (portlet)	This portlet lets community managers specify an RSS or ATOM feed to display on a community page. This portlet is stored in the Portal Resources/RSS Reader folder, but is available only if you installed the Remote Portlet Service and imported the RSS Reader migration package.
Submit to KD Portlet	Available only if the Remote Portlet Service is installed. This portlet enables you to submit a document to the Knowledge Directory. This portlet is stored in the Portal Resources folder. **Note:** The Submit to KD Portlet supports only adaptive layout mode; it does not work in classic mode.
Tagging Engine Items	Available only if the Tagging Engine is installed. This portlet enables you to search for objects using a text string or by clicking a tag. It also provides access to the Tagging Engine application. This portlet is stored in the Tagging Engine folder.
Tagging Engine People	Available only if the Tagging Engine is installed. This portlet enables you to search for users using a text string or by clicking a tag. It also provides access to the Tagging Engine application. This portlet is stored in the Tagging Engine folder.

Object	Description
Tagging Engine Search	Available only if the Tagging Engine is installed. This portlet is used in conjunction with the Tagging Engine Results portlet. It enables you to search for objects using a text string and the results appear in the Tagging Engine Results portlet. This portlet is stored in the Tagging Engine folder.
Tagging Engine Tag Cloud	Available only if the Tagging Engine is installed. This portlet displays the tags that have been applied to objects in the portal. The tag cloud results can be filtered by selecting a view from the view drop-down list. When you click a tag, the results appear in the Tagging Engine Results portlet. This portlet is stored in the Pathways folder.
Tagging Engine Results	Available only if the Tagging Engine is installed. This portlet displays the results from the Tagging Engine Search portlet or the Tagging Engine Tag Cloud portlet. This portlet is stored in the Tagging Engine folder.
Total Profile Views	Available only if the Remote Portlet Service is installed. This portlet displays the total number of times your profile has been viewed within a specified time (specified in the administrative preferences for the portlet). This portlet is stored in the Profile Portlets folder.
User Status (portlet)	This portlet lets users post their current status. This portlet is stored in the Activity Service folder, but is available only if you installed the Remote Portlet Service and imported the Activity Service migration package.
User Activities (portlet)	This portlet displays a user's status history and any other recent activities that are submitted by other applications. This portlet is stored in the Activity Service folder, but is available only if you installed the Remote Portlet Service and imported the Activity Service migration package. To view another user's activities, open the user's profile and look at the User Activities portlet displayed in the profile. To subscribe to e-mail notification or an RSS feed of the user's activity, click the appropriate button at the bottom of the user's User Activities portlet.
Community Links Portlet Template (portlet template)	This template is used by the portal to create portlets that display the links saved in a Community Knowledge Directory folder. This portlet template is stored in the Portal Resources folder.
Content Snapshots (portlet template)	This template is used by the portal to create portlets that display the results of a Snapshot Query. This portlet template is stored in the Portal Resources folder.

2.4.3 Portal Utilities

The following table describes the portal utilities accessible through the **Select Utility** list in the Administrative Objects Directory.

Utility	Description
Access Unclassified Documents	Access documents imported by a content crawler and placed in the Unclassified Documents folder in the Knowledge Directory.
Activity Manager	Create, modify, or delete activities.
Approve Directory Content	Approve directory content submitted to the Knowledge Directory.
Approve Objects for Migration	Approve migration packages.
Audit Manager	Audit user activity or object activity.

Utility	Description
Automation Service	Configure and run jobs.
Credential Vault Manager	Manage lockboxes corresponding to external systems that users can access through the portal.
Default Profiles	Configure default user profiles.
Experience Rules Manager	Define and prioritize Experience Rules.
Global ACL Sync Map	Configure the global access control list (ACL) synchronization map.
Global Content Type Map	Configure the Global Content Type Map.
Global Document Property Map	Configure the global document property map.
Global Object Property Map	Configure the global object properties map.
Knowledge Directory Preferences	Configure Knowledge Directory preferences.
Localization Manager	Localize the portal.
Migration - Export	Create a portal export package.
Migration - Import	Import a portal export package.
Object Migration Status	View the status of portal objects that have been requested for migration.
Portal Settings	Modify Portal settings.
Release Disabled Logins	Manage user locks.
Release Item Locks	Manage object locks.
Search Cluster Manager	Check status and manage search topology and checkpoints.
Search Results Manager	Manage search results preferences.
Search Service Manager	Manage Search Service settings.
Smart Sort	Run the Smart Sort utility.
System Health Monitor	View diagnostic information.
Tag Library Manager	Displays the tag libraries loaded on the computer that hosts the portal.
User Profile Manager	Modify the user profiles map.
(Custom Utility)	Administrative users with the Create Activities activity right or portal developers can create custom utilities that display in the **Select Utility** list.

2.4.4 Administration Utilities in the Portal Installation

Oracle WebCenter Interaction includes several command-line administration utilities in the portal installation directory and a tag library utility in the portal administrative interface.

Note: The command-line utilities are located on the computer that hosts the portal, in *install_dir*/ptportal/10.3.3/bin. Replace *install_dir* with the portal installation directory, for example C:\Oracle\Middleware\wci for Windows or /oracle/middleware/wci for UNIX or Linux.

Utility (.sh or .bat file)	Purpose
automationserverd	The Automation Service daemon ensures the Automation Service is running. For information on the Automation Service daemon, see the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Interaction for Windows* or the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Interaction for Unix and Linux*. For information on modifying Automation Service defaults, see Configuring the Automation Service.
cryptoutil	The Cryptographic Password utility generates the passwords you might set during installation. To display the man pages for the Cryptographic Password utility, enter the following command: `install_dir/ptportal/10.3.3/bin/cryptoutil.sh -h`
diagnostic	The Diagnostic utility enables you to verify connectivity for installation components and the portal database. To display the man pages for the Diagnostic utility, enter the following command: `install_dir/ptportal/10.3.3/bin/diagnostic.sh -h` For details, see the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Interaction for Windows* or the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Interaction for Unix and Linux*.
portalenv	The Portal Environment utility sets the portal environment for tools in *install_dir*/ptportal/10.3.3/bin. To display the man pages for the Portal Environment utility, enter the following command: `install_dir/ptportal/10.3.3/bin/portalenv.sh -h`
ptmigration	The Migration Wizard manages import packages that enable you to migrate portal objects to new host portals, such as migration from a development environment to a QA environment or production environment, or from a remote server host computer to the portal host computer. The command-line interface (CLI) of the Migration Wizard enables you to import migration packages from the command line. To display the man pages for the Migration Wizard CLI, enter the following command: `install_dir/ptportal/10.3.3/bin/ptmigration.sh -h` For information on object migration, see Section 12, "Migrating, Backing-Up, and Restoring Your Portal."
Tag Library Manager	This Tag Library Manager enables you to view the tag libraries installed on the computer that hosts the portal. To access the Tag Library Manager, in the portal, click **Administration**, then, in the **Select Utility** menu, click **Tag Library Manager**.

2.5 Overview of Portal Security

Oracle WebCenter Interaction provides many features that work together to secure your portal and its content.

- Object level security in the form of Access Control Lists (ACLs). See Section 2.5.1, "About Access Controls Lists and Access Privileges."
- Activity security in the form of activity rights. See Section 2.5.2, "About Activity Rights."
- Automatic user lockout. See Section 6.2.3.1, "Automatically Locking User Accounts."
- Document security imported from source repositories. See Section 7.10.5, "Example of Importing Content Security."
- Web application credential management in the form of lockboxes. See Section 8.6, "Working with Lockboxes."
- Password management, which enables you to define password rules. See Appendix A, "Configuring Portal Settings."
- Audit records, which you should periodically review to keep track of actions performed by users. See Appendix A, "Configuring Portal Settings."
- Single sign-on. See Appendix E, "Deploying Single Sign-On."

Note: By default, you can log in to the administrative portal as Administrator with no password. If the default Administrator password has not yet been changed, you should do so as soon as possible. Ensure that you document the change and inform the appropriate portal administrators.

In addition to the security available through the portal, you must also secure your hardware and back-end systems (for example, your portal and user databases) to fully protect your portal. You should follow all security guidance provided in your hardware and software documentation.

You must also create strong passwords not only for administrators, but for all portal users and you must advise everyone to keep their passwords safe.

For additional security considerations, see the *Oracle Fusion Middleware Deployment Guide for Oracle WebCenter Interaction*.

2.5.1 About Access Controls Lists and Access Privileges

An access control list (ACL) is a list of privileges associated with each document and object in the portal. You add users and groups to a document's or object's ACL and grant them access privileges to determine what they can do with the document or object.

Access privileges determine which documents and objects a user can see while browsing or searching the portal, which documents and objects a user can select (for example, which portlets they can add to My Pages and community pages), and which documents and objects a user can edit. Each document and object in the portal is controlled through the following access privileges:

Access Privilege	Description
Read	Allows users or groups to see the object.
Select	Allows users or groups to add the object to other objects. For example, it allows users to add portlets to their My Pages, add users to groups, or associate remote servers with Web services.
Edit	Allows users or groups to modify the object (with the exception of deleting or setting access to the object).
Admin	Allows users or groups full administrative control of the object, including deleting the object or approving it for migration.

For information on setting access privileges, see Section 5.17, "Setting Security on an Object."

Note:

- The Everyone group (all users) has mandatory Read access to authentication sources, content types, filters, invitations, and properties.
- If a user is a member of more than one group included in the list, or if they are included as an individual user and as part of a group, that user gets the highest privilege available to the user for the document or object. For example, if a user is part of the Everyone group (which has Read access) and the Administrators group (which has Admin access), that user gets the higher privilege to the document or object: Admin.
- Access privileges are based on the security of the folder in which the document or object is stored. Changes to the security of a folder apply to all the documents or objects within that folder. For example, if a document in the folder is shared with another folder (such as when a document is copied from one folder to another), the security of the document is changed in both locations.

2.5.2 About Activity Rights

Activity rights determine which portal objects a user can create and which portal utilities a user can execute to create or modify portal objects. For example, you can specify that users can create communities, create folders, create content types, and create portlets.

Activity rights are global and cumulative. If a user is a member of multiple groups, each with different rights, that user inherits all the activity rights of all the parent groups. That user can exercise all of those rights in any area of the portal to which that user has the appropriate access. Groups can also inherit activity rights.

In addition to the default activity rights, you can also create custom portal activities. For example, if you have an inventory control system accessed through the portal and only certain users are allowed to edit it, you can create an Edit Inventories activity. You can then create inventory-control portlets that verify whether a user has the correct activity right before receiving access to the portlet.

2.5.2.1 Activity Rights Required to Create Portal Objects

To create a portal object, you must have at least Edit access to the parent folder (the folder that will store the object), the Access Administration activity right, and the required activity right listed in the table.

Object	Required Activity Right
Administrative Folder	Create Admin Folders
Authentication Source - Remote	Create Authentication Sources
Community	Create Communities
Community Template	Create Community Infrastructure
Content Crawler - Remote	Create Content Crawlers
Content Crawler - WWW	Create Content Crawlers
Content Source - Remote	Create Content Sources
Content Source - WWW	Create Content Sources
Content Type	Create Content Types
Experience Definition	Create Experience Definitions
External Operation	Create External Operations
Federated Search - Incoming	Create Federated Searches
Federated Search - Outgoing	Create Federated Searches
Filter	Create Filters
Group	Create Groups
Invitation	Create Invitations
Job	Create Jobs
Page (Only displays when in a community folder)	No activity right needed; just need at least Edit access to community
Page Template	Create Community Infrastructure
Portlet	Create Portlets
Portlet Bundle	Create Web Service Infrastructure
Portlet Template	Create Web Service Infrastructure
Profile Source - Remote	Create Profile Sources
Property	Create Properties
Remote Server	Create Web Service Infrastructure
Snapshot Query	Create Snapshot Queries
User	Create Users
Web Service - Authentication	Create Web Service Infrastructure
Web Service - Content	Create Web Service Infrastructure
Web Service - Intrinsic Portlet	Create Web Service Infrastructure
Web Service - Profile	Create Web Service Infrastructure
Web Service - Remote Pagelet	Create Web Service Infrastructure
Web Service - Remote Portlet	Create Web Service Infrastructure

Object	Required Activity Right
Web Service - Search	Create Web Service Infrastructure

2.5.2.2 Activity Rights and Group Membership Required to Access Portal Utilities

To access a utility, you must have the Access Administration activity right, the Access Utilities activity right, and the required activity right or group membership listed in the table.

Utility	Required Activity Right (AR) or Group Membership (GM)
Access Unclassified Documents	Access Unclassified Documents (AR)
Activity Manager	Create Activities (AR)
Approve Directory Content	Access Utilities (AR)
Approve Objects for Migration	Administrators Group (GM)
Audit Manager	Administrators Group (GM)
Automation Service	Administrators Group (GM)
Credential Vault Manager	Administrators Group (GM)
Default Profiles	Create User (AR)
Experience Rules Manager	Access Experience Rules Manager (AR)
Global ACL Sync Map	Administrators Group (GM)
Global Content Type Map	Administrators Group (GM)
Global Document Property Map	Administrators Group (GM)
Global Object Property Map	Administrators Group (GM)
Knowledge Directory Preferences	Administrators Group (GM)
Localization Manager	Administrators Group (GM)
Migration - Export	Administrators Group (GM)
Migration - Import	Administrators Group (GM)
Object Migration Status	Access Utilities (AR)
Portal Settings	Administrators Group (GM)
Release Disabled Logins	Administrators Group (GM)
Release Item Locks	Administrators Group (GM)
Search Cluster Manager	Administrators Group (GM)
Search Results Manager	Access Search Results Manager (AR)
Search Service Manager	Administrators Group (GM)
Smart Sort	Access Smart Sort (AR)
System Health Monitor	Administrators Group (GM)
Tag Library Manager	Administrators Group (GM)
User Profile Manager	Access User Profile Manager (AR)
(Custom Utility)	Read access to the custom utility's Web service

3

The Web Service Architecture and Remote Servers

This chapter describes how remote servers and Web services help to manage the services available through Oracle WebCenter Interaction.

It includes the following sections:

3.1 Overview of the Web Service Architecture

Many of the objects in the portal use Web services, which are components that run on a logically separate computer from the one that runs the portal and communicate with the portal through HTTP. We refer to this separate computer as a remote server. The Web service architecture allows multiple types of remote services (authentication sources, content crawlers, outgoing federated searches, portlets, and profile sources) to share a logical remote server, making it easier to manage the computers that make up the portal.

Web services also allow you to share settings (sometimes rather complex settings) with the objects created from those services. For example, administrative users creating portlet Web services need a greater understanding of the structure of the portlet, because they must specify whether the portlet has preferences or whether it sends user information; whereas users creating portlets from that Web service might only must set configuration settings appropriate for a non-technical user.

In addition, Web services enable you to create composite applications that use functionality from multiple Web services. For example, you might have several Web services accessing an application that requires user credentials. Rather than creating a separate configuration page for each Web service and requiring users to specify the same information multiple times, you can create a link to these shared settings, allowing users to specify the information only once for all of these Web services.

Objects that use Web services follow this general structure:

- The remote server contains the base URL and credentials.
- The Web service defines configuration settings for the associated object: remote authentication source, remote content source (used to create remote content crawlers), outgoing federated search, portlet, and remote profile source.

- The associated object defines any remaining configuration settings.

3.2 About Remote Servers

Remote servers group together Web services that are installed on the same computer and require the same type of authentication. With a remote server, you enter the base URL and authentication settings just once for multiple Web services, and, if you must move the Web services, you just must change the remote server settings.

Remote servers do not must be visible from beyond your firewall. The portal can function as a gateway to the content on the remote servers.

You can use a remote server to create the following administrative objects:

- Search Web Service

  For information on search Web services, see Section 10.5, "About Providing Search Access to External Repositories with Federated Searches."

- Profile Web Service

  For information on profile Web services, see Section 6.13, "About Importing User Profile Information."

- Authentication Web Service

  For information on authentication Web services, see Section 6.7, "About Importing and Authenticating Users and Groups."

- Remote Portlet Web Service

  For information on remote portlet Web services, see Chapter 8, "Extending Portal Services with Portlets."

- Content Web Service

  For information on content Web services, see Section 7.10.4, "Content Crawlers."

3.3 Working with Remote Servers

This section describes the following main tasks:

- Chapter 3.3.1, "Creating or Editing a Remote Server."
- Section 3.3.2, "Deleting a Remote Server"

It also covers the following low-level tasks:

- Section 3.3.3, "Specifying the Location of a Remote Server"
- Section 3.3.4, "Specifying the Authentication Information Needed to Access a Remote Server"
- Section 3.3.5, "Specifying a Public Encryption Key for a Remote Server"

3.3.1 Creating or Editing a Remote Server

Remote servers group together Web services that are installed on the same computer and require the same type of authentication. With a remote server, you enter the base URL and authentication settings just once for multiple Web services, and, if you must move the Web services, you just must change the remote server settings.

Note: For information on creating a remote server for Oracle WebCenter Pagelet Producer, see Section 8.3.1, "Creating the Oracle WebCenter Pagelet Producer Remote Server."

To create a remote server you must have the following rights and privileges:

- Access Administration activity right
- Create Web Service Infrastructure activity right
- At least Edit access to the parent folder (the folder that will store the remote server)

To edit a remote server you must have the following rights and privileges:

- Access Administration activity right
- At least Edit access to the remote server

To create or edit a remote server:

1. Click **Administration**.
2. Open the Remote Server Editor.
   - To create a remote server, open the folder in which you want to store the remote server. In the Create Object list, click **Remote Server**.
   - To edit a remote server, open the folder in which the remote server is stored and click its name.
3. On the Main Settings page, complete the following tasks:
   - Section 3.3.3, "Specifying the Location of a Remote Server"
   - Section 3.3.4, "Specifying the Authentication Information Needed to Access a Remote Server"
   - Section 3.3.5, "Specifying a Public Encryption Key for a Remote Server"
4. On the Properties and Names page, perform tasks as necessary:
   - Section 5.15, "Naming and Describing an Object"
   - Section 5.16, "Managing Object Properties"
5. On the Security page, perform tasks as necessary:
   - Section 5.17, "Setting Security on an Object"

   The default security for this remote server is based on the security of the parent folder.
6. If you are editing a remote server, on the Migration History and Status page, perform tasks as necessary:
   - Section 5.18, "Viewing Migration History and Status for an Object"

   Note: The Migration History and Status page is not available when creating an object.

3.3.2 Deleting a Remote Server

To delete a remote server you must have the following rights and privileges:

- Access Administration activity right
- Admin access to the remote server

To delete a remote server:

1. Click **Administration**.
2. Navigate to the remote server.
3. Select the remote server you want to delete and click the delete icon.

> **Note:** Deleting a remote server will break any associated objects.

3.3.3 Specifying the Location of a Remote Server

You can specify the location of a remote server on the Main Settings page of the Remote Server Editor.

1. If the Remote Server Editor is not already open, open it now and display the **Main Settings** page.
2. In the **Base URL** text box, type the URL to the parent folder of the Web services installed on this server.

   This can be the root of the Web Server (for example, http://server/) or a specific application or virtual directory (for example, http://server/app/). Because the URL specifies a folder rather than a specific resource, it should always end with a slash.

   The portal must be able to resolve the server name. Therefore, you might want to use Fully-Qualified Domain Names (FQDNs) such as "http://server.companyname.com" rather than just "http://server". In some cases, when the portal is in a demilitarized zone (DMZ), you might must use an IP address like "10.1.2.140".

   You need a remote server for each port (for example, http://server:8082/ requires a different remote server than http://server:7071/). You also need a separate remote server if some services use SSL (for example, https://server/).

   > **Note:** If you are sending any type of basic authentication information (specified in step 2), and you are not using a secured network, such as a separate subnet or a Virtual Private Network (VPN) connection, we strongly recommend that the Base URL use SSL (the URL must begin with https://). Basic authentication uses Base 64 encoding, which can be easily decoded back to clear text.

3.3.4 Specifying the Authentication Information Needed to Access a Remote Server

You can specify the authentication needed to access a remote server on the Main Settings page of the Remote Server Editor.

1. If the Remote Server Editor is not already open, open it now and display the **Main Settings** page.
2. Under **Base Authentication Type**, specify what authentication information, if any, you want this remote server to pass to its associated Web services.
   - To use no authentication information, choose **None**.

- To use credentials from a user's login, choose **User's Basic Authentication Information**.

  Confirm that the portal configuration file has been edited so that the portal stores the user name and password in memory for as long as the user is logged in to the portal (as described in the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Interaction for Windows* or the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Interaction for Unix and Linux*. This option is not supported for configurations in which users log in without typing a password (for example, single sign-on or Remember My Password) because the password is not available to the portal.

- To specify a user name and password, choose **Administrator's Basic Authentication Information** and type the user name and password in the associated text boxes.

  This information is encrypted, stored in the portal database, and sent with all requests to this remote server.

3.3.5 Specifying a Public Encryption Key for a Remote Server

You can enable users to access external Web applications through portlets, passing authentication information in portlet headers. To do so, you must specify a public encryption key on the Main Settings page of the Remote Server Editor.

1. If the Remote Server Editor is not already open, open it now. The Remote Server Editor displays the **Main Settings** page.
2. To send credentials in portlet headers, using RSA public key/private key encryption, in the **Public Encryption Key** box, enter the public key for RSA encryption.
3. Set up a lockbox in the Credential Vault Manager. For details, see Section 8.6, "Working with Lockboxes."
4. Associate the lockbox with the remote portlet Web service (on the **Authentication Settings** page). For details, see Section 8.2.2, "Creating or Editing a Remote Portlet Web Service."
5. Use the IDK to provide the private key for RSA encryption (see the *Oracle Fusion Middleware Web Service Developer's Guide for Oracle WebCenter Interaction*).

3.4 Working with Web Services

This section describes common tasks in the Web Services Editors:

- Section 3.4.1, "Associating a Remote Server with a Web Service"
- Section 3.4.2, "Specifying the Location of the Web Service Provider or Code"
- Section 3.4.3, "Specifying Web Service Time-Out Settings"
- Section 3.4.4, "Enabling and Disabling a Web Service"
- Section 3.4.6, "Specifying How Gatewayed Content is Handled"
- Section 3.4.7, "Specifying What Content is Gatewayed for a Web Service"
- Section 3.4.11, "Specifying Encoding Style for a Web Service"
- Section 3.4.8, "Adding a Service Configuration Page to a Web Service Editor"

- Section 3.4.9, "Adding an Administrative Configuration Link to the Select Utility Menu"
- Section 3.4.10, "Adding a User Configuration Link to the My Account Page"
- Section 3.4.12, "Sending Activity Rights from a Web Service to Associated Objects"
- Section 3.4.13, "Specifying Authentication Settings for a Web Service"
- Section 3.4.14, "Sending User Preferences from the Web Service to Associated Objects"
- Section 3.4.15, "Sending User Information from a Web Service to Associated Objects"
- Section 3.4.16, "Enabling Error Tracing for a Web Service"
- Section 3.4.17, "Viewing Objects Associated with a Web Service"

3.4.1 Associating a Remote Server with a Web Service

Note: This setting is available for authentication Web services, content Web services, profile Web services, remote portlet Web services, and search Web services.

1. If the Web Service Editor is not already open, open it now. The Web Service Editor displays the Main Settings page.
2. Under Server Information, you can establish and manage remote server association for this Web service:
   - To associate a remote server (or to change an existing association), click **Browse**, then, in the Choose Remote Server dialog box, choose the remote server you want to associate and click **OK**.
   - To edit the remote server, click its name.
   - To remove the remote server association, click **Remove**.

3.4.2 Specifying the Location of the Web Service Provider or Code

Note: You specify the location of intrinsic portlet Web services and remote pagelet Web services differently than other Web services. See Section 8.2.1, "Creating or Editing an Intrinsic Portlet Web Service" and Section 8.3.2, "Creating or Editing a Remote Pagelet Web Service"

To specify the location of the Web service provider or code:

1. If the Web Service Editor is not already open, open it now. The Web Service Editor displays the Main Settings page.
2. For each URL setting, specify the location of the provider or code on which your Web service is based. If you associated a remote server, the base URL displays to the left of the box. You can either type a relative path, finishing the path that starts with the base URL (for example, `/myPortlet/Portlet.htm` or `/myWebService/myProvider.asmx`), or you can type an absolute path, ignoring the base URL (for example,

`http://myServer/myPortlet/Portlet.htm` or `http://myServer/myWebService/myProvider.asmx`).

- Authentication Web Services
  - In the **Authentication URL** box, type the path to the authentication provider.
  - In the **Synchronization URL** box, type the path to the synchronization provider.
- Content Web Services
  - In the **Container URL** box, type the path to the crawl provider, which tells the portal how to navigate through the content hierarchy.
  - In the **Document URL** box, type the path to the document provider, which tells the portal how to get information from a document of this type.
  - In the **Upload URL** box, type the path to the upload provider, which tells the portal how to copy a document into the Document Repository. If you associated a remove server, you can type a relative path or an absolute path.
- Profile Web Services
  - In the **Synchronization URL** box, type the path to the profile provider (the .asmx file).
- Remote Portlet Web Services
  - In the **Portlet URL** box, type the path to the remote portlet code.
- Search Web Services
  - In the **Search URL** box, type the path to the search provider.

    If you are searching another Oracle WebCenter Interaction portal that runs .NET, use the format: http://*hostname*:*portnumber*/ptapi/Search.asmx

    If you are searching another Oracle WebCenter Interaction portal that runs Java, use the format: http://*hostname*:*portnumber*/ptapi/services/PTSearchServiceSoap

3.4.3 Specifying Web Service Time-Out Settings

Note: This setting is available for authentication Web services, content Web services, profile Web services, remote portlet Web services, and search Web services.

To specify the Web service's time-out settings:

1. If the Web Service Editor is not already open, open it now. The Web Service Editor displays the Main Settings page.
2. For each time-out setting, specify how long you want the portal to try to get the content from the host computer. If the host computer does not return content before the time-out period ends, an error message displays (for example, to the user upon login, in the portlet, or in the job log upon completion of an associated authentication source job).

In each time-out text box, type the number of seconds or minutes you want the portal to wait; then, in the drop-down list click **Second(s)** or **Minute(s)**.

Note:

- The **Portlet Timeout** setting for remote portlet Web services and remote pagelet Web services and the **SOAP Timeout** setting for search Web services applies only to non-gatewayed content. You probably want to set a relatively short time for these settings because users might have to wait for the entire time-out period to elapse before a My Page, community page, or search results display.
- The **Gateway Timeout** setting for remote portlet Web services, remote pagelet Web services, and search Web services applies only to gatewayed content (for example, linked content from Oracle WebCenter Collaboration that is not displayed on a My Page or community page). You can probably set a slightly longer time here than for the portlet timeout, because gatewayed content is often secured or of a more complicated nature and therefore users are willing to wait longer for it to display.

3.4.4 Enabling and Disabling a Web Service

Note: This setting is available for all Web services.

You can quickly disable a Web service at any time. For example, you might want to disable a Web service if you must do maintenance on the host computer or on the Web service itself.

1. If the Web Service Editor is not already open, open it now. The Web Service Editor displays the Main Settings page.
2. Under Status of Web Service, specify what should happen when a user tries to access authentication sources associated with this Web service (for example, through login or by running an associated authentication source job):
   - To allow this Web service to authenticate or synchronize users, click **Enabled**.
   - To display a message to users when they try to access this Web service, click **Disabled with message** and type a message in the box.

3.4.5 Specifying Caching Settings for a Web Service

Note: This setting is available for remote pagelet Web services and remote portlet Web services.

To specify caching settings for a Web service:

1. If the Web Service Editor is not already open, open it now.
2. Click the **HTTP Configuration** page.
3. Using the **Minimum Cache Time** and **Maximum Cache Time** settings, specify the amount of time you want the content to be cached. In the text box, type the

number of seconds, minutes, hours, or days you want the portal to cache the content; then, in the drop-down list, click the appropriate period.

Note:

- You should cache content for as long as possible, to lower the burden on your remote servers.
- If the content should not be cached, you can disable caching on the portal by setting both the minimum and maximum to **0** (also, disable error suppression).
- You can also control caching through the portlet or pagelet code. For more information on portlet caching, refer to the *Oracle Fusion Middleware Web Service Developer's Guide for Oracle WebCenter Interaction*.

4. If you want to display cached content if an error occurs, rather than displaying an error message, select **Suppress errors where possible (show cached content instead)**. This option is enabled (selected) by default.

3.4.6 Specifying How Gatewayed Content is Handled

Note: This setting is available for content Web services, remote portlet Web services, and search Web services.

To specify how gatewayed content is handled by the Web service:

1. If the Web Service Editor is not already open, open it now.
2. Click the **HTTP Configuration** page.
3. Under Settings, specify how gatewayed content is handled:
   - Select **Use hosted display mode on gateway pages** if you want to display gatewayed content in the entire region between the portal header and footer. Otherwise, the content is displayed within the portlet that presents the gateway pages. This setting allows users to maintain their portal navigation and other features while working in the remote application.
   - (Recommended) Select **Transform JavaScript files** to run JavaScript files of a remote Web application through the portal transformer. This ensures that pages are displayed correctly and that portal navigation is not lost.
   - (Recommended) Select **Transform CSS** files to run CSS files of a remote Web application through the portal transformer. This ensures that pages are displayed correctly and that portal navigation is not lost.

3.4.7 Specifying What Content is Gatewayed for a Web Service

Note: This setting is available for authentication Web services, content Web services, profile Web services, remote portlet Web services, and search Web services.

To allow users access to remote content they would not normally be able to access, you might must gateway the content. Gatewayed content is downloaded from the computer hosting the content to the portal.

> **Note:** Do not gateway content that is openly accessible over the Internet, as this will unnecessarily burden your portal servers.

1. If the Web Service Editor is not already open, open it now.
2. Click the **HTTP Configuration** page.
3. To specify gateway settings for a Web service:
   - To add a prefix for which you want to gateway content, click **Add Gateway Prefix** and type the prefix in the newly displayed box. For example, if you enter http://myServer/ContentCrawler/ as the prefix, all content having a URL beginning with this prefix will be gatewayed, and all other content will be left in its original location. If you associated a remote server on the Main Settings page, you can type a relative path (/myPortlet/) or an absolute path (http://myServer/myPortlet/). If you enter an absolute path, ignore the base URL.

     To gateway everything on the remote server, type a period followed by a slash (./).

     > **Note:** Gateway URL prefixes must end with a slash (/).

   - If you are creating or editing a remote portlet Web service and you want the content in the portlet to refresh when a gatewayed link with a particular prefix is clicked, in the **Inline Refresh** column, check the box next to the prefix.
   - To delete a prefix, select the prefix and click the delete icon.
   - To select or clear all of the prefix check boxes, select or clear the box to the left of **Prefix**.

3.4.8 Adding a Service Configuration Page to a Web Service Editor

> **Note:** This setting is available for authentication Web services, content Web services, profile Web services, and search Web services.

Your Web service might require object-specific configuration settings. If so, you can include a page for these settings in the editor for the object associated with the Web service. For example, you might have an authentication source that needs information to limit the users or groups imported into the portal, so you could include a page for these settings in the associated Authentication Source Editor.

1. If the Web Service Editor is not already open, open it now.
2. On the left, under Edit Object Settings, click **Advanced Settings** (for an authentication Web service or a profile Web service) or **Advanced URL Settings** (for a content Web service or a search Web service).
3. In the **Service Configuration URL** box, type the path to the configuration page.

Note: If you associated a remote server, the base URL displays to the left of the box. You can either type a relative path, finishing the path that starts with the base URL (/myWebService/ServiceConfig.htm), or you can type an absolute path, ignoring the base URL (http://myServer/myWebService/ServiceConfig.htm).

3.4.9 Adding an Administrative Configuration Link to the Select Utility Menu

Note: This setting is available for content Web services and search Web services.

Your Web service might require administrative configuration settings that affect more than just one Web service. For example, you might have server settings that are stored in a remote database and requires administrative user authentication. Rather than creating a separate configuration page for each Web service and requiring users to specify the same information multiple times, you can create a link to these shared settings in the Select Utility menu, allowing users to specify the information only once for all of these Web services.

Because the link will have the same name as the Web service, do one of the following:

- Give the Web service (and thus the link) a name that clarifies what the shared settings are for.
- Create a Web service that is not used for anything but these links.

Note: If you create a Web service specifically for the configuration links the Web service will not be used to create any associated objects, so you can use any URL for the URL settings on the Main Settings page.

To add an administrative configuration link to the Select Utility menu:

1. If the Web Service Editor is not already open, open it now.
2. On the left, under Edit Object Settings, click **Advanced URL Settings**.
3. In the **Administration Configuration URL** box, type the path to the configuration page.

Note: If you associated a remote server, the base URL displays to the left of the box. You can either type a relative path, finishing the path that starts with the base URL (/myWebService/AdminConfig.htm), or you can type an absolute path, ignoring the base URL (http://myServer/myWebService/AdminConfig.htm).

3.4.10 Adding a User Configuration Link to the My Account Page

Note: This setting is available for content Web services and search Web services.

Your Web service might require user preferences that affect more than just one Web service. For example, you might have several Web services accessing an application that requires user credentials. Rather than creating a separate configuration page for each Web service and requiring users to specify the same information multiple times, you can create a link to these shared settings on the My Account page, allowing users to specify the information only once for all of these Web services.

Because the link will have the same name as the Web service, do one of the following:

- Give the Web service (and thus the link) a name that clarifies what the shared settings are for.
- Create a Web service that is not used for anything but these links.

> **Note:** If you create a Web service specifically for the configuration links the Web service will not be used to create any associated objects, so you can use any URL for the URL settings on the Main Settings page.

To add a user configuration link to the My Account page:

1. If the Web Service Editor is not already open, open it now.
2. On the left, under Edit Object Settings, click **Advanced URL Settings**.
3. In the **User Configuration URL** box, type the path to the configuration page.

> **Note:** If you associated a remote server, the base URL displays to the left of the box. You can either type a relative path, finishing the path that starts with the base URL (/myWebService/UserConfig.htm), or you can type an absolute path, ignoring the base URL (http://myServer/myWebService/UserConfig.htm).

> **Note:** To send these settings to a Web service, specify the names of the preferences you want to send on the Preferences page of that Web service, as described in Section 3.4.14, "Sending User Preferences from the Web Service to Associated Objects."

3.4.11 Specifying Encoding Style for a Web Service

> **Note:** This setting is available for authentication Web services, content Web services, profile Web services, and search Web services.

To specify encoding style for a Web service:

1. If the Web Service Editor is not already open, open it now.
2. On the left, under Edit Object Settings, click **Advanced Settings**.
3. Under SOAP Encoding Style, specify how information from this Web service is encoded:
   - **RPC/Encoded**: Choose this setting if this Web service uses Java.
   - **Document/Literal**: Choose this setting if this Web service uses .NET.

3.4.12 Sending Activity Rights from a Web Service to Associated Objects

> **Note:** This setting is available for content Web services and remote portlet Web services.

You can send objects associated with a Web service the activity rights settings for the user. For example, you must send a content crawler the activity rights for the user running the content crawler (this tells the content crawler which types of portal objects the user can create).

To specify which activity rights the Web service passes to associated objects:

1. If the Web Service Editor is not already open, open it now.
2. Click the **Advanced Settings** page.
3. Under Activity Rights, specify which activity rights settings you want to send to associated objects:
   - To send activity rights settings, click **Add Rights**, select the settings you want to add, clear the settings you want to remove and click **OK**.
   - To remove activity rights settings, select the settings you want to remove and click the remove icon.
   - To select or clear all of the activity rights settings check boxes, select or clear the box to the left of Rights.
   - To toggle the order in which the rights are sorted (ascending/descending), click **Rights** or click the icon to the right of that.

3.4.13 Specifying Authentication Settings for a Web Service

> **Note:** This setting is available for authentication Web services, content Web services, profile Web services, remote portlet Web services, and search Web services.

1. If the Web Service Editor is not already open, open it now.
2. On the left, under Edit Object Settings, click **Authentication Settings**.
3. Under Basic Authentication Settings, specify what authentication information, if any, you want this Web service to pass to its associated objects:
   - If you associated a remote server on the Main Settings page of the Web Service Editor and you want to use the authentication information specified for that remote server, choose **Use Remote Server Basic Authentication Information**.
   - To use credentials from a user's login, choose **User's Basic Authentication Information**. Confirm that the CaptureBasicAuthenticationForPortlets parameter in the portal configuration file has been set so that the portal stores the user name and password in memory for as long as the user is logged in to the portal (as described in Appendix A, "Configuring Portal Settings"). This option is not supported for configurations in which users log in without typing a password (for example, single sign-on or Remember My Password) because the password will not be available to the portal.

Note: This setting is available only for content Web services, remote portlet Web services, or search Web services.

- If you selected a lockbox, and want to use the credentials supplied by the user in the Password Manager for this lockbox, choose **User's Lockbox Credentials**.

Note: This setting is available only for remote portlet Web services.

- To specify a user name and password, choose **Administrator's Basic Authentication Information** and type the user name and password in the associated text boxes. This information is encrypted, stored in the portal database, and sent with all requests to this Web service.

3.4.14 Sending User Preferences from the Web Service to Associated Objects

Note: This setting is available for content Web services, remote portlet Web services, and search Web services. However, remote portlet Web services can also send community and session preferences, so, for remote portlet Web services, refer to Section 8.2.6, "Sending General Settings from a Remote Portlet Web Service to Associated Portlets" rather than this section.

Your Web service might require user preferences that affect more than just one Web service. For example, you might have several Web services accessing an application that requires user credentials. Rather than creating a separate preference page for each Web service and requiring users to specify the same user credentials multiple times, you can create a link on the My Account page, allowing users to specify these credentials only once for all of these Web services.

To send preferences from a Web service:

1. To create the link on the My Account page, in a Web service, specify the path to the user preferences link on the Advanced URL Settings page, as described in Section 3.4.10, "Adding a User Configuration Link to the My Account Page."
2. In each Web service, on the Preferences page, specify, by name, the user preferences you want to send to the objects associated with the Web service.

To specify which user preferences to send from the Web service to associated objects:

1. If the Web Service Editor is not already open, open it now.
2. On the left, under Edit Object Settings, click **Preferences**.
3. Specify which user preferences to send:
   - To send a user preference to the objects associated with this Web service, type the name of the preference in the box below User Preferences.
   - To include another user preference, click **Add User Preference** and type the name of the preference in the additional box.
   - To delete a user preference, select the preference and click the delete icon.

- To select or clear all of the preference check boxes, select or clear the box to the left of **User Preferences**.

3.4.15 Sending User Information from a Web Service to Associated Objects

> **Note:** This setting is available for content Web services, remote portlet Web services, and search Web services.

You can send user information from an external source to objects associated with a Web service. This information can be either imported into the portal database or generated dynamically (with custom code) when a user logs in.

You use profile sources to import user information into the portal from an external user repository, and you use the User Information Property Map to map that imported information to user properties in the portal. Objects associated with Web services can use the imported information instead of having users enter this information on a separate preference page.

To send user information to objects associated with a Web service:

1. If the Web Service Editor is not already open, open it now.
2. On the left, under Edit Object Settings, click **User Information**.
3. If you want to send information mapped to user properties by default, under User Information Settings, select the desired properties.

> **Note:** The **Host Page URL Query String** setting sends the actual query string of the My Page or community that a user hits. Select this if you have custom code that requires the actual string (which can include extra query string parameters) rather than the simplified host page URL.

4. If you want to send other user information, under Additional User Info Settings, perform any of the following actions:
   - To send unmapped user information, click **Add User Info** and type the name of a user property in the field.
   - To send mapped user information, click **Add User Properties**, select the properties, and click **OK**.
   - To delete user information, select the setting you want to delete and click the delete icon.
   - To select or clear all of the settings check boxes, select or clear the box to the left of User Info.

3.4.16 Enabling Error Tracing for a Web Service

> **Note:** This setting is available for authentication Web services, content Web services, profile Web services, remote pagelet Web services, remote portlet Web services, and search Web services.

Error tracing sends information to the portal's debugging tools, allowing you to troubleshoot problems by analyzing error logs. For information on how to set up and use the debugging tools, see Appendix B, "Logging Features."

1. If the Web Service Editor is not already open, open it now.
2. On the left, under Edit Object Settings, click **Debug Settings**.
3. Under Debugging Configuration, select whether to enable **HTTP request** and **HTTP response** tracing.
4. Under User Selection, select whether to enable tracing for a specific user. Otherwise, tracing is on for all users. To select a specific user, click **Browse**, select the user, and click **OK**.
5. Under Portlet Selection, select whether to enable tracing for a specific portlet associated with this Web service. To select a specific portlet, click **Browse**, select the portlet, and click **OK**.

> **Note:** This setting is only available for portlet Web services.

3.4.17 Viewing Objects Associated with a Web Service

> **Note:** This setting is available for all Web services.

To view all the objects associated with a Web service:

1. If the Web Service Editor is not already open, open it now.
2. On the left, under Edit Object Settings, click **Associated Objects**.

Table 3–1 Information Displayed for Associated Objects

Column	Description
Name	Displays the name of the associated object. To edit the associated object, click its name.
Path	Displays the location where the associated object is stored.
Type	Displays what type of object this is (such as a portlet or an authentication source).

If you change the settings for a Web service, the changes will affect all objects displayed on the Associated Objects page.

4

About User Interface Customization

Oracle WebCenter Interaction provides several features that work together to control your portal user interface: adaptive layouts, experience definitions, branding portlets, navigation schemes, and user display settings.

- Adaptive layouts let you quickly change the look and feel of areas in the portal user interface using adaptive tags in standard XHTML. Adaptive layouts are displayed in the portal through remote portlet Web services. Adaptive page layouts are applied at the experience definition level and affect the entire experience definition. Adaptive portlet layouts are applied at the My Page and community page level and affect only that page. For details, see Section 4.1, "About Customizing the User Interface with Adaptive Layouts."
- Experience definitions provide multiple user experiences within a single portal. An experience definition defines certain elements of a user experience, such as adaptive page layout settings, branding style, and navigation. For details, see Section 4.3, "About Controlling the User Interface with Experience Definitions and Experience Rules."
- Branding portlets customize the look of your portal with headers and footers. For example, you probably want to add your company logo and tagline to the header and you might want to add contact information or copyrights to the footer. For details, see Section 4.4, "About Branding with Header and Footer Portlets."
- The portal includes navigation schemes that allow you to select the menu layout and core navigation structure most appropriate for your bandwidth constraints, browser requirements, design needs, deployment size, and end-user expectations. You can also create your own navigation schemes, using the existing code as a starting point. For details, see Section 4.5, "About Navigation Options."
- Users can change their portal display to accommodate assistive technologies or slow internet connections. For details, see Section 4.6, "About Portal Interface Types."
- Users can change their portal display to accommodate their time zone and locale. For details, see Section 4.7, "About Locale Settings."

4.1 About Customizing the User Interface with Adaptive Layouts

Adaptive layouts let you quickly change the look and feel of areas in the portal user interface using adaptive tags in standard XHTML. Adaptive layouts are displayed in the portal through remote portlet Web services. Adaptive page layouts are applied at the experience definition level and affect the entire experience definition. Adaptive portlet layouts are applied at the My Page and community page level and affect only that page.

You can create different layouts for each area in the portal:

Layout Type	Description
Base Page (adaptive page layout)	Controls the layout of everything surrounding the content area, such as the header, footer, banner, and navigation. **Note**: The base page layout applies to all areas of the portal except for profile pages.
Profile Page (adaptive page layout)	Controls the layout of everything surrounding the content area in user profile pages, such as the header, footer, banner, and navigation.
Knowledge Directory (adaptive page layout)	Controls the layout for the content area in the Knowledge Directory.
Search Results (adaptive page layout)	Controls the layout for the content area in search results.
Advanced Search Page (adaptive page layout)	Controls the layout for the content area of the advanced search page.
Portlet Selection (adaptive page layout)	Controls the layout of the flyout page editor used to select portlets on My Pages and community pages.
Login Page (adaptive page layout)	Controls the layout for the content area on the Login page.
My Account Page (adaptive page layout)	Controls the layout for the content area on My Account pages.
Error Page (adaptive page layout)	Controls the layout for the content area on error pages.
Community Selection (adaptive page layout)	Controls the layout of the flyout page editor used to select communities on the Edit My Communities page.
Portlet Layout (adaptive portlet layout)	Controls the column layout for the content area (where portlets are placed) and the look of portlets (the borders and portlet toolbar) in My Pages, profile pages, and community pages. **Note**: As long as adaptive portlet layouts are enabled in the portal configuration file, adaptive portlet layouts can be used in any user interface, whether the interface uses adaptive page layouts or a legacy user interface.
iPhone Layout (adaptive portlet layout)	Displays a layout specifically for iPhone and iTouch devices. You should create an experience definition specifically for iPhone and iTouch users which always displays the iPhone portlet layout for My Pages and community pages. The portlet layouts selected in individual My Pages and community pages could still apply in other experience definitions where the portlet layout override is disabled.

The default adaptive page and portlet layout files are stored on the computer that hosts the Image Service in *install_dir*\ptimages\imageserver\plumtree\portal\private\pagelayouts\, where *install_dir*

is the directory in which you installed the Image Service (for example, C:\Oracle\Middleware\wci for Windows or /oracle/middleware/wci for UNIX or Linux). For information on creating adaptive layouts, see the Adaptive Page Layouts section of the *Oracle Fusion Middleware User Interface Customization Guide for Oracle WebCenter Framework Interaction*.

The remote portlet Web services that display adaptive layouts must be stored in the **Page Layouts** administrative folder in the portal, in the subfolder corresponding to the type of layout. For example, all the layouts stored in the **Base Page Layouts** subfolder are available in the **Base Page Layouts** list in the Experience Definition Editor. All the layouts stored in the **Portlet Layouts** subfolder are available in the list in the Select Page Layout dialog box when editing a My Page or community page and in the list in the **Layout Chooser for Portlet Layouts** section on the Adaptive Page Layout Settings page in the Experience Definition Editor.

When you create an experience definition that uses adaptive page layouts, you select an appropriate page layout for each area of the portal. When users create a My Page or community page, they select whether to display the adaptive portlet layout or a legacy user interface.

Note: If, for any reason, the page layouts cannot be loaded, the user interface will revert to the legacy user interface.

4.1.1 Customizing the User Interface with Adaptive Layouts

To customize the user interface with adaptive layouts, the following steps must be completed by the person indicated:

1. System administrator: Ensure that adaptive layouts are enabled in the portal configuration file.

   You can enable both adaptive page layouts and adaptive portlet layouts or just one or the other.

2. Portal developer: Create the adaptive layouts as described in the Adaptive Page Layouts section of the *Oracle Fusion Middleware User Interface Customization Guide for Oracle WebCenter Framework Interaction*.

3. Portal administrator or administrative user: Create remote portlet Web services that point to the adaptive layouts, as described in Section 4.1.1.1, "Creating a Remote Portlet Web Service for an Adaptive Layout." For information on portlets, see Chapter 8, "Extending Portal Services with Portlets."

4. Portal administrator or administrative user: If you want to use adaptive page layouts, create at least one experience definition that uses them, as described in Section 4.1.1.2, "Creating an Experience Definition to Display Adaptive Page Layouts." For information on Experience Definitions, see Section 4.3, "About Controlling the User Interface with Experience Definitions and Experience Rules."

If you enabled adaptive portlet layouts, users can select them for their My Pages, community managers can select them for their community pages, and administrative users with the Access User Profile Manager activity right can select them for the profile pages.

4.1.1.1 Creating a Remote Portlet Web Service for an Adaptive Layout

The tasks described below assume that you have already created the adaptive layouts as described in the Adaptive Page Layouts section of the *Oracle Fusion Middleware User Interface Customization Guide for Oracle WebCenter Framework Interaction*.

Before you create a remote portlet Web service, if necessary, create the remote server the Web service will point to. If your adaptive layouts are stored on the computer that hosts the Image Service, you can use the **ImageServer Remote Server**.To create a remote portlet Web service you must have the following rights and privileges:

- Access Administration activity right
- Create Web Service Infrastructure activity right
- At least Edit access to the parent folder (the folder that will store the Web service)
- At least Select access to the remote server the Web service will point to

1. Click **Administration**.
2. Open the **Page Layouts** folder.

   Remote portlet Web services for adaptive layouts must be stored in this folder to be available in the Experience Definition Editor and the Select Page Layout dialog box for My Pages and community pages.
3. Open the folder for the type of layout for which you are creating a Web service.

   For example, if you are creating a Web service for a layout that applies to search results pages, open the **Search Results Page Layouts** folder.
4. In the **Create Object** list, click **Web Service — Remote Portlet**.
5. Next to **Remote Server**, click **Browse**.

   The Choose Remote Server dialog box opens.
6. Select the remote server this Web service should point to and click **OK**.

   If your adaptive layouts are stored on the computer that hosts the Image Service, you can use the **ImageServer Remote Server**.
7. In the **Portlet URL** box, complete the path to the adaptive layout.

   For example:
   `plumtree/portal/private/pagelayouts/searchresultslayout.html`

The default security for this Web service is based on the security of the parent folder. You can change the security when you save this Web service (on the **Security** tab page in the Save As dialog box), or by editing this Web service (on the **Security** page of the Web Service Editor).

Note:

- If you are creating a Web service for a portlet layout, provide at least Select access to any users you want to be able to select the layout in My Pages or community pages.
- If you are creating a Web service for a page layout, provide at least Select access to any users you want to be able to select the layout in experience definitions.

4.1.1.2 Creating an Experience Definition to Display Adaptive Page Layouts

Before you create an experience definition that displays adaptive page layouts, you must:

- Create any custom adaptive page layouts you want to use
- Create remote portlet Web services for the custom adaptive page layouts

- Create the guest user you want to associate with the experience definition
- Create any header and footer portlets you want to use to brand the experience definition

To create an experience definition that displays adaptive page layouts you must have the following rights and privileges:

- Access Administration activity right
- Create Experience Definitions activity right
- At least Edit access to the parent folder (the folder that will store the experience)
- At least Select access to the remote portlet Web services for the adaptive page layouts
- At least Select access to the guest user you want to associate with the experience definition
- At least Select access to any header and footer portlets you want to add to the experience definition

1. Click **Administration**.
2. Open the folder in which you want to store the experience definition.

   Note: You might want to store all of the resources needed by a particular audience of users in the same folder in which you store those users. By securing the folder appropriately and applying experience definition settings to it you can create completely separate and discreet user experiences for each audience of users.

3. In the **Create Object** list, click **Experience Definition**.

   The Experience Definition Editor opens.
4. On **Experience Definition Features** page, complete the following tasks:
   - Section 4.3.4.1.1, "Associating Folders with an Experience Definition"
   - Section 4.3.4.2, "Selecting the Portal Menus and Home Page for an Experience Definition"
5. Click the **Choose Header, Footer & Style** page and complete the following task:
   - Section 4.3.4.3, "Branding Experience Definitions with Headers and Footers"
6. Click the **Edit Navigation Options** page and complete the following tasks:
   - Under **Navigation Type**, select **Portlet-Ready Navigation**.
   - Section 4.3.4.5, "Defining Mandatory Links to Display in an Experience Definition"
7. Click the **Login Settings** page and complete the following task:
   - Section 4.3.4.6, "Defining the Guest User Experience for an Experience Definition"
   - Section 4.3.4.7, "Disabling Single Sign-On (SSO) for an Experience Definition"
8. Click the **Adaptive Page Layout Settings** page and complete the following task:
   - Section 4.3.4.8, "Applying Adaptive Page Layouts"

9. Click the **Properties and Names** page and complete the following tasks:
   - Section 5.15, "Naming and Describing an Object"

     You can instead enter a name and description when you save this experience definition.
   - Section 5.15.1, "Localizing the Name and Description for an Object" (optional)
   - Section 5.16, "Managing Object Properties" (optional)

The default security for this experience definition is based on the security of the parent folder. You can change the security when you save this experience definition (on the **Security** tab page in the Save As dialog box), or by editing this experience definition (on the **Security** page of the Experience Definition Editor).

4.2 Reverting to a Legacy User Interface

If you want to display the user interface used in previous versions of the portal you can do so with settings in the Experience Definition Editor.

1. Open the Experience Definition Editor by creating a new experience definition or editing an existing one.
2. Click the **Adaptive Page Layout Settings** page.
3. Under **Adaptive Page Layout Mode**, clear the **Enable Adaptive Page Layout Mode** box.
4. Perform tasks on the remaining pages as necessary:
   - Section 4.3.4.1.1, "Associating Folders with an Experience Definition"
   - Section 4.3.4.2, "Selecting the Portal Menus and Home Page for an Experience Definition"
   - Section 4.3.4.3, "Branding Experience Definitions with Headers and Footers"
   - Section 4.3.4.4, "Selecting a Navigation Scheme for an Experience Definition"

     Note: You must select different header and footer portlets (the layout header and footer portlets will not work in a legacy user interface). If you select a header portlet that does not include navigation, you cannot use **Portlet-Ready Navigation** (or users will not see any navigation).
   - Section 4.3.4.5, "Defining Mandatory Links to Display in an Experience Definition"
   - Section 4.3.4.6, "Defining the Guest User Experience for an Experience Definition"
   - Section 4.3.4.7, "Disabling Single Sign-On (SSO) for an Experience Definition"
   - Section 5.15, "Naming and Describing an Object"

     You can instead enter a name and description when you save this experience definition.
   - Section 5.15.1, "Localizing the Name and Description for an Object" (optional)
   - Section 5.16, "Managing Object Properties" (optional)
   - Section 5.17, "Setting Security on an Object"

4.3 About Controlling the User Interface with Experience Definitions and Experience Rules

Experience definitions provide multiple user experiences within a single portal. An experience definition defines certain elements of a user experience, such as adaptive page layout settings, branding style, and navigation. An experience rule defines the conditions that, when met, display the associated experience definition to a user.

4.3.1 Experience Definitions

The experience definition specifies the following:

- Which portal menus to display (My Pages, My Communities, Directory)
- What navigation scheme to display
- Which header and footer to display

> **Note:** The headers and footers can be overridden at the community level.

- Any mandatory links to display
- The default page displayed when a user logs in (such as a My Page, a particular community, or a Knowledge Directory folder)

Users are directed to a particular experience definition in three ways (in the following order):

1. The users satisfy a rule you create in the Experience Rules Manager. These rules may specify the URL used to access the portal, a community the user accesses, a group to which the user belongs, or the user's IP address.
2. The users are stored in a folder that is associated with the experience definition.
3. If neither of the above conditions are met, users experience the default experience definition for the portal.

> **Note:** You might want to store all of the resources needed by a particular audience of users in the same folder in which you store those users. By securing the folder appropriately and applying experience definition settings to it you can create completely separate and discreet user experiences for each audience of users.

4.3.2 Experience Rules

When you create an experience rule, you must also place it in rank order in relation to existing rules. The first rule to evaluate to true will be applied. For example, you might create a rule that says that users in the Marketing group see the user interface defined in the Marketing experience definition, and another rule that says that users in the Management group see the user interface defined in the Management experience definition. Since some users may be in both groups, you may decide that you want the Management experience definition to have priority. In this case, you order the two rules so that the Management experience rule is above the Marketing experience rule.

4.3.3 Guest User Experiences

If you want to have different user experiences for different audiences of guest users (users that have not logged in), you might want to create several guest users and assign them different experience definitions. For an example, see the Guest Users section in Section 6.1, "About Users."

4.3.4 Creating an Experience Definition to Control the User Interface

Before you create an experience definition you must:

- Create any custom adaptive page layouts you want to use
- Create remote portlet Web services for any custom adaptive page layouts
- Create the guest user you want to associate with the experience definition
- Create any header and footer portlets you want to use to brand the experience definition

To create an experience definition you must have the following rights and privileges:

- Access Administration activity right
- Create Experience Definitions activity right
- At least Edit access to the parent folder (the folder that will store the experience)
- If you want to apply adaptive page layouts to the experience definition, at least Select access to the remote portlet Web services for the adaptive page layouts
- At least Select access to the guest user you want to associate with the experience definition
- At least Select access to any header and footer portlets you want to add to the experience definition

1. Click **Administration**.
2. Open the folder in which you want to store the experience definition.

   Note: You might want to store all of the resources needed by a particular audience of users in the same folder in which you store those users. By securing the folder appropriately and applying experience definition settings to it you can create completely separate and discreet user experiences for each audience of users.

3. In the **Create Object** list, click **Experience Definition**.

   The Experience Definition Editor opens.
4. Complete the tasks on **Experience Definition Features** page:
   - Section 4.3.4.1.1, "Associating Folders with an Experience Definition"
   - Section 4.3.4.2, "Selecting the Portal Menus and Home Page for an Experience Definition"
5. Click the **Choose Header, Footer & Style** page and complete the following task:
   - Section 4.3.4.3, "Branding Experience Definitions with Headers and Footers"
6. Click the **Edit Navigation Options** page and complete the following tasks:
   - Section 4.3.4.4, "Selecting a Navigation Scheme for an Experience Definition"

- Section 4.3.4.5, "Defining Mandatory Links to Display in an Experience Definition"

7. Click the **Login Settings** page and complete the following task:
   - Section 4.3.4.6, "Defining the Guest User Experience for an Experience Definition"
   - Section 4.3.4.7, "Disabling Single Sign-On (SSO) for an Experience Definition"
8. Click the **Adaptive Page Layout Settings** page and complete the following task:
   - Section 4.3.4.8, "Applying Adaptive Page Layouts"
9. Click the **Properties and Names** page and complete the following tasks:
   - Section 5.15, "Naming and Describing an Object"

     You can instead enter a name and description when you save this experience definition.
   - Section 5.15.1, "Localizing the Name and Description for an Object" (optional)
   - Section 5.16, "Managing Object Properties" (optional)
10. Click the **Security** page and complete the following task:
    - Section 5.17, "Setting Security on an Object"

Note: Changes made to an experience definition take 15 minutes to be updated in the cache and be reflected to users.

4.3.4.1 Specifying a User Experience for Users in a Folder

You can specify a user experience for users in a folder by associating an experience definition with the folder.

Note: Users will see the associated experience definition only if no other experience rules apply.

You can associate an experience definition with a folder in the Folder Editor or in the Experience Definition Editor.

- Section 4.3.4.1.2, "Applying an Experience Definition to a Folder"
- Section 4.3.4.1.1, "Associating Folders with an Experience Definition"

Note: When a folder has been associated with an experience definition, the icon representing the folder changes to:

Note: You might want to store all of the resources needed by a particular audience of users in the same folder in which you store those users. By securing the folder appropriately and applying experience definition settings to it you can create completely separate and discreet user experiences for each audience of users.

4.3.4.1.1 Associating Folders with an Experience Definition

You can specify a user experience for users in a folder by associating an experience definition with the folder.

> **Note:** Users will see the associated experience definition only if no other experience rules apply.

1. If the Experience Definition Editor is not already open, open it now.
2. Select the administrative folders you want to associate with this experience definition.
   - To associate an existing folder, click **Add Folder**.
   - To create a new folder, click **Create Folder**.

> **Note:** When a folder has been associated with an experience definition, the icon representing the folder changes to:
>
> 

> **Note:** You might want to store all of the resources needed by a particular audience of users in the same folder in which you store those users. By securing the folder appropriately and applying experience definition settings to it you can create completely separate and discreet user experiences for each audience of users.

4.3.4.1.2 Applying an Experience Definition to a Folder

You can specify a user experience for users in a folder by associating an experience definition with the folder.

> **Note:** Users will see the associated experience definition only if no other experience rules apply.

1. Click **Administration**.
2. Open the folder to which you want to apply an experience definition in Folder Editor.
3. Click the **Experience Definition Settings** page.
4. In the list, select the experience definition you want to apply to users stored in this folder.
5. To change the settings for the selected experience definition, click **Edit Profile**.

   This opens the Experience Definition Editor.

> **Note:** When a folder has been associated with an experience definition, the icon representing the folder changes to:
>
> 

> **Note:** You might want to store all of the resources needed by a particular audience of users in the same folder in which you store those users. By securing the folder appropriately and applying experience definition settings to it you can create completely separate and discreet user experiences for each audience of users.

4.3.4.2 Selecting the Portal Menus and Home Page for an Experience Definition

For each experience definition you can specify which portal menus appear and which page users should see when they log in to the portal.

1. If the Experience Definition Editor is not already open, open it now.
2. In the **Enable** column, select the menus (and associated features) you want to include in this experience definition.

   For example, to include the My Pages menu and features, select the box associated with **My Pages**.

   > **Note:** If you disable the Knowledge Directory, users cannot browse document folders, but they can still search for portal documents.

3. In the **Home** column, select the portal area you want to display when users log in to the portal.

   For example, to display a particular community when a user logs in, select the button associated with **Communities**.
4. If you selected **Communities** as the home page you must also select a particular community.
   - To choose a home community from existing communities, click **Choose Home Community**.
   - To create a new home community, click **Create Home Community**.

   > **Note:** Users viewing this experience definition must have at least Read access to the community you choose, or they will receive an error after logging in.

5. If you selected the **Knowledge Directory** as the home page you must also select a particular folder.
   - To choose a home folder from existing folders, click **Choose Home Folder**.
   - To create a new home folder, click **Create Home Folder**.

   > **Note:** Users viewing this experience definition must have at least Read access to the folder you choose, or they will receive an error after logging in.

6. If you enabled the **Knowledge Directory**, under **Include these Knowledge Directory Features**, select which related object features you want to display in the Knowledge Directory.

By default, objects specified as related to a Knowledge Directory folder display to users viewing that folder. To hide a type of related object, clear the associated check box.

4.3.4.3 Branding Experience Definitions with Headers and Footers

The Choose Header, Footer & Style page of the Experience Definition Editor enables you to add special branding portlets to an experience definition (as well as change the color scheme) to control what certain groups of users see at the top and bottom of portal pages.

You must create the header and footer portlets you want to use before branding the experience definition.

1. If the Experience Definition Editor is not already open, open it now.
2. Click the **Choose Header, Footer & Style** page.
3. In the **Default Style** list, select a color scheme.

   Note: If you are using adaptive page layouts, the layout will override the style selected here.

4. Under **Add Header**, select the header portlet you want to apply to the experience definition:
   - To add or change the header, click **Add Header**.
   - To remove the header, select it, then click the Remove icon.
5. Under **Add Footer**, select the footer portlet you want to apply to the experience definition:
   - To add or change the header, click **Add Footer**.
   - To remove the footer, select it, then click the Remove icon.

   Note: The community template header and footer can be set to override the experience definition header and footer.

4.3.4.4 Selecting a Navigation Scheme for an Experience Definition

For each experience definition you can specify a default navigation style to define the menu layout and core navigation structure most appropriate for your bandwidth constraints, browser requirements, design needs, deployment size, and end-user expectations.

1. If the Experience Definition Editor is not already open, open it now.
2. Click the **Edit Navigation Options** page.
3. Under **Navigation Type**, choose a navigation scheme.
   - **Horizontal Combo Box Drop-Down Navigation**: This navigation scheme uses standard HTML controls to place navigational elements in drop-down menus. Because it does not use JavaScript for rendering menus, this option is bandwidth-efficient.
   - **Tabbed Section Left Vertical Navigation**: This navigation scheme uses horizontal tabs at the top for the main portal areas, which, when clicked,

display links on the left to the options available within that portal area. This scheme is similar to the navigation for sites such as Amazon.com and MSN.

- **Left Vertical Navigation**: This navigation scheme lists all available links unless the user minimizes particular elements. It is very easy to use, because users see all links without additional clicks. Because it does not use JavaScript for rendering menus, this option is bandwidth-efficient. However, if users join a large number of communities, they have to scroll to see some links.
- **Mandatory Links Only**: This navigation scheme displays only the mandatory links (which you specify in the experience definition) using the same menu style used in Horizontal Drop-Down Navigation. Users can see only their home page (the page that displays when they log in) and any areas for which you have created mandatory links. However, they can still access documents through search and might be able to access other areas if those areas are available through portlets. You might use this scheme if you want to severely limit portal access to users. For example, you might want a group of customers to access only a particular community to learn about a new product.
- **No Navigation**: This navigation scheme displays no navigation, but includes the top bar. However, there is a link to Administration if the user has access. As with the Mandatory Links Only navigation scheme, users can access portal content and areas through search and portlets.
- **Horizontal Drop-Down Navigation**: This navigation scheme uses horizontal tabs and JavaScript-based drop-down menus to access navigation elements. Clicks, not mouse-overs, display the menus. The drop-down menus expand both vertically and horizontally, but cover only the portal's banner to avoid covering the portlets. If a user belongs to more communities than can fit in the allotted space, a vertical scroll bar appears in the drop-down. You can configure the extent of the vertical and horizontal tiling of the drop-down menus.
- **Low Bandwidth and Accessibility Navigation**: Low Bandwidth and Accessibility Navigation is used by low bandwidth and accessibility modes of the portal. This navigation is used by those modes no matter which navigation is selected by the experience definition for standard mode.
- **Portlet-Ready Navigation**: Portlet-Ready Navigation disables all navigation areas except the header and footer. The top bar, which includes the search box, is also disabled. This navigation scheme is only used when you are using adaptive page layouts or when navigation is controlled by portlets (usually header or footer portlets) using navigation tags. Adaptive page layouts and navigation tags provide developers a faster, easier way to customize navigation than modifying the other available navigation schemes.

Note:

- If you have written your own navigation styles, they should also be available on this page.
- Vertical navigation styles lessen the page width available for portlets on My Pages and community pages.
- If you have selected any navigation option other than Portlet-Ready Navigation, do not use the default adaptive page layouts available with the portal. If you use the default adaptive page layouts with other navigation options, users will see two methods of navigation.
- The experience definition you log in to might have a different navigation style than the experience definition you are creating. To ensure that the experience definition you are creating has the appropriate appearance, log in as a user that sees that experience definition.

If you selected **Mandatory Links Only**, you must now define the mandatory links. See Section 4.3.4.5, "Defining Mandatory Links to Display in an Experience Definition."

If you selected **Portlet-Ready Navigation**, you must select the header and footer and/or the adaptive page layout settings that define your navigation. See Section 4.3.4.3, "Branding Experience Definitions with Headers and Footers" and Section 4.3.4.8, "Applying Adaptive Page Layouts."

4.3.4.5 Defining Mandatory Links to Display in an Experience Definition

For each experience definition you can define links to Web pages, experts, documents, and community pages that are displayed to users as part of the navigation.

1. If the Experience Definition Editor is not already open, open it now.
2. Click the **Edit Navigation Options** page.
3. Under **Edit Links**, add and modify links to Web pages, experts, documents, and community pages.
   - Click **Add Links** to add links to Web pages.
   - Click **Add Experts** to add links to experts.
   - Click **Add Documents** to add links to documents and document folders in the Knowledge Directory.
   - Click **Add Pages** to add links to community pages.
   - To remove links, select the links you want to delete and click the Remove icon.

     To select or clear all link boxes, select or clear the box under **Navigation Link Heading**.
   - If these links are shared with another experience definition and you do not want to share them, click **Separate**.

     If this is a copy of another experience definition or if this experience definition has been copied, you see a warning that the navigation links are shared between the experience definitions. Any changes you make to these links are reflected in the linked experience definitions.

- To change the menu heading that displays to users, type the text in the **Navigation Link Heading** box.

  When you add navigation links, they display in a new menu, similar to the My Pages menu.

  Note: You might have access to resources to which members of your experience definition do not have access. If users do not have access to a resource listed as a navigation link, they will not see the link.

4.3.4.6 Defining the Guest User Experience for an Experience Definition

For each experience definition you can associate a guest user, which lets you define the initial page an unauthenticated user sees when coming to this experience definition. For example, if an unauthenticated user is directed to this experience definition (through application of an experience rule), you can choose to have that user see the My Page layout of the guest user you associate with this experience definition, even if the experience definition is not set to display My Pages. You can also specify what page users see when they log out of an experience definition.

1. If the Experience Definition Editor is not already open, open it now.
2. Click the **Login Settings** page.
3. Under **Guest Settings**, click **Select a Guest User**, and choose a guest user to associate with this experience definition.
4. Under **Login Page Settings**, select what page unauthenticated users should see when they access this experience definition.

   - To display the default My Page for the selected guest user, select **Guest MyPage**.
   - To display the default login page shared across all experience definitions, select **Default Login Page**.

   Unauthenticated users viewing this experience definition will be directed to the page you select here if, in the portal configuration file, GuestRedirectToLogin is set to 1, or if they click **Log In**. Otherwise, unauthenticated users see the home page selected for this experience definition.

   Note: If you selected **Guest MyPage** ensure that the Portal Login portlet displays on the selected guest user's default My Page so that unauthenticated users can log in.

5. Under **Login Page Settings**, select what page users should see when they log out of this experience definition.

   - To display the default My Page for the selected guest user, select **Guest MyPage**.
   - To display the default login page shared across all experience definitions, select **Default Login Page**.

   Users will be directed to the page you select here if, in the portal configuration file, RedirectOnLogout is set to 1. Otherwise, upon logout, users see the home page specified for this experience definition.

Note: If you selected **Guest MyPage** ensure that the Portal Login portlet displays on the selected guest user's default My Page so that unauthenticated users can log in.

4.3.4.7 Disabling Single Sign-On (SSO) for an Experience Definition

You can override portal SSO settings for users in this experience definition. Otherwise the SSO settings in the portal configuration file will apply.

1. If the Experience Definition Editor is not already open, open it now.
2. Click the **Login Settings** page.
3. Under **Disable Single Sign On (SSO)**, specify whether you want to disable SSO for this experience definition.

   Select **Disable SSO Setting** to override portal SSO settings for users in this experience definition. Otherwise the SSO settings in the portal configuration file will apply.

   Note: This check box is unavailable (grayed-out) if the "SSOVendor" setting is 0 in the portal configuration file.

4.3.4.8 Applying Adaptive Page Layouts

For each experience definition you can specify whether to use adaptive page layouts to display the user interface or use a legacy user interface used in previous versions of the portal.

The tasks described below assume that adaptive page layouts have not been disabled in the portal configuration file and that you have already created the adaptive page layouts as described in the Adaptive Page Layouts section of the *Oracle Fusion Middleware User Interface Customization Guide for Oracle WebCenter Framework Interaction*.

Before you apply adaptive page layouts to an experience definition, you must create remote portlet Web services for the adaptive page layouts.

To apply adaptive page layouts you must have at least Select access to the remote portlet Web services for the adaptive page layouts.

1. If the Experience Definition Editor is not already open, open it now.
2. Click the **Adaptive Page Layout Settings** page.
3. Under **Adaptive Page Layout Mode**, specify if this experience definition should display adaptive page layouts.

   To enable adaptive page layouts for this experience definition, select **Enable Adaptive Page Layout Mode**.

Note:

- This setting is not available if adaptive layouts are disabled in the portal configuration files.
- This setting controls only adaptive page layouts, not adaptive portlet layouts, which are controlled by the page layouts selected for My Pages and community pages.
- If you disable adaptive page layouts, this experience definition will display a legacy user interface used in previous versions of the portal.

4. If you enabled adaptive page layouts, under **Layout Chooser for Page Layouts**, specify the layouts you want to display for each page layout type.
   - In the **Base Page Layouts** list, select the layout for components that are common to each page (header, footer, navigation, content area).

     The layouts listed in this list correspond to the remote portlet Web services stored in the **Page Layouts/Base Page Layouts** administrative folder.
   - In the **Profile Page Layouts** list, select the layout for components that are common to each user profile page (header, footer, navigation, content area).

     The layouts listed in this list correspond to the remote portlet Web services stored in the **Page Layouts/Profile Page Layouts** administrative folder.
   - In the **Knowledge Directory Layouts** list, select the layout for the content area of the Directory.

     The layouts listed in this list correspond to the remote portlet Web services stored in the **Page Layouts/Knowledge Directory Page Layouts** administrative folder.

     Note: The common components of the Directory are specified in the base page layout.

   - In the **Search Results Layouts** list, select the layout for the content area of the search results.

     The layouts listed in this list correspond to the remote portlet Web services stored in the **Page Layouts/Search Results Page Layouts** administrative folder.

     Note: The common components of the search results are specified in the base page layout.

   - In the **Advanced Search Layouts** list, select the layout for the content area of the advanced search page.

     The layouts listed in this list correspond to the remote portlet Web services stored in the **Page Layouts/Advanced Search Page Layouts** administrative folder.
   - In the **Portlet Selection Layouts** list, select what layout to use for the pop-up or fly-out editor used to select portlets.

The layouts listed in this list correspond to the remote portlet Web services stored in the **Page Layouts/Portlet Selection Page Layouts** administrative folder.

If you have not already done so, you must select **Portlet Ready Navigation** on the **Edit Navigation Options** page of this editor.

4.4 About Branding with Header and Footer Portlets

Branding portlets customize the look of your portal with headers and footers. For example, you probably want to add your company logo and tagline to the header and you might want to add contact information or copyrights to the footer.

Note: The easiest way to apply branding (and control the look of your user interface) is with adaptive page layouts, which are then applied through experience definitions.

There are several ways to brand your portal:

- The easiest way to apply branding (and control the look of your user interface) is with adaptive tags and adaptive page layouts. There are two example branding portlets that use adaptive tags and are installed with the portal: Layout Footer Portlet and Layout Header Portlet. For information on adaptive tags, adaptive page layouts, and the example portlets, see the *Oracle Fusion Middleware User Interface Customization Guide for Oracle WebCenter Framework Interaction*.
- You can also create your own custom branding portlets. There are two example branding portlets that are installed with the portal: Classic Footer Portlet and Classic Header Portlet. For information on creating custom branding portlets, see the *Oracle Fusion Middleware User Interface Customization Guide for Oracle WebCenter Framework Interaction*.

4.4.1 About Header and Footer Portlet Precedence

You apply header and footer portlets at the community template, community, or experience definition level. The community template settings determine what header and footer are used in the community.

- The community template can force the community to use the experience definition branding.
- The community template can include its own branding that cannot be overridden in the community. This branding overrides the experience definition branding.
- If the community template does not specify any branding restrictions, the community can include its own branding. This branding overrides the experience definition branding.

4.5 About Navigation Options

The portal includes navigation schemes that allow you to select the menu layout and core navigation structure most appropriate for your bandwidth constraints, browser requirements, design needs, deployment size, and end-user expectations. You can also create your own navigation schemes, using the existing code as a starting point.

For information on customizing navigation and other user interface elements, see the *Oracle Fusion Middleware User Interface Customization Guide for Oracle WebCenter Framework Interaction*.

The navigation schemes included with the portal can be divided into horizontal and vertical groups, based on the alignment of the navigational elements. In horizontal navigation, links to My Pages, communities, the Knowledge Directory, Administration, and any mandatory links you specify appear at the top of the page in drop-down menus, maximizing the space available for portlets. In vertical navigation, links appear on the left side of the screen.

You can select one of the following navigation schemes for each experience definition you create:

- **Horizontal Combo Box Drop-Down Navigation**: This navigation scheme uses standard HTML controls to place navigational elements in drop-down menus. Because it does not use JavaScript for rendering menus, this option is bandwidth-efficient.
- **Tabbed Section Left Vertical Navigation**: This navigation scheme uses horizontal tabs at the top for the main portal areas, which, when clicked, display links on the left to the options available within that portal area. This scheme is similar to the navigation for sites such as Amazon.com and MSN.
- **Left Vertical Navigation**: This navigation scheme lists all available links unless the user minimizes particular elements. It is very easy to use, because users see all links without additional clicks. Because it does not use JavaScript for rendering menus, this option is bandwidth-efficient. However, if users join a large number of communities, they have to scroll to see some links.
- **Mandatory Links Only**: This navigation scheme displays only the mandatory links (which you specify in the experience definition) using the same menu style used in Horizontal Drop-Down Navigation. Users can see only their home page (the page that displays when they log in) and any areas for which you have created mandatory links. However, they can still access documents through search and might be able to access other areas if those areas are available through portlets. You might use this scheme if you want to severely limit portal access to users. For example, you might want a group of customers to access only a particular community to learn about a new product.
- **No Navigation**: This navigation scheme displays no navigation, but includes the top bar. However, there is a link to Administration if the user has access. As with the Mandatory Links Only navigation scheme, users can access portal content and areas through search and portlets.
- **Horizontal Drop-Down Navigation**: This navigation scheme uses horizontal tabs and JavaScript-based drop-down menus to access navigation elements. Clicks, not mouse-overs, display the menus. The drop-down menus expand both vertically and horizontally, but cover only the portal's banner to avoid covering the portlets. If a user belongs to more communities than can fit in the allotted space, a vertical scroll bar appears in the drop-down. You can configure the extent of the vertical and horizontal tiling of the drop-down menus.
- **Low Bandwidth and Accessibility Navigation**: Low Bandwidth and Accessibility Navigation is used by low bandwidth and accessibility modes of the portal. This navigation is used by those modes no matter which navigation is selected by the experience definition for standard mode.
- **Portlet-Ready Navigation**: Portlet-Ready Navigation disables all navigation areas except the header and footer. The top bar, which includes the search box, is also

disabled. This navigation scheme is only used when you are using adaptive page layouts or when navigation is controlled by portlets (usually header or footer portlets) using navigation tags. Adaptive page layouts and navigation tags provide developers a faster, easier way to customize navigation than modifying the other available navigation schemes.

Any navigation scheme (except the No Navigation scheme) can include mandatory links to Web sites, user profiles of portal experts, documents from the portal Knowledge Directory, and pages in communities. These links display in the navigation scheme under a category (like My Pages, My Communities, or Directory) with the name of your choosing. You might want to use these links to promote new portlets, communities, or important documents.

4.6 About Portal Interface Types

Interface Type	Description
Standard Portal	The fully-featured user interface for the Oracle WebCenter Interaction software. Use it to provide the richest user interface experience for internal and external users. This version does not support assistive technologies.
Assistive Technology Portal	Designed for people with disabilities. It supports only portlets that meet requirements for use with assistive technologies. Section 508 of the Rehabilitation Act is a federal statute requiring federal agencies' electronic and information technology to be accessible to people with disabilities, including employees and members of the public. The federal criteria for web-based technology are based on access guidelines developed by the Web Accessibility Initiative of the World Wide Web Consortium (W3C). Designed to adhere to the federal criteria for web-based technology, the Assistive Technology Portal allows end users with visual disabilities to access the portal through assistive browsing technologies, such as screen readers, screen magnifiers, voice recognition and Braille devices. The interface is text-based with a linear presentation of information, and with no embedded client-side JavaScript or Java applets.
Low Bandwidth Portal	Accommodates users with slower internet connections. This version supports all Oracle WebCenter portlets, but does not support assistive technologies. Remote users have two options for viewing portal pages—the standard version and the Low Bandwidth version. Users can switch from one version to the other during a portal session and the change occurs immediately. The Low Bandwidth Portal provides better performance for end users accessing the portal remotely when network performance is slow due to low bandwidth or heavy traffic. This version presents a user interface with far fewer graphics and no embedded JavaScript or Java applets.

4.7 About Locale Settings

Users can change their portal display to accommodate their time zone and locale (from the **My Account** menu, they can click **Edit Locale Settings**). The locale determines:

- The language displayed in the portal interface (portlet names and content display in the language you choose only if those portlets support your chosen language).
- The format for portal entries (including search requests). For example, if you choose British English, the portal displays and expects dates in the DD/MM/YYYY format, whereas in American English, the portal displays and expects dates in the MM/DD/YYYY format.

Note: Only the portal interface and localized objects display in the language you choose. Your personal greeting does not change if you change your locale.

4.8 About Controlling the Initial Portal Experience

Oracle WebCenter Interaction includes several features that work together to control users' initial portal experience, such as the user interface and access to content.

Feature	How the Feature is Applied to Users Created Manually	How the Feature is Applied to Users Self-Registered	How the Feature is Applied to Users Imported Through an Authentication Source	How the Feature is Applied to Users Created Through Acceptance of an Invitation
Default Profiles Each user is assigned a default profile at creation. Default profiles define initial My Account settings, such as language, time zone, and portal interface type; the name and number of My Pages; and the layout of the portlets on those My Pages. Default profiles provide an initial view of the portal, which users can then change to fit their needs. For information on default profiles, see	Automatically assigned the "Default Profile" created at installation	Automatically assigned the "Default Profile" created at installation	Automatically assigned the default profiles specified in the Authentication Source Editor	Automatically assigned the default profile specified in the Invitation Editor
Group Membership	All users are automatically added to the Everyone group and can be assigned to groups manually in the User Editor or Group Editor after creation.			
The most efficient way to manage access to content is to assign access privileges to groups. The only way to assign activity rights (which control access to features) is to assign the rights to groups. You can then add new users to the appropriate groups.	Manually assigned in the User Editor during creation	(No additional membership assigned during creation; assigned only to the Everyone group)	Automatically assigned to groups based on the mappings in the Global ACL Sync Map (and any mappings that occur automatically if the authentication source category matches the domain name)	Automatically assigned to groups specified in the Invitation Editor

Feature	How the Feature is Applied to Users Created Manually	How the Feature is Applied to Users Self-Registered	How the Feature is Applied to Users Imported Through an Authentication Source	How the Feature is Applied to Users Created Through Acceptance of an Invitation
Mandatory Communities and Portlets Mandatory communities are communities to which the user cannot unsubscribe. Mandatory portlets are portlets that cannot be removed from a user's My Page.	The most efficient way to manage mandatory communities and portlets is to make them mandatory for particular groups. You then add new users to the appropriate groups as mentioned in the previous entry.			
Experience Definitions	All users are assigned the experience definition associated with the folder in which the user is stored. You can also use experience rules to assign experience definitions to users.			
	Manually create the user in the folder of your choice	Automatically created in the "Default Experience Definition" folder created at installation	Automatically created in the folders specified in the Authentication Source Editor	Automatically created in the folder specified in the Invitation Editor

5

Managing Administrative Objects and Portal Utilities

This chapter describes the Administration area and the Administrative Objects Directory, which enable you to create and manage administrative objects, and access the portal utilities.

This chapter describes the following tasks:

5.1 Planning Your Administrative Object Hierarchy

The Administrative Object Directory is a hierarchical folder structure that stores administrative objects such as content sources, portlets, and users.

The following guidelines can assist you in planning an administrative object hierarchy:

- Start with the end-user hierarchy rather than an organizational or management structure. End-users can see the administrative hierarchy in a few places in the portal. For example, by default, the Add Portlets and Join Communities pages search the administrative hierarchy for available portlets and communities and display a list of objects without showing their parent folders.

  Start by creating the hierarchy for communities and portlets (including portlet bundles) only and hide the administrative objects created during installation. For example, move all objects meant for administrators to a particular folder and restrict access to the folder so that end-users will not see it if they browse the hierarchy.

  The organization of the objects meant for administrators should be based on administrative structure or topic.
- Organize objects by topic rather than by object type. Objects are automatically grouped by type within each folder.
- Set ACLs for folders as early as possible. Objects created in a folder inherit the ACL of the folder. By planning access control early, you simplify managing object security.
- Manage user access by managing groups. Assigning a user to a group with permissions to a set of objects is easier than assigning each user to each object in the set.

5.2 Viewing Objects

You can view objects through the Administrative Objects Directory and through some portal utilities.

Note: To view an object you must have the Access Administration activity right and at least Read access to the object.

To display the Administrative Objects Directory and access portal utilities, click **Administration**.

- To view the contents of a folder, click its name.
- To view all objects of a particular type stored in the folder, click the object type (for example, crawler, portlet, or user). To hide these objects, click the object type again.
- To expand all the object types so you can view all objects stored in this folder, click the Expand All icon.
- While viewing a subfolder, to navigate up to the parent folder, click **Up**, or click the parent folder name in folder path.
- By default, only the first 50 objects display. To view the next 50 objects, click **Next >>**, or to view another set of 50 objects, click a number range.
- To view default profiles, in the **Select Utilities** list, select **Default Profiles**.

5.3 Searching for Objects in the Administrative Objects Directory

You can search for objects in the Administrative Objects Directory.

1. Click **Administration**.

2. Specify your criteria in the **Object Search** boxes:
   - To limit your search to particular types of objects (for example, crawler, portlet, or user), in the first list, select the object type.
   - To limit your search to particular folders, in the second list, choose whether to search all administrative folders, only the folder you are currently viewing, or the folder you are viewing plus its subfolders.
   - In the text box, type the text you want to search for and click the Search icon.

     You can use the text search rules described in Section F.3, "Using Text Search Rules."

5.4 Searching for Objects or Documents Using Advanced Search

You can perform an advanced search, using metadata properties and location, to find objects or documents.

In the portal banner or in the Administrative Objects Directory, click **Advanced Search**.

- Specify how you want your search criteria handled:
  - To meet all the conditions you define, select **All Criteria**.

    Selecting All Criteria is equivalent to using AND.
  - If you want your search results to meet at least one of the conditions you define, select **Any Criterion**.

    Selecting Any Criterion is equivalent to using OR.
- To search for text in the name or description of an object or document, type the text you want to search for in the **Search** for text box.

  You can use the text search rules described in Section F.3, "Using Text Search Rules."
- To search for property values, click **Add Criteria**, and specify the property criteria in the boxes that appear:

  1. In the first list (property), select the searchable property for which you want to filter the values.
  2. In the second list (operator), select the operator to apply to this condition.

     This list will vary depending on the property selected:
     - For any text property you can search for a value that contains your search string (Contains), or you can search for properties that are blank (Contains No Value).

     Note: To exclude results with particular values, select **Contains**, then type “not” followed by words to exclude from your search. For example, if you want to search for jobs, excluding database update jobs, type "jobs" in the Search for text box, select Contains from the drop-down list, and type "not database update" in the text box.

     - For any date property you can search for a value that comes after, comes before, is, or is not the date and time you choose or for a value that occurs in the last number of minutes, hours, days, or weeks that you specify.

  - For any number property you can search for a value that is greater than, is less than, is, is not, is greater than or equal to, or is less than or equal to the number you enter in the text box.

3. In the **Value** text box, enter the value the property must have, or not have, depending on which operator you selected.

Note: If you are searching for a text property, you can use the text search rules.

- To remove a property condition, select the condition and click the Remove icon (next to **Add Criteria**).
- To restrict your search to specific Knowledge Directory folders, click **Add Document Folder**. In the Select folder for search dialog box, select the folders you want to search and click **OK**.
- To restrict your search to specific Administrative Objects Directory folders, click **Add Administration Folder**. In the Select folder for search dialog box, select the folders you want to search and click **OK**.
- To remove folders from your list, select the folders and click the Remove icon (next to **Add Administration Folder**).

  To select or clear all folder boxes, select or clear the box next to **Folder Names**.
- By default, the portal searches subfolders. To exclude subfolders from your search, clear the box next to **Include subfolders**.
- To specify the number of results to display on a page, in the **Results per page** list, choose a value.
- To restrict your search to a specific language, in the **This language only** list, choose a language.
- To limit your search to specific object types, in the **Result Types** list, select the object types you want to search.

  To select or clear all object type boxes, select or clear the box next to **Object Type**.
- To set all search conditions back to the defaults, click **Clear**.
- To perform your search, click **Search**.

5.4.1 Complex Property Search Example

You can use multiple property criteria to define complex property searches.For example, if you want to find administrative items created after a certain date by a specific branch of a company, you could set the property criteria to the following values:

- First Criterion:
  - Property = Object Created
  - Operator = Comes After
  - Value = December 30, 2003

  Your search results would be limited to objects created after December 30, 2003.
- Second Criterion:

  - Property = Company
  - Operator = Contains
  - Value = Company A

  Your search results would be limited to objects where the company property contains Company A.

- Third Criterion:
  - Property = Address
  - Operator = Contains
  - Value = San Francisco

  Your search results would be limited to objects that contain San Francisco in the address.

5.5 Creating an Administrative Folder

Administrative folders provide a hierarchical structure that make it easy to organize portal objects and manage security.

> **Note:** You might want to store all of the resources needed by a particular audience of users in the same folder in which you store those users. By securing the folder appropriately and applying experience definition settings to it you can create completely separate and discreet user experiences for each audience of users.

To create an administrative folder you must have the following rights and privileges:

- Access Administration activity right
- Create Admin Folders activity right
- At least Edit access to the parent folder (the folder in which you are creating the new folder)

Creating an administrative folder is different than creating other administrative objects. To create an administrative folder:

1. Click **Administration**.
2. If necessary, open the folder in which you want to store the new folder.
3. In the Create Object list, click **Administrative Folder**.

   The Create Administrative Folder dialog box opens.
4. In the **Name** box, type a name for the folder.

   This name appears in lists of objects from which users will sometimes choose; therefore, the name should clearly convey the purpose of this folder.
5. In the **Description** box, type a description for the folder.

   This description appears in the Administrative Objects Directory to provide other administrators further details on the purpose of this folder.
6. Click **OK**.

You can perform additional tasks when you edit this folder:

- Section 4.3.4.1.2, "Applying an Experience Definition to a Folder"
- Section 5.15, "Naming and Describing an Object"
- Section 5.16, "Managing Object Properties"
- Section 5.17, "Setting Security on an Object"
- Section 5.18, "Viewing Migration History and Status for an Object"

5.6 Creating an Object

You can create objects such as folders, portlets, and users in the Administrative Objects Directory.

> **Note:** To create an object you must have the Access Administration activity right and the activity right associated with creating that type of object. You must also have at least Edit access to the parent folder (the folder that will store the object).

1. Click **Administration**.
2. If necessary, open the folder in which you want to store the object.

   You can create folders in the root of the Administrative Objects Directory, but other objects must be created in a folder.

   > **Note:** You can create default profiles only from the Default Profiles Utility: in the **Select Utilities** list, select **Default Profiles**.

3. In the Create Object list, select the type of object you want to create.

   The list displays only those objects you have permission to create in the folder.

   Depending on the type of object you are creating, either the object editor opens, or a dialog box opens prompting you to choose a content source, template, or Web service.

4. If necessary, select the appropriate content source, template, or Web service and click **OK**.

   A remote authentication source, a remote content source, an outgoing federated search, or a profile source requires a Web service. A portlet requires a template or Web service. A content crawler requires a content source.

   The object editor opens.

5. Perform tasks as necessary on the object-specific pages. For details on these settings, see the chapter associated with the object or click the help icon on the editor page.
6. If the object needs a job to run, perform tasks as necessary on the Set Job page:
   - Section 5.14, "Associating an Object with a Job"
7. Perform tasks as necessary on the Properties and Names page:
   - Section 5.15, "Naming and Describing an Object"
     - Section 5.15.1, "Localizing the Name and Description for an Object"

  - Section 5.15.2, "Viewing Top Best Bets for an Object"
- Section 5.16, "Managing Object Properties"

8. Perform tasks as necessary on the Security page:
   - Section 5.17, "Setting Security on an Object"

5.7 Editing an Administrative Folder

Editing an administrative folder is different than editing other administrative objects. To edit an administrative folder you must have at least Edit access to the folder.

1. Click **Administration**.
2. Navigate to the folder you want to edit.
3. Select the folder you want to edit and click **Edit Subfolder**.
4. Perform tasks as necessary on the Experience Definition Settings page:
   - Section 4.3.4.1.2, "Applying an Experience Definition to a Folder"
5. Perform tasks as necessary on the Properties and Names page:
   - Section 5.15, "Naming and Describing an Object"
   - Section 5.15.1, "Localizing the Name and Description for an Object"
   - Section 5.16, "Managing Object Properties"
   - Section 5.15.2, "Viewing Top Best Bets for an Object"
6. Perform tasks as necessary on the Security page:
   - Section 5.17, "Setting Security on an Object"
7. Perform tasks as necessary on the Migration History and Status page:
   - Section 5.18, "Viewing Migration History and Status for an Object"

5.8 Editing Object Settings in the Object Editor

Note: You must have at least Edit access to the object you want to edit. To edit an object from the Administrative Objects Directory, you must have the Access Administration activity right.

To edit an object in the object editor:

1. Open the object editor:
   - To edit a community while viewing it, in the My Communities menu, select the community you wan to edit, then click **Edit Page**.
   - To edit an object from the search results page, perform a search and click the name of the object you want to edit.
   - To edit an administrative folder or community, click **Administration**, open the folder or community you want to edit, and click the Edit this Folder/Edit this Community icon.
   - To edit any other object, click **Administration**, navigate to the object you want to edit, and click the name of the object.

2. Edit settings as necessary on the object-specific pages. For details on these settings, see the chapter associated with the object or click the help icon on the editor page.
3. If the object needs a job to run, edit settings as necessary on the Set Job page:
   - Section 5.14, "Associating an Object with a Job"
4. Edit settings as necessary on the Properties and Names page:
   - Section 5.15, "Naming and Describing an Object"
     - Section 5.15.1, "Localizing the Name and Description for an Object"
     - Section 5.15.2, "Viewing Top Best Bets for an Object"
   - Section 5.16, "Managing Object Properties"
5. Edit settings as necessary on the Security page:
   - Section 5.17, "Setting Security on an Object"
6. Perform tasks as necessary on the Migration History and Status page:
   - Section 5.18, "Viewing Migration History and Status for an Object"

5.9 Moving Objects

To move objects to a different folder, select one or more objects and click the Move Folder icon. In the Target Folder dialog box, expand the folders as necessary, select a folder, and click **OK**.

5.10 Copying Objects

To copy objects to a different folder, select one or more objects and click the Copy icon. In the Target Folder dialog box, expand the folders as necessary, select a folder, and click **OK**.

5.11 Deleting Objects

To delete objects, select one or more objects and click the Delete icon. In the confirmation dialog box, click **Apply Now**.

5.12 Modifying Security Settings for Objects

To modify the security settings for objects, select one or more objects and click the Security icon.

5.13 Migrating Objects

Object migration lets you copy resources from one portal to another. You might want to do this for several reasons. You might have multiple portals to handle a global deployment or you might want to create multiple portals to separate development, testing, and production.

For details, see Section 12, "Migrating, Backing-Up, and Restoring Your Portal."

5.14 Associating an Object with a Job

On the Set Job page, you can associate an object with a new or existing job. You run jobs to import users with authentication sources, import content with content crawlers, run external operations, and import user information with profile sources.

Before you can run jobs, you must:

- Confirm that the Oracle WCI Automation Service is running on the Automation Service computer. If it is not running, start it now, as described in Section 11.5.1, "Starting the Oracle WCI Automation Service."
- Register the Automation Service with the portal, as described in Section 11.5.2, "Registering Automation Services."
- Assign administrative folders to the registered Automation Services, as described in Section 11.5.3, "Registering Job Folders with Automation Services."

To associate an object with a job:

1. Open the object's editor by creating a new object or editing an existing object.
2. On the left, under Edit Object Settings, click **Set Job**.
3. Associate the object with one or more jobs:
   - To run this object with an existing job, click **Add Job**; then, in the Choose Jobs dialog box, select the jobs you want to add this object to and click **OK**.
   - To create a new job to run this object, click **Create Job**, then, in the Job Editor, schedule your job and click **Finish**.
   - To remove a job, select the job and click the Remove icon.

     To select or clear all of the job check boxes, select or clear the check box to the left of **Job Name**.
   - To edit a job, click the job name.

     If you added this object to an existing job, you might want to verify that the job is scheduled to run.
   - To change the order in which the jobs are sorted, click **Job Name**.

5.14.1 Changing the Owner of an Object

The owner of an object is displayed on the Set Job page. If you have Admin privileges to the object, you can change the owner.

You might want to change object owner for several reasons:

- If the owner is deleted from the portal, you must assign an existing portal user as the object owner before you can run the job.
- When a job runs, it might require access to portal objects that the current owner does not have access to. For example, a content crawler needs access to the folders into which it imports content. You might must change the owner to provide the proper access.

1. Open the object's editor by creating a new object or editing an existing object.
2. On the left, under Edit Object Settings, click **Set Job**.
3. To change the owner, click **Change Owner**; then, in the Choose User dialog box, choose the user whom you want to make the object owner and click **OK**.

Note: If you do not have Admin privileges to the object, you see the name of the owner, but you cannot change it.

5.15 Naming and Describing an Object

You can add or edit a name and description for an object.

1. Open the object's editor by creating a new object or editing an existing object.
2. On the left, under Edit Standard Settings, click **Properties and Names**.
3. In the **Name** box, type a name for this object.

   The name should clearly convey what this object is or what it can be used for.

   If you are naming an authentication-only authentication source, this name appears in the Authentication Partners list when you create the associated synchronization-only authentication source.
4. In the **Description** text box, type a description for this object.

   The description should provide additional detail to convey what this object is or what it can be used for.

   If you are naming an authentication source that synchronizes users, this description appears in the Authentication Source list when users log in. Users imported from an external source must choose the appropriate authentication source to log in to the portal.
5. If you did not set a mandatory object language in the portal configuration file, in the **Primary Language** list, select the language for the name and description you entered.

   If you did set a mandatory object language in the portal configuration file, you see the mandatory language instead of a list. You cannot change this setting. The name and description you entered must be in the mandatory language.

   If a localized name and description is not available in a user's selected language, the user will see the name and description in the specified primary language.

If you want to add names and descriptions for other languages, see Section D.1, "Localizing Object Names and Descriptions."

5.15.1 Localizing the Name and Description for an Object

You can localize object names and descriptions, so that users see the names and descriptions in their chosen language. For example, if you have an object called “Engineering,” you could add “Ingénierie” as the localized entry for French. A user viewing the French user interface would see the Ingénierie as the object name, as well as any other names and descriptions localized into French.

Note:
- You can localize names and descriptions into only the languages supported by the portal.
- You cannot localize names and descriptions for users.
- You can localize the names and descriptions for all objects at the same time using the Localization Manager.

1. Open the object's editor by creating a new object or editing an existing object.

2. On the left, under Edit Standard Settings, click **Properties and Names**.
3. Select **Supports Localized Names**.

   The **Localized Names and Descriptions** section appears.
4. Add or edit the localized names and descriptions:
   - To remove existing entries, select the entries you want to remove and click.

     To select or clear all entries, select or clear the check box to the left of **Name**.
   - To edit an existing entry, click the entry you want to change, then, in the Name and Description dialog box, edit the entry as necessary, and click **Finish**.
   - To remove existing entries, select the entries you want to remove and click the Remove icon.

     To select or clear all entries, select or clear the check box to the left of **Name**.

5.15.2 Viewing Top Best Bets for an Object

The Properties and Names page displays the top best bet terms set for this object. When users do a top best bet search on these terms, they go directly to this object instead of seeing the normal search results.

- To link to the end user view of this object, click the link under **URL**.

  You can use this URL to go directly to a top best bet. This can be useful if you want to direct users to an object or document related to a particular issue, but the object or document changes frequently. For example, you might want to direct customers to your current privacy statement, but you must keep copies of older privacy statements in your portal for internal reference. You could create a top best bet that points to the current privacy statement and add a link to that top best bet on your customer account page. When your privacy statement is updated, you can change the top best bet without having to change any links you made to the privacy statement.

5.16 Managing Object Properties

You can add or edit properties for an object.

1. Open the object's editor by creating a new object or editing an existing object.
2. On the left, under Edit Standard Settings, click **Properties and Names**.
3. Under Object Properties, change the properties and values:
   - To add or delete properties for all objects of this type, click **Open Properties Map**.

     This displays the Global Object Property Map.
   - To enter values for properties, type the value in the box to the right of the property.

Note: The Object Properties section does not display if you are creating or editing a property.

5.17 Setting Security on an Object

By default, a new object inherits the security of the parent folder, but you can override the inherited security.

> **Note:** You cannot override the inherited security for users; user security is always the same as the folder in which the user is stored. If you do not want a user to be returned in some users' searches, ensure that those users are not allowed access to the folder in which the user is stored.

1. Open the object's editor by creating a new object or editing an existing object.
2. On the left, under Edit Standard Settings, click **Security**.
3. Specify which users and groups can access this object and what type of access they have:
   - To allow additional users or groups access to this object, click **Add Users/Groups**.
   - To specify the type of access a user or group has, in the list under the **Privilege** column, select the access type.

     For a description of the available privileges, see Section 2.5.1, "About Access Controls Lists and Access Privileges."

     > **Note:** If a user is a member of more than one group included in the list, or if they are included as an individual user and as part of a group, that user gets the highest access available to her for this object. For example, if a user is part of the Everyone group (which has Read access) and the Administrators Group (which has Admin access), that user gets the higher privilege to the community: Admin.

   - To delete a user or group, select the user or group and click the Remove icon.

     To select or clear all of the user and group check boxes, select or clear the check box to the left of **Users/Groups**.
   - To see what users are included in a group, click the group name.
   - To change the column used for sorting or to toggle the sort order between ascending and descending, click the column name.

     You see an the Sort Ascending icon or the Sort Descending icon to the right of the column name by which the objects are sorted.

5.18 Viewing Migration History and Status for an Object

You can see if an object was imported from another portal or if it has been requested for migration.

1. Open the object's editor by editing an existing object.
2. On the left, under Edit Standard Settings, click **Migration History and Status**.

If this object was imported from another portal, information displays under **Import History**:

Column	Description
Migration Date	Displays the date the object was copied into this portal.
Migration Comment	Displays the comment entered by the user who requested migration of the object.
Source Portal UUID	Displays the unique identifier of the originating portal.

If this object has been requested for migration, under **Migration Status**, you see whether the request is waiting for approval, has been approved, or has been rejected, as well as the requesting user's comments and any comments from the portal administrator approving or rejecting the request.

If you are a member of the Administrators group and the object is waiting for migration approval, you can approve the request on this page. Select **Approve this object for migration**.

> **Note:** Users who are not members of the Administrators group do not see this option.

For more information on migrating objects, see Chapter 12, "Migrating, Backing-Up, and Restoring Your Portal."

6

Managing Portal Users and Groups

This chapter describes the portal conventions for user and group management and provides the steps you take to implement managed access to portal objects.

It includes the following sections:

Before you begin the task of managing portal groups and users, develop a plan to manage the administrative roles, groups, and users for your enterprise portal. For detailed information on developing a plan, refer to the *Oracle Fusion Middleware Deployment Guide for Oracle WebCenter Interaction*.

6.1 About Users

Portal users enable you to authenticate the people who access your portal and assign appropriate security for the documents and objects in your portal. Users can be

imported from external user repositories, created through the portal, created through invitations, self-registered, or just guests (unauthenticated users).

This section describes the types of users you might have in your deployment:

- Section 6.1.1, "Users Imported From External User Repositories"
- Section 6.1.2, "Users Created Through Invitations"
- Section 6.1.3, "Self-Registered Users"
- Section 6.1.4, "Guest Users"

6.1.1 Users Imported From External User Repositories

You can use authentication sources to import users that are already defined in your enterprise in existing user repositories, such as Active Directory or LDAP servers. After users are imported, you can authenticate them with the credentials from those user repositories. For more information on authentication sources, see Section 6.7, "About Importing and Authenticating Users and Groups."

You can also use profile sources to import user information (such as name, address, or phone number), which can then be used to populate user profiles or can be passed to content crawlers, remote portlets, or federated searches as user information. For more information on profile sources, see Section 6.13, "About Importing User Profile Information."

6.1.2 Users Created Through Invitations

You can invite users to your portal through invitations, making it easy for them to create their own accounts and letting you customize their initial portal experiences with content that is of particular interest to them. For more information on invitations, see Section 6.16, "About Invitations."

6.1.3 Self-Registered Users

Users can create their own accounts through your portal by clicking **Create an account** on the login page. These users are stored in the **Default Experience Definition** portal folder and are included in the WCI Authentication Source. They are automatically given security privileges based on the “Default Profile” created at installation. Based on this security, users can personalize their views of the portal with My Pages, portlets, and community memberships, and can view portal content.

Note: Your system administrator can disable the **Create an account** functionality.

6.1.4 Guest Users

The portal lets you create multiple guest users. This is useful when you want to have different user experiences for different sets of unauthenticated users. You can accomplish this by creating a guest user for each group of unauthenticated users to see a different user experience. You then associate each guest user with a different experience definition, customize the My Page for each guest user, and use experience rules to direct the guest users to the appropriate experience definition.

For example, you could create one guest user for employees that have not yet logged in to the portal and one for customers visiting your portal. The My Page for the employee guest user would include the login portlet so employees can log in. The My

Page for customers might include information about your company, such as contact numbers and descriptions of your products or services. You would create two experience definitions, associating one guest user with each. Then you would create two experience rules that would direct users to the appropriate experience definition based on the URL they use to access your portal.

6.2 Working with Users

This section describes the following main tasks:

- Section 6.2.1, "Creating or Editing a User"
- Section 6.2.2, "Deleting a User"
- Section 6.2.3, "Locking and Unlocking User Accounts"

It also covers the following low-level tasks:

- Section 6.2.4, "Specifying Authentication Settings for a User"
- Section 6.2.5, "Adding a User to Groups"
- Section 6.2.6, "Viewing a User's Dynamic Group Memberships"

6.2.1 Creating or Editing a User

To create a user you must have the following rights and privileges:

- Access Administration activity right
- Create Users activity right
- At least Edit access to the parent folder (the folder that will store the user)
- At least Select access to any groups to which you want to add this user

To edit a user you must have the following rights and privileges:

- Access Administration activity right
- At least Edit access to the user
- At least Select access to any groups to which you want to add this user

To create or edit a user:

1. Click **Administration**.
2. Open the User Editor.
   - To create a user, open the folder in which you want to store the user. In the Create Object list, click **User**.
   - To edit a user, open the folder in which the user is stored and click the user name.
3. On the Main Settings page, perform tasks as necessary:
   - Section 6.2.4, "Specifying Authentication Settings for a User"
   - Section 6.2.5, "Adding a User to Groups"
   - Section 6.2.6, "Viewing a User's Dynamic Group Memberships"
4. On the Mobile Device Authentication page, perform tasks as necessary:
   - Section 5.15, "Naming and Describing an Object"

- Section 5.16, "Managing Object Properties"

5. On the Properties and Names page, perform tasks as necessary:
   - Section 5.15, "Naming and Describing an Object"
   - Section 5.16, "Managing Object Properties"
6. If you are editing a user, on the Migration History and Status page, perform tasks as necessary:
   - Section 5.18, "Viewing Migration History and Status for an Object"

Note: The Migration History and Status page is not available when creating an object.

Note: User security is inherited from the folder in which the user is stored. If you do not want a user to be returned in some users' searches, ensure that those users are not allowed access to the folder in which the user is stored.

6.2.2 Deleting a User

You should delete users that should no longer have access to your portal.

To delete a user you must have the following rights and privileges:

- Access Administration activity right
- Admin access to the user

To delete a user (whose account is not locked):

1. Click **Administration**.
2. Navigate to the user.
3. Select the user you want to delete and click the delete icon.

To delete a user whose account is locked:

1. Click **Administration**.
2. In the **Select Utilities** list, click **Release Disabled Logins**.
3. Select the user you want to delete and click the delete icon.

6.2.3 Locking and Unlocking User Accounts

You lock user accounts to disable access to the portal. You can configure automatic locking based on repeated failed login attempts, or you can lock user accounts any time with the User Editor.

This section describes the following tasks:

- Section 6.2.3.1, "Automatically Locking User Accounts"
- Section 6.2.3.2, "Manually Locking a User Account"
- Section 6.2.3.3, "Unlocking User Accounts"

6.2.3.1 Automatically Locking User Accounts

You can automatically lock user accounts based on failed login attempts.

1. Click **Administration**.
2. In the Select Utility list, click **Portal Settings**.
3. On the User Settings Manager page, select **Enable account locking** and specify how long failed logins are tracked, the total number of failed logins required before an account will be locked, and the number of minutes for which automatically locked accounts remain locked.

   Your individual security needs will determine what settings to use for automatic account locking. For example, to meet a strength of password function rating of SOF-basic as defined in the Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005, you might set the following values:

   - **Minutes to track failed Logins**: 60 minutes or more
   - **Number of failed Login attempts allowed**: 5 or fewer
   - **Minutes to keep user account locked**: 60 minutes or more

6.2.3.2 Manually Locking a User Account

To manually lock a user account:

1. Click **Administration**.
2. Navigate to the user whose account you want to lock and click the user name.
3. Select **Disable Login**.

6.2.3.3 Unlocking User Accounts

The lock on user accounts that are locked automatically will eventually expire, but you can remove account locks with the Release Disabled Logins utility or the User Editor.

You unlock user accounts differently depending on how the account was locked:

- Admin Lock: An administrative user with Admin access to the user locked the user account.
- Automatic Lock: If the user repeatedly types the wrong user name or password when logging into the portal, the portal locks the account. The number of login attempts allowed before the user is locked out is determined in the Portal Settings utility.

  Note: Locks on accounts that are locked automatically eventually expire.

- Agent Lock: A user account might be locked if it is not found in the external authentication server during a synchronization job. This lock might be unexpected if the synchronization job did not find the user because the job failed.

  Note: Users can remove the lock by specifying the correct credentials the next time they log in.

To remove an Admin Lock or an Automatic Lock with the Release Disabled Logins Utility:

1. Click **Administration**.
2. In the Select Utilities list, click **Release Disabled Logins**.

To remove an Admin Lock or an Automatic Lock with the User Editor:

1. Click **Administration**.
2. Navigate to the user whose account you want to unlock and click the user name.
3. Clear the check box next to **Disable Login**.

To remove an Agent Locks for all affected users:

1. Click **Administration**.
2. Navigate to the authentication source and click its name.
3. Click **Fully Synchronized Groups** page.
4. Click **Re-Enable Users**.

   Unlocking these accounts may take a few minutes.

6.2.4 Specifying Authentication Settings for a User

To specify the authentication settings for a user:

1. If the User Editor is not already open, open it now. The User Editor displays the Main Settings page.
2. In the **Login Name** box, type the name this user must enter to log in to the portal.
3. In the **Password** box, type the password this user must enter to log in to the portal.
4. In the **Confirm Password** box, type the same password as in step 3.
5. If you do not want this user to be allowed to log in, select **Disable Login**.
6. To make this a guest user, select **This is a guest account**. Once you save this user, this check box is unavailable (grayed out). You can create multiple guest users and associate them to different experience definitions. Click here for an example.

6.2.5 Adding a User to Groups

To add a user to groups:

1. If the User Editor is not already open, open it now. The User Editor displays to the Main Settings page.
2. Under Group Memberships, specify the groups of which this user should be a member. This user will have access to all the content and portal activities to which these groups have access. All users are part of the Everyone group:
   - To add this user to a group, click **Add Group**, in the Select Groups dialog box, select the groups you want to add, and click **OK**.
   - To remove this user from a group, select the group and click the Remove icon.
   - To select or clear all of the group boxes, select or clear the box to the left of **Groups**.
   - To toggle the order in which the groups are sorted (ascending/descending), click **Groups**.

6.2.6 Viewing a User's Dynamic Group Memberships

Dynamic group membership is based on dynamic membership rules, specific values in the user's profile, or membership in other groups. You can view the dynamic group memberships for a user on the Main Settings page of the User Editor, under Dynamic Group Memberships.

6.3 About Default Profiles

Each user is assigned a default profile at creation, based on settings in the authentication source or the invitation (manually created users and self-registered users are automatically assigned the "Default Profile" created at installation. Default profiles define initial My Account settings, such as language, time zone, and portal interface type; the name and number of My Pages; and the layout of the portlets on those My Pages. Default profiles provide an initial view of the portal, which users can then change to fit their needs.

> **Note:** Portlet preferences, group memberships, and community memberships are not inherited by users created from default profiles.

Default profiles are defined through special users, created in the Default Profiles folder (accessed through the Default Profiles Utility). These special users cannot log in to the portal. They are solely used to assign settings to new users.

6.4 Working with Default Profiles

This section describes the following tasks:

- Section 6.4.1, "Creating and Editing a Default Profile"
- Section 6.4.2, "Customizing a Default Profile Experience"

6.4.1 Creating and Editing a Default Profile

When new authenticated users are created in the portal, the following settings are based on default profiles: initial My Account settings, name and number of My Pages, and layout of the portlets on those My Pages.

To create or edit a default profile you need the following rights:

- Access Administration activity right
- Access Utilities activity right

To create or edit a default profile:

1. Click **Administration**.
2. In the Select Utility list, click **Default Profiles**.

   The Default Profiles folder opens.
3. Open the Default Profile Editor.
   - To create a default profile, in the Create Object list, click **User**.
   - To edit a default profile, click the default profile name.
4. In the **Login Name** box, type a name for this default profile.

Users created from this default profile will have their own user names and passwords.

Note:

- Do not select **This is a guest account**. Instead, to create a guest user, go to a different administrative folder, create a user there, and make that user a guest.
- Do not add this user to any groups. Group memberships are not inherited by users created from default profiles. You set group membership through invitations or authentication sources.

After you have created or edited a default profile, edit its layout.

6.4.2 Customizing a Default Profile Experience

When new authenticated users are created in the portal, the following settings are based on default profiles: initial My Account settings, name and number of My Pages, and layout of the portlets on those My Pages.

To customize a default profile experience you need the following rights:

- Access Administration activity right
- Access Utilities activity right

To customize a default profile:

1. If you are not already in the Default Profiles folder, click **Administration**, and, in the Select Utility list, click **Default Profiles**.
2. Select the profile to customize.
3. Click **Edit Profile Layout**.
4. Specify My Account settings, create and delete My Pages, and change the layout of the My Pages.

Note:

- Portlet preferences are not inherited by users created from the default profile. Users set their own preferences.
- Community membership and access to documents and objects are granted through group membership.

After you have customized the default profile, use invitations and authentication sources to assign the profile to new portal users and to assign group membership.

6.5 About Groups

Groups are created in the portal either by adding them individually as portal objects, or by synchronizing with authentication sources (user repositories such as LDAP or Active Directory).

Membership to a group is determined in two ways:

- Members are explicitly defined as specific users and/or other groups on the Group Memberships page.
- Members are dynamically determined based on rules you set up on the Dynamic Membership Rules page.

This section describes the types of groups you might have in your deployment:

- Section 6.5.1, "Dynamic Group Membership"
- Section 6.5.2, "Community Groups"
- Section 6.5.3, "Roles"
- Section 6.5.4, "Groups Created Upon Installation"

6.5.1 Dynamic Group Membership

You might want to have users automatically added to or removed from groups based on properties in their user profiles or other group membership. This is called dynamic group membership. For example, you might want to give users access to a community based on their location, title, department, or any other property in their profile. If you have a community for all the branches in Texas, you could set up a rule that states that all employees in Texas are part of the group. If an employee moves to Arizona, and the "State" property in her profile changes, the employee no longer satisfies this rule.

6.5.2 Community Groups

You can create groups inside a community without affecting portal groups. You create community groups so that you can easily assign responsibilities to community members. For example, you might have a group that is responsible for maintaining schedules in the community.

Community groups are available only within the community. However, you can make a community group available outside of the community by moving the group to a non-community administrative folder.

6.5.3 Roles

A role is not a portal object; it is an association between a group and the activity rights required to perform a job function. For example, the Knowledge Directory administrator role is not an object you define; it relates to administrative responsibilities for those who manage content in the Knowledge Directory.

Before you create portal groups for assigning roles, you should familiarize yourself with the definition and scope of the administrative tasks you plan to delegate and the activity rights needed to complete those administrative tasks. Some users will handle many tasks, but those tasks might actually encompass several roles. Before creating a role to cover all these tasks, consider if there are situations where the tasks will be broken down into smaller roles. You can easily assign more than one role to a user.

6.5.3.1 Example Roles

The following table describes the activity rights that are defined by default during installation and provides an example map between activity rights and administrative roles. In the example, the role called Content Administrator provides the activity rights required to populate the portal with document records crawled from remote content sources; a separate role called Knowledge Directory Administrator provides the activity rights required to create Knowledge Directory structure. Although some

users might fill both roles, others might not. By creating two separate roles, you can assign the roles separately or together.

Role	Activity Rights Needed
Portal Administrator: Manages all areas of the portal	All activity rights; add the user to the Administrators group, which has all activity rights
Content Administrator: Populates the portal with document records crawled from remote content sources	■ Edit Knowledge Directory – to manage the Directory ■ Create Folders – to create new folders in the Directory ■ Access Administration – to access the remaining features ■ Create Filters – to automatically sort content info Directory folders ■ Create Content Types – to force metadata onto documents ■ Create Content Sources – to provide access to new external document repositories ■ Create Content Crawlers – to import new content ■ Create Jobs – to create jobs to run content crawlers ■ Access Utilities – to approve content, access smart sort, and access unclassified documents ■ Access Smart Sort– to re-sort entire folders of already categorized documents ■ Access Unclassified Documents – to find documents that did not sort into any Directory folder
Community Creator	■ Access Administration ■ Create Communities – to create communities ■ Create Community Infrastructure – to create community and page templates
Portlet Creator	■ Access Administration ■ Create Web Service Infrastructure – to create remote servers and portlet Web services to create custom portlets ■ Create Portlets – to create portlets
Group/User Creator	■ Access Administration ■ Create Admin Folders – to make new admin folders to store users ■ Create Experience Definitions – to modify the user experience of users ■ Create Authentication Sources – to import new users and groups ■ Create Profile Sources – to apply user information to synchronized users ■ Create Jobs – to create jobs to synchronize authentication sources and profile sources ■ Create Groups – to create groups ■ Create Users – to create users ■ Access Utilities – to create default profiles to apply initial layouts to users ■ Delegate Rights – to delegate rights to users (create activity groups)

6.5.4 Groups Created Upon Installation

The following groups are created in the **Portal Resources** folder when you install the portal:

- **Administrators Group**: This group provides full access to everything in the portal: all objects, all utilities, and all portal activities.
- **Everyone**: This group includes all portal users, whether created manually through the administration menu, imported from authentication sources, created through acceptance of an invitation, or created through the Create an Account page.

6.5.5 Planning Your Group Hierarchy

When creating a group hierarchy, begin with the users with the least rights and work towards the most powerful users. A group inherits the rights of its parent group, so the broadest groups with the least rights should be parent to more specific groups with greater rights.

For example, the engineering department creates an Engineer group (for all members of the department). The QA subset of the engineering department requires special access to certain bug tracking software, so a QA group should be created with the Engineer group as a parent. Administrative tasks on the bug tracking software is restricted to QA managers, so a group inheriting from the QA group is created for QA managers.

6.6 Working with Groups

This section describes the following main tasks:

- Section 6.6.1, "Creating or Editing a Group"
- Section 6.6.2, "Deleting a Group"

It also covers the following low-level tasks:

- Section 6.6.4, "Adding Users to a Group"
- Section 6.6.5, "Configuring Dynamic Group Membership"
- Section 6.6.6, "Assigning Activity Rights to a Group"

6.6.1 Creating or Editing a Group

Groups are sets of users, sets of other groups, or both. Groups enable you to more easily control security because you assign each group different activity rights and access privileges.

To create a group you must have the following rights and privileges:

- Access Administration activity right
- Create Groups activity right
- At least Edit access to the parent folder (the folder that will store the group)
- At least Select access to any groups to which you want to add this group
- At least Select access to any users you want to add to the group

To edit a group you must have the following rights and privileges:

- Access Administration activity right

- At least Edit access to the group
- At least Select access to any groups to which you want to add this group
- At least Select access to any users you want to add to the group

To create or edit a a group:

1. Click **Administration**.
2. Open the Group Editor.
   - To create a group, open the folder in which you want to store the group. In the Create Object list, click **Group**.
   - To edit a group, open the folder in which the group is stored and click the group name.
3. On the Group Memberships page, perform tasks as necessary:
   - Section 6.6.3, "Adding a Group to Other Groups"
   - Section 6.6.4, "Adding Users to a Group"
4. On the Dynamic Membership Rules page, perform tasks as necessary:
   - Section 6.6.5, "Configuring Dynamic Group Membership"
5. On the Activity Rights page, perform tasks as necessary:
   - Section 6.6.6, "Assigning Activity Rights to a Group"
6. On the Properties and Names page, perform tasks as necessary:
   - Section 5.15, "Naming and Describing an Object"
   - Section 5.16, "Managing Object Properties"
7. On the Security page, perform tasks as necessary:
   - Section 5.17, "Setting Security on an Object"
8. If you are editing a user, on the Migration History and Status page, perform tasks as necessary:
   - Section 5.18, "Viewing Migration History and Status for an Object"

Note: The Migration History and Status page is not available when creating an object.

6.6.2 Deleting a Group

To delete a group you must have the following rights and privileges:

- Access Administration activity right
- Admin access to the group

To delete a group:

1. Click **Administration**.
2. Navigate to the group.
3. Select the group you want to delete and click the delete icon.

Caution: If users were previously granted rights and privileges based on being a member of this group, they will no longer have those rights and privileges.

6.6.3 Adding a Group to Other Groups

To specify the groups to which this group should be a member:

1. If the Group Editor is not already open, open it now. The Group Editor displays the Group Memberships page.
2. Under Parent Group Memberships, specify the groups to which this group should be a member:
   - To make this group a member of another group, click **Add Group**, in the Select Groups dialog box, select the groups to which you want to add this group, and click **OK**.
   - To remove a parent group, select it and click the remove icon.

     To select or clear all of the group boxes, select or clear the box to the left of **Members**.
   - To toggle the order in which the groups are sorted, click **Members**.

6.6.4 Adding Users to a Group

To specify the members of this group:

1. If the Group Editor is not already open, open it now. The Group Editor displays the Group Memberships page.
2. Under Group Members, specify the members of this group:
   - To add members to this group, click **Add User/Group**, in the Select Members dialog box, select the groups and users you want to add to this group, and click **OK**.
   - To remove a member, select it and click the remove icon.
   - To remove a member, select it and click the remove icon.

     To select or clear all of the member boxes, select or clear the box to the left of **Members**.
   - To toggle the order in which the members are sorted, click **Members**.

6.6.5 Configuring Dynamic Group Membership

You might want to have users automatically added to or removed from groups based on properties in their user profiles or other group membership. This is called dynamic group membership. For example, you might want to give users access to a community based on their location, title, department, or any other property in their profile. If you have a community for all the branches in Texas, you could set up a rule that states that all employees in Texas are part of the group. If an employee moves to Arizona, and the "State" property in her profile changes, the employee no longer satisfies this rule.

Dynamic membership rules are made up of statements that define what must or must not be true to include a user in the group. The statements are collected together in groupings. The grouping defines whether the statements are evaluated with an AND operator (all statements are true) or an OR operator (any statement is true). If some

statements should be evaluated with an AND operator and some should be evaluated with an OR operator, you can create separate groupings for the statements. You can also create subgroupings or nested groupings, where one grouping is contained within another grouping. The statements in the lowest-level grouping are evaluated first to define a set of users. Then the statements in the next highest grouping are applied to that set of users to further filter the set of users. The filtering continues up the levels of groupings until all the groupings of statements are evaluated.

1. If the Group Editor is not already open, open it now.
2. On the left, under Edit Object Settings, click **Dynamic Membership Rules**.
3. Select the operator for the grouping of statements you are about to create:
   - If a user should be added to the group only when all statements in the grouping are true, select **AND**.
   - If a user should be added to the group when any statement in grouping is true, select **OR**.

   Note: The operator you select for a grouping applies to all its statements and subgroupings directly under it.

4. Define each statement in the grouping:
   a. Click **Add Statement**.
   b. In the first list, select a property.

      This list includes the properties included in the user profile and **Member Of**, which enables you to select a group whose members you want to include or exclude.
   c. In the second list, select an operator:
      – If you selected a user profile property, you can select **Contains** or **Contains No Value**.
      – If you selected **Member Of**, you can select **includes** or **excludes**.
   d. If you selected **Contains** as the operator, in the text box, enter a value for the property.

      You can use wildcards.
   e. If you selected **Member Of**, select the groups whose members you want to include or exclude. Click the Edit icon, in the Group Chooser dialog box, select a group, and click **OK**.

      Note: The Group Chooser dialog box displays only statically defined groups.

      – To add more statements, repeat these steps.
      – To remove the last statement in a grouping, select the grouping and click **Remove Statement**.
5. If necessary, add more groupings:

- To add another grouping, select the grouping to which you want to add a subgrouping and click **Add Grouping**. Then define the statements for that grouping.

  Note: You cannot add a grouping at the same level as **Grouping 1**.

- To remove a grouping, select the grouping, and click **Remove Grouping**.

  Note:

  - Any groupings and statements in that grouping will also be removed.
  - You cannot remove the top level **Grouping 1**.

6. Click **Preview Members** to see the dynamic members resulting from the rules you defined.

   Only 1000 members will be displayed.

The dynamic members are updated for this group when you click **Finish**.

The next time you open this group editor, dynamic members are displayed on the **Group Memberships** page.

Dynamic memberships are updated for all groups as part of the **Dynamic Membership Update Agent** job (located in the **Intrinsic Operations** folder). When user profile data changes, the resulting dynamic group membership changes are updated as part of this job.

6.6.6 Assigning Activity Rights to a Group

Activity rights determine which portal objects a user can create and which portal utilities a user can execute to create or modify portal objects.

It is not necessary to grant a user the right to create a type of object for that user to manage an object of that type. Management of an object is based solely on a user's access privilege to that object.

1. If the Group Editor is not already open, open it now.
2. On the left, under Edit Object Settings, click **Activity Rights**.
3. Under Activity Rights, click **Add Activity Rights**.

   The Select Activity Rights dialog box opens.
4. Select the activity rights you want to grant to the group and click **OK**.

   For example, if you select Create Jobs, the members of the group will be able to create jobs in the portal.

   To remove activity rights, select the activity right to remove and click the Remove icon.

Under **Inherited Activity Rights** you see any activity rights granted to the parent groups of this group.

6.7 About Importing and Authenticating Users and Groups

Rather than recreating users, groups, and group memberships to use in your portal, you can leverage the structure and security you already have defined in your existing user repositories, such as Active Directory or LDAP servers.

This section describes the components involved in importing and authenticating users and how the process works:

- Section 6.7.1, "How Authentication Works"
- Section 6.7.2, "Authentication Providers"
- Section 6.7.3, "Authentication Web Services"
- Section 6.7.4, "Authentication Sources"

6.7.1 How Authentication Works

When you use authentication sources to authenticate portal users, the user credentials are left in the external repository; they are not stored in the portal database. When someone attempts to log in to your portal through an imported user account, the portal confirms the password with the external repository, meaning that the user's portal password always matches the password in the external repository. For example, if a user with a portal account imported from Active Directory changes the Active Directory password, the user can immediately log in to the portal with that password. If the user is already logged in to the portal, the user must log in again with the new password, because the portal will no longer be able to recognize the old password.

6.7.2 Authentication Providers

An authentication provider is a piece of software that tells the portal how to use the information in the external user repository.

Oracle provides authentication providers for the following types of user repositories as part of Oracle WebCenter Interaction:

- LDAP
- Microsoft Active Directory

Note: You must install the authentication provider before you can create the associated authentication Web service. For information on installing authentication providers, refer to the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Interaction for Windows* or the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Interaction for Unix and Linux*).

If your users and groups reside in a custom system, such as a custom database, you can import and authenticate them by writing your own authentication provider using the IDK. For details, see the *Oracle Fusion Middleware Web Service Developer's Guide for Oracle WebCenter Interaction*.

6.7.3 Authentication Web Services

Authentication Web services enable you to specify general settings for your external user repository, leaving the more detailed settings (like domain specification) to be set in the associated remote authentication sources, enabling you to create different

authentication sources to import each domain without having to repeatedly specify all the settings.

6.7.4 Authentication Sources

Authentication sources can import users and/or groups, authenticate imported users, or both import and authenticate. Your security needs determine how many authentication sources to create and what functionality they need. You might be able to create just one authentication source that imports and authenticates all users and groups, but here are a couple examples of when that would not suffice:

- If you want to use single sign-on (SSO), create a synchronization-only authentication source.
- If you want to distinguish users and groups from different domains, create separate synchronization-only authentication sources for each domain, and create an authentication-only authentication source to authenticate users from all domains (assuming they are from the same user repository).

  Creating separate synchronization-only authentication sources for each domain enables you to store users and groups imported from different domains in different portal folders or to create separate users or groups with the same name but from different domains.

If you are importing users and groups into the portal, you run a job for the initial import and then continue to run the job periodically to keep the users and groups in the portal synchronized with those in the source user repository.

Note: When you run the job to import users and groups, the portal also creates a group that includes all users imported through the authentication source. This group is named after the authentication source; for example, if your authentication source is called *mySource*, the group would be called *Everyone in mySource*.

6.7.4.1 WCI Authentication Source

The WCI Authentication Source is automatically created upon installation. It is the authentication source used for users stored in the portal database (users created upon install, users created manually through the portal, and self-registered users). This authentication source cannot be modified or deleted.

6.8 Working with Authentication Web Services

This section describes the following main tasks:

- Section 6.8.1, "Creating or Editing an Authentication Web Service"
- Section 6.8.2, "Deleting an Authentication Web Service"

6.8.1 Creating or Editing an Authentication Web Service

Before you create an authentication Web service, you must:

- Install the authentication provider on the computer that hosts the portal or on another computer
- Create a remote server pointing to the computer that hosts the authentication provider (optional, but recommended)

To create an authentication Web service you must have the following rights and privileges:

- Access Administration activity right
- Create Web Service Infrastructure activity right
- At least Edit access to the parent folder (the folder that will store the authentication Web service)
- At least Select access to the remote server that the authentication Web service will use

To edit an authentication Web service you must have the following rights and privileges:

- Access Administration activity right
- At least Edit access to the authentication Web service
- If you must change the remote server association, at least Select access to the remote server that the authentication Web service will use

To create or edit an authentication Web service:

1. Click **Administration**.
2. Open the Authentication Web Service Editor.
   - To create an authentication Web service, open the folder in which you want to store the authentication Web service. In the Create Object list, click **Web Service — Authentication**.
   - To edit an authentication Web service, open the folder in which the authentication Web service is stored and click the authentication Web service name.
3. On the Main Settings page, perform tasks as necessary:
   - Section 3.4.1, "Associating a Remote Server with a Web Service"
   - Section 3.4.2, "Specifying the Location of the Web Service Provider or Code"
   - Section 3.4.3, "Specifying Web Service Time-Out Settings"
   - Section 3.4.4, "Enabling and Disabling a Web Service"
4. On the HTTP Configuration page, perform tasks as necessary:
   - Section 3.4.7, "Specifying What Content is Gatewayed for a Web Service"
5. On the Advanced Settings page, perform tasks as necessary:
   - Section 3.4.11, "Specifying Encoding Style for a Web Service"
   - Section 3.4.8, "Adding a Service Configuration Page to a Web Service Editor"
6. On the Authentication Settings page, perform tasks as necessary:
   - Section 3.4.13, "Specifying Authentication Settings for a Web Service"
7. On the Debug Settings page, perform tasks as necessary:
   - Section 3.4.16, "Enabling Error Tracing for a Web Service"
8. On the Associated Objects page, perform tasks as necessary:
   - Section 3.4.17, "Viewing Objects Associated with a Web Service"
9. On the Properties and Names page, perform tasks as necessary:

- Section 5.15, "Naming and Describing an Object"

  You can instead enter a name and description when you save this authentication Web service.

- Section 5.16, "Managing Object Properties"

10. On the Security page, perform tasks as necessary:

    - Section 5.17, "Setting Security on an Object"

    The default security for this authentication Web service is based on the security of the parent folder. Administrative users with at least Select access to this authentication Web service and the Create Authentication Source activity right can create authentication sources based on the Web service.

11. If you are editing an authentication Web service, on the Migration History and Status page, perform tasks as necessary:

    - Section 5.18, "Viewing Migration History and Status for an Object"

    Note: The Migration History and Status page is not available when creating an object.

6.8.2 Deleting an Authentication Web Service

To delete an authentication Web service you must have the following rights and privileges:

- Access Administration activity right
- Admin access to the authentication Web service

To delete an authentication Web service:

1. Click **Administration**.
2. Navigate to the authentication Web service.
3. Select the authentication Web service you want to delete and click the delete icon.

Note: Deleting an authentication Web service will break any associated authentication sources.

6.9 Working with Authentication Sources

This section describes the following main tasks:

- Section 6.9.1, "Creating an Authentication Source to Import and Authenticate Users"
- Section 6.9.2, "Creating a Synchronization-Only Authentication Source"
- Section 6.9.3, "Creating an Authentication-Only Authentication Source"
- Section 6.9.4, "Creating a Single Sign-On Authentication Source"
- Section 6.9.5, "Editing an Authentication Source"
- Section 6.9.6, "Deleting an Authentication Source"

It also covers the following subtasks:

- Section 6.9.7, "Setting an Authentication Source Category to Distinguish Users and Groups Imported from a Particular Domain"
- Section 6.9.8, "Setting Default Profiles and Target Folders for Imported Users"
- Section 6.9.9, "Setting a Target Folder for Imported Groups"
- Section 6.9.10, "Specifying Which Users and Groups to Synchronize"
- Section 6.9.11, "Selecting Groups from Which to Import Users"
- Section 6.9.12, "Specifying What to Do with Users and Groups Deleted from the Source User Repository"

6.9.1 Creating an Authentication Source to Import and Authenticate Users

You can create a remote authentication source to import and authenticate users and groups from external user repositories.

Before you create an authentication source, you must:

- Install the authentication provider on the computer that hosts the portal or on another computer.
- Create a remote server that points to the computer that hosts the authentication provider.
- Create an authentication Web service on which to base the authentication source.
- Create and configure the default profiles you want to apply to imported users.
- Create the folders in which you want to store the imported users.

To create an authentication source you must have the following rights and privileges:

- Access Administration activity right
- Create Authentication Sources activity right
- At least Edit access to the parent folder (the folder that will store the authentication source)
- At least Select access to the authentication Web service on which this authentication source will be based
- At least Select access to the default profiles you want to apply to imported users
- At least Select access to the folders in which you want to store the imported users

To create an authentication source to import and authenticate users:

1. Click **Administration**.
2. Open the folder in which you want to store the authentication source.
3. In the Create Object list, click **Authentication Source - Remote**.

   The Choose Web Service dialog box opens.
4. Select the Web service that provides the basic settings for your authentication source and click **OK**.

   The Remote Authentication Source Editor opens.
5. On the Main Settings page, perform the following tasks:
   a. Section 6.9.7, "Setting an Authentication Source Category to Distinguish Users and Groups Imported from a Particular Domain"

b. Section 6.9.8, "Setting Default Profiles and Target Folders for Imported Users"

c. Section 6.9.9, "Setting a Target Folder for Imported Groups"

6. On the Synchronization page, perform the following tasks:

   a. Under General Info, select **Authentication and Synchronization**.

   b. Specify what to synchronize. For details, see Section 6.9.10, "Specifying Which Users and Groups to Synchronize."

7. On the Fully Synchronized Groups page, perform the following task:

   - Section 6.9.12, "Specifying What to Do with Users and Groups Deleted from the Source User Repository"

8. On the Set Job page, perform the following task:

   - Section 5.14, "Associating an Object with a Job"

9. On the Properties and Names page, perform the following tasks:

   - Section 5.15, "Naming and Describing an Object"

   Note: The authentication source name appears in lists of objects from which users will sometimes choose; therefore, the name should clearly convey the purpose of this authentication source.

   You can instead enter a name and description when you save this authentication source.

   - Section 5.16, "Managing Object Properties" (optional)

10. On the Security page, perform the following task:

    - Section 5.17, "Setting Security on an Object" (optional)

    The default security for this authentication source is based on the security of the parent folder.

11. Run the job you associated with this authentication source.

12. If you are importing only partial users or groups or are applying different default profiles to each group of users, after the associated job runs once, return to the Authentication Source Editor and perform any necessary additional tasks.

6.9.2 Creating a Synchronization-Only Authentication Source

You can import users with an authentication source and have them authenticated through an associated authentication partner.

Before you create an authentication source, you must:

- Install the authentication provider on the computer that hosts the portal or on another computer.
- Create a remote server that points to the computer that hosts the authentication provider.
- Create an authentication Web service on which to base the authentication source.
- Create and configure the default profiles you want to apply to imported users.
- Create the folders in which you want to store the imported users.

- Create an authentication source that will authenticate users imported with this authentication source.

To create an authentication source you must have the following rights and privileges:

- Access Administration activity right
- Create Authentication Sources activity right
- At least Edit access to the parent folder (the folder that will store the authentication source)
- At least Select access to the authentication Web service on which this authentication source will be based
- At least Select access to the authentication source that will authenticate users imported with this authentication source.

To create a synchronization-only authentication source:

1. Click **Administration**.
2. Open the folder in which you want to store the authentication source.
3. In the Create Object list, click **Authentication Source - Remote**.

   The Choose Web Service dialog box opens.
4. Select the Web service that provides the basic settings for your authentication source and click **OK**.

   The Remote Authentication Source Editor opens.
5. On the Main Settings page, perform the following tasks:
   a. Section 6.9.7, "Setting an Authentication Source Category to Distinguish Users and Groups Imported from a Particular Domain"
   b. Section 6.9.8, "Setting Default Profiles and Target Folders for Imported Users"
   c. Section 6.9.9, "Setting a Target Folder for Imported Groups"
6. On the Synchronization page, perform the following tasks:
   a. Under General Info, select **Synchronization with Authentication Partner**.
   b. In the Authentication Partners list, select the authentication source you want to use for authentication.

      Note: If the authentication partner is unavailable, this authentication source will attempt to authenticate users.

   c. Section 6.9.10, "Specifying Which Users and Groups to Synchronize"
7. On the Fully Synchronized Groups page, perform the following task:
   - Section 6.9.12, "Specifying What to Do with Users and Groups Deleted from the Source User Repository"
8. On the Set Job page, perform the following task:
   - Section 5.14, "Associating an Object with a Job"
9. On the Properties and Names page, perform the following tasks:
   - Section 5.15, "Naming and Describing an Object"

Note: The authentication source name appears in lists of objects from which users will sometimes choose; therefore, the name should clearly convey the purpose of this authentication source.

You can instead enter a name and description when you save this authentication source.

- Section 5.16, "Managing Object Properties" (optional)

10. On the Security page, perform the following task:
    - Section 5.17, "Setting Security on an Object" (optional)

    The default security for this authentication source is based on the security of the parent folder.
11. Run the job you associated with this authentication source.
12. If you are importing only partial users or groups or are applying different default profiles to each group of users, after the associated job runs once, return to the Authentication Source Editor and perform any necessary additional tasks.

6.9.3 Creating an Authentication-Only Authentication Source

If you have more than one authentication source importing users from the same user repository, create an authentication-only authentication source to authenticate your users.

Before you create an authentication source, you must:

- Install the authentication provider on the computer that hosts the portal or on another computer.
- Create a remote server that points to the computer that hosts the authentication provider.
- Create an authentication Web service on which to base the authentication source.

To create an authentication source you must have the following rights and privileges:

- Access Administration activity right
- Create Authentication Sources activity right
- At least Edit access to the parent folder (the folder that will store the authentication source)
- At least Select access to the authentication Web service on which this authentication source will be based

To create an authentication-only authentication source:

1. Click **Administration**.
2. Open the folder in which you want to store the authentication source.
3. In the Create Object list, click **Authentication Source - Remote**.

   The Choose Web Service dialog box opens.
4. Select the Web service that provides the basic settings for your authentication source and click **OK**.

   The Remote Authentication Source Editor opens.

5. On the Main Settings page, perform the following task:
   - Section 6.9.7, "Setting an Authentication Source Category to Distinguish Users and Groups Imported from a Particular Domain"
6. On the Synchronization page, under General Info, select **Authentication Only**.
7. On the Properties and Names page, perform the following tasks:
   - Section 5.15, "Naming and Describing an Object"

     Note: The authentication source name appears in lists of objects from which users will sometimes choose; therefore, the name should clearly convey the purpose of this authentication source.

     You can instead enter a name and description when you save this authentication source.
   - Section 5.16, "Managing Object Properties" (optional)
8. On the Security page, perform the following task:
   - Section 5.17, "Setting Security on an Object" (optional)

   The default security for this authentication source is based on the security of the parent folder.
9. Add this authentication source as the authentication partner for a synchronization-only authentication source.

6.9.4 Creating a Single Sign-On Authentication Source

You can import users with an authentication source and have them authenticated transparently through single sign-on (SSO).

Before you create an SSO authentication source, you must:

- Install the authentication provider on the computer that hosts the portal or on another computer.
- Create a remote server that points to the computer that hosts the authentication provider.
- Create an authentication Web service on which to base the authentication source.
- Create and configure the default profiles you want to apply to imported users.
- Create the folders in which you want to store the imported users.

To create an SSO authentication source you must have the following rights and privileges:

- Access Administration activity right
- Create Authentication Sources activity right
- At least Edit access to the parent folder (the folder that will store the authentication source)
- At least Select access to the authentication Web service on which this authentication source will be based

To create an SSO authentication source:

1. Click **Administration**.

2. Open the folder in which you want to store the authentication source.
3. In the Create Object list, click **Authentication Source - Remote**.

   The Choose Web Service dialog box opens.
4. Select the Web service that provides the basic settings for your authentication source and click **OK**.

   The Remote Authentication Source Editor opens.
5. On the Main Settings page, perform the following tasks:
   a. Section 6.9.7, "Setting an Authentication Source Category to Distinguish Users and Groups Imported from a Particular Domain"

      Make a note of this string, Unless this string matches the PrefixHeading of the authentication provider, you must configure for the DefaultAuthSourcePrefix setting in the portalconfig.xml file, as described in Section E.3, "Configuring the Portal for SSO."
   b. Section 6.9.8, "Setting Default Profiles and Target Folders for Imported Users"
   c. Section 6.9.9, "Setting a Target Folder for Imported Groups"
6. On the Synchronization page, perform the following tasks:
   a. Under General Info, select **Synchronization with Authentication Partner**.
   b. In the Authentication Partners list, select **SSO Authentication Source**.
   c. Section 6.9.10, "Specifying Which Users and Groups to Synchronize"
7. On the Fully Synchronized Groups page, perform the following task:
   - Section 6.9.12, "Specifying What to Do with Users and Groups Deleted from the Source User Repository"
8. On the Set Job page, perform the following task:
   - Section 5.14, "Associating an Object with a Job"
9. On the Properties and Names page, perform the following tasks:
   - Section 5.15, "Naming and Describing an Object"

     Note: The authentication source name appears in lists of objects from which users will sometimes choose; therefore, the name should clearly convey the purpose of this authentication source.

     You can instead enter a name and description when you save this authentication source.
   - Section 5.16, "Managing Object Properties" (optional)
10. On the Security page, perform the following task:
    - Section 5.17, "Setting Security on an Object" (optional)

    The default security for this authentication source is based on the security of the parent folder.
11. Run the job you associated with this authentication source.

12. If you are importing only partial users or groups or are applying different default profiles to each group of users, after the associated job runs once, return to the Authentication Source Editor and perform any necessary additional tasks.
13. If you have not already done so, modify the portal configuration to enable SSO. For details, see Appendix E, "Deploying Single Sign-On."

6.9.5 Editing an Authentication Source

To edit an authentication source you must have the following rights and privileges:

- Access Administration activity right
- At least Edit access to the authentication source

To edit an authentication source:

1. Click **Administration**.
2. Open the folder in which the authentication source is stored and click the authentication source name.
3. On the Main Settings page, perform tasks as necessary:
   - Section 6.9.8, "Setting Default Profiles and Target Folders for Imported Users"
   - Section 6.9.9, "Setting a Target Folder for Imported Groups"
4. On the Synchronization page, perform tasks as necessary:
   a. Under **General Info**, choose whether you want to use this authentication source to authenticate user credentials, import users and groups, or both:
      – To import users and groups and authenticate user credentials, choose **Authentication and Synchronization**. You must also specify what you want to synchronize (step 3).
      – To authenticate user credentials, but not import users and groups, choose **Authentication Only**.
      – To import users and groups, but use an authentication partner to authenticate user credentials, choose **Synchronization with Authentication Partner**. You must also specify the authentication partner (step 2), and what you want to synchronize (step 3).
   b. If you chose **Synchronization with Authentication Partner**, in the Authentication Partners list, choose the authentication source you want to use for authentication (SSO or another authentication source).

      Note: If the authentication partner is unavailable, this authentication source will attempt to authenticate users.

      To use SSO as specified in the portal configuration file, choose **SSO Authentication Source**.
   c. If you chose **Authentication and Synchronization** or **Synchronization with Authentication Partner**, specify what you want to synchronize.

      See Section 6.9.10, "Specifying Which Users and Groups to Synchronize."
   d. If you have users and groups distributed among different authentication sources, you can allow groups in this authentication source to include users

from another authentication source. To do this, select **Import user and group memberships from other authentication sources**.

e. In the **Import batches of** text box, type the number of users you want to import at a time.

The default batch setting is 1000 users. Some databases cannot support a batch of 1000; the most common reason is that the database runs out of space in the rollback segment because it attempts to add all 1000 users within one transaction. This situation terminates the transaction, and no users are imported.

Note: Raising the import batch number can improve the time it takes to synchronize.

---

5. On the Fully Synchronized Groups page, perform tasks as necessary:
   - Section 6.9.11, "Selecting Groups from Which to Import Users"
   - Section 6.9.12, "Specifying What to Do with Users and Groups Deleted from the Source User Repository"
6. On the Set Job page, perform tasks as necessary:
   - Section 5.14, "Associating an Object with a Job"
7. On the Properties and Names page, perform tasks as necessary:
   - Section 5.15, "Naming and Describing an Object"
   - Section 5.16, "Managing Object Properties"
8. On the Security page, perform tasks as necessary:
   - Section 5.17, "Setting Security on an Object"
9. On the Migration History and Status page, perform tasks as necessary:
   - Section 5.18, "Viewing Migration History and Status for an Object"
10. If this authentication source is set to synchronize users or groups, run the job associated with it.

6.9.6 Deleting an Authentication Source

To delete an authentication source you must have the following rights and privileges:

- Access Administration activity right
- Admin access to the authentication source

To delete an authentication source:

1. Click **Administration**.
2. Navigate to the authentication source.
3. Select the authentication source you want to delete and click the delete icon.

Note: Deleting an authentication source that authenticates users will mean that the users will not be able to log in to the portal.

6.9.7 Setting an Authentication Source Category to Distinguish Users and Groups Imported from a Particular Domain

On the Main Settings page of the Authentication Source Editor, you set the prefix you want to add to user and group names to distinguish the domain from which they were imported. For example, if you enter *myDomain*, each user name and each group name will be prefixed by the string *myDomain*; myUser becomes *myDomain/myUser* and myGroup becomes *myDomain/myGroup*.

This prefix is used in conjunction with the Global ACL Sync Map to map security from source content repositories to the security in the portal. For details on the Global ACL Sync Map, see Section 6.10, "Mapping External Document Security to Imported Portal Users with the Global ACL Sync Map."

1. If the Authentication Source Editor is not already open, open it now by creating an authentication source.

   Note: You can set the category only during authentication source creation.

2. Under Category, in the **Authentication Source Category** box, type the prefix you want to add to user and group names to distinguish that they were imported from this domain.

   Generally, you can set the category to any value you want, but there are a few important considerations:

   - Do not include spaces in the prefix.
   - After you create this authentication source you cannot change the category value.
   - If you are using Windows Integrated Authentication (WIA) as your single sign-on (SSO) authentication provider, your authentication source category must match the domain name.
   - You might want the authentication source category to match the domain name if you plan to import security information. Some content crawlers have the ability to import security information with the imported content, making portal security much easier to maintain. For this to work, the users with access to the imported content must correspond to portal users, as specified in the Global ACL Sync Map. If the authentication source category matches the name of the source domain, this correspondence is automatic.
   - Multiple authentication sources can use the same category. However, because the prefix is prepended to the user and group names, you must be certain that the domains involved do not have different users or groups with the same name. That is, if a LizaR user exists on one domain, and a LizaR user exists on another domain, they must be the same user because only one user will be created.

6.9.8 Setting Default Profiles and Target Folders for Imported Users

Specify which default profiles to apply to users imported by an authentication source. A default profile includes portlets, portlet preferences, My Pages, and personalization settings. By assigning a default profile to the imported users, you can control what users see when they first log in to your portal. After that, users can further personalize their views of the portal.

You must have at least Select access to the folder in which you want to store imported groups.

If the Authentication Source Editor is not already open, open it now.

- To apply the same default profile to all users imported by this authentication source, you can specify the following settings when you create the authentication source:

  1. In the Default Profile drop-down list, select the default profile to apply to the imported users.
  2. Under Target Folder, click **Browse** to select the folder in which to store the imported users.

     If you want to display an experience definition interface to the imported users when they log in, choose a folder to which the experience definition has been applied or apply the experience definition to the chosen folder before you import users.

     By default, users imported by this authentication source are stored in the same folder that stores the authentication source.

- To apply different default profiles to the users in some groups:

  1. Perform a Partial Users Synchronization to import all the groups.
  2. Return to the Authentication Source Editor.
  3. Click **Add Group**; then, in the Add Group dialog box, select the groups to which you want to apply different default profiles and click **OK**.

     Note: To view the members of a group or edit a group, click the group name.

  4. For each group, perform the following actions:

     a. In the Default Profile drop-down list, select the default profile to apply to the imported users.

     b. Under Target Folder, click **Browse** to select the folder in which to store the imported users.

        If you want to display an experience definition interface to the imported users when they log in, choose a folder to which the experience definition has been applied or apply the experience definition to the chosen folder before you import users.

        By default, users imported by this authentication source are stored in the same folder that stores the authentication source.

  5. Prioritize the default profiles by changing the order of the groups.

     If a user is a member of more than one group in this list, the uppermost default profile is applied. If necessary, move groups up or down in the list.

After you have configured all the settings for this authentication source, you must run a job to import the users and groups.

6.9.9 Setting a Target Folder for Imported Groups

By default, groups imported by an authentication source are stored in the same folder that stores the authentication source, but you can select a different folder if you want.

You must have at least Select access to the folder in which you want to store imported groups.

1. If the Authentication Source Editor is not already open, open it now.
2. Under New Groups, click **Browse** to select the folder in which to store the imported groups.

   The Change Folder dialog box opens.
3. Select the select a folder and click **OK**.

After you have configured all the settings for this authentication source, you must run a job to import the users and groups.

6.9.10 Specifying Which Users and Groups to Synchronize

When you set an authentication source to synchronize users and/or groups from a source user repository, you can specify which users and groups to synchronize.

> **Note:** When you synchronize users/groups, new users/groups are imported into the portal and deleted users/groups are removed from the portal.

1. If the Authentication Source Editor is not already open, open it now.
2. Click the **Synchronization** page.
3. Specify which users and groups to synchronize.
   - To import all users and groups from the source domain, select **Full Synchronization**.

     Each time you run the job associated with this authentication source all users and groups will be synchronized with the portal.
   - To import the users from selected groups, but not all of the users found on the source domain, perform the following steps:
     a. Select **Partial Users Synchronization**.
     b. Run the job associated with this authentication source.

        All of the groups in the source user repository are imported into the portal, but no users are imported.
     c. Return to the Authentication Source Editor and click the **Fully Synchronized Groups** page.
     d. Select the groups you want to fully synchronize.
     e. Run the job associated with this authentication source again.

        Each time you run the job associated with this authentication source all groups are synchronized, but the only users that are synchronized are the ones that are members of the fully synchronized groups.
   - To import all users, but only selected groups, perform the following steps:

a. Select **Full Synchronization** or **Partial Users Synchronization**.

b. Run the job associated with this authentication source.

c. Delete all unwanted groups from the portal.

d. Return to the Authentication Source Editor and click the **Synchronization** page.

e. Select **Partial Groups Synchronization**.

f. Run the job associated with this authentication source again.

Each time you run the job associated with this authentication source all users are synchronized, but no new groups are imported. Groups are still removed from the portal if they are deleted from the source user repository.

- To import selected users and selected groups, perform the following steps:

a. Select **Partial Users Synchronization**.

b. Run the job associated with this authentication source.

All of the groups on the source domain are imported into the portal, but no users are imported.

c. Delete all unwanted groups from the portal.

d. Return to the Authentication Source Editor and click the **Fully Synchronized Groups** page.

e. Select the groups from which you want to import users.

f. Click the **Synchronization** page.

g. Select **Partial Users and Partial Group Synchronization**.

h. Run the job associated with this authentication source again.

Each time you run the job associated with this authentication source the only users that are synchronized are the ones that are members of the fully synchronized groups, and no new groups are imported. Groups are still removed from the portal if they are deleted from the source user repository.

- To import no users or groups, choose **No Synchronization**.

4. If users from another authentication source are members of groups from this authentication source or vice versa, select **Import user and group memberships from other authentication sources**.

5. In the **Import batches of** box, type the number of users you want to import at a time.

The default batch setting is 1000 users. Some databases cannot support a batch of 1000; the most common reason is that the database runs out of space in the rollback segment because it attempts to add all 1000 users within one transaction. This situation terminates the transaction, and no users are imported.

Note: Raising the import batch number can improve the time it takes to synchronize.

6.9.11 Selecting Groups from Which to Import Users

The Fully Synchronized Groups page of the Authentication Source Editor enables you to choose groups from which you want to import users. The groups that you list on this page are synchronized with the corresponding groups on the source server.

Before you can select groups to fully synchronize, you must import the groups by running the authentication source in Partial Users Synchronization or Partial Users and Partial Group Synchronization mode.

1. If the Authentication Source Editor is not already open, open it now.
2. Click the **Fully Synchronized Groups** page.
3. Select groups from which to import users:
   - To add a group, click **Add Group**; then, in the Add Group dialog box, select the groups you want to add and click **OK**.
   - To add every group imported by this authentication source, click **Add All Groups**.
   - To delete a group, select the group and click the Delete icon.

     To select or clear all of the group boxes, select or clear the box to the left of **Group**.
   - To edit a group, click the group name.

6.9.12 Specifying What to Do with Users and Groups Deleted from the Source User Repository

The Fully Synchronized Groups page of the Authentication Source Editor enables you to specify what to do with users and groups deleted from the source user repository. By default the portal users are disabled and groups are moved to a folder for future deletion, but you can change this behavior.

1. If the Authentication Source Editor is not already open, open it now.
2. Click the **Fully Synchronized Groups** page.
3. To delete users rather than disabling them, clear the box next to **Disable users instead of deleting them**.
4. To delete groups rather than moving them to a folder for future deletion, clear the box next to **Defer deletion of groups instead of deleting**.
5. To change the folder in which groups deferred for deletion are stored, click **Browse** and, in the Change Folder dialog box, select the folder and click **OK**.

   By default, groups deferred for deletion are moved to a **Groups to Delete** folder in the same folder that stores the authentication source.

6.10 Mapping External Document Security to Imported Portal Users with the Global ACL Sync Map

Users imported through an authentication source can automatically be granted access to the content imported by some remote content crawlers through mappings in the Global ACL Sync Map.

The Global ACL Sync Map is used by content crawlers bringing security settings, in the form of Access Control Lists (ACLs), into your portal along with documents. The Global ACL Sync Map shows content crawlers how the users and groups found on

source document ACLs correspond with portal users and groups. Using this information, a content crawler can set portal security on imported content. For an example-based explanation of this process, see Section 7.10.5, "Example of Importing Content Security."

Every authentication source has a prefix. This prefix is used to distinguish the users and groups imported through the authentication source. If you plan to import security information with imported content, you might must map your authentication source prefixes to the source domains or map portal groups to external groups through the Global ACL Sync Map.

Note: If your authentication source prefix matches the domain name, the mapping occurs automatically and you do not must add the mapping to this page.

To access the Global ACL Sync Map you must be a member of the Administrators group.

To open the Global ACL Sync Map:

1. Click **Administration**.
2. From the Select Utility menu, choose **Global ACL Sync Map**.
3. On the Prefix: Domain Map page map authentication source prefixes to source domains:
   - To add a prefix to the map, click **Add Mapping**; then, in the Select Authentication Sources dialog box, select the authentication sources you want to map and click **OK**.

     Note: If more than one authentication source uses the same prefix, you only must map one of the authentication sources.

   - To edit the prefix in this mapping (this will not affect the prefix in the authentication source), in the **Authentication Source Prefix** column, click the edit icon. In the text box that displays, edit the name, then click the arrow icon to save your change.
   - To specify which domains map to a selected prefix, in the **Domain Name** column, click the edit icon and, in the text box that displays, type the domains you want to map, separated by commas (,). Click the arrow icon to save the mapping.
   - To remove a mapping, select the mapping and click the remove icon.
   - To select or clear all of the mapping check boxes, select or clear the box to the left of **Authentication Source Prefix**.
   - To toggle the order in which the mappings are sorted (ascending/descending), click **Authentication Source Prefix** or click the icon to the right of that.

6.11 About User Profiles

User profiles provide information about users, such as address, position, or whatever other information you want. User profiles can be accessed from several different

contexts, but are always available to end users as a series of portlets accessible through the My Account menu, with the **View User Profile** option.

There are several features associated with controlling and populating user profiles:

- You can change the portlets displayed on the user profile pages through the User Profile Manager (see Section 6.12.7, "Editing a Profile Page").

  Some user profile portlets are installed with the portal software and automatically added to the user profile pages:

  - **General Information** includes general contact information such as name, position, and phone number.
  - **Folder Expertise** lists the Knowledge Directory folders for which the user is a related expert.
  - **Managed Communities** lists the communities that the user has permission to manage. To view a listed community, click the community name.

  > **Note:** The Folder Expertise and Managed Communities portlets do not display if your portal uses adaptive layouts.

  You can also create new portlets to suit your needs. For more information on portlets, see Chapter 8, "Extending Portal Services with Portlets."

- You can change the properties displayed in the user profile portlets through the administrative preferences page of the user profile portlet (accessible through the Main Settings page of the Portlet Editor). For information on these administrative preferences, see Section 6.12.2, "Configuring a User Profile Portlet".
- The values for properties in the user profile are either manually entered by the user on the Edit User Profile page or automatically populated by a profile source.

  > **Note:** The Folder Expertise portlet displays the list of folders for which the user is an expert. You can add users to a folder as an expert through the Related Resources page of the Folder Editor, or, if users have the Self-Selected Experts activity right, they can add themselves as experts when they are browsing folders in the Directory. The Managed Communities portlet displays the list of communities managed by the user. This portlet is automatically populated with all the communities to which the user has Edit or Admin access.

- You can limit the information displayed in user profiles by restricting access to the user profile portlets and the properties displayed in those portlets. For example, you might want to display employee contact information both to customers and employees but want to restrict reporting hierarchy information to display only to employees. You could create two separate user profile portlets—one for your customers (containing the contact information properties) and another one for your employees (containing the contact information and reporting hierarchy properties). However, you could instead just create one user profile portlet, containing the contact information and reporting hierarchy properties, but limit the security on the reporting hierarchy properties to allow only employees Select access. Users that have Select access to a property can view the value of that property for other users. Users who have Read access to a property can view only their own values; when they view the profile of another user, that property is hidden.

6.12 Working with the User Profile

The user profile is really just a special community, accessed through the User Profile Manager. By default, the user profile consists of a single page populated with three user profile portlets—General Information, Folder Expertise, and Managed Communities. As with any community, you can add additional portlets and pages and can change the community template used for the user profile to enhance the user experience.

This section describes the following main tasks:

- Section 6.12.1, "Editing the User Profile"
- Section 6.12.2, "Configuring a User Profile Portlet"

It also covers the following low-level tasks:

- Section 6.12.3, "Changing the User Profile Community Template"
- Section 6.12.4, "Ordering Profile Pages"
- Section 6.12.5, "Adding a Profile Page"
- Section 6.12.6, "Deleting a Profile Page"
- Section 6.12.7, "Editing a Profile Page"
- Section 6.12.8, "Adding or Editing the Header and Footer on User Profile Pages"
- Section 6.12.9, "Associating User Information with Properties Using the User Information — Property Map"

6.12.1 Editing the User Profile

To access the User Profile Manager you must have the following rights and privileges:

- Access Administration activity right
- Access Utilities activity right

To manage the user profile:

1. Click **Administration**.
2. In the Select Utility list, select **User Profile Manager**.
3. On the Profile Pages page, perform tasks as necessary:
   - Section 6.12.3, "Changing the User Profile Community Template"
   - Section 6.12.4, "Ordering Profile Pages"
   - Section 6.12.5, "Adding a Profile Page"
   - Section 6.12.6, "Deleting a Profile Page"
   - Section 6.12.7, "Editing a Profile Page"
4. On the Header and Footer page, perform tasks as necessary:
   - Section 6.12.8, "Adding or Editing the Header and Footer on User Profile Pages"
5. On the This Community's Portlets page, perform tasks as necessary:
   - Section 9.5.13, "Creating a Community Portlet"
6. On the User Information - Property Map page, perform tasks as necessary:

- Section 6.12.9, "Associating User Information with Properties Using the User Information — Property Map"

7. On the Properties and Names page, perform tasks as necessary:
   - Section 5.15, "Naming and Describing an Object"
   - Section 5.16, "Managing Object Properties"
8. On the Security page, perform tasks as necessary:
   - Section 5.17, "Setting Security on an Object"
9. On the Migration History and Status page, perform tasks as necessary:
   - Section 5.16, "Managing Object Properties"

6.12.2 Configuring a User Profile Portlet

User profile portlets are made up of:

- **Properties**: Profile information—such as name, author, and title—are stored with users as properties. These properties, like those associated with any other type of object—such as content crawlers and documents—can be searched (if they are set as searchable in the Property Editor).

  Just as with other objects, a property of a user has the same value regardless of where it is displayed. For example, if you want to display your users' home phone numbers in a Home Information Profile portlet and their work phone numbers in a Work Information Profile portlet, you must create separate "Work Phone" and "Home Phone" properties and display them in the respective portlets. If you only have a single "Phone" property, then the value of the Phone property would be the same in both profile portlets.
- **Categories**: Categories are organized groups of properties. Categories let you organize the display order of properties and provide context for what type of information is being displayed.

You can change the categories and properties displayed in the user profile portlets through the administrative preferences page of the user profile portlet.

To configure a user profile portlet:

1. Click **Administration**.
2. Navigate to the user profile portlet you want to edit and click its name.
3. Add or edit properties and categories as necessary:
   - To add a new category, click **New Category**. In the New Category dialog box, type a name and description, then click **Finish**.
   - To add a new property to a category, under the category, click **Add Property**. In the Add Properties dialog box, select the properties you want to add, and click **OK**.
   - To change a category name or description, click **Rename Categories**. In the Rename Categories dialog box, click the category you want to rename. In the Names and Descriptions dialog box, type a name and a description, and click **Finish**. When you are done renaming all the categories, click **Close**.
   - To arrange the order of properties and categories (for categories, click **Manage Categories** first):
     – To move the selection to the top of the list, click the move to top icon.

  - To move the selection up, click the move up icon.
  - To move the selection down, click the move down icon.
  - To move the selection to the bottom of the list, click the move to bottom icon.
- To remove a property or a category (for categories, click **Manage Categories** first), select the properties or categories you want to delete and click the remove icon.

4. To localize a category name and description:
   a. Click **Rename Categories**.
   b. In the Rename Categories dialog box, select the category you want to localize. The Names and Descriptions dialog box appears.
   c. If you did not set a mandatory object language in the portal configuration file, in the **Primary Language** list, select the language for the name and description you entered.

      If you did set a mandatory object language in the portal configuration file, you see the mandatory language instead of a list. You cannot change this setting. The name and description you entered must be in the mandatory language.

      If a localized name and description is not available in a user's selected language, the user will see the name and description in the specified primary language.
   d. Select **Supports Localized Names**.

      The Localized Names and Descriptions section appears.
   e. Add localized names and descriptions as necessary. Click **New Localized Name**. This displays the Name and Description dialog box. In the **Name** box, type the localized name for this category. In the **Language** drop-down list, choose the language for which you are adding a name and description. In the **Description** box, type the localized description for this category. When you are done, click **Finish**.

6.12.3 Changing the User Profile Community Template

The community template determines a set of required pages and—if configured—enforces a header and a footer.

Caution: When changing the community template, note the following:

- Any pages from the old community template that are not part of the new community template will be removed.
- If you have set special headers and footers for the profile pages, switching to a community template that enforces a header or footer will remove your header or footer.

To change the community template:

1. If the User Profile Manager is not already open, open it now.
2. In the Community Template section, click **Change Community Template**. This displays the Community Templates dialog box.

3. Select a template and click **OK**.
4. If you do not want the profile pages to inherit future changes to the template, clear the box next to **Inherit the Template**.

   If you select to inherit changes, any change applied to the community template affects the profile pages. For example, if a page is removed from the community template, the page will be removed from the profiles as well. Additionally, if you inherit changes, you cannot delete pages associated with the template, but you can add new pages and change the order of the pages.
5. Click **OK**.

6.12.4 Ordering Profile Pages

The order in which pages are displayed in the Profile Pages list is the order in which the page links will display to users.

1. If the User Profile Manager is not already open, open it now.
2. In the Profile Pages section, change the order of the pages:
   - To move a page to the top of this list, click the move to top icon.
   - To move a page up one space in this list, click the move up icon.
   - To move a page down one space in this list, click the move down icon.
   - To move a page to the bottom of this list, click the move to bottom icon.

6.12.5 Adding a Profile Page

When you create a new page, you must choose a page template. This page template determines the default page name, a set of required portlets, and the page layout.

To add a profile page:

1. If the User Profile Manager is not already open, open it now.
2. In the Profile Pages section, click **New Page**.
3. Select a page template and click **OK**.
4. If you do not want the profile pages to inherit future changes to the template, clear the box next to **Inherit the Template**.

   If you select to inherit changes, any change applied to the community template affects the profile pages. For example, if a page is removed from the community template, the page will be removed from the profiles as well. Additionally, if you inherit changes, you cannot delete pages associated with the template, but you can add new pages and change the order of the pages.
5. Click **OK**.

6.12.6 Deleting a Profile Page

You can delete any page that says No in the From Community Template column. If you chose to inherit changes from the community template, pages that are part of that template say Yes in the From Community Template column and cannot be deleted.

To delete a profile page:

1. If the User Profile Manager is not already open, open it now.
2. In the Profile Pages section, select the page and click the delete icon.

6.12.7 Editing a Profile Page

Depending on whether you are inheriting changes, you can change the page name, add portlets, delete portlets, rearrange portlets, change the page layout, and set page security.

To edit a profile page:

1. If the User Profile Manager is not already open, open it now.
2. In the Profile Pages section, click the name of the page.
3. Edit the page as necessary.

6.12.8 Adding or Editing the Header and Footer on User Profile Pages

You can add header and footer portlets to user profiles to control what users see at the top and bottom of the user profile pages.

To add or edit the headers and footers you must have the following rights and privileges:

- Access Administration activity right
- Access Utilities activity right
- At least Select access to the header and footer portlets you want to add

To add or edit the headers and footers on user profile pages:

1. If the User Profile Manager is not already open, open it now.
2. Click the **Header and Footer** page.
3. Select the header and footer for the user profile pages.
    a. To add or change the header, under Community Header, click **Browse**, then, in the Select a Header dialog box, select the header you want, and click **OK**.
    b. To add or change the footer, under Community Footer, click **Browse**, then, in the Select a Footer dialog box, select the footer you want, and click **OK**.
    c. To remove the header, under Community Header, click **Remove**.
    d. To remove the footer, under Community Footer, click **Remove**.

6.12.9 Associating User Information with Properties Using the User Information — Property Map

The User Information — Property Map enables you to map user information to user properties in the portal. The information in these user properties can then be displayed in the user's profile, or it can be sent to content crawlers, remote portlets, or federated searches so that users do not have to enter this information on a separate preference page.

To map user information to portal properties you must have the following rights and privileges:

- Access Administration activity right
- Access Utilities activity right
- At least Select access to the properties you want to map

Note: The Full Name attribute is automatically mapped to display name of the user unless you override it on this page.

1. If the User Profile Manager is not already open, open it now.
2. Under Edit Object Settings, click **User Information - Property Map**.
3. Add a property. Click **Add**; then, in the **Choose Property** dialog box, select the property you want to add and click **OK**.
4. Map attributes to the property:
   a. Click the Edit icon next to the property name.
   b. In the text box, type the attribute.

      To map the property to multiple attributes, separate the attribute names with commas (,).
5. Repeat Steps 3 and 4 to map additional properties.

   To remove properties, select the property you want to remove and click the Remove icon.

After mapping user information to portal properties, you must import the user information through profile sources or have users manually enter the information by editing their user profiles.

6.13 About Importing User Profile Information

Profile sources allow you to import user information (such as name, address, or phone number) that is already defined in your enterprise in existing user repositories, such as Active Directory or LDAP servers. The imported user information can be used to populate user profiles or can be passed to content crawlers, remote portlets, or federated searches as user information.

This section describes the pieces that work together to make importing user information work. It covers the following topics:

- Section 6.13.1, "Profile Providers"
- Section 6.13.2, "Profile Web Services"
- Section 6.13.3, "Profile Sources"

6.13.1 Profile Providers

A profile provider is a piece of software that tells the portal how to use the information in the external user repository. Oracle provides profile providers as part of the Oracle WebCenter Interaction Identity Services. The Oracle WebCenter Identity Service for LDAP is used to import user information from LDAP servers. The Oracle WebCenter Identity Service for Microsoft Active Directory is used to import user information from Active Directory servers. If your user information resides in a custom system, such as a custom database, you can import it by writing your own profile provider using the IDK.

Note:

- You must install the profile provider before you can create the associated profile Web service. For information on installing profile providers, refer to the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Interaction for Windows* or the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Interaction for Unix and Linux*).
- To learn about developing your own profile provider, refer to the *Oracle Fusion Middleware Web Service Developer's Guide for Oracle WebCenter Interaction*.

6.13.2 Profile Web Services

Profile Web services enable you to specify general settings for your external user repository, leaving the more detailed settings (like domain specification) to be set in the associated remote profile sources, enabling you to create different profile sources to import information each domain without having to repeatedly specify all the settings.

6.13.3 Profile Sources

Profile sources allow you to import user information (such as name, address, or phone number) from external user repositories. User information can exist anywhere in your enterprise:

- If the information resides on an Active Directory server, you can create an Active Directory remote profile source to extract it.
- If the information resides on an LDAP server, you can create an LDAP remote profile source to extract it.
- If the information resides in a custom system, such as a custom database, you can easily extract the information by writing your own remote profile provider, using IDK and then create a remote profile source to extract the information.

Note:

- You must map the user information to portal properties on the User Information — Property Map (in the User Profile Manager) before you import the user information.
- You must import users through an authentication source before you can import the associated user information.
- You must run a job associated with the profile source to import the user information. You should continue to run the job periodically to keep the user information in the portal synchronized with the information in the source user repository.

6.14 Working with Profile Web Services

This section describes the following main tasks:

- Section 6.14.1, "Creating or Editing a Profile Web Service"
- Section 6.14.2, "Deleting a Profile Web Service"

6.14.1 Creating or Editing a Profile Web Service

Profile Web services enable you to specify general settings for your external user repository, leaving the more detailed settings (like domain specification) to be set in the associated remote profile sources, enabling you to create different profile sources to import information each domain without having to repeatedly specify all the settings.

Before you create a profile Web service, you must:

- Install the profile provider on the computer that hosts the portal or on another computer
- Create a remote server pointing to the computer that hosts the profile provider (optional, but recommended)

To create a profile Web service you must have the following rights and privileges:

- Access Administration activity right
- Create Web Service Infrastructure activity right
- At least Edit access to the parent folder (the folder that will store the profile Web service)
- At least Select access to the remote server that the profile Web service will use

To edit a profile Web service you must have the following rights and privileges:

- Access Administration activity right
- At least Edit access to the profile Web service
- If you plan to change the remote server association, at least Select access to the remote server that the profile Web service will use

To create or edit a profile Web service:

1. Click **Administration**.
2. Open the Profile Web Service Editor.
   - To create a profile Web service, open the folder in which you want to store the profile Web service. In the Create Object list, click **Web Service — Profile**.
   - To edit a profile Web service, open the folder in which the profile Web service is stored and click the profile Web service name.
3. On the Main Settings page, perform tasks as necessary:
   - Section 3.4.1, "Associating a Remote Server with a Web Service"
   - Section 3.4.2, "Specifying the Location of the Web Service Provider or Code"
   - Section 3.4.3, "Specifying Web Service Time-Out Settings"
   - Section 3.4.4, "Enabling and Disabling a Web Service"
4. On the HTTP Configuration page, perform tasks as necessary:
   - Section 3.4.7, "Specifying What Content is Gatewayed for a Web Service"
5. On the Advanced Settings page, perform tasks as necessary:
   - Section 3.4.11, "Specifying Encoding Style for a Web Service"
   - Section 3.4.8, "Adding a Service Configuration Page to a Web Service Editor"
6. On the Authentication Settings page, perform tasks as necessary:

- Section 3.4.13, "Specifying Authentication Settings for a Web Service"

7. On the Debug Settings page, perform tasks as necessary:
   - Section 3.4.16, "Enabling Error Tracing for a Web Service"
8. On the Associated Objects page, perform tasks as necessary:
   - Section 3.4.17, "Viewing Objects Associated with a Web Service"
9. On the Properties and Names page, perform tasks as necessary:
   - Section 5.15, "Naming and Describing an Object"

     You can instead enter a name and description when you save this authentication Web service.
   - Section 5.16, "Managing Object Properties"
10. On the Security page, perform tasks as necessary:
    - Section 5.17, "Setting Security on an Object"

    The default security for this profile Web service is based on the security of the parent folder. Administrative users with at least Select access to this profile Web service can create profiles sources based on the Web service.
11. If you are editing a profile Web service, on the Migration History and Status page, perform tasks as necessary:
    - Section 5.18, "Viewing Migration History and Status for an Object"

Note: The Migration History and Status page is not available when creating an object.

6.14.2 Deleting a Profile Web Service

To delete a profile Web service you must have the following rights and privileges:

- Access Administration activity right
- Admin access to the profile Web service

To delete a profile Web service:

1. Click **Administration**.
2. Navigate to the profile Web service.
3. Select the profile Web service you want to delete and click the delete icon.

Note: Deleting a profile Web service will break any associated profile sources.

6.15 Working with Profile Sources

This section describes the following main tasks:

- Section 6.15.1, "Creating or Editing a Remote Profile Source"
- Section 6.15.2, "Deleting a Profile Source"

It also covers the following low-level tasks:

- Section 6.15.3, "Selecting a Unique Key for a Profile Source"

- Section 6.15.4, "Selecting the Users and Groups for Which to Import Profile Information"
- Section 6.15.5, "Mapping Source User Attributes to Portal Properties"
- Section 6.15.6, "Clearing User Information Imported by a Profile Source"

6.15.1 Creating or Editing a Remote Profile Source

Profile sources allow you to import user information (such as name, address, or phone number) that is already defined in your enterprise in existing user repositories, such as Active Directory or LDAP servers. The imported user information can be used to populate user profiles or can be passed to content crawlers, remote portlets, or federated searches as user information.

Before you create a remote profile source, you must:

- Import users with an authentication source.
- If necessary, create portal properties for the attributes you want to import.
- Associate the portal properties with the user object through the Global Object Property Map.
- Map user attributes from the source user repository to portal properties with the User Information Property Map.
- Install the profile provider on the computer that hosts the portal or on another computer.
- Create a remote server that points to the computer that hosts the profile provider.
- Create a profile Web service on which to base the profile source.

To create a profile source you must have the following rights and privileges:

- Access Administration activity right
- Create Profile Sources activity right
- At least Edit access to the parent folder (the folder that will store the profile source)
- At least Select access to the profile Web service on which this profile source will be based

To create a profile source you must have the following rights and privileges:

- Access Administration activity right
- At least Edit access to the profile source

To create or edit a profile source:

1. Click **Administration**.
2. Open the Profile Source Editor.
   - To create a profile source, open the folder in which you want to store the profile source. In the Create Object list, click **Profile Source - Remote**. In the Choose Web Service dialog box, select the Web service that provides the basic settings for your profile source and click **OK**.
   - To edit a profile source, open the folder in which the profile source is stored and click the profile source name.
3. On the Main Settings page, perform tasks as necessary:

- Section 6.15.3, "Selecting a Unique Key for a Profile Source"
- Section 6.15.4, "Selecting the Users and Groups for Which to Import Profile Information"

4. On the Property Map page, perform tasks as necessary:
   - Section 6.15.5, "Mapping Source User Attributes to Portal Properties"
5. On the Set Job page, perform tasks as necessary:
   - Section 5.14, "Associating an Object with a Job"
6. On the Properties and Names page, perform tasks as necessary:
   - Section 5.15, "Naming and Describing an Object"

     You can instead enter a name and description when you save this profile source.
   - Section 5.16, "Managing Object Properties"
7. On the Security page, perform tasks as necessary:
   - Section 5.17, "Setting Security on an Object"

   The default security for this profile source is based on the security of the parent folder.
8. If you are editing a profile Web service, on the Migration History and Status page, perform tasks as necessary:
   - Section 5.18, "Viewing Migration History and Status for an Object"

   Note: The Migration History and Status page is not available when creating an object.
9. Run the job associated with this profile source.

6.15.2 Deleting a Profile Source

To delete a profile source you must have the following rights and privileges:

- Access Administration activity right
- Admin access to the profile source

To delete a profile source:

1. Click **Administration**.
2. Navigate to the profile source.
3. Select the profile source you want to delete and click the delete icon.

6.15.3 Selecting a Unique Key for a Profile Source

Each profile source must include a unique key that is used to identify the user to the profile provider.

1. If the Profile Source Editor is not already open, open it now and display the Main Settings page.
2. Under Profile Unique Key, select the key that will be used to identify the user to the profile provider.

- **Remote Unique Name** — This is the default. The user's imported unique name will be sent to the remote provider to identify the user. Common examples are the GUID or User Name.
- **Remote Authentication Name** — The user's imported authentication name will be sent to the remote provider. In most cases, this is the same as the unique name.
- **User Property Value** — The value of a property associated with each user will be sent to identify this user. Typically, this value is imported by another profile source.

  If you select this option, you must also select which property to use: click **Choose Property**, in the Choose Property dialog box, select a property and click **OK**.

  To change the selected property, click the property name.

6.15.4 Selecting the Users and Groups for Which to Import Profile Information

You can select the users and groups for which user information should be imported.

1. If the Profile Source Editor is not already open, open it now and display the Main Settings page.
2. Under Profile Source Membership, select the users and groups for which user information should be imported.
   - To add users or groups, click **Add Users/Groups**; then, in the Profile Source Membership dialog box, select the users and groups you want to add and click **OK**.
   - To remove a user or group, select the user or group and click the Remove icon.

     To select or clear all of the user and group boxes, select or clear the box to the left of **Users/Groups**.
   - To toggle the order in which the folders are sorted, click **Users/Groups**.

6.15.5 Mapping Source User Attributes to Portal Properties

You can select the users and groups for which user information should be imported.

1. If the Profile Source Editor is not already open, open it now and display the Property Map page.
2. Specify how to map source user attributes to portal properties.
   - To add properties, click **Add Property**; then, in the Choose Property dialog box, select the properties you want to add and click **OK**.
   - To map a source user attribute to a portal property, click the Edit icon to the far right of the property, type the name of the attribute in the box, and click the Save icon to save the mapping.
   - To remove a mapping, select the mapping and click the Remove icon.
   - To select or clear all of the mapping boxes, select or clear the box to the left of **Properties**.
   - To toggle the order in which the properties are sorted, click **Properties**.

6.15.6 Clearing User Information Imported by a Profile Source

You can delete all user information previously imported by a profile source. This is useful when you add a new user property and want to look it up and update it for all users, or when you change a property from read-write to read-only and want to overwrite previous user modifications.

To delete user information imported by a profile source you must have the following rights and privileges:

- Access Administration activity right
- At least Edit access to the profile source

1. Click **Administration**.
2. Navigate to and open the profile source.

   The Remote Portlet Editor opens, displaying the Main Settings page.
3. Click **Clear History**.

Run the job associated with the profile source to import the user information again.

6.16 About Invitations

Invitations allow you to direct potential users to your portal, making it easy for them to create their own user accounts and letting you customize their initial portal experiences with content that is of particular interest to them.

You should create a single invitation for all potential users who should be added to the same portal groups and should see the same communities, portlets, and My Pages when they first log in to your portal. After you create an invitation, you generate an invitation link to send to invitees. The invitation link expires after a specified number of users is created from the link or after the specified date. You can generate multiple invitation links for one invitation, each with different expiration settings.

To accept the invitation, the user clicks the link included in the e-mail and follows the directions to create a new user and log in to the portal. When the user logs in, the portlets, content, and communities specified in the invitation are displayed to the new user.

Users added by invitation are stored in the folder you specify in the invitation and are included in the WCI Authentication Source. They are automatically given security privileges based on the default profile you specify in the invitation. Based on this security, users can personalize their views of the portal with My Pages, portlets, and community memberships, and can view portal content.

6.17 Working with Invitations

This section describes the following tasks:

- Section 6.17.1, "Creating or Editing an Invitation"
- Section 6.17.2, "Sending an Invitation"
- Section 6.17.3, "Deleting an Invitation"

6.17.1 Creating or Editing an Invitation

Before you create an invitation, you must:

- Create the default profile you want to apply to the users who accept the invitation.

- Create the folder in which you want to store the users who accept the invitation.

To create an invitation you must have the following rights and privileges:

- Access Administration activity right
- Create Invitations activity right
- At least Edit access to the parent folder (the folder that will store the invitation)

To edit an invitation you must have the following rights and privileges:

- Access Administration activity right
- At least Edit access to the invitation

To create or edit an invitation:

1. Click **Administration**.
2. Open the Invitation Editor.
   - To create an invitation, open the folder in which you want to store the invitation. In the Create Object list, click **Invitation**.
   - To edit an invitation, open the folder in which the invitation is stored and click the invitation name.
3. Select a folder in which to store the users who accept this invitation. Click **Browse**; then, in the **Select a Folder** dialog box, choose a folder and click **OK**.

   If you want to display a particular experience definition interface to users when they log in, choose a folder to which the experience definition has been applied or apply the experience definition to the chosen folder before you send the invitation.
4. In the **Default User Image** list, select the default profile to apply to users who accept the invitation.

   The default profile defines the user's initial view of the portal.
5. Select the groups to which you want to add users who accept the invitation.
   - To add invitees to a group, click **Add Group**; then, in the **Select Groups** dialog box, select the groups you want to add and click **OK**.
   - To remove a group from the list, select the group and click the Remove icon.

     To select or clear all of the group check boxes, select or clear the box to the left of **Group Name**.
   - To toggle the order in which the groups are sorted, click **Group Name**.

After creating the invitation, you must generate an invitation link and e-mail it to your invitees.

6.17.2 Sending an Invitation

To send an invitation, you generate a link to e-mail to recipients. Recipients who follow this link are prompted to create a new account in your portal and can then begin customizing their views of your portal and exploring its contents.

Before you send an invitation, you must:

- Create the invitation.

To send an invitation you must have the following rights and privileges:

- Access Administration activity right

- At least Edit access to the invitation

You can create

1. Click **Administration**.
2. Open the folder in which the invitation is stored.
3. Select the invitation and click **Send Invitation**.

   The Send Invitation page opens.
4. If you have not already done so, create an invitation link. Click **Create New Invitation Link**.

   If you have already created an invitation link with the expiration settings you want to use, skip to Step 6.
5. In the Create New Invitation Link dialog box, specify settings to prevent this link from being circulated and allowing unintended users access to secured content in your portal.
   a. In the **Name** box, type a name for this link that makes clear to you and other administrative users what this link is for.
   b. In the **Number of Invitations** box, type the maximum number of users that can be created from this link.
   c. In the **Expiration Date** box, type the date after which this link displays an error and will not allow users to create a portal account.

      To choose the date from a calendar, click the Calendar icon.
   d. To create the link, click **Finish**.
6. To display the invitation link, click the link name.
7. Copy and paste the invitation link into an e-mail, modify the message as desired, and send it to your invitees.

> **Note:** The only way to cancel an invitation is to delete the invitation, so be sure your invitation is correct before you e-mail it to anyone.

6.17.3 Deleting an Invitation

To delete an invitation you must have the following rights and privileges:

- Access Administration activity right
- Admin access to the invitation

To delete an invitation:

1. Click **Administration**.
2. Navigate to the invitation.
3. Select the invitation you want to delete and click the delete icon.

6.18 Auditing User Accounts and Actions

The portal logs user activities, which enables you to query for actions taken by particular users, actions taken on a particular administrative object, or actions taken within a specified time period.

To configure user activity auditing and audit user activity you must have the following rights:

- Access Administration activity right
- Access Utilities activity right

> **Note:** You should configure activity logging to adequately meet the security auditing needs of your portal deployment and then implement procedures for periodically reviewing the audit records.

To configure user activity auditing and audit user activity:

1. Click **Administration**.
2. In the Select Utility list, click **Audit Manager**.
3. On the Main Settings page, perform tasks as necessary:
   - Section 6.18.1, "Configuring User Activity Auditing"
4. On the Create Audit Query page, perform tasks as necessary:
   - Section 6.18.2, "Querying User Activity Audit Information"
5. On the Run Query page, you see the results of your query. For details, see Section 6.18.3, "User Activity Audit Query Results."

6.18.1 Configuring User Activity Auditing

You can specify what types of events should be logged.

To access the Audit Manager you must be a member of the Administrators Group.

1. If the Audit Manager is not already open, open it now.
2. Under Message Types, specify what types of events should be logged:

Message Type	Description
Item Change	Creates an entry every time an object is edited.
Item Deletion	Creates an entry every time an object is deleted.
Locked Account	Creates an entry every time a user account is locked after a number of failed login attempts.
Security Change	Creates an entry every time an object's security is edited.
User Login	Creates an entry every time a user successfully logs in to the portal.
Global System Change	Creates an entry every time an edit is made to the Global ACL Sync Map, the Global Property Map, the Global Content Type Map, the Global Object Property Map, or the User Information Property Map; every time job folders or Automation Services are registered; and every time global system settings are changed through the various portal utilities.

6.18.2 Querying User Activity Audit Information

You can query the user activity logs.

To access the Audit Manager you must be a member of the Administrators Group.

1. If the Audit Manager is not already open, open it now.

2. Click the **Create Audit Query** page.
3. Under Search Criteria, limit the information returned by your query:

> **Note:** If you do not specify any information on this page, your query returns a description of every audit record that is stored in the database.

- To limit your query to a particular type of object, in the **Item Type** list, choose the object.

  For example, you might want to see only audit messages referring to modifications of content crawlers.

- To limit your query to objects of a particular name, in the **Item Name** box, type the text you want to search for and, in the list, choose whether you want your search for approximate or exact matches.

  If you search for approximate matches, the portal returns items that include your text in any part of the name; if you search for exact matches, the portal returns only those items in which the item name equals the text you specify. For example, you could request only audit messages referring to actions on Sales content crawlers or Sales portlets by entering `Sales` in the text box and choosing **Approximate**.

- To limit your query to actions performed by a particular user, in the **Username** box, type the text you want to search for and, in the list, choose whether you want to search for approximate or exact matches.

- To limit your query to actions performed on a particular portal server, in the **Server Name** box, type the text you want to search for and, in the list, choose whether you want to search for approximate or exact matches.

  For example, you could retrieve messages for all jobs run on the Automation Service named PortalJobs.

- To limit your query to audit messages containing a particular word, in the **Word in Message** box, type the text you want to search for.

  For example, to limit your query to all messages relating to a particular group, type the group name in this box.

- To limit your query to particular types of messages, choose the types.

Message Type	Description
Item Change	Entries corresponding to every time an object is edited.
Item Deletion	Entries corresponding to every time an object is deleted.
Locked Account	Entries corresponding to every time a user account is locked after a number of failed login attempts.
Security Change	Entries corresponding to every time an object's security is edited.
User Login	Entries corresponding to every time a user successfully logs in to the portal.

Message Type	Description
Global System Change	Entries corresponding to every time an edit is made to the Global ACL Sync Map, the Global Property Map, the Global Document Type Map, the Global Object Property Map, or the User Information Property Map; every time job folders or Automation Services are registered; and every time global system settings are changed through the various portal utilities.

4. To limit your query to a particular period, in the **Time Interval** boxes, enter the starting and ending date and time you want to search.
5. Select the order in which you want to sort audit messages.

   By default, the most recent audit messages are displayed first. To change the sort to display the oldest audit messages first, choose **Oldest to newest**.
6. In the **Results per page** box, type the maximum number of messages to display per page.
7. Click the **Run Query** page. For details on the results, see User Activity Audit Query Results.

6.18.3 User Activity Audit Query Results

When you run an audit query, the results display on the Run Query page of the Audit Manager.

Column	Description
Item Type	Displays the type of object that was modified: for example, Content Crawler, Portlet, or User.
Item Name	Displays the name of the object that was modified: for example, the Meeting Minutes Content Crawler.
User	Displays the name of the user who performed the action on the object.
Server	Displays the server from which the object was modified.
Message Type	Displays the type of action performed on the object: for example, User Login or Item Change.
Time	Displays the date and time the object was modified.
Message	Displays the text of the message.

6.18.4 Archiving Audit Messages

You can specify how and when to archive audit messages.

To access the Audit Manager you must be a member of the Administrators Group.

The Audit Log Management agent moves audit messages from the portal database into a collection of archive files and deletes old archive files based on the settings you configure in the Audit Manager. The Audit Log Management agent runs in the Audit Log Management Job, created upon installation and stored in the **Intrinsic Operations** folder. By default, this job runs daily. To change the frequency, edit the Audit Log Management Job.

1. If the Audit Manager is not already open, open it now.
2. Under Archiving Agent, specify the settings for your auditing archive:

a. In the **Network path of archive files** box, type the path to the folder in which you want to store audit archive files.

b. In the **Days to keep messages in database** box, type the number corresponding to how many days worth of messages you want to store in the portal database.

   Only messages in the portal database are available for audit query. After the specified amount of time, messages are moved from the database into the archive files.

c. In the **Days to keep messages in files** box, type the number corresponding to the number of days you want to store the message files.

   After the specified period, messages are deleted from these files and no longer available.

6.18.5 Deleting Audit Messages and Archives

When you configure user activity auditing, you can specify the frequency with which audit messages are deleted automatically.

To access the Audit Manager you must be a member of the Administrators Group.

1. If the Audit Manager is not already open, open it now.
2. Under Delete Messages, specify which messages you want to delete from the portal database (they are not moved into the audit archive) and which archives you want to delete from your file system:

   a. In the **Delete Messages and Archives before** box, type the date for which you want to delete messages and archives.

      Any messages and archives with this date or an earlier date are deleted.

   b. In the **Message types to delete** section, choose the types of messages to delete from the database.

Message Type	Description
Item Change	Entries corresponding to every time an object is edited.
Item Deletion	Entries corresponding to every time an object is deleted.
Locked Account	Entries corresponding to every time a user account is locked after a number of failed login attempts.
Security Change	Entries corresponding to every time an object's security is edited.
User Login	Entries corresponding to every time a user successfully logs in to the portal.
Global System Change	Entries corresponding to every time an edit is made to the Global ACL Sync Map, the Global Property Map, the Global Document Type Map, the Global Object Property Map, or the User Information Property Map; every time job folders or Automation Services are registered; and every time global system settings are changed through the various portal utilities.

   c. If you want to delete these messages and archives when you click **Finish**, select **Yes** next to **Delete Messages and Archives when 'Finish' is clicked**.

7

Managing Portal Content

This chapter explains how to make content available through the portal's Knowledge Directory and how to manage that content in the portal using portal tools such as filters and crawlers.

It includes the following sections:

For additional information about Oracle WebCenter Console for Microsoft SharePoint, see

7.1 About Portal Content

The portal is designed to enable users to discover all of the enterprise content related to their employee role by browsing or searching portal areas.

Portal users should be able to assemble a My Page that provides access to all of the information they need. For example, to write user documentation, technical writers must be able to assemble a My Page that includes portlet- or community-based access to documentation standards and conventions, solution white papers, product data sheets, product demonstrations, design specifications, release milestones, test plans, and bug reports, as well as mail-thread discussions that are relevant to customer support and satisfaction. To perform their role, technical writers do not need access to the personnel records that an HR employee or line-manager might require, or to the company financial data that the controller or executive staff might need, for example.

A properly designed enterprise portal, then, would reference all of these enterprise documents so that any employee performing any function can access all of the information they need; but a properly designed enterprise portal would also ensure that only the employee performing the role can discover the information.

Complete the following tasks to enable managed discovery of enterprise content through the portal:

- For all file types you plan to support in your portal, configure document properties to store document metadata and to enable document filters used by the Knowledge Directory, content crawlers, the Smart Sort utility, and the Search Service. For details, see Section 7.4, "About Document and Object Properties."
- Configure access to content sources that can be selected by users or content crawlers to add document records to the Knowledge Directory and search index. For details, see Section 7.10, "About Importing Content."
- Configure content crawlers and crawl jobs to create links to back-end content sources, such as internet locations, file system locations, Documentum Content Servers, Exchange Servers, Lotus Notes Servers, or other IMAP-compliant servers. For details, see Section 7.10.4, "Content Crawlers."
- Allow users at least Edit access to the folders in the Knowledge Directory to which you want them to be able to upload document records.
- Configure portlets that users can add to their My Pages. For details, see Chapter 8, "Extending Portal Services with Portlets."
- Create communities that users can add to their My Communities list. For details, see Chapter 9, "Providing Content and Services to Users through Communities."
- Run a Search Update job to index these documents so that they can be discovered with the search. For details, see Section 10.4, "About the Search Update Job."

7.1.1 Permissions Required for Accessing, Crawling, and Submitting Documents

There are several kinds of permissions a user must view, submit, or crawl documents.

Action	Permissions Needed
Access documents imported into the portal	■ Read access to the document link in the Knowledge Directory ■ Read access to the Knowledge Directory folder in which the link is stored ■ Read access to the content source used to import the document ■ If the document is not gatewayed, access to the document in the source repository
Crawl documents into the portal	■ Edit access to the Knowledge Directory folder into which they are crawling documents ■ Edit access to the administrative folder in which they are creating the content crawler ■ Select access to the content source ■ Access Administration activity right ■ Create Content Crawlers activity right ■ Select access to a job that can run the content crawler or Create Jobs activity right plus Edit access to an administrative folder that is registered to an Automation Service

Action	Permissions Needed
Submit a document into the portal	■ Edit access to the Knowledge Directory folder into which they are submitting a document ■ Select access to a content source that supports document submission ■ If the associated content Web service does not support browsing, knowledge of the path to the document

Note: If you have content sources that access sensitive information, be aware that users that have access to the content source and have the additional permissions listed in the table could access anything that the user that the content source impersonates can access. For this reason, you might want to create multiple content sources that access the same repository but that use different authentication information and for which you allow different users access.

7.2 About the Portal Knowledge Directory

The Knowledge Directory is similar to a file system tree in that documents are organized in folders and subfolders. A folder can contain documents uploaded by users or imported by content crawlers, as well as links to people, portlets, and communities. If your administrator has given you permission, you might also be allowed to add documents to the Knowledge Directory, or submit yourself as an expert on a particular topic.

The default portal installation includes a Knowledge Directory root folder with one subfolder named Unclassified Documents. Before you create additional subfolders, define a taxonomy, as described in the *Oracle Fusion Middleware Deployment Guide for Oracle WebCenter Interaction*. For example, you probably want to organize the Knowledge Directory in a way that enables you to easily delegate administrative responsibility for the content and facilitate managed access with access control lists (ACLs).

After you have opened a Directory folder, you see additional features: documents, document display options, subfolders, and related objects.

7.2.1 Documents

On the left, you see the documents to which you have at least Read access. Each document includes an icon to signify what type of document it is (for example: Web page, PDF, MS Word document), the document name, the document description, when the document was last modified, a link to view additional document properties, and a link that displays the URL to this document (enabling you to e-mail a link to the document). At the bottom of the list of documents, you see page numbers indicating how many pages of documents exist in this folder.

7.2.2 Document Display Options

At the top of the list of documents, you see lists that let you change how documents are sorted, how many documents are displayed per page, and filter what types of documents are displayed.

7.2.3 Tags

A tag is a keyword that you create and apply to an item or person to describe its function, usefulness, content, or any other characteristic. Tags can include any combination of words, except those that your administrator has defined as restricted. If your administrator has enabled auto-tagging, the system automatically creates and applies tags to items and people.

> **Note:** Tag features are only available if the Tagging Engine has been installed with the portal and you have tag permissions. Tag features are available in Browse mode in the Directory, in search results, and in Tagging Engine portlets.

Following are some reasons why tags are useful:

- Tags help you find what you are looking for.

  If you want to find information on a certain topic—but you do not know the name of the item that contains that information—you can search for tags that describe what you are looking for. Similarly, if you want to find a person who has an area of expertise—but you do not know the name of the person—you can search for tags that describe that area of expertise. When you tag items and people, you are also helping others find what they are looking for.

- Tags save you time.

  When you scan an item's tags, you are more able to quickly determine whether that item is useful to you without going through the trouble of opening it and viewing its contents. Similarly, if you scan a person's tags, you can gain a greater understanding of that person's job function, interests, and areas of expertise without spending the time to communicate with that person. When you tag items and people, you are also helping others save time.

- Tags make use of the "wisdom of the crowd."

  When a large number of people apply tags to the same items and people, the group of people collectively expresses its knowledge about those items and people. Leveraging this collective knowledge helps you perform searches from a more informed perspective.

7.2.4 Subfolders and Related Objects

On the right, you see the subfolders in this folder, and any objects that the folder administrator has specified as related to this folder.

> **Note:** You see only those folders and objects to which you have at least Read access.

- Under **Subfolders**, you see the subfolders in this folder.
- Under **Related Communities**, you see communities that have information related to the documents in this folder.
- Under **Related Folders**, you see other Directory folders that have information related to the documents in this folder.
- Under **Related Portlets**, you see portlets that have information or functionality related to the documents in this folder.

- Under **Related Experts**, you see the users that are familiar with the documents in this folder (for example, an expert might have written one of the documents in the folder).
- Under **Related Content Managers**, you see the users that manage the documents in this folder and the content sources and content crawlers associated with this folder.

7.2.5 The Unclassified Documents Folder

The Unclassified Documents folder stores documents that were crawled in, but did not sort into any of the folders selected in the content crawler. If a document cannot be placed in any target folders or subfolders, the content crawler might place the document in the Unclassified Documents folder. This is determined by a setting on the Advanced Settings page of the Content Crawler Editor. If you have the correct permissions, you can view the Unclassified Documents folder when you are editing the Directory or by clicking **Administration**, then, in the Select Utility list, selecting **Access Unclassified Documents**.

7.3 Working in the Portal Knowledge Directory

This section describes the following main tasks:

- Section 7.3.1, "Setting Knowledge Directory Preferences"
- Section 7.3.2, "Browsing the Directory"
- Section 7.3.3, "Creating a Directory Folder"
- Section 7.3.4, "Editing a Directory Folder"
- Section 7.3.7, "Deleting Folders and Documents"
- Section 7.3.5, "Submitting Content to the Directory"
- Section 7.3.8, "Sending a Link to a Document"
- Section 7.3.9, "Working with Tags"
- Section 7.3.10, "Moving Folders and Documents"
- Section 7.3.11, "Copying Folders and Documents"
- Section 7.3.12, "Modifying Security on Folders and Documents"
- Section 7.3.13, "Requesting Migration for Folders and Documents"
- Section 7.3.14, "Troubleshooting Security Changes to Folders and Documents"

It also covers the following low-level tasks:

- Section 7.3.15, "Specifying How Folder Contents Are Sorted"
- Section 7.3.16, "Specifying How Content Is Sorted Into a Folder"
- Section 7.3.17, "Adding Filters to a Folder"
- Section 7.3.18, "Adding Related Resources to a Folder"
- Section 7.3.19, "Specifying a Default Content Source for a Folder"
- Section 7.3.20, "Adding or Editing Properties for a Document"
- Section 7.3.21, "Specifying Expiration Settings for a Document"
- Section 7.3.22, "Specifying Refresh Settings for a Document"

7.3.1 Setting Knowledge Directory Preferences

You can specify how the Knowledge Directory displays documents and folders, including whether to generate the display of contents from a Search Service search or a database query, by setting Knowledge Directory preferences.

To access the Knowledge Directory Preferences Utility you must be a member of the Administrators group.

1. Click **Administration**.
2. In the Select Utility list, click **Knowledge Directory Preferences**.
3. In the **Subfolder Description type** list, choose the type of subfolder description to display in the Knowledge Directory:

Option	Description
none	Displays no subfolder description
abbreviated	Displays only the first 100 characters of the folder description
full	Displays the full subfolder description

4. In the **Maximum number of subfolders to display** list, choose the number of subfolders to display under the current folder.
5. In the **Number of subfolder columns** list, choose a number of columns to display subfolders.

Note:

- Documents are always displayed in a single column.
- This setting does not apply in adaptive page layout mode.

6. In the **Number of documents to show per page** box, type a number.
7. In the **Document Description type** list, choose the type of document description to display in the Knowledge Directory:

Option	Description
none	Displays no document description
abbreviated	Displays only the first 100 characters of the document description
full	Displays the full document description

8. In the **Related Resources placement** list, choose the desired placement, relative to folders and documents: **Left**, **Right**, **Top**, or **Bottom**.

Note: Related resources are specified on the Related Resources page of the Folder Editor.

9. In the **Browsing Source** list, choose the source of the folder information that displays when browsing the Knowledge Directory:

Option	Description
Search	Uses the portal Search Service to generate the list of folder contents
Database	Queries the portal database

Note: If you have a large collection of documents, you can improve browsing performance by choosing **Search**.

10. In the **Default Document Submission Content Type** list, choose the default content type, which is used when you submit a document that is not mapped to any content type.

    If you do not want to specify a default, choose **None**.

11. Under Browsing Column Properties, select the properties you want to display as custom columns when browsing documents the Knowledge Directory:

    - To add a property, click **Add Property**, then, in the list that appears, select the desired property.

      Note: Only numeric and date properties can be selected as custom column properties.

    - To delete properties, select the properties you want to delete and click the Delete icon.
    - To change the order in which properties display use the icons to the right of the properties:
      * To move a property to the top of this list, click the Move to Top icon.
      * To move a property up one space in this list, click the Move Up icon.
      * To move a property down one space in this list, click the Move Down icon.
      * To move a property to the bottom of this list, click the Move to Bottom icon.

      The order in which properties appear on this page is the order in which the columns appear in the Knowledge Directory.

7.3.2 Browsing the Directory

When you open the Directory, you see the folders and subfolders to which you have at least Read access.

- To open a folder or subfolder, click its name.

  Note: If the folder includes a description, it appears as a tooltip. To view the description, place your mouse over the folder name.

> **Note:** Beneath the banner, you see the parent hierarchy for the folder you are viewing (sometimes referred to as a breadcrumb trail). To move quickly to one of these folders, click the folder's name.

After you have opened a Directory folder, you see the documents to which you have at least Read access and the following additional features.

- To change the sort order of documents between ascending and descending, in the **Sort by** drop-down list, select the desired option: **Document Name Ascending** or **Document Name Descending**.
- To change the number of documents that are displayed per page, in the **Items per page** drop-down list, select the desired number. By default, 20 items are shown per page.
- To filter the documents by document type (for example, MS Word documents or PDF documents), in the **Show only item type** drop-down list, select the desired document type.
- To open a document, click its name.
- To view the properties of a document, click the **Properties** link under the document description.
- To find objects with a particular tag, under the document description, click the tag. For information about tags, see Section 7.2.3, "Tags."
- To view a related community, under **Related Communities**, click the community name.

> **Note:** If you have at least Select access to the community, you can join the community.

- To open a related folder, under **Related Folders**, click the folder name.
- To preview a related portlet, under **Related Portlets**, click the portlet name.

> **Note:** If you have at least Select access to the portlet, from the portlet preview page, you can add the portlet to one of your My Pages.

- To view the user profile for a related expert, under **Related Experts**, click the user's name.

> **Note:** If you have the Self-Selected Experts activity right, and are not already listed as an expert, click **Add Me** to add yourself as an expert on the folder's topic.

- To view the user profile for a related content manager, under **Related Content Managers**, click the user's name.

At the bottom of the list of documents, you see page numbers indicating how many pages of documents exist in this folder.

- To view another page of items, at the bottom of the list of documents, click a page number or click **Next >>**.

There are other tasks you can perform in edit mode. To enter edit mode, click **Edit Directory**.

- To modify the settings for a folder or document, to the far-right of the folder or document, click the edit icon.

If the folder you are viewing contains documents, you see the following additional features:

- To approve documents, so that they display in the Directory, select the documents and click the approve icon.
- To unapprove documents, so they do not display in the Directory, select the documents and click the unapprove icon.
- To view and modify document settings, click the document settings icon.

7.3.3 Creating a Directory Folder

To create a folder in the Directory you must have the following rights and privileges:

- Edit Knowledge Directory activity right
- Create Knowledge Directory Folders activity right
- At least Edit access to the parent folder (the folder in which you are creating the new folder)

To create a folder in the Directory:

1. Click **Directory**.
2. Click **Edit Directory**.
3. Navigate to the folder in which you want to create a new folder.
4. Click the create folder icon.
5. In the **Create Document Folder** dialog box, type a name and description for the folder, and click **OK**.

You can perform additional tasks when you edit the folder.

7.3.4 Editing a Directory Folder

To edit a Directory folder you must have the following rights and privileges:

- Edit Knowledge Directory activity right
- At least Edit access to the folder

To edit a Directory folder:

1. Click **Directory**.
2. Click **Edit Directory**.
3. Navigate to the folder you want to edit.
4. Click the edit icon to the right of the folder you want to edit.

   To edit the current folder (the open folder), click the edit folder icon (in the folder title bar).

   The Folder Editor opens.
5. On the Main Settings page, perform tasks as necessary:

- Edit the folder name and description.
- Section 7.3.15, "Specifying How Folder Contents Are Sorted"
- Section 7.3.16, "Specifying How Content Is Sorted Into a Folder"
- Section 7.3.17, "Adding Filters to a Folder"

6. On the Related Resources page, perform tasks as necessary:
   - Section 7.3.18, "Adding Related Resources to a Folder"
7. On the Advanced Settings page, perform tasks as necessary:
   - Section 7.3.19, "Specifying a Default Content Source for a Folder"

7.3.5 Submitting Content to the Directory

This section describes the methods for submitting content to the Directory:

- Section 7.3.5.1, "Using Simple Submission to Submit or Upload Documents to the Portal Knowledge Directory"
- Section 7.3.5.2, "Using Advanced Submission to Submit or Upload Documents to the Portal Knowledge Directory"
- Section 7.3.5.3, "Using Advanced Submission to Submit Web Documents to the Portal Knowledge Directory"

You can also import content with content crawlers. For details, see Section 7.10.4, "Content Crawlers."

7.3.5.1 Using Simple Submission to Submit or Upload Documents to the Portal Knowledge Directory

With the proper permissions, you can submit documents to the Knowledge Directory.

Before you submit or upload a document to the Knowledge Directory:

- Ensure that the language of the document you are submitting matches the language specified as your locale on the **Edit Locale Settings** page of **My Account**. For example, if your default locale is Japanese, the document you are submitting must also be in Japanese. If you are submitting a document in a language different from your default locale, either change your default locale to match the language of the document before you submit it, or, if you have permission to edit the Knowledge Directory, you can use Remote Document or Web Document submission to select a different language.

To submit or upload a document to the Knowledge Directory you must have the following rights and privileges:

- At least Edit access to the parent folder (the folder that will store the document)
- At least Select access to the content source that provides access to the location where the document is stored

> **Note:** If you want to use a content type other than the default content type associated with the content source, if you want to submit a document to more than one Knowledge Directory folder, or if you want to submit a document in a language different from your default locale, use Remote Document or Web Document submission, available when editing the Knowledge Directory.

To submit or upload a document to the Knowledge Directory:

1. Click **Directory**.
2. Open the folder in which you want to place the document.
3. Click **Submit Documents**.

   The Submit a Document dialog box opens.

   If you are editing the Knowledge Directory, you open the Submit a Document dialog box by selecting **Simple Submit** in the **Submit Document** list on the right.
4. In the **Document source** list, accept the default document source or select another.

   The document source tells the portal how to find the document you are submitting.

   Note: If you are uploading a file, you must select **Content Upload**.

5. Specify a file by performing one of the following actions:
   - If you are submitting a Web document, in the **URL** text box, type the document's URL.
   - If you are submitting or uploading a file, specify a file by performing one of the following actions:
     - Type the UNC path to the document in the **File path** text box.

       If you are leaving the file in the remote location, you must type a network path (for example, `\\myComputer\myFolder\myFile.txt`). If you are uploading the file, the path can be a local path (for example, `C:\myFolder\myFile.txt`) or a network path.
     - Click **Browse** to navigate to the location of the file you want to submit.

       If you are leaving the file in the remote location, you must supply a network path to the file, and therefore, you cannot browse your local drives; you must browse the network to your computer and then to the location of the file. If you are uploading the file, you can browse to local drives or network drives.

   Note:
   - Depending on how the administrator configured the content source, the **Browse** button might not appear, therefore you might not be able to browse to the file. If you do not see a **Browse** button, type the path in the **File path** text box.
   - If the **Browse** button does display but you cannot browse to the folder where the file you want to submit is located, the content source you chose might not have the necessary privileges to access the file location. Click **Cancel** and resubmit the file using a different content source.

6. If desired, override the default name or description.
   - To override the default name, select **Use this name** and, in the text box, type the name.

- To override the default description, select **Use this description** and, in the text box, type the description.

Once the folder administrator (one who has Admin access to the folder) approves your submission, links to the document you submitted or uploaded appear in the Knowledge Directory.

7.3.5.2 Using Advanced Submission to Submit or Upload Documents to the Portal Knowledge Directory

With the proper permissions, you can use advanced submission to submit documents to the Knowledge Directory. Advanced submission enables you to select a content type other than the default content type associated with the content source, submit a document to more than one Knowledge Directory folder, or submit a document in a language different from your default locale. Depending on your portal configuration, you might also be able to upload a file to the Knowledge Directory. When you upload a file, it is copied from the remote repository into the portal's document repository and a pointer is created to that copied file.

To use advanced submission to submit or upload a document to the Knowledge Directory you must have the following rights and privileges:

- Edit Knowledge Directory activity right
- At least Edit access to the parent folder (the folder that will store the document)
- At least Select access to the content source that provides access to the location where the document is stored

To use advanced submission to submit or upload a document to the Knowledge Directory:

1. Click **Directory**.
2. Click **Edit Directory**.
3. Open the folder in which you want to place the document.
4. In the Submit Document list on the right, select **Remote Document**.

   The Choose a Content Source dialog box opens.
5. Select the content source that provides access to the content you want to submit or upload and click **OK**.

   Note: If you are uploading a file, you must select **Content Upload**.

6. Specify a file by performing one of the following actions:
   - Type the UNC path to the document in the **File path** text box.

     If you are leaving the file in the remote location, you must type a network path (for example, `\\myComputer\myFolder\myFile.txt`). If you are uploading the file, the path can be a local path (for example, `C:\myFolder\myFile.txt`) or a network path.
   - Click **Browse** to navigate to the location of the file you want to submit.

     If you are leaving the file in the remote location, you must supply a network path to the file, and therefore, you cannot browse your local drives; you must browse the network to your computer and then to the location of the file. If you are uploading the file, you can browse to local drives or network drives.

Note:

- Depending on how the administrator configured the content source, the **Browse** button might not appear, therefore you might not be able to browse to the file. If you do not see a **Browse** button, type the path in the **File path** text box.
- If the **Browse** button does display but you cannot browse to the folder where the file you want to submit is located, the content source you chose might not have the necessary privileges to access the file location. Click **Cancel** and resubmit the file using a different content source.

7. If you want to override the default name or description, click the **Name and Description** page and edit the values.
   - To override the default name, edit the value in the **Name** box.
   - To override the default description, edit the value in the **Description** box.

Once the folder administrator (one who has Admin access to the folder) approves your submission, links to the document you submitted or uploaded appear in the Knowledge Directory.

7.3.5.3 Using Advanced Submission to Submit Web Documents to the Portal Knowledge Directory

To use advanced submission to submit a document to the Knowledge Directory you must have the following rights and privileges:

- Edit Knowledge Directory activity right
- At least Edit access to the parent folder (the folder that will store the document)
- At least Select access to the content source that provides access to the location where the document is stored

To use advanced submission to submit a document to the Knowledge Directory:

1. Click **Directory**.
2. Click **Edit Directory**.
3. Open the folder in which you want to place the document.
4. In the Submit Document list on the right, select **Web Document**.

   The Choose a Content Source dialog box opens.
5. Select the content source that provides access to the content you want to submit and click **OK**.

Note: If you are submitting an unsecured Web document, you can select **World Wide Web**.

6. In the **URL** text box, type the document's URL.
7. Under Choose Content Type, select the content type to apply to this document.
   - To use the folder's default content type, leave **Default Content Type** selected.

- To choose a different content type, select **This content type**, click **Change**, in the dialog box, select the content type you want to use, and click **OK**.

8. Under Choose Knowledge Directory Folders, specify into which folders you want to submit this document.
   - To add a folder, click **Add Folder**.
   - To remove folders, select the folders you want to delete and click the Remove icon.
   - To change the order of the names in the list from ascending to descending alphabetical order (or vice versa), click **Folder Names**.
9. Under Document Content Language, choose the language used for the majority of the document's content.

   The language you choose is the language by which the document is indexed. The search engine uses the language when searching.
10. If you want to override the default name or description, click the **Name and Description** page and edit the values.
    - To override the default name, edit the value in the **Name** box.
    - To override the default description, edit the value in the **Description** box.

Once the folder administrator (one who has Admin access to the folder) approves your submission, links to the document you submitted or uploaded appear in the Knowledge Directory.

7.3.6 Editing the Settings for a Document

To edit the settings for a document you must have the following rights and privileges:

- Edit Knowledge Directory activity right
- At least Edit access to the document

To edit the settings for a document:

1. Click **Directory**.
2. Click **Edit Directory**.
3. Navigate to the document you want to edit.
4. Click the edit icon to the right of the document you want to edit.

   The Document Editor opens.
5. On the Main Settings page, perform tasks as necessary:
   - Edit the name and description for the document.
   - Section 7.3.20, "Adding or Editing Properties for a Document"
6. On the Document Settings page, perform tasks as necessary:
   - Section 7.3.21, "Specifying Expiration Settings for a Document"
   - Section 7.3.22, "Specifying Refresh Settings for a Document"
7. On the Security page, perform tasks as necessary:
   - Section 5.17, "Setting Security on an Object"

   The default security for this document is based on the security of the parent folder.

8. On the Migration History and Status page, perform tasks as necessary:
   - Section 5.18, "Viewing Migration History and Status for an Object"

7.3.7 Deleting Folders and Documents

To delete Directory content you must have the following rights and privileges:

- Edit Knowledge Directory activity right
- Admin access to the Directory content you want to delete

To delete Directory content:

1. Click **Directory**.
2. Click **Edit Directory**.
3. Navigate to the content you want to delete.
4. Select the folders and/or documents you want to delete and click the delete icon.

7.3.8 Sending a Link to a Document

To send a link to a document in the Directory:

1. Click **Directory**.
2. Navigate to the document.
3. Under the document description, click **Send Document Link**.
4. In the **Document Link** dialog box, copy the text, then click **Close**.
5. In your e-mail application, paste the text into an e-mail message and send it.

   When other portal users click the URL in your e-mail, the document opens. If a user does not have permission to see the document, an error message is displayed.

7.3.9 Working with Tags

- To add a tag to a document:
  1. Under the document description, click **Add Tag**.
  2. In the text box, type the tag you want to apply to the document. To add more than one tag, separate tags with commas (,).
  3. To save your tag, click outside of the text box or press ENTER.
- To rename a tag you added to a document:
  1. Under the document description, place your cursor over the tag icon and click **Rename Tag**.
  2. In the text box, edit the tag.
  3. To save your changes, click outside of the text box or press ENTER.

  Note: You cannot rename a tag that you did not add. Tags you did not add have a read-only tag icon.

- To delete a tag you added to a document, place your cursor over the tag icon, click **Delete Tag**, then click **OK** in the confirmation dialog box.

Note: You cannot delete a tag that you did not add. Tags you did not add have a read-only tag icon. If you are an administrator, you can delete tags created by other users through the Tagging Engine Administration utility (accessed by clicking **Administration**, then, in the Select Utility menu, clicking **Tagging Engine Administration**).

7.3.10 Moving Folders and Documents

To move Directory content you must have the following rights and privileges:

- Edit Knowledge Directory activity right
- At least Edit access to the target folder (the folder to which you are moving the content)
- At least Edit access to the content you want to move

To move Directory content:

1. Click **Directory**.
2. Click **Edit Directory**.
3. Navigate to the content you want to move.
4. Select the folders and/or documents you want to move and click the move icon.
5. In the Choose Target Folder dialog box, expand the folders as necessary, choose a folder, and click **OK** to move the content.

7.3.11 Copying Folders and Documents

To copy Directory content you must have the following rights and privileges:

- Edit Knowledge Directory activity right
- At least Edit access to the target folder (the folder to which you are copying the content)
- At least Edit access to the content you want to copy

To copy Directory content:

1. Click **Directory**.
2. Click **Edit Directory**.
3. Navigate to the content you want to copy.
4. Select the folders and/or documents you want to copy and click the copy icon.
5. In the Choose Target Folder dialog box, expand the folders as necessary, choose a folder, and click **OK** to copy the content.

7.3.12 Modifying Security on Folders and Documents

To modify security on Directory content you must have the following rights and privileges:

- Edit Knowledge Directory activity right
- At least Edit access to the content for which you want to modify security

To modify security on Directory content:

1. Click **Directory**.
2. Click **Edit Directory**.
3. Navigate to the content for which you want to modify security.
4. Select the folders and/or documents and click the security icon.
5. In the Edit Security dialog box, perform the following actions:
   - To allow more users or groups access to the folders or documents, click **Add Users/Groups**.
   - To specify the type of access a user or group has, to the right of the user or group, select the proper access from the drop-down list under the name of the folder or document.

     For a description of the available privileges, see Section 2.5.1, "About Access Controls Lists and Access Privileges."

     Note: If a user is a member of more than one group included in the list, or if they are included as an individual user and as part of a group, that user gets the highest access available to her for this folder or document. For example, if a user is part of the Everyone group (which has Read access) and the Administrators Group (which has Admin access), that user gets the higher privilege to the community: Admin.
   - To cancel your changes and reset the security to what it was, click **Reset**.
   - To delete a user or group from the security of all selected folders or documents, select the user or group and click the remove icon.
   - To see which users are included in a group, click the group name.
   - To set identical access rights to a folder or document for every user or group, repeatedly click the column icon in the Set Column area at the bottom of the desired column until the desired access level displays in the lists.
   - To set identical access rights to every folder or document for a user or group, repeatedly click the row icon in the Set Row area at the right of the desired user or group until the desired access level displays in the lists.

7.3.13 Requesting Migration for Folders and Documents

To request migration of Directory content you must have the following rights and privileges:

- Edit Knowledge Directory activity right
- At least Select access to the content for which you want to request migration

To request migration of Directory content:

1. Click **Directory**.
2. Click **Edit Directory**.
3. Navigate to the content for which you want to request migration.
4. Select the folders and/or documents and click the migration icon.

5. In the Script Prompt dialog box, type a comment about why you need this content migrated and click **OK**.

7.3.14 Troubleshooting Security Changes to Folders and Documents

If you get a time-out error when applying a security change to all child objects in a Knowledge Directory hierarchy, you can use the following workaround.

This issue is most likely caused by trying to apply changes too many levels of nested subfolders with a large number of child objects (other folders or documents). In this situation, you can perform the following steps to work around the issue:

1. To find out which folders are updated with the security changes, select all first level subfolders then select the security icon.
2. Scroll through the list to see at which folder the security changes stopped being applied.
3. Work with the remaining folders and apply the needed security changes: open each first level folder separately, set the security, save, and select **Yes** to apply the security changes to all the child objects for that folder.
4. Repeat this process for all remaining first level subfolders that did not get the security applied to them successfully due to the error.

7.3.15 Specifying How Folder Contents Are Sorted

1. If the Folder Editor is not already open, open it now.
2. Under Sorting, specify how folder contents are sorted:
   a. In the Order this way when browsing list, choose the property by which you want folder contents sorted in Browse Mode. Only numeric, date, and name properties are displayed in the list.
   b. In the Order this way when editing list, choose the fixed property by which you want folder contents sorted in Edit Mode.

7.3.16 Specifying How Content Is Sorted Into a Folder

You can edit the way content is sorted into this folder by crawlers or the Smart-Sort Editors.

1. If the Folder Editor is not already open, open it now.
2. Under When sorting, allow into this folder, choose the criteria that links must meet to be imported into the folder:
   - **All links**: All links can sort into this folder.
   - **No links**: No links are sorted into this folder or its subfolders, but you can still add links manually.
   - **Links that pass**: Choose whether links must pass all filters or at least one filter to sort into this folder. You can manually add links that do not pass the filters.
3. Under Default folder, choose the folder in which to put links that cannot be sorted into this folder or any of its subfolders.

   If you choose **No folder**, content that cannot be sorted into this folder or any of its subfolders is not sorted into any folder in this branch. However, a crawler might still place this content into another branch or in the Unclassified Documents folder.

7.3.17 Adding Filters to a Folder

> **Note:** Filters in this section are disregarded if you chose **All links** or **No links** under Filter Settings.

1. If the Folder Editor is not already open, open it now.
2. In Filters, specify the filters that links must pass to sort into this folder:
   - To add a filter, click **Add Filter**, select filters, and click **OK**.
   - To create a filter, click **Create Filter**.
   - To remove filters, select the filters you want to remove and click the remove icon.
   - To toggle the names in the list between ascending and descending alphabetical order, click **Filter Names**.

For information on filters, see Section 7.6, "About Filters."

7.3.18 Adding Related Resources to a Folder

Related resources enable you to associate communities, other folders, portlets, experts, and content managers with a folder. The folder's associated objects display in Browse Mode when enabled in the user's experience definition.

1. If the Folder Editor is not already open, open it now.
2. On the left, under General Settings, click **Related Resources**.
3. Add related resources as necessary:
   - To add related communities, under Communities, click **Add Community**, select communities, and click **OK**.
   - To add related folders, under Folders, click **Add Folder**, select folders, and click **OK**.
   - To add related portlets, under Portlets, click **Add Portlet**, select portlets, and click **OK**.
   - To add related experts (users who are knowledgeable about the contents of the folder), under Experts, click **Add Expert**, select users, and click **OK**.
   - To add related content managers (users who are responsible for managing the content in the folder), under Content Managers, click **Add Content Managers**, select users, and click **OK**.

7.3.19 Specifying a Default Content Source for a Folder

You can specify the default content source for documents submitted to a folder. When a user submits a document, the content source you choose is selected by default. However, users can change the content source to any content source to which they have at least Select access.

> **Note:** If no default content source has been set for the folder to which a user wants to submit a document, the portal searches recursively up through the folder hierarchy until it locates a folder for which a default content source has been set, and uses that content source as the default.

1. If the Folder Editor is not already open, open it now.
2. On the left, under General Settings, click **Advanced Settings**.
3. Under Default Content Source, select the default content source for documents submitted to the folder:
   - To use the same default content source as the folder's parent folder uses, click **Parent folder's content source**. The parent folder's default content source is displayed in parentheses next to this option.

     > **Note:** Because the root folder does not have a parent folder, the Parent folder's content source option does not display if you are editing the root folder.

   - To select another content source, click **This content source**, and select a content source from the list.

7.3.20 Adding or Editing Properties for a Document

Document properties are metadata about the document that the search engine uses to index the document, similar to a library card catalog.

1. If the Document Editor is not already open, open it now.
2. Under Customized Document Properties, modify properties for the selected document:
   - To add a property, click **Add Property**. This adds a property to the bottom of the list. Select the property you want from the drop-down list and enter a value.
   - To create a property, click **Create Property**. To learn about creating properties, see Chapter 7.5.1, "Creating or Editing a Property."
   - To remove properties, select the properties you want to remove and click the remove icon.
   - To change a property value, modify the property's Value column.
   - To toggle the properties in the list between ascending and descending alphabetical order, click **Property**.

7.3.21 Specifying Expiration Settings for a Document

You might want to set a document to expire if the document will become irrelevant at some point.

These settings are referenced by the Document Refresh Agent when the Document Refresh job runs.

1. If the Document Editor is not already open, open it now.

2. Click the **Document Settings** page.
3. Under Document Expiration, choose whether the link to the document should expire:
   - If you do not want the document link to expire, select **Never expire**.

     Note: If you set a document to be refreshed and to be deleted if the source document is not found, even a document set to never expire can be deleted.

   - If you want the document link to expire, chose **Delete on**, and type a date in the box or click the date picker icon to choose a date.

     When the Document Refresh job runs, it will delete any document links that have reached the expiration date.

7.3.22 Specifying Refresh Settings for a Document

You can have the Document Refresh Agent periodically update the document and its properties. When a link is refreshed, the Document Refresh Agent verifies whether the source document still exists. If the document exists, the Document Refresh Agent updates the associated property values from the source document. If the document does not exist, the Document Refresh Agent applies the settings you specify for dealing with broken links.

These settings are referenced by the Document Refresh Agent when the Document Refresh job runs.

1. If the Document Editor is not already open, open it now.
2. Click the **Document Settings** page.
3. Under Link and Property Refresh, specify the refresh settings that should be used by the Document Refresh Agent:
   - If you do not want to refresh the document, select **Never**.
   - If you want to refresh the document, select **Every**, and type a number in the box and choose an interval from the list.
   - To prevent the Document Refresh Agent from refreshing document properties, select **Only confirm the validity of the links to these documents**.
4. Under Broken Links, specify what happens to links to the document if the Document Refresh Agent finds that the source document does not exist:
   - If you want to leave the broken link in the portal, select **Left alone**.
   - If you want to remove the broken link from the portal immediately, select **Deleted immediately**.
   - If you want to leave the broken link for a specified amount of time, select **Deleted after**, and type a number in the box and choose an interval from the list.

     You might want to leave a broken link in the portal for a short while in case the source document repository is temporarily inaccessible.

7.4 About Document and Object Properties

Properties provide information about, as well as a way to search for, documents and objects in your portal. For example, you might want to create an Author property so users can find all the documents or objects created by a particular user.

When you add documents to the portal, the portal maps source document fields to portal properties according to mappings you specify in the Global Content Type Map, the particular content type definition, the Global Document Property Map, and any content crawler-specific content type mappings.

7.4.1 Global Document Property Map

The Global Document Property Map provides default mappings for properties common to the documents in your portal. When users import documents into the portal (either manually or through a content crawler), property values can be extracted from the source documents according to the property mappings you specify in the associated content types and the property mappings from the Global Document Property Map.

When a user imports a document into the portal, the portal performs the following actions:

1. The portal determines which content type to use, based on the Global Content Type Map or the content crawler's content type settings.
2. The portal populates property values based on the property mappings in the content type.
3. If there are additional mapped properties in the Global Content Type Map (not included in the content type's property mappings), the portal populates the property values, based on those property mappings.

Therefore, you can map common properties in the Global Document Property Map and specify only special mappings, default values, and override values in content types.

Note: Some property mappings are set when the portal is installed so that the portal can produce some general metadata even if you do not create any specialized mappings.

7.4.2 Global Object Property Map

The Global Object Property Map displays all the types of portal objects with which you can associate properties. When users create a portal object, they can specify values for the associated properties on the Properties and Names page of the object's editor.

7.4.3 User Information - Property Map

The User Information — Property Map enables you to map user information to user properties in the portal. The information in these user properties can then be displayed in the user's profile, or it can be sent to content crawlers, remote portlets, or federated searches so that users do not have to enter this information on a separate preference page.

7.5 Working with Properties

This section describes how to perform the following tasks:

- Section 7.5.1, "Creating or Editing a Property"
- Section 7.5.2, "Mapping Source Document Attributes to Portal Properties Using the Global Document Property Map"
- Section 7.5.3, "Associating Properties with Portal Objects Using the Global Object Property Map"
- Section 7.5.4, "Associating User Information with Properties Using the User Information — Property Map"

7.5.1 Creating or Editing a Property

To create a property you must have the following rights and privileges:

- Access Administration activity right
- Create Properties activity right
- At least Edit access to the parent folder (the folder that will store the property)

To edit a property you must have the following rights and privileges:

- Access Administration activity right
- At least Edit access to the property

To create or edit a property:

1. Click **Administration**.
2. Open the Property Editor.
   - To create a property, open the folder in which you want to store the property. In the Create Object list, click **Property**.
   - To edit a property, open the folder in which the property is stored and click the property name.
3. In the Property Type list, choose what kind of information this property stores.
   - **Textual** stores text values.
   - **Simple Number** stores whole numbers.
   - **Floating Point Number** stores numbers that include decimal points.
   - **Date** stores date values.
   - **Reference** stores a reference to an administrative object in the portal.

     After choosing this option, in the second list, choose what type of administrative object this property references.
   - **Encrypted Text** stores encrypted text values.

   Note: After you save this property, the property type cannot be changed.
4. If this property stores a Web address, select **Treat this property like an URL**.

If you choose this option, users can click-through the property, so the values for this property must always be URLs.

Note: This option is only available for textual properties.

5. If this property applies to documents imported into the portal, select **This property is supported for use with documents**.

   Note: This option is not available for reference properties.

6. If this property is generated automatically and you want to store the value in the database but not display it on the Properties and Names page of object editors, clear the **This Property is visible in the UI** check box.
7. If you do not want users to be able to edit the values for this property, select **Read Only**.
8. If you want users to be able to search for objects based on the values for this property, select **Searchable**.

   For example, if you specify that the Author property is searchable, users can search for all the objects created by a particular person.
9. If you want to require that users specify a value for this property before they can save the associated object, select **Make this property mandatory**.

   Note: This option is not available if this property is set to Read Only.

10. If you want to allow users to specify more than one value for this property, select **Multiple values can be selected for this Property**.
11. In the Property Chooser Type list, specify what format should be used for value selection.
    - **None** displays a text box in which users can type property values.
    - **Managed Dropdown** displays a list of values you specify from which users can choose.
      - To create the values users can choose from, click **Add Value** and type a value in the text box.
      - To remove a value, select the value and click the Remove icon.

        To select or clear all value check boxes, select or clear the box to the left of **Value Names**.
    - **Unmanaged Dropdown** displays a list populated with the values from a database table from which users can choose.
      a. In the **Database Table Name** box, type the name of the table from which you want to populate your list.
      b. In the **Pick Column** box, specify the column from which you want to populate the list.
      c. In the **Sort Column** box, type the name of the column upon which the values are sorted.

- **Tree** displays a hierarchical list populated with the values from a database table from which users can choose.
  a. In the **Database Table Name** box, type the name of the table from which you want to populate the list.
  b. In the **Pick Column** box, specify the column from which you want to populate the list.
  c. In the **Sort Column** box, type the name of the column upon which the values are sorted.
  – To add a column, click **Add Value** and enter the **Pick Column** and **Sort Column** values.
  – To remove a column, select it and click the Remove icon.
  – To select or clear all the column check boxes, select or clear the box to the left of **Pick Column**.

  Note: This option is not available for date or reference properties.

12. On the Names and Descriptions page, perform tasks as necessary:
    - Section 5.15, "Naming and Describing an Object"

    You can instead enter a name and description when you save this property.
13. On the Security page, perform tasks as necessary:
    - Section 5.17, "Setting Security on an Object"

    The default security for this property is based on the security of the parent folder.
14. If you are editing a property, on the Migration History and Status page, perform tasks as necessary:
    - Section 7.16, "Working with Snapshot Queries"

    Note: The Migration History and Status page is not available when creating an object.

If you set this property to be searchable, you must rebuild the search index.

7.5.2 Mapping Source Document Attributes to Portal Properties Using the Global Document Property Map

To access the Global Document Property Map you must be a member of the Administrators Group.

To map source document attributes to portal properties:

1. Click **Administration**.
2. In the Select Utility list, choose **Global Document Property Map**.
3. Create mappings between portal properties and document attributes.

Note: Some property mappings are set when the portal is installed so that content crawlers can produce some general metadata even if you do not create any specialized mappings.

- To add a property mapping, click **Add Property**; then, in the Add Property dialog box, select the properties you want to add and click **OK**.
- To associate an attribute, click the property name and, in the text box, type the associated attributes, separated by commas (,).

  The first attribute with a value populates the property.
- To delete a mapping, select the mapping and click the Delete icon.

  To select or clear all of the mapping check boxes, select or clear the box to the left of **Property Name**.
- To toggle the order in which the properties are sorted, click **Property Name**.

Note: You can map any attribute from the source document. For information on source document attributes, refer to the documentation for the third-party software.

7.5.2.1 HTML Metadata Handling

Generally, you will be able to determine what source document attributes can be mapped to portal properties, but it might not be as clear in HTML documents.

This table shows the names of the attributes that are returned by the HTML accessor. You can map the attribute names to portal properties.

Note: The HTML Accessor handles all common character sets used on the web, including UTF-8.

HTML Metadata	Name of Attribute Returned by HTML Accessor	Default Mapping or Mapping Suggestion
<TITLE> Tag	Title	Title (default)
<META> Tag	The attribute name is the NAME value. Example: `<META NAME="creation_date" CONTENT="18-Jan-2004">` The attribute that would be extracted from the example would be named “creation_date”	Using the example, you could map creation_date to the Created property.

HTML Metadata	Name of Attribute Returned by HTML Accessor	Default Mapping or Mapping Suggestion

Headline Tags	The attribute name is the name of the tag followed by an ordinal, one-based index in parentheses.
	The Accessor returns a value for each headline tag (<H1>, <H2>, <H3>, <H4>, <H5>, and <H6>) and each bold tag (<B>).
	Example:
	`<H1>Value 1</H1>`
	`<H3>Value 2</H3>`
	`<H1>Value 3</H1>`
	`<B>Value 4</B>`
	The HTML Accessor returns the following source document attribute-value pairs:
	`<h1>(1) Value 1`
	`<h3>(1) Value 2`
	`<h1>(2) Value 3`
	`<B>(1) Value 4`
		If on a particular news site, the second <H2> tag contains the name of the article and the third <B> tag contains the name of the author, you could map the portal property Title to <H2>(2) and the portal property Author to <B>(3).

HTML Comments	It is common practice to store metadata in HTML comments using the following format:
	`<!-- Writer: jm -->`
	`<!-- AP: md -->`
	`<!-- Copy editor: mr -->`
	`<!-- Web editor: ad -->`
	In other words, the format is the HTML comment delimiter followed by the name, a colon, the value, and a close comment delimiter. The HTML Accessor parses data in this format and returns the following source document attribute-value pairs:
	`Writer jm`
	`AP md`
	`Copy editor mr`
	`Web editor ad`
		Using the example, you could map Writer to the portal property Author.

Parent URL	Documents imported through a Web content crawl return an attribute named Parent URL with the value of the URL of the parent page that contains a link to the document.	URL (default)

HTML Metadata	Name of Attribute Returned by HTML Accessor	Default Mapping or Mapping Suggestion
Anchors	The HTML Accessor provides special handling for internal anchors (<a name="target">) and URLs that reference them (http://server/page#target).	You might map anchors to portal attributes in the following ways: ■ Alternate Sources for the portal Title attribute When the document URL for an HTML document contains a fragment identifier (for example, #target in the example above) and the Accessor finds that anchor in the document, it discards all title and headline tags preceding the anchor and returns, as the suggested document title, the first subsequent headline tag. All subsequent tags are indexed relative to the anchor tag, so mapping a property to <H1>(2) means "use the second <H1> tag after the anchor tag named in the document URL." ■ Mapping Anchor Section to Document Description or Summary The HTML Accessor returns an attribute named Anchor Section containing text immediately following the named anchor tag (stripped of markup tags and HTML decoded). Mapping this property to the document description allows the portal to generate a relevant description for each section of a large document. The HTML Accessor generates its own summary by returning the first summary-sized chunk of text in the document stripped of HTML markup tags and correctly HTML decoded. It returns this summary as an attribute named Summary. The Accessor executes the DocumentSummary method, which returns the value of the Anchor Section attribute, if available. If this attribute is not available, its second choice is the value of the Description attribute from the <META NAME="description"> tag. If this is not available, its third and final choice is the Summary attribute.

7.5.3 Associating Properties with Portal Objects Using the Global Object Property Map

To access the Global Object Property Map you must be a member of the Administrators group.

1. Click **Administration**.
2. In the Select Utility list, click **Global Object Property Map**.
3. To associate properties, click the Edit icon; then, in the Choose Property dialog box, select the properties you want to associate with the object, and click **OK**.

   To toggle the order in which the objects are sorted, click **Objects**.

7.5.4 Associating User Information with Properties Using the User Information — Property Map

To map user information to portal properties you must have the following rights and privileges:

- Access Administration activity right
- Access Utilities activity right
- At least Select access to the properties you want to map

> **Note:** The Full Name attribute is automatically mapped to display name of the user unless you override it on this page.

1. Click **Administration**.
2. In the Select Utility list, click **User Profile Manager**.
3. Under Edit Object Settings, click **User Information - Property Map**.
4. Add a property. Click **Add**; then, in the **Choose Property** dialog box, select the property you want to add and click **OK**.
5. Map attributes to the property:
   a. Click the Edit icon next to the property name.
   b. In the text box, type the attribute.

      To map the property to multiple attributes, separate the attribute names with commas (,).
6. Repeat Steps 4 and 5 to map additional properties.

   To remove properties, select the property you want to remove and click the Remove icon.

After mapping user information to portal properties, you must import the user information through profile sources or have users manually enter the information by editing their user profiles.

7.6 About Filters

Filters control what content goes into which folder when crawling in documents or using Smart Sort to filter content into new folders. A filter sets conditions that document links must pass to be sorted into associated folders in the Knowledge Directory.

A filter is a combination of a basic fields search and statements. The basic fields search operates on the name, description, and content of documents. Statements can operate on the basic fields or any other additional document properties. Statements define what must or must not be true to allow the document to pass the filter. The statements are collected together in groupings. The grouping defines whether the statements are evaluated with an AND operator (all statements are true) or an OR operator (any statement is true). If some statements should be evaluated with an AND operator and some should be evaluated with an OR operator, you can create separate groupings for the statements. You can also create subgroupings or nested groupings, where one grouping is contained within another grouping. The statements in the lowest-level grouping are evaluated first to define a set of results. Then the statements in the next highest grouping are applied to that set of results to further filter the results. The filtering continues up the levels of groupings until all the groupings of statements are evaluated.

7.7 Working with Filters

This section describes the following tasks:

- Section 7.7.1, "Creating or Editing a Filter"
- Section 7.7.2, "Deleting a Filter"
- Section 7.7.3, "Defining Filter Conditions"
- Section 7.7.4, "Testing Filters"
- Section 7.7.5, "Applying a Filter to a Folder"

7.7.1 Creating or Editing a Filter

To create a filter you must have the following rights and privileges:

- Access Administration activity right
- Create Filters activity right
- At least Edit access to the parent folder (the folder that will store the filter)

To edit a filter you must have the following rights and privileges:

- Access Administration activity right
- At least Edit access to the filter

To create or edit a filter:

1. Click **Administration**.
2. Open the Filter Editor.
   - To create a filter, open the folder in which you want to store the filter. In the Create Object list, click **Filter**.
   - To edit a filter, open the folder in which the filter is stored and click the filter name.
3. On the Main Settings page, perform tasks as necessary:
   - Section 7.7.3, "Defining Filter Conditions"
4. On the Properties and Names page, perform tasks as necessary:
   - Section 5.15, "Naming and Describing an Object"

You can instead enter a name and description when you save this filter.

- Section 5.16, "Managing Object Properties"

Add the filter to folders.

7.7.2 Deleting a Filter

To delete a filter you must have the following rights and privileges:

- Access Administration activity right
- Admin access to the filter

To delete a filter:

1. Click **Administration**.
2. Navigate to the filter.
3. Select the filter you want to delete and click the delete icon.

7.7.3 Defining Filter Conditions

A filter is a combination of a basic fields search and statements. The basic fields search operates on the name, description, and content of documents. Statements can operate on the basic fields or any other additional document properties. Statements define what must or must not be true to allow the document to pass the filter. The statements are collected together in groupings. The grouping defines whether the statements are evaluated with an AND operator (all statements are true) or an OR operator (any statement is true). If some statements should be evaluated with an AND operator and some should be evaluated with an OR operator, you can create separate groupings for the statements. You can also create subgroupings or nested groupings, where one grouping is contained within another grouping. The statements in the lowest-level grouping are evaluated first to define a set of results. Then the statements in the next highest grouping are applied to that set of results to further filter the results. The filtering continues up the levels of groupings until all the groupings of statements are evaluated.

A filter needs at least a basic fields search or a statement.

1. If the Filter Editor is not already open, open it now.
2. To search the name, description, and content values, type the text you want to search for in the **Basic fields search** text box.

   You can use the text search rules described in Section F.3, "Using Text Search Rules."
3. Select the operator for the grouping of statements you are about to create:
   - If a document should pass the filter only when all statements in the grouping are true, select **AND**.
   - If a document should pass the filter when any statement in grouping is true, select **OR**.

   Note: The operator you select for a grouping applies to all its statements and subgroupings directly under it.
4. Define each statement in the grouping:

a. Click **Add Statement**.

b. In the first list, select the searchable property for which you want to filter the values.

c. In the second list, select the operator to apply to this condition.

   This list will vary depending on the property selected:

   – For any text property, you can search for a value that contains your search string, or you can search for properties that have never had a value (**Contains No Value**).

   Note: If the property contained a value at some point, but the value has been deleted, the property will not match the Contains No Value condition.

   – For any date property, you can search for a value that comes after, comes before, is, or is not the date and time you enter in the boxes. You can also search for a value within the last number of minutes, hours, days, or weeks that you enter in the box.

   – For any number property, you can search for a value that is greater than, is less than, is, is not, is greater than or equal to, or is less than or equal to the number you enter in the text box.

d. In the box (or boxes), specify the value the property must meet.

   Note: If you are searching for a text property, you can use the text search rules described in Section F.3, "Using Text Search Rules."

   To remove the last statement in a grouping, select the grouping, and click **Remove Statement**.

5. If necessary, add more statements by repeating Step 4.

6. If necessary, add more groupings:

   - To add another grouping, select the grouping to which you want to add a subgrouping, click **Add Grouping**, then define the statements for that grouping (as described in Step 4).

     Note: You cannot add a grouping at the same level as **Grouping 1**.

   - To remove a grouping, select the grouping, and click **Remove Grouping**.

     Note:

     - Any groupings and statements in that grouping will also be removed.
     - You cannot remove **Grouping 1**.

7. To verify that the filter works, click **Test Filter**.

   The results of the test appear under **Filter Test Report**.

You might want to test your filters before you use them extensively. See Section 7.7.4, "Testing Filters."

7.7.4 Testing Filters

You might want to test your filters before you use them extensively.

- To test filters, crawl content into a test folder; then perform one of the following tests:
  - Run an advanced search on the folder using the same criteria you used for your filter.

    If your advanced search returns the content you expected, you can apply the filter to the appropriate folder, confident that the filter will allow the proper documents into the folder.
  - Add the filters to subfolders and perform a smart sort to sort the content into the subfolders according to the filters.

    If the subfolders contain the content you expected, the filters work correctly.

7.7.5 Applying a Filter to a Folder

After you create a filter, you assign it to folders to control what content goes into the folder when crawling in documents or using Smart Sort to filter content into new folders.

Note: When users submit documents, the filters do not apply.

1. Click **Directory**.
2. Click **Edit Directory**.
3. Open the Folder Editor for the folder to which you want to apply a filter.
   - To edit the root folder (or folder you are in), in the action toolbar in the upper-right of the Edit Directory page, click the Edit Folder icon.
   - To edit a subfolder, click the Edit icon to the right of the folder name.
4. Under Filter Settings, select **Links that pass** and choose whether documents must pass all filters or at least one filter to sort into this folder.
5. Under Filters, specify the filters that documents must pass to sort into this folder.
   - To add a filter, click **Add Filter**, select filters, and click **OK**.
   - To create a filter, click **Create Filter**.
   - To remove filters, select the filters you want to remove and click the Remove icon.
   - To toggle the names in the list between ascending and descending alphabetical order, click **Filter Names**.

7.8 About Content Types

Content types specify several options — the source content format (such as Microsoft Office, Web page, or Lotus Notes document), whether the text of the content should be indexed for searching, and how to populate values for document properties. You

should create a separate content type for each unique combination of these options. For example, if departments use different Microsoft Word attributes for document descriptions, you might have to create one content type that pulls the description from the Subject attribute and one that pulls it from the Comments attribute.

7.9 Working with Content Types

This section describes the following tasks:

- Section 7.9.1, "Creating or Editing a Content Type"
- Section 7.9.2, "Deleting a Content Type"
- Section 7.9.3, "Mapping Content Types to Imported Content Using the Global Content Type Map"

7.9.1 Creating or Editing a Content Type

You should create a separate content type for each unique combination of these options. For example, if departments use different Microsoft Word attributes for document descriptions, you might have to create one content type that pulls the description from the Subject attribute and one that pulls it from the Comments attribute.

To create a content type you need the following rights and privileges:

- Access Administration activity right
- Create Content Types activity right
- At least Edit access to the parent folder (the folder that will store the content type)

To edit a content type you need the following rights and privileges:

- Access Administration activity right
- At least Edit access to the content type

To create or edit a content type:

1. Click **Administration**.
2. Open the Content Type Editor.
   - To create a content type, open the folder in which you want to store the content type. In the Create Object list, click **Content Type**.
   - To edit a content type, open the folder in which the content type is stored and click the content type name.
3. In the **Document Accessor** list, choose the accessor associated with the type of document for which you are creating this content type.

   The accessor determines how the portal extracts information from these documents. Use the File Accessor to extract general information (such as name and description) from any type of document. Use other accessors to extract more detailed information; for example, the HTML Accessor can extract title and author values.
4. If these documents include textual content and you want that content to be searchable, select **Index documents of this type for Search**.

   For example, you would not want to index .zip files, but you probably would want to index .txt files.

5. Specify property mappings.
   - To add a property mapping, click **Add Property**; then, in the Select Properties dialog box, select the properties you want to map and click **OK**.
   - To change the source document attributes that are associated with a property or to add a default or override value, click the Edit icon to the far-right of the property and type the settings in the appropriate text boxes.
     – If you want the values for this property to be extracted from the source document attributes, in the **Mapped Attributes** box, type the associated attributes, separated by commas (,).

       Content crawlers search the attributes in the order in which you list them here; if there is no value for the first listed attribute, the content crawler looks for the second listed attribute, and so on.
     – If you want this property to have a value even when the source document does not have a value for any mapped attribute, in the **Default Value** box, type the value you want this property to be given.
     – If you want this property to have the same value for all documents, in the **Override Value** box, type the value you want this property to be given.

     Note: If you set an override value, the attribute mappings and default value for this property are ignored.

     – To save your settings, click the Save icon.
   - To remove a mapping, select it and click the Remove icon.

     To select or clear all of the mapping check boxes, select or clear the box to the left of **Properties**.
   - To toggle the order in which the properties are sorted, click **Properties**.
6. On the Properties and Names page, perform tasks as necessary:
   - Section 5.15, "Naming and Describing an Object"

     You can instead enter a name and description when you save this content type.
   - Section 5.16, "Managing Object Properties"
7. On the Security page, perform tasks as necessary:
   - Section 5.17, "Setting Security on an Object"

   The default security for this content type is based on the security of the parent folder.
8. If you are editing a content type, on the Migration History and Status page, perform tasks as necessary:
   - Section 5.18, "Viewing Migration History and Status for an Object"

   Note: The Migration History and Status page is not available when creating an object.

7.9.2 Deleting a Content Type

To delete a content type you must have the following rights and privileges:

- Access Administration activity right
- Admin access to the content type

To delete a content type:

1. Click **Administration**.
2. Navigate to the content type.
3. Select the content type you want to delete and click the delete icon.

7.9.3 Mapping Content Types to Imported Content Using the Global Content Type Map

The Global Content Type Map enables you to map file extensions (for example, .doc, .txt, .html) to content types, to define which content types are applied to imported content (whether imported by a content crawler or uploaded by a user).

To access the Global Content Type Map you must be a member of the Administrators group.

The initial content types and mappings enable you to import any type of content into the portal, but you will probably want to create custom content types and mappings to import metadata specific to your company's needs.

Note:

- Users with the Advanced Document Submission activity right can use remote document submission or Web document submission and can override the default content type specified in the Global Content Type Map.
- When users create content crawlers, the **Content Type** page displays the default mappings specified in the Global Content Type Map. They can then override these mappings to fit the needs of the individual content crawler.

---

1. Click **Administration**.
2. In the Select Utility list, choose **Global Content Type Map**.
3. Configure identifiers for content types.

   You probably want to index full-text and import specific metadata from the majority of content you import into the portal. However, there are some file types that do not include much metadata and cannot be full-text indexed (for example, .exe or .zip files). You can map these file types to the **Non Indexed Files** content type. Initially, the Global Content Type Map specifies that any file extension that is not mapped uses the **Non Indexed Files** content type (the last identifier in the list is *, which includes all file extensions).

   The * identifier mapping allows any type of file to be imported into the portal.

   - If you want to limit the types of files that can be imported into the portal:
     - Remove the mappings for any file types you want to exclude from the portal.

  - Add mappings for any non-indexed files you want to include in the portal (for example, .zip files).
  - Remove the * mapping.
- If you do not want to limit the types of files that can be imported into the portal, keep the * mapping at the bottom of the list so that it is not applied to a file type that has a mapping.

7.9.3.1 Prioritizing a List of Objects

You can change the order of objects

- To move a group to the top of the list, click the Move to Top icon.
- To move a group up one space in the list, click the Move Up icon.
- To move a group down one space in the list, click the Move Down icon.
- To move a group to the bottom of the list, click the Move to Bottom icon.

7.10 About Importing Content

You can provide access through your portal to existing content in external document repositories, such as secured Web sites or Windows NT file systems.

This section describes the components involved in importing content and how you can import content security:

- Section 7.10.1, "Content Providers"
- Section 7.10.2, "Content Web Services"
- Section 7.10.3, "Content Sources"
- Section 7.10.5, "Example of Importing Content Security"

7.10.1 Content Providers

A content provider is a piece of software that tells the portal how to use the information in the external content repository. There are three different types of content providers:

- Crawl providers tell the portal how to navigate through the content hierarchy.
- Document providers tell the portal how to get information from a particular type of document.
- Upload providers tell the portal how to copy a document into the Document Repository.

Oracle provides content providers for the following types of content repositories as part of Oracle WebCenter Interaction:

- Windows NT File System
- Documentum
- Microsoft Exchange
- Lotus Notes
- Oracle Universal Content Management

> **Note:** You must install the content provider before you can create the associated content Web service. For information on installing content providers, refer to the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Interaction for Windows* or the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Interaction for Unix and Linux*).

If your content resides in a custom system, such as a custom database, you can import it by writing your own content provider using the IDK. For details, see the *Oracle Fusion Middleware Web Service Developer's Guide for Oracle WebCenter Interaction*.

7.10.2 Content Web Services

Content Web services enable you to specify general settings for your external user repository, leaving the target and security settings to be set in the associated remote content source and remote content crawler, enabling you to crawl multiple locations of the same content repository without having to repeatedly specify all the settings.

7.10.3 Content Sources

Content sources provide access to external content repositories, enabling users to submit documents and content managers to create content crawlers to import documents into the Knowledge Directory. Each content source is configured to access a particular document repository with specific authentication. For example, a content source for a secured Web site can be configured to fill out the Web form necessary to gain access to that site. Register a content source for each secured Web site or back-end repository from which content can be imported into your portal.

There are two types of content sources: Web content sources and remote content sources. Web content sources provide access to Web sites. Remote content sources provide access to external content repositories, such as a Windows NT file system, Documentum, Microsoft Exchange, or Lotus Notes.

> **Note:** If you delete a content source from which documents have been imported into the portal, the links to the documents will still exist, but users will no longer be able to access these documents.

7.10.3.1 Content Source Histories

Content sources keep track of what content has been imported, deleted, or rejected by content crawlers accessing the content source. It keeps a record of imported files so that content crawlers do not create duplicate links. To prevent multiple copies of the same link being imported into your portal, set multiple content crawlers that are accessing the same content source to only import content that has not already been imported from that content source.

7.10.3.2 Content Sources and Security

Because a content source accesses secured documents, you must secure access to the content source itself. Content sources, like everything in the portal, have security settings that allow you to specify exactly which portal users and groups can see the content source. Users that do not have at least Select access to a content source cannot select it, or even see it, when submitting content or building a content crawler.

7.10.3.3 Using Content Sources and Security to Control Access

You can create multiple content sources that access the same repository of information. For example, you might have two Web content sources accessing the same Web site. One of these content sources could access the site as an executive user that can see all of the content on the site. The other content source would access the site as a managerial user that can see some secured content, but not everything. You could then grant executive users access to the content source that accesses the Web site as an executive user, and grant managerial users access to the content source that accesses the Web site as a managerial user.

> **Note:** If you crawled the same repository using both of these content sources, you would import duplicate links into your portal, as described previously in Content Source Histories.

7.10.3.4 Content Sources Available with the Portal

Some content sources (and their necessary content Web services and remote servers) are automatically created in the **Portal Resources** folder when you install the portal. There are also content sources that are available with the portal installation, but require additional steps to complete installation. For information on the additional installation steps, refer to the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Interaction for Windows* or the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Interaction for Unix and Linux*.

- **World Wide Web:** This content source provides access to any unsecured Web site.
- **Content Upload:** This content source lets users upload a document from an internal network. You should upload a document if it is not normally accessible by the users you want to see it. For example, if the document is located on your computer and your computer is not accessible by other users, you should upload the document. Additionally, if you run an extranet, where users may not typically have access to your internal network, you should upload documents you want to make accessible externally.

7.10.4 Content Crawlers

Content crawlers enable you to import content into the portal. Web content crawlers enable you to import content from Web sites. Remote content crawlers enable you to import content from external content repositories such as a Windows NT file system, Documentum, Microsoft Exchange, Lotus Notes, or Oracle Universal Content Management.

7.10.4.1 Metadata Imported by Content Crawlers

Content crawlers index the full document text, but some content crawlers can import additional metadata.

Content Crawler	Import Links to Documents	Import Document Security	Import Folder Security
Web Content Crawler	Yes	No	No
Remote Windows Content Crawler	Yes	Yes (Windows)	Yes (Windows)
Remote Exchange Content Crawler (Windows)	Yes	No	No

Content Crawler	Import Links to Documents	Import Document Security	Import Folder Security
Remote Lotus Notes Content Crawler (Windows)	Yes	Yes	No
Remote Documentum Content Crawler	Yes	Yes	Yes

7.10.4.2 Content Crawler Best Practices

- To facilitate maintenance, we recommend you implement several instances of each content crawler type, configured for limited, specific purposes.
- For file system content crawlers, you might want to implement a content crawler that mirrors an entire file system folder hierarchy by specifying a top-level starting point and its subfolders. Although the content in your folder structure is available on your network, replicating this structure in the portal offers several advantages:
  - Users are able to search and access the content over the web.
  - Interested users can receive regular updates on new content with snapshot queries.
  - You can use default profiles to direct new users to important folders.

  However, you might find it easier to maintain controlled access, document updates, or document expiration by creating several content crawlers that target specific folders.
- If you plan to crawl Web locations, familiarize yourself with the pages you want to import. Often, you can find one or two pages that contain links to everything of interest. For example, most companies offer a list of links to their latest press releases, and most Web magazines offer a list of links to their latest articles. When you configure your content crawler for this source, you can target these pages and exclude others to improve the efficiency of your crawl jobs.
- If you know that certain content will no longer be relevant after a date—for example, if the content is related to a fiscal year, a project complete date, or the like—you might want to create a content crawler specifically for the date-dependent content. When the content is no longer relevant, you can run a job that removes all content created by the specific content crawler.
- For remote content crawlers, you might want to limit the target for mail content crawlers to specific user names; you might want to limit the target for document content crawlers to specific content types.

For additional considerations and best practices, see the *Oracle Fusion Middleware Deployment Guide for Oracle WebCenter Interaction*.

7.10.5 Example of Importing Content Security

Assume that you create an authentication source called *myAuthSource* importing users and groups into the portal from a source domain called *myDomain*. This authentication source uses the category *Employees*. Therefore, the text "Employees\" is prepended to each user's name and each group's name to distinguish these users and groups from those imported through other authentication sources. For example, if you have a user *myDomain/Mary* in the source domain, the user is imported into the portal as *Employees/Mary*.

Every authentication source automatically creates a group that includes all the users imported through that authentication source. In this example, because the

authentication source is called *myAuthSource*, the group that includes all imported users is called *Everyone in myAuthSource*.

Suppose that you want to import content from a Lotus Notes system called *myNotes*, which includes users and groups equivalent to those found in the myDomain domain. Because you have already imported these groups and users into the portal, your Notes content crawler can import Notes security information along with each Notes document. The groups in the Notes system do not have to have the same names as their corresponding groups in the myDomain domain or in the portal; the important thing is that there are Notes groups that have equivalent portal groups. If there are Notes groups that do not have equivalent groups in the portal, your Notes content crawler will ignore security settings referring to such groups.

When your Notes content crawler finds a document, it creates a list of the Notes groups that have access to it. This list is called an ACL (Access Control List). The ACLs created for Notes documents do not contain entries for specific Notes users, only for Notes groups. (Notes content crawlers only grant access to portal groups. Windows File content crawlers do grant access to portal users.) Each ACL entry is written as {Notes Server Name}\{Notes Group Name}. In this example, the content crawler creates an ACL with the single entry *myNotes\Engineering*, because this is the only Notes group that has access to that document.

The content crawler then refers to the Global ACL Sync Map to determine which portal group corresponds to this Notes group. This is a two-stage process:

1. Knowing that you would import documents and security through Notes content crawlers, on the Prefix: Domain Map page, you mapped the myAuthSource category *Employees* to the source domain *myNotes*. Guided by this entry, your content crawler modifies the ACL entry from *myNotes\Engineering* to *Employees\Engineering*.
2. Knowing that your Notes system uses a different group name than your myDomain domain, on the Portal: External Group Map page, you mapped the Notes system group *Engineering* to the myDomain group, now, the portal group, *Developers*. Guided by this entry, your content crawler modifies the ACL entry from *Employees\Engineering* to *Employees\Developers*.

As a result, all the users in the portal group *Developers* are automatically granted access to the document.

7.11 Working with Content Web Services

This section describes the following main tasks:

- Section 7.11.1, "Creating or Editing a Content Web Service"
- Section 7.11.2, "Deleting a Content Web Service"

It also cover the following low-level tasks:

- Section 7.11.3, "Sending General Settings from a Web Service to Associated Content Crawlers"

7.11.1 Creating or Editing a Content Web Service

Before you create a content Web service, you must:

- Install the content provider on the computer that hosts the portal or on another computer

- Create a remote server pointing to the computer that hosts the content provider (optional, but recommended)

To create a content Web service you must have the following rights and privileges:

- Access Administration activity right
- Create Web Service Infrastructure activity right
- At least Edit access to the parent folder (the folder that will store the content Web service)
- At least Select access to the remote server that the content Web service will use

To edit a content Web service you must have the following rights and privileges:

- Access Administration activity right
- At least Edit access to the content Web service)
- If you plan to change the remote server association, at least Select access to the remote server that the content Web service will use

To create or edit a content Web service:

1. Click **Administration**.
2. Open the Content Web Service Editor.
   - To create a content Web service, open the folder in which you want to store the content Web service. In the Create Object list, click **Web Service — Content**.
   - To edit a content Web service, open the folder in which the content Web service is stored and click its name.
3. On the Main Settings page, complete the following tasks:
   - Section 3.4.1, "Associating a Remote Server with a Web Service"
   - Section 3.4.2, "Specifying the Location of the Web Service Provider or Code"
   - Section 3.4.3, "Specifying Web Service Time-Out Settings"
   - Section 3.4.4, "Enabling and Disabling a Web Service"
4. On the HTTP Configuration page, perform tasks as necessary:
   - Section 3.4.6, "Specifying How Gatewayed Content is Handled"
   - Section 3.4.7, "Specifying What Content is Gatewayed for a Web Service"
5. On the Advanced URL Settings page, perform tasks as necessary:
   - Section 3.4.8, "Adding a Service Configuration Page to a Web Service Editor"
   - Section 3.4.9, "Adding an Administrative Configuration Link to the Select Utility Menu"
   - Section 3.4.10, "Adding a User Configuration Link to the My Account Page"
6. On the Advanced Settings page, perform tasks as necessary:
   - Section 7.11.3, "Sending General Settings from a Web Service to Associated Content Crawlers"
   - Section 3.4.11, "Specifying Encoding Style for a Web Service"
   - Section 3.4.12, "Sending Activity Rights from a Web Service to Associated Objects"

7. On the Authentication Settings page, perform tasks as necessary:
   - Section 3.4.13, "Specifying Authentication Settings for a Web Service"
8. On the Preferences page, perform tasks as necessary:
   - Section 3.4.14, "Sending User Preferences from the Web Service to Associated Objects"
9. On the User Information page, perform tasks as necessary:
   - Section 3.4.15, "Sending User Information from a Web Service to Associated Objects"
10. On the Debug Settings page, perform tasks as necessary:
    - Section 3.4.16, "Enabling Error Tracing for a Web Service"
11. On the Associated Objects page, perform tasks as necessary:
    - Section 3.4.17, "Viewing Objects Associated with a Web Service"
12. On the Properties and Names page, perform tasks as necessary:
    - Section 5.15, "Naming and Describing an Object"

      You can instead enter a name and description when you save this authentication Web service.
    - Section 5.16, "Managing Object Properties"
13. On the Security page, perform tasks as necessary:
    - Section 5.17, "Setting Security on an Object"

    The default security for this content Web service is based on the security of the parent folder. Administrative users with at least Select access to this content Web service and the Create Content Source activity right can create content sources based on the Web service.
14. If you are editing a content Web service, on the Migration History and Status page, perform tasks as necessary:
    - Section 5.18, "Viewing Migration History and Status for an Object"

    Note: The Migration History and Status page is not available when creating an object.

7.11.2 Deleting a Content Web Service

To delete a content Web service you must have the following rights and privileges:

- Access Administration activity right
- Admin access to the content Web service

To delete a content Web service:

1. Click **Administration**.
2. Navigate to the content Web service.
3. Select the content Web service you want to delete and click the delete icon.

Note: Deleting a content Web service will break any associated content sources.

7.11.3 Sending General Settings from a Web Service to Associated Content Crawlers

To specify what information the content Web service passes to associated content crawlers:

1. If the Content Web Service Editor is not already open, open it now.
2. Click the **Advanced Settings** page.
3. Under Settings, specify what general information, if any, you want this Web service to pass to its associated content crawlers:
   - To allow users to import documents into the Directory, select one or both of the following options:
     - If this Web service requires only a file path to import a document, select **Support Document Submission using file paths**.
     - This Web service might require detailed configuration information; for example, a content Web service that imports information from Lotus Notes requires users to navigate to the document they want to import. If this is the case, select **Support Document Submission using Remote UI**.
     - If you want to allow users to upload documents into the Document Repository (rather than just creating a link to the source document), select **Supports Document Submission Upload**. If the documents that users submit come from repositories that are not accessible over the network, you should choose this option.
   - If content crawlers associated with this Web service can copy the source folder structure into the portal, select **Supports mirroring the source folder structure**.
   - If content crawlers associated with this Web service can copy the source document security into the portal, select **Supports importing security with each document**.
   - To send the time zone of the user from which the portlet request is sent, select **Send timezone to Portlets**.
   - If this Web service requires the user to have an API session (for example, if the Web service uses the SOAP API), select **Send Login token to Portlets**; in the **Login Token duration** box, type the number of minutes you want the API session to last.
   - To send the ID of the experience definition from which the request is sent, select **Send Experience Definition ID to Portlets**.

7.12 Working with Content Sources

This section describes the following main tasks:

- Section 7.12.1, "Creating or Editing a Remote Content Source"
- Section 7.12.2, "Creating or Editing a Web Content Source"
- Section 7.12.3, "Deleting a Content Source"

It also covers the following low-level tasks:

- Section 7.12.4, "Gatewaying Imported Content"
- Section 7.12.5, "Providing Access to Web Content Through a Proxy Server"
- Section 7.12.6, "Selecting a Web Service for Gatewayed Content"
- Section 7.12.7, "Providing Access to Web Content by Impersonating a User"
- Section 7.12.8, "Providing Access to Web Content Through a Login Form"
- Section 7.12.9, "Providing Access to Web Content Through Cookies"
- Section 7.12.10, "Providing Access to Web Content Through Header Information"

7.12.1 Creating or Editing a Remote Content Source

Before you create a remote content source, you must:

- Install the crawl provider on the computer that hosts the portal or on another computer
- Create a remote server pointing to the computer that hosts the crawl provider (optional, but recommended)
- Create a crawler Web service on which to base this content source

To create a remote content source you must have the following rights and privileges:

- Access Administration activity right
- Create Content Sources activity right
- At least Edit access to the parent folder (the folder that will store the content source)

To edit a remote content source you must have the following rights and privileges:

- Access Administration activity right
- At least Edit access to the content source

To create or edit a remote content source:

1. Click **Administration**.
2. Open the Remote Content Source Editor.
   - To create a remote content source, open the folder in which you want to store the content source. In the Create Object list, click **Content Source - Remote**. In the Choose Web Service dialog box, select the Web service that provides the basic settings for your content source and click **OK**.
   - To edit a remote content source, open the folder in which the user is stored and click the content source name.
3. On Main Settings page, perform tasks as necessary:
   - If necessary, edit the content Web service associated with this content source by clicking the Web service name.
   - Section 7.12.4, "Gatewaying Imported Content"

   Note: Depending on what type of remote content source you are creating, you might see additional settings and additional pages.
4. On the Properties and Names page, perform tasks as necessary:

- Section 5.15, "Naming and Describing an Object"

  You can instead enter a name and description when you save this content source.

- Section 5.16, "Managing Object Properties"

5. On the Security page, perform tasks as necessary:
   - Section 5.17, "Setting Security on an Object"
6. If you are editing a content source, on the Migration History and Status page, perform tasks as necessary:
   - Section 5.18, "Viewing Migration History and Status for an Object"

   Note: The Migration History and Status page is not available when creating an object.

Users with at least Select access to this content source can now submit documents from this content source or create content crawlers that will access this content source.

7.12.2 Creating or Editing a Web Content Source

Note: The World Wide Web content source, created upon install, provides access to any unsecured Web site.

To create a Web content source you must have the following rights and privileges:

- Access Administration activity right
- Create Content Sources activity right
- At least Edit access to the parent folder (the folder that will store the content source)

To edit a Web content source you must have the following rights and privileges:

- Access Administration activity right
- At least Edit access to the content source

To create or edit a Web content source:

1. Click **Administration**.
2. Open the Web Content Source Editor.
   - To create a Web content source, open the folder in which you want to store the content source. In the Create Object list, click **Content Source - WWW**. In the Choose Web Service dialog box, select the Web service that provides the basic settings for your content source and click **OK**.
   - To edit a remote content source, open the folder in which the user is stored and click the content source name.
3. On the Main Settings page, perform tasks as necessary:
   - Section 7.12.7, "Providing Access to Web Content by Impersonating a User"
   - Section 7.12.4, "Gatewaying Imported Content"

- Section 7.12.6, "Selecting a Web Service for Gatewayed Content" (only necessary if you selected to gateway content)

4. On the Proxy Server Configuration page, perform tasks as necessary:
   - Section 7.12.5, "Providing Access to Web Content Through a Proxy Server"
5. On the Login Form Settings page, perform tasks as necessary:
   - Section 7.12.8, "Providing Access to Web Content Through a Login Form"
6. On the Cookie Information page, perform tasks as necessary:
   - Section 7.12.9, "Providing Access to Web Content Through Cookies"
7. On the Header Information page, perform tasks as necessary:
   - Section 7.12.10, "Providing Access to Web Content Through Header Information"
8. On the Properties and Names page, perform tasks as necessary:
   - Section 5.15, "Naming and Describing an Object"

     You can instead enter a name and description when you save this content source.
   - Section 5.16, "Managing Object Properties"
9. On the Security page, perform tasks as necessary:
   - Section 5.17, "Setting Security on an Object"
10. If you are editing a content source, on the Migration History and Status page, perform tasks as necessary:
    - Section 5.18, "Viewing Migration History and Status for an Object"

> **Note:** The Migration History and Status page is not available when creating an object.

Users with at least Select access to this content source can now submit documents from this content source or create content crawlers that will access this content source.

7.12.3 Deleting a Content Source

To delete a content source you must have the following rights and privileges:

- Access Administration activity right
- Admin access to the content source

To delete a content source:

1. Click **Administration**.
2. Navigate to the content source.
3. Select the content source you want to delete and click the delete icon.

> **Note:** Deleting a content source will break the links to any content imported, submitted, or uploaded from that content source.

7.12.4 Gatewaying Imported Content

When users click a link to an imported document, they can either be directed to the actual location of the source document or the content can be gatewayed, and the user will be redirected to a URL (generated from the settings in your portal configuration file) that, in turn, displays the document. Gatewaying content allows users to view documents they might not otherwise be able to view, either due to security on the source repository or firewall restrictions. You configure gateways settings on the Main Settings page of the Content Source Editor.

1. If the Content Source Editor is not already open, open it now.
2. Under URL Type, specify what happens when users follow document links:
   - If you want to direct users to the actual location of the document, choose **Does not use the Gateway to open documents**. Be warned, however, that with this option, even users with access to this content source's documents will not be able to open the documents if the documents are not publicly available and the users are not connected to your network.
   - If you want to redirect users to a URL (generated by the settings in your portal configuration file) that, in turn, displays the document, choose **Uses the gateway to open documents**.

     Note:

     - If you want your users to be able to view documents even when they are not connected to your network, you should choose this option.
     - If the associated content Web service supports content upload (specified on the Advanced Settings page of the Content Web Service Editor), you must use the gateway or content uploads will fail.

   By default Web content sources do not gateway content, whereas remote content sources do.

7.12.5 Providing Access to Web Content Through a Proxy Server

If you use a proxy server to access the internet, you can specify the proxy server settings on the Proxy Server Configuration page of the Content Source Editor.

1. If the Content Source Editor is not already open, open it now.
2. Click the **Proxy Server Configuration** page.
3. In the **Address** box, type the name of your proxy server.
4. In the **Port** box, type the port number for your proxy server.
5. If this proxy server requires security information:
   a. In the **User name** box, type the name of the user you want the portal to impersonate to access this proxy server.
   b. In the **Password** box, type the password for the user you specified.
   c. In the **Confirm** box, type the password again.
6. If you do not require the proxy server to access computers hosted on your local network, select **Bypass proxy server for local addresses**.

7. If there are other sites that do not require the proxy server, in the **Do not use for addresses beginning with** box, type the base URLs of these Web sites.

   Separate multiple URLs with semicolons (;).

7.12.6 Selecting a Web Service for Gatewayed Content

If you selected to gateway the content from this content source, you must select a Web service to associate with this content source. You can specify that information on the Main Settings page of the Web Content Source Editor.

1. If the Content Source Editor is not already open, open it now.
2. Under Web Service, associate a content Web service with this content source:

   This section appears only if you selected to gateway content.

   - To associate an existing content Web service, click **Browse**; then, in the **Choose Web Service** dialog box, choose a content Web service and click **OK**.
   - To remove the association, click **Remove**.
   - To edit the associated content Web service, click its name.

7.12.7 Providing Access to Web Content by Impersonating a User

If the Web site accessed by this content source requires a specific user name and password to access the site, you can specify that information on the Main Settings page of the Web Content Source Editor.

1. If the Content Source Editor is not already open, open it now.
2. Under Target Site Security, specify the security information required to access this Web site:

   a. In the **User name** box, type the name of the user that this portal will impersonate to access content from this Web site.

   b. In the **Password** box, type the password for the user.

   c. In the **Confirm password** box, type the password again.

7.12.8 Providing Access to Web Content Through a Login Form

If the Web site accessed by this content source requires users to complete a form to access the site, you can specify the login form settings on the Login Form Settings page of the Content Source Editor.

1. If the Content Source Editor is not already open, open it now.
2. Click the **Login Form Settings** page.
3. In the **Login URL** box, type the URL to the login form that must be completed.
4. In the **Post URL** box, type the URL to which this login form posts data.

   To find the URL, search the form's source HTML for the <FORM> tag; the ACTION attribute contains the URL to which the form posts.

5. Under Form Fields, specify the information needed to gain access to this site:

   To determine this information, you can either contact the person who wrote the form or search the form's source HTML for each <INPUT> tag.

   - To add information for an <INPUT> tag:

a. Click **Add**.

b. In the **Name** box, type the text after "name=" from the `<INPUT>` tag.

   For example, if the form includes `<INPUT type="password" name="Password" size="10">`, type **`Password`**.

c. In the **Value** box, type the text you would normally type in the form field.

   Using the example from the previous step, you would type the password needed to access the site.

- To remove a name/value pair, select the name/value and click the Remove icon.

  To select or clear all of the name/value pair boxes, select or clear the box to the left of **Name**.

7.12.9 Providing Access to Web Content Through Cookies

If the Web site accessed by this content source requires information to be sent in the form of cookies, you can specify the cookie settings on the Cookie Information page of the Content Source Editor.

1. If the Content Source Editor is not already open, open it now.
2. Click the **Cookie Information** page.
3. Determine what cookie information you must send through one of the following methods:
   - Contact the person who wrote the form.
   - Viewing the cookies through your internet browser:
     a. Set your internet browser to prompt you before accepting cookies.

        Refer to your browser's online help for instructions.

     b. Navigate to the Web site this content source will access.

     c. When prompted to accept a cookie, view the cookie information.

        For each cookie you receive, make note of the name and data values and the base URL from which it was sent.
4. Under Cookies, specify the cookie information needed to gain access to this site:
   - To add information for a cookie:
     a. Click **Add**.

     b. In the **Name** box, type the text displaying in the Name field for the cookie.

     c. In the **Value** box, type the text displaying in the Data field for the cookie.

     d. In the **Cookie URL** box, type the base URL from which the cookie was sent.

        For example, if you need a cookie to access all areas of a Web site, you might type `http://www.mysite.com`, but if the cookie is needed to access only a particular area of a Web site, you might type `http://www.mysite.com/securedcontent`.

   - To remove a cookie, select the cookie and click the Remove icon.

     To select or clear all of the cookie boxes, select or clear the box to the left of **Name**.

7.12.10 Providing Access to Web Content Through Header Information

If the Web site accessed by this content source requires header information to access the site, you can specify the header information on the Header Information page of the Content Source Editor.

1. If the Content Source Editor is not already open, open it now.
2. Click the **Header Information** page.
3. Paste the required header information into the text box if one of the following is true:
   - The Web site accessed by this content source only responds to requests with specific information in the included HTTP header.
   - Your proxy server sends requests beyond your firewall only if there is specific information in the header.

7.13 Working with Content Crawlers

This section describes the following main tasks:

- Section 7.13.1, "Creating or Editing a Remote Content Crawler"
- Section 7.13.2, "Creating or Editing a Web Content Crawler"
- Section 7.13.3, "Deleting a Content Crawler"

It also cover the following low-level tasks:

- Section 7.13.4, "Specifying Where and How Far to Crawl"
- Section 7.13.5, "Setting Destination Folders for Imported Content"
- Section 7.13.6, "Mirroring the Source Folder Structure"
- Section 7.13.7, "Setting a Content Crawler to Obey Folder Filters"
- Section 7.13.8, "Automatically Approving Imported Documents"
- Section 7.13.9, "Importing Security with Imported Documents"
- Section 7.13.10, "Manually Granting Access to Imported Documents"
- Section 7.13.11, "Avoiding Importing Unwanted Content"
- Section 7.13.12, "Specifying a Time-Out Setting for a Web Content Crawler"
- Section 7.13.13, "Specifying Expiration and Refresh Settings for Imported Documents"
- Section 7.13.14, "Customizing the Content Type Mappings for a Content Crawler"
- Section 7.13.15, "Specifying What to Do with Rejected Documents"
- Section 7.13.16, "Specifying What to Do on Subsequent Crawls"
- Section 7.13.17, "Marking Imported Documents with a Crawler Tag"
- Section 7.13.18, "Configuring the Number of Threads Used to Crawl Content"
- Section 7.13.19, "Testing a Content Crawler"
- Section 7.13.20, "Troubleshooting the Results of a Crawl"
- Section 7.13.21, "Destination Folder Flowchart"

7.13.1 Creating or Editing a Remote Content Crawler

You can create a remote content crawler to import content (and security) from external document repositories.

Before you create a remote content crawler, you must:

- Install the content provider on the computer that hosts the portal or on another computer.
- Create a remote server.
- Create a content Web service.
- Create a content source.
- Create the folders in which you want to store the imported content.
- Create and apply any filters to the folders to control the sorting of imported content.
- Create any users and groups to which you want to grant access to the imported content.

To create a remote content crawler you must have the following rights and privileges:

- Access Administration activity right
- Create Content Crawlers activity right
- At least Edit access to the parent folder (the folder that will store the content crawler)
- At least Select access to the content source on which this content crawler will be based
- At least Select access to the folders in which you want to store the imported content
- At least Select access to the users and groups to which you want to grant access to the imported content

To edit a remote content crawler you must have the following rights and privileges:

- Access Administration activity right
- At least Edit access to the remote content crawler
- At least Select access to the content Web service on which this content crawler will be based
- If you plan to change the folders into which you will store the imported content, at least Select access to the folders
- If you plan to change the users and groups to which you will grant access to the imported content, at least Select access to the users and groups

To create or edit a remote content crawler:

1. Click **Administration**.
2. Open the Remote Content Crawler Editor.
    - To create a remote content crawler, open the folder in which you want to store the content crawler. In the Create Object list, click **Content Crawler — Remote**. In the Choose Content Source dialog box, select the content source that provides access to the content you want to crawl and click **OK**.

- To edit a remote content crawler, open the folder in which the content crawler is stored and click the remote content crawler name.

3. On the Main Settings page, perform tasks as necessary:
   - Define where and how far to crawl. Depending on what type of content repository you are crawling, you see different options.
   - Section 7.13.5, "Setting Destination Folders for Imported Content"
   - Section 7.13.6, "Mirroring the Source Folder Structure"
   - Section 7.13.7, "Setting a Content Crawler to Obey Folder Filters"
   - Section 7.13.8, "Automatically Approving Imported Documents"
   - Section 7.13.9, "Importing Security with Imported Documents"
   - Section 7.13.10, "Manually Granting Access to Imported Documents"
4. On the Document Settings page, perform tasks as necessary:
   - Section 7.13.13, "Specifying Expiration and Refresh Settings for Imported Documents"
5. On the Content Type page, perform tasks as necessary:
   - Section 7.13.14, "Customizing the Content Type Mappings for a Content Crawler"
6. On the Advanced Settings page, perform tasks as necessary:
   - In the list under Content Language, choose the language in which the majority of content to import is written.
   - Section 7.13.15, "Specifying What to Do with Rejected Documents"
   - Section 7.13.16, "Specifying What to Do on Subsequent Crawls"
   - Section 7.13.17, "Marking Imported Documents with a Crawler Tag"
   - Section 7.13.18, "Configuring the Number of Threads Used to Crawl Content"
7. On the Set Job page, perform tasks as necessary:
   - Section 5.14, "Associating an Object with a Job"
8. On the Properties and Names page, perform tasks as necessary:
   - Section 5.15, "Naming and Describing an Object"

     You can instead enter a name and description when you save this authentication Web service.
   - Section 5.16, "Managing Object Properties"
9. On the Security page, perform tasks as necessary:
   - Section 5.17, "Setting Security on an Object"

   The default security for this content crawler is based on the security of the parent folder.
10. If you are editing a content crawler, on the Migration History and Status page, perform tasks as necessary:
    - Section 5.18, "Viewing Migration History and Status for an Object"

Note: The Migration History and Status page is not available when creating an object.

To import content, run the job you associated with this content crawler.

7.13.2 Creating or Editing a Web Content Crawler

You can create a Web content crawler to import content from Web sites and RSS feeds.

Before you create a Web content crawler, you must:

- Create a content source, if necessary, to access secured content.
- Create the folders in which you want to store the imported content.
- Create and apply any filters to the folders to control the sorting of imported content.
- Create any users and groups to which you want to grant access to the imported content.

To create a Web content crawler you must have the following rights and privileges:

- Access Administration activity right
- Create Content Crawlers activity right
- At least Edit access to the parent folder (the folder that will store the content crawler)
- At least Select access to the content source on which this content crawler will be based
- At least Select access to the folders in which you want to store the imported content
- At least Select access to the users and groups to which you want to grant access to the imported content

To edit a Web content crawler you must have the following rights and privileges:

- Access Administration activity right
- At least Edit access to the Web content crawler
- If you plan to change the folders into which you will store the imported content, at least Select access to the folders
- If you plan to change the users and groups to which you will grant access to the imported content, at least Select access to the users and groups

To create or edit a Web content crawler:

1. Click **Administration**.
2. Open the Web Content Crawler Editor.
    - To create a Web content crawler, open the folder in which you want to store the content crawler. In the Create Object list, click **Content Crawler — WWW**. In the Choose Content Source dialog box, select the content source that provides access to the content you want to crawl and click **OK**.
    - To edit a Web content crawler, open the folder in which the content crawler is stored and click the Web content crawler name.

3. On the Main Settings page, perform the following tasks as necessary:
   - Section 7.13.4, "Specifying Where and How Far to Crawl"
   - Section 7.13.5, "Setting Destination Folders for Imported Content"
   - Section 7.13.7, "Setting a Content Crawler to Obey Folder Filters"
   - Section 7.13.8, "Automatically Approving Imported Documents"
   - Section 7.13.10, "Manually Granting Access to Imported Documents"
4. On the Web Page Exclusions page, perform the following tasks as necessary:
   - Section 7.13.11, "Avoiding Importing Unwanted Content"
5. On the Target Settings page, perform the following tasks as necessary:
   - Section 7.13.12, "Specifying a Time-Out Setting for a Web Content Crawler"
6. On the Document Settings page, perform the following tasks as necessary:
   - Section 7.13.13, "Specifying Expiration and Refresh Settings for Imported Documents"
7. On the Content Type page, perform the following tasks as necessary:
   - Section 7.13.14, "Customizing the Content Type Mappings for a Content Crawler"
8. On the Advanced Settings page, perform tasks as necessary:
   - In the list under Content Language, choose the language in which the majority of content to import is written.
   - Section 7.13.15, "Specifying What to Do with Rejected Documents"
   - Section 7.13.16, "Specifying What to Do on Subsequent Crawls"
   - Section 7.13.17, "Marking Imported Documents with a Crawler Tag"
   - Section 7.13.18, "Configuring the Number of Threads Used to Crawl Content"
9. On the Set Job page, perform the following tasks as necessary:
   - Section 5.14, "Associating an Object with a Job"
10. On the Properties and Names page, perform tasks as necessary:
    - Section 5.15, "Naming and Describing an Object"

      You can instead enter a name and description when you save this authentication Web service.
    - Section 5.16, "Managing Object Properties"
11. On the Security page, perform tasks as necessary:
    - Section 5.17, "Setting Security on an Object"

    The default security for this content crawler is based on the security of the parent folder.
12. If you are editing a content crawler, on the Migration History and Status page, perform tasks as necessary:
    - Section 5.18, "Viewing Migration History and Status for an Object"

Note: The Migration History and Status page is not available when creating an object.

To import content, run the job you associated with this content crawler.

7.13.3 Deleting a Content Crawler

To delete a content crawler you must have the following rights and privileges:

- Access Administration activity right
- Admin access to the content crawler

To delete a content crawler:

1. Click **Administration**.
2. Navigate to the content crawler.
3. Select the content crawler you want to delete and click the delete icon.

7.13.4 Specifying Where and How Far to Crawl

To specify where and how far to crawl:

1. If the Content Crawler Editor is not already open, open it now.
2. On the Main Settings page, in the **URL to crawl** box, type the URL to the site from which you want to import content.
3. In the **Crawl radius** list, specify the maximum number of links away from the target page to crawl. For example, if you select 1, this content crawler attempts to import every page directly linked to the target page; if you select 2, this content crawler attempts to import every page directly linked to the target page, and every page directly linked to those linked pages.
4. By default, this content crawler creates a link to the URL you entered in step 3. If you do not want to create a link to this page, clear the **Import the target page** check box. For example, if you crawl the results of a search, you would not want to import the target page (the search results page); you would want to import each linked page (each result).

7.13.5 Setting Destination Folders for Imported Content

To set the destination folder for imported content:

1. If the Content Crawler Editor is not already open, open it now.
2. Under Destination Folders, specify into which folders you want to import content. The content crawler attempts to import a link to every document it finds into the most subordinate subfolder within the destination folder that allows the link to pass.

   To view a flowchart showing how the content crawler determines into which folders it will import content, see Section 7.13.21, "Destination Folder Flowchart."

   - To add destination folders, click **Add Folder**; then, in the Choose Folders dialog box, select the folders you want to add and click **OK**. To crawl documents into a folder, you must have at least Edit access to that folder.
   - To remove a folder, select the folder and click the remove icon.

- To select or clear all of the folder check boxes, select or clear the box to the left of Folder Path.
- To toggle the order in which the folders are sorted (ascending/descending), click Folder Path or click the icon to the right of that.

7.13.6 Mirroring the Source Folder Structure

If the content Web service used by the content crawler supports folder mirroring (specified on the Advanced Settings page of the Content Web Service Editor), you can have the content crawler create Directory folders that duplicate the folder structure of the content repository being crawled.

Note:

- If you mirror the folder structure and import security information with each document (described in step 5), the folder security is imported for the mirrored folders.
- If you mirror the folder structure, upon successive runs the content crawler removes any portal folders that do not have corresponding source folders. For this reason, if you run this content crawler periodically, neither you nor anyone else should modify the mirrored portal folders or documents in any way.
- You cannot change the mirror setting after creation of this content crawler. That is, if you set this content crawler to mirror the folder structure, you cannot edit this setting later.

To mirror the source folder structure:

1. If the Content Crawler Editor is not already open, open it now.
2. On the Main Settings page, select **Mirror the source folder structure**.

7.13.7 Setting a Content Crawler to Obey Folder Filters

By default, crawled documents do not must pass the filters of destination folders, so all documents will be imported into all destination folders. If you want the content crawler to obey the filters applied to the destination folders when importing content, change the setting in the content crawler.

Note: This feature is not available if you mirror the source folder structure.

To set a content crawler to obey folder filters:

1. If the Content Crawler Editor is not already open, open it now.
2. On the Main Settings page, select **Apply Filter of Destination Folder**.

7.13.8 Automatically Approving Imported Documents

By default, documents require approval, meaning that before the link to the imported document is available to users, it must be approved by a portal administrator with at least Edit access to the destination folder. You can instead automatically approve all imported documents.

To automatically approve imported documents:

1. If the Content Crawler Editor is not already open, open it now.
2. On the Main Settings page, select **Automatically approve imported documents**.

If you are mirroring the folder structure, you might want to set imported documents to be approved automatically and restrict users to Read access (users in the Administrators group always have Admin access). If you set imported documents to require approval, be aware that any portal administrator who has at least Edit access can also modify the folders and content, and can therefore make your portal folders and content out of sync with your source repository.

7.13.9 Importing Security with Imported Documents

If the content Web service used by this content crawler supports security importation and the source repository users and groups correspond to portal users and groups (specified in the Global ACL Sync Map), you can have this content crawler import the security settings for each document. This automatically makes documents that are available to source repository users available to the mapped portal users.

Note: Because read access is equivalent in the source repository and the portal, but write access is not, only read access is imported; write access is ignored because write access to a document in an external repository enables you to edit the document, but write access (referred to as Edit access) in the portal enables you to edit the properties and security settings of that document.

To import security with imported documents:

1. If the Content Crawler Editor is not already open, open it now.
2. On the Main Settings page, select **Import security with each document**.

7.13.10 Manually Granting Access to Imported Documents

To manually grant users and groups access to the content imported by a content crawler:

1. If the Content Crawler Editor is not already open, open it now.
2. On the Main Settings page, under Document Access Privileges, perform the following actions:
   - To add users or groups, click **Add Users/Groups**; then, in the Choose Groups and Users dialog box, select the users and groups you want to add and click **OK**.

     To add a user or group, you must have at least Select access to that user or group.
   - For each user or group, in the associated Privilege list, choose the access privilege you want to grant for content imported by this content crawler.
   - To remove a user or group, select the user or group and click the remove icon.
   - To select or clear all of the user and group check boxes, select or clear the box to the left of Users/Groups.

- To toggle the order in which the users and groups are sorted (ascending/descending), click **Users/Groups** or click the icon to the right of that.
- To view the members of a group, click the group name.

7.13.11 Avoiding Importing Unwanted Content

To configure this content crawler to avoid importing unwanted Web pages into your portal:

1. If the Content Crawler Editor is not already open, open it now.
2. Click the **Web Page Exclusions** page.
3. By default, this content crawler follows the Web server's recommendations about which pages might be of value to automated crawlers. If you want to ignore these recommendations, clear the **Obey the target site's robot exclusion protocols** check box.

   In general, these recommendations help limit unwanted content from being crawled into the portal. However, some sites offer very strict recommendations. If your content crawler is not importing any content from a site, try turning this option off.
4. By default, this content crawler saves the URLs to imported Web pages in the case used on the source Web site. To change the URLs to lower case, select **Convert all URLs to lower case**.
5. To avoid importing content from an area of a Web site or to avoid importing particular pages:
   - To specify an area to avoid, click **Add exclusion filter**; then, in the text box, type the URL to the area of the Web site to avoid.

     You can use wildcard notation (*) to make the exclusion more general. For example, to avoid crawling sales information from a site, you might type `http://mycompany.com*sales`. As a result, this crawler would not import any pages from mycompany.com that have "sales" anywhere in the URL.

     Note:

     - Wildcards are assumed on either side of your text. For example, if you type `sales`, the crawler will not import any pages from *any* site accessible from the target URL that has "sales" anywhere in the URL.
     - If you list exclusions and inclusions (described below), the exclusions apply only to the *included* pages. For example, if you excluded `sales` and included `http://mycompany.com`, your crawler would import all pages from http://mycompany.com except for those pages that had "sales" anywhere in the URL.
   - To remove an exclusion filter, select it and click the remove icon.
   - To select or clear all exclusion filter check boxes, select or clear the box to the left of Exclusion Filters.
6. By default, this content crawler does not crawl or import any pages specified in the exclusions. If your content crawler will navigate from a link on an excluded

page to a page that is not excluded and that *should* be imported, choose **Crawl excluded pages, but do not import them**.

7. To limit your crawl to an area of a Web site or a particular page:

   - To specify where this content crawler may crawl, click **Add inclusion filter**; then, in the text box, type the URL to the area of the Web site to which you want to restrict your crawl. Because Web sites can contain links to other sites, you might want to use inclusions to keep your content crawler on a particular site. To avoid crawling other sites, add the base URL of the site you want to crawl to the inclusion list; for example, `http://mycompany.com`.

     You can use wildcard notation (*) to make the inclusion more general. For example, if you want to crawl only information on single sign-on (SSO), you might type `http://mycompany.com*sso`. As a result, this content crawler would import only pages from mycompany.com that have "sso" anywhere in the URL.

     Note:

     - Wildcards are assumed on either side of your text. For example, if you type sso, the content crawler will import any pages from *any* site accessible from the target URL that has "sso" anywhere in the URL.
     - If you list inclusions and exclusions, the exclusions apply only to the included pages. For example, if you included `http://mycompany.com` and excluded `sso`, your content crawler would import all pages from http://mycompany.com except for those pages that had "sso" anywhere in the URL.

   - To remove an inclusion filter, select the it and click the remove icon.
   - To select or clear all inclusion filter check boxes, select or clear the box to the left of Inclusion Filters.

7.13.12 Specifying a Time-Out Setting for a Web Content Crawler

To specify a time-out for a Web content crawler:

1. If the Content Crawler Editor is not already open, open it now.
2. Click the **Target Settings** page.
3. To specify the maximum amount of time that this content crawler waits for a Web page to load, next to Time-out period, type a number in the box and choose a period in the drop-down list. If the page does not load in this time, the content crawler moves on to the next page.

7.13.13 Specifying Expiration and Refresh Settings for Imported Documents

You can have the Document Refresh Agent periodically verify that the source documents for links in the portal still exist, update document properties, or expire document links.

You might want to set document links to expire if the document will become irrelevant at some point. For example, if you import forms for 2010 company benefits, you might want to have them expire at the end of the year, so that users do not use outdated forms.

When a link is refreshed, the Document Refresh Agent verifies whether the source document still exists. If the document exists, the Document Refresh Agent updates the associated property values from the source document. If the document does not exist, the Document Refresh Agent applies the settings you specify for dealing with broken links.

These settings are referenced by the Document Refresh Agent when the Document Refresh job runs.

1. If the Content Crawler Editor is not already open, open it now.
2. Click the **Document Settings** page.
3. Under Document Expiration, choose whether the link to the document should expire:
   - To specify that document links should not be deleted due to expiration, choose **Never expire**.
   - To specify that document links should be deleted after a specified period, choose **Delete after**, type a number in the box, and choose a period in the drop-down list.

     When the Document Refresh job runs, it will delete any document links that have reached the expiration date.

     Tip: If you want to delete all documents previously imported by this content crawler, you can set the documents to expire immediately (for example, setting them to delete after 1 minute) and apply these settings to existing documents as described in step 4. The next time the Document Refresh job runs, it deletes all documents previously imported by this content crawler.
4. Under Link and Property Refresh, specify the refresh settings that should be used by the Document Refresh Agent:
   - If you do not want to refresh the document, select **Never**.
   - If you want to refresh the document, select **Every**, and type a number in the box and choose an interval from the list.
   - To prevent the Document Refresh Agent from refreshing document properties, select **Only confirm the validity of the links to these documents**.
5. Under Broken Links, specify what happens to links to documents if the Document Refresh Agent finds that the source documents do not exist:
   - If you want to leave broken links in the portal, select **Left alone**.
   - If you want to remove broken links from the portal immediately, select **Deleted immediately**.
   - If you want to leave broken links for a specified amount of time, select **Deleted after**, and type a number in the box and choose an interval from the list.

     You might want to leave broken links in the portal for a short while in case the source document repository is temporarily inaccessible.
6. If you change the settings on this page after this content crawler has run and you want to apply these new settings to previously imported documents, select **Apply these settings to existing documents created by this content crawler**. These

settings will be applied when you click **Finish**, but documents will not be deleted and properties will not be updated until you run the Document Refresh job.

7.13.14 Customizing the Content Type Mappings for a Content Crawler

By default, a content crawler uses the content type mappings specified in the Global Content Type Map. However you can customize these mappings to fit the needs of the content you are crawling.

Content type mappings show a content crawler how to assign content types to imported content. When a content crawler finds a new document, it starts at the top of its content type mappings list and looks for an extension that matches the document. It uses the content type that is mapped to the first matching extension. If it cannot find a matching extension, it does not import the document.

To customize the content type mappings for a content crawler:

1. If the Content Crawler Editor is not already open, open it now.
2. Click the **Content Type** page.
3. Perform the following actions to change the mappings for this content crawler:
   - To add a mapping to this list, under the appropriate type map grouping, click **New Identifier**; then, in the Identifier Editor, type the file extension, choose a content type, and click **Finish**. The new mapping displays at the bottom of the list.
   - To create a new content type to map to a new or existing extension, click **Create Content Type**; then, in the Content Type Editor, choose a document accessor and click **Finish**.
   - To remove a mapping, select the mapping and click the remove icon.
   - To select or clear all of the mapping check boxes, select or clear the box to the left of Identifiers.
     - To move a mapping to the top of this list, click the move to top icon.
     - To move a mapping up one space in this list, click the move up icon.
     - To move a mapping down one space in this list, click the move down icon.
     - To move a mapping to the bottom of this list, click the move to bottom icon.
   - To edit a mapping, click the edit icon and change the mapping in the Identifier Editor.

7.13.15 Specifying What to Do with Rejected Documents

To customize the content type mappings for a content crawler:

1. If the Content Crawler Editor is not already open, open it now.
2. Click the **Advanced Settings** page.
3. Under Rejected Documents, specify what to do with documents that do not successfully sort into a folder:
   - To import these documents anyway, choose **Import into the Unclassified Documents folder**.

> **Note:** The Unclassified Documents folder is available to users with the Access Unclassified Documents activity right. To access unclassified documents, in the Directory menu, click **Edit Directory** and open the Unclassified Documents folder. You can also click **Administration**, then, in the Select Utilities menu, choose **Access Unclassified Documents**.

- To avoid importing these documents, choose **Do not import**.

4. If you are editing an existing content crawler, you see additional options under Rejected Documents that allow you to specify what to do when this content crawler finds a previously rejected document. The definition of "previously rejected" depends on how you defined new links, as described in Section 7.13.16, "Specifying What to Do on Subsequent Crawls."

   - If you chose **by this Content Crawler**, previously rejected documents include all documents rejected *by this content crawler*.
   - If you chose **from this Content Source**, previously rejected documents include all documents rejected *from this content source*.

   Specify what to do with previously rejected documents:

   - To have this content crawler try to import previously rejected documents, select **Re-Import**.
   - To avoid importing these documents, choose **Do not import**.

5. If absolutely necessary, you can delete the history of previously rejected documents. Again, the definition of "previously rejected" depends on how you defined new links, as described in Section 7.13.16, "Specifying What to Do on Subsequent Crawls." If you chose **from this Content Source**, you are deleting the rejection history for all content crawlers that import documents from this content source. If you are still sure that you must delete the history of previously rejected documents, click **Clear Rejection History**.

7.13.16 Specifying What to Do on Subsequent Crawls

You can refresh metadata and import new content from content crawlers that have previously imported content.

If you are editing an existing content crawler, you see the section Importing Documents. Under Importing Documents, specify whether to import only new documents. By default, the content crawler attempts to import only new documents (those that have not been previously imported by this content crawler or other content crawlers that access this same content source). You can change the content crawler setting to import multiple copies of each document, which might be useful while testing your content crawlers. You can also specify whether the content metadata should be updated.

1. If the Content Crawler Editor is not already open, open it now.
2. Click the **Advanced Settings** page.
3. To import only new documents, select **Import only new links**.

   New options display.If you want to import all content again the next time this content crawler runs, leave the option unselected and skip the rest of the steps.

4. Specify what new links means:

- To import only those documents that have not been previously imported by this content crawler, choose **by this Content Crawler**.
- To import only those documents that have not been imported from the associated content source (either by this content crawler, another content crawler, or manually by a user), choose **from this Content Source**.

> **Note:** The option you choose here also applies to the rejection history (discussed in Section 7.13.15, "Specifying What to Do with Rejected Documents") and deletion history (discussed below). For example, if you select **from this Content Source**, the rejection history includes content rejected by any content crawler that has crawled the content source.

5. To refresh the previously imported documents as specified on the Document Settings page, select **refresh them**.

   Generally, refreshing documents is the job of the Document Refresh Agent; refreshing documents slows the content crawler down. However, if you changed the document settings for this content crawler or changed the property mappings in the associated content types, refreshing documents updates these settings for the previously imported documents.

   > **Note:** If you are crawling an RSS feed, the **refresh them** option refreshes the properties (such as the title and description) with the values from the target documents, not the RSS feed. If you want to retain the properties from the RSS feed, do not select **refresh them**.

6. If you created additional folders or applied different filters to destination folders, select **try to sort them into additional folders** to sort the previously imported documents into new Knowledge Directory folders.

   Another content crawler might have imported documents from the same content source but into different folders than the destination folders specified for this content crawler. Ensure that you really want to re-sort those documents into the destination folders specified for this content crawler.

7. To re-import documents that were previously deleted (manually, due to expiration, or due to missing source documents), select **regenerate deleted links**.

   > **Note:** This might re-import documents that were at one time deemed inappropriate for your portal.

If absolutely necessary, you can delete the history of documents that have been deleted from the portal. Remember that the deletion history is defined by what you specified as new documents in step 4.

- If you chose **by this Content Crawler**, the history includes all documents imported by this content crawler that have been deleted.
- If you chose **from this Content Source**, the history includes all documents imported from this content source that have been deleted. Therefore, you are deleting the history for all content crawlers that import documents from this content source.

If you are still sure that you must delete the record of documents deleted from the portal, click **Clear Deletion History**.

7.13.17 Marking Imported Documents with a Crawler Tag

For troubleshooting purposes, you might want to mark imported documents with a unique crawler tag so you know which content crawler imported a particular document.

To mark imported documents with a crawler tag:

1. If the Content Crawler Editor is not already open, open it now.
2. Click the **Advanced Settings** page.
3. Type a unique tag in the **Mark imported documents with the following Content Crawler Tag** box.

7.13.18 Configuring the Number of Threads Used to Crawl Content

> **Note:** The allowable ranges for these settings are set in the portal configuration file. The values set here are also limited by the maximum threads allowable in the automation service used for the job associated with the content crawler.

To configure the number of threads used to crawl content for a content crawler:

1. If the Content Crawler Editor is not already open, open it now.
2. Click the **Advanced Settings** page.
3. Under Runtime Configuration, set the following:
   - In the **Maximum document-fetching threads** box, type the maximum number of concurrent threads used to fetch content from the content source.
   - In the **Maximum card-indexing threads** box, type the maximum number of concurrent threads used in processing content once it has been crawled into the portal.

7.13.19 Testing a Content Crawler

Before you have a content crawler import content into the public folders of your portal, test it by running a job that crawls document records into a temporary folder.

Create a test folder and remove the Everyone group, and any other public groups, from the **Security** page on the folder to ensure that users cannot access the test content.

1. Ensure that the content crawler creates the correct links.

   Examine the target folder and ensure the content crawler has generated records and links for desired content and has not created unwanted records and links.

   If you iterate this testing step after modifying the content crawler configuration, ensure that you delete the contents of the test folder and clear the deletion history for the content crawler.
2. Ensure that the content crawler creates correct metadata.

Ensure that all documents are given the right content types, and that these content types correctly map properties to source document attributes.

Go to the Knowledge Directory, and look at the properties and content types of a few of the documents this content crawler imported to see if they are the properties and content types you expected.

To view the properties and content type for a document:

1. Click **Directory** and navigate to the folder that contains the document whose properties and content type you want to view.
2. Click **Properties** under the document to display the information about the document. The properties are displayed in a table along with their values. The content type is displayed at the bottom of the page.

If you iterate this testing step after modifying the content crawler configuration, ensure that you configure the content crawler to refresh these links.

3. Test properties, filters, and search.

   To test that document properties have been configured to enable filters and search, browse to the test folder, and perform a search using the same expression used by the filter you are testing. Either cut and paste the text from the filter into the portal search box or use the Advanced Search tool to enter expressions involving properties. Select **Search Only in this Folder**. The links that are returned by your search are for the documents that will pass your filter.

7.13.20 Troubleshooting the Results of a Crawl

There are several things you can troubleshoot if your content crawler does not import the expected content.

- Ensure that your folder filters are correctly filtering content.

  To learn about testing your filters, see Section 7.7.4, "Testing Filters."

- Ensure that your content crawler did not place unwanted content into the target folder.

  If a document does not filter into any subfolders, your content crawler might place the document in the target folder. This is determined by a setting on the Main Settings page of the Folder Editor.

- Ensure that the content crawler did not place content into the Unclassified Documents folder.

  If a document cannot be placed in any target folders or subfolders, your content crawler might place the document in the Unclassified Documents folder. This is determined by a setting on the Advanced Settings page of the Content Crawler Editor.

  If you have the correct permissions, you can view the Unclassified Documents folder when you are editing the Knowledge Directory or by clicking **Administration**, then, in the **Select Utility** list, select **Access Unclassified Documents**.

- Ensure that you have at least Edit access to the target folder.

- For Web content crawlers, ensure that the robot exclusion protocols or any exclusions or inclusions are not keeping your content crawler from importing the expected content.

This is determined by a setting on the Web Page Exclusions page of the Content Crawler Editor.

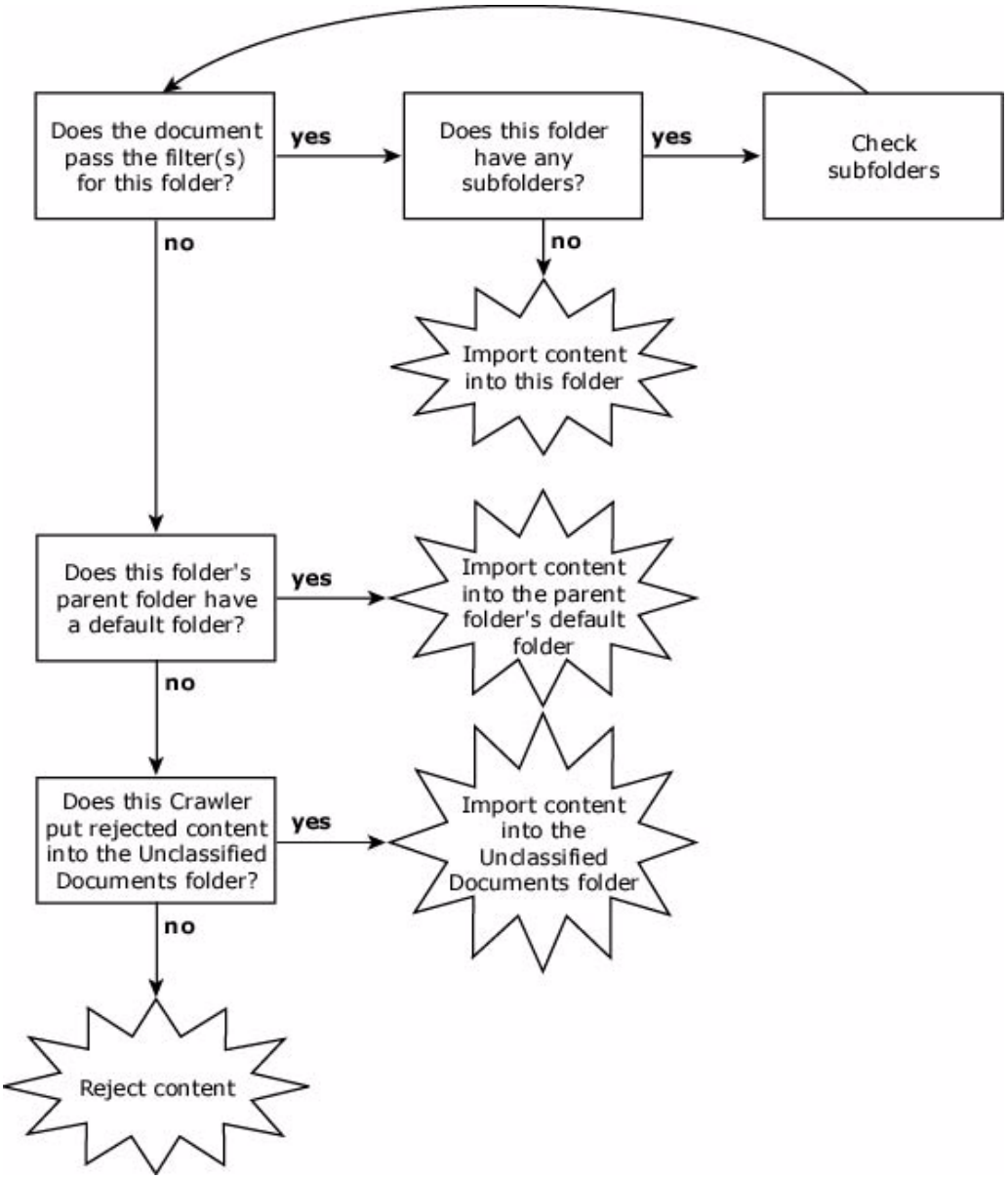
- Ensure that the authentication information specified in the associated content source allows the portal to access content.
- Review the job history for additional information.

7.13.21 Destination Folder Flowchart

This flowchart shows how a content crawler determines into which folders to import content. The process starts in the upper-left corner. The content crawler goes through this process for the destination folder you select and then continues down the levels of subfolders, if necessary. The content crawler repeats this process for each destination folder you add to the Main Settings page of the Content Crawler Editor.

If the content crawler is set to ignore the filters of destination folders, the first step in this flowchart is treated as if the document passes the filters for the folder. Be aware that only the filters of the destination folders will be ignored; if the destination folder has any *subfolders* with filters, these subfolder filters will not be ignored.

Note: If the document does not pass the filters of the destination folder, the content crawler checks to see if the destination folder has a default folder. It is only for subfolders of the destination folder that the content crawler checks to see if the *parent folder* has a default folder.



7.14 Mapping External Document Security to Imported Portal Users with the Global ACL Sync Map

Users imported through an authentication source can automatically be granted access to the content imported by some remote content crawlers through mappings in the Global ACL Sync Map. The Global ACL Sync Map maps authentication source prefixes to domain names and external groups to portal groups.

Every authentication source has a prefix. This prefix is used to distinguish the users and groups imported through the authentication source. If you plan to import security information with imported content, you might must map your authentication source prefixes to the source domains or map portal groups to external groups through the Global ACL Sync Map.

When a content crawler finds an ACL entry for a source document referring to any of the mapped external groups, the content crawler replaces the external group name with a reference to the mapped portal group.

You can use these mappings to unify disparate group names existing across document repositories. For example, you might want make Notes documents that are available to the Notes group Engineers and Exchange messages that are available to the Exchange group Engineering available to the portal group Developers. To do so, you would add the Developers group to this page and map "Engineers,Engineering" to it.

The Global ACL Sync Map is used by content crawlers bringing security settings, in the form of Access Control Lists (ACLs), into your portal along with documents. The Global ACL Sync Map shows content crawlers how the users and groups found on source document ACLs correspond with portal users and groups. Using this information, a content crawler can set portal security on imported content. For an example-based explanation of this process, see Section 7.10.5, "Example of Importing Content Security."

To access the Global ACL Sync Map you must be a member of the Administrators group. To open the Global ACL Sync Map:

1. Click **Administration**.
2. From the Select Utility menu, choose **Global ACL Sync Map**.
3. On the Prefix: Domain Map page, map authentication source prefixes to source domains:
   - To add a prefix to the map, click **Add Mapping**; then, in the Select Authentication Sources dialog box, select the authentication sources you want to map and click **OK**.

     Note:

     - If your authentication source prefix matches the domain name, the mapping occurs automatically and you do not must add the mapping to this page.
     - If more than one authentication source uses the same prefix, you only must map one of the authentication sources.

   - To edit the prefix in this mapping (this will not affect the prefix in the authentication source), in the **Authentication Source Prefix** column, click the edit icon. In the text box that displays, edit the name, then click the arrow icon to save your change.
   - To specify which domains map to a selected prefix, in the **Domain Name** column, click the edit icon and, in the text box that displays, type the domains you want to map, separated by commas (,). Click the arrow icon to save the mapping.
   - To remove a mapping, select the mapping and click the remove icon.
   - To select or clear all of the mapping check boxes, select or clear the box to the left of **Authentication Source Prefix**.
   - To toggle the order in which the mappings are sorted (ascending/descending), click **Authentication Source Prefix** or click the icon to the right of that.
4. On the left, under Utility Settings, click **Portal: External Group Map**.
5. On the Portal: External Group Map, map portal groups to external groups:

- To add a portal group to the map, click **Add Mapping**; then, in the Select Groups dialog box, select the groups you want to map and click **OK**.
- To edit the portal group name in this mapping (this will not affect the actual portal group), in the Portal Group Name column, click the edit icon. In the text box that displays, edit the name, then click the arrow icon to save your change.
- To specify which external groups map to a selected portal group, in the External Group Name column, click the edit icon and, in the text box that displays, type the external groups you want to map, separated by commas (,). Click the arrow icon to save the mapping.
- To remove a mapping, select the mapping and click the remove icon.
- To select or clear all of the mapping check boxes, select or clear the box to the left of **Portal Group Name**.
- To toggle the order in which the mappings are sorted (ascending/descending), click **Portal Group Name** or click the icon to the right of that.

7.15 About Snapshot Queries

Snapshot queries enable you to display the results of a search in a portlet or e-mail the results to users. You can select which repositories to search (including Oracle WebCenter Collaboration), and limit your search by language, object type, folder, property, and text conditions.

7.16 Working with Snapshot Queries

This section describes the following tasks:

- Section 7.16.1, "Creating a or Editing a Snapshot Query"
- Section 7.16.3, "Defining Snapshot Query Conditions"
- Section 7.16.4, "Limiting a Snapshot Query"
- Section 7.16.5, "Formatting the Results of a Snapshot Query"
- Section 7.16.6, "Previewing the Results of a Snapshot Query"
- Section 7.16.7, "E-mailing the Results of a Snapshot Query"
- Section 7.16.8, "Creating a Snapshot Portlet to Display the Results of a Snapshot Query"

7.16.1 Creating a or Editing a Snapshot Query

To create a snapshot query you must have the following rights and privileges:

- Access Administration activity right
- Create Snapshot Queries activity right
- At least Edit access to the parent folder (the folder that will store the snapshot query)
- At least Select access to any properties by which you want to filter your results
- At least Select access to any Knowledge Directory or administrative folders to which you want to restrict your results

To edit a snapshot query you must have the following rights and privileges:

- Access Administration activity right
- At least Edit access to the snapshot query
- At least Select access to any properties by which you want to filter your results
- At least Select access to any Knowledge Directory or administrative folders to which you want to restrict your results

To create or edit a snapshot query:

1. Click **Administration**.
2. Open the Snapshot Query Editor.
   - To create a snapshot query, open the folder in which you want to store the snapshot query. In the Create Object list, click **Snapshot Query**.
   - To edit snapshot query, open the folder in which the snapshot query is stored and click the snapshot query name.
3. On the Construct Snapshot Query page, perform tasks as necessary:
   - Section 7.16.3, "Defining Snapshot Query Conditions"
   - Section 7.16.4, "Limiting a Snapshot Query"
4. On the Format Snapshot Query Result page, perform tasks as necessary:
   - Section 7.16.5, "Formatting the Results of a Snapshot Query"
5. On the Preview Snapshot Query Result page, perform tasks as necessary:
   - Section 7.16.6, "Previewing the Results of a Snapshot Query"
6. On the Snapshot Portlet List page, perform tasks as necessary:
   - Section 7.16.8, "Creating a Snapshot Portlet to Display the Results of a Snapshot Query"
7. On the Properties and Names page, perform tasks as necessary:
   - Section 5.15, "Naming and Describing an Object"

     You can instead enter a name and description when you save this snapshot query.
   - Section 5.16, "Managing Object Properties"
8. On the Security page, perform tasks as necessary:
   - Section 5.17, "Setting Security on an Object"

   The default security for the snapshot query is based on the security of the parent folder.
9. If you are editing a snapshot query, on the Migration History and Status page, perform tasks as necessary:
   - Section 5.18, "Viewing Migration History and Status for an Object"

   Note: The Migration History and Status page is not available when creating an object.

If you did not create a snapshot portlet on the Snapshot Portlet List page, a snapshot portlet is automatically created when you save this snapshot query.

7.16.2 Deleting a Snapshot Query

To delete snapshot query you must have the following rights and privileges:

- Access Administration activity right
- Admin access to the snapshot query

To delete snapshot query:

1. Click **Administration**.
2. Navigate to the snapshot query.
3. Select the snapshot query you want to delete and click the delete icon.

> **Note:** Deleting a snapshot query will break any associated snapshot portlets.

7.16.3 Defining Snapshot Query Conditions

A snapshot query is a combination of a basic fields search and statements. The basic fields search operates on the name, description, and content of documents and objects. Statements can operate on the basic fields or any other additional document or object properties. Statements define what must or must not be true to return the document or object in the results. The statements are collected together in groupings. The grouping defines whether the statements are evaluated with an AND operator (all statements are true) or an OR operator (any statement is true). If some statements should be evaluated with an AND operator and some should be evaluated with an OR operator, you can create separate groupings for the statements. You can also create subgroupings or nested groupings, where one grouping is contained within another grouping. The statements in the lowest-level grouping are evaluated first to define a set of results. Then the statements in the next highest grouping are applied to that set of results to further filter the results. The filtering continues up the levels of groupings until all the groupings of statements are evaluated.

A snapshot query needs at least a basic fields search or a statement.

1. If the Snapshot Query Editor is not already open, open it now.
2. Click the **Construct Snapshot Query** page.
3. To search the name, description, and content values, type the text you want to search for in the **Basic fields search** text box.

   You can use the text search rules described in Section F.3, "Using Text Search Rules."
4. Select the operator for the grouping of statements you are about to create:
   - If a document or object should be returned only when all statements in the grouping are true, select **AND**.
   - If a document or object should be returned when any statement in grouping is true, select **OR**.

Note: The operator you select for a grouping applies to all its statements and subgroupings directly under it.

5. Define each statement in the grouping:
   a. Click **Add Statement**.
   b. In the first list, select the searchable property for which you want to filter the values.
   c. In the second list, select the operator to apply to this condition.

      This list will vary depending on the property selected:

      – For any text property, you can search for a value that contains your search string, or you can search for properties that have never had a value (**Contains No Value**).

      Note: If the property contained a value at some point, but the value has been deleted, the property will not match the Contains No Value condition.

      – For any date property, you can search for a value that comes after, comes before, is, or is not the date and time you enter in the boxes. You can also search for a value within the last number of minutes, hours, days, or weeks that you enter in the box.
      – For any number property, you can search for a value that is greater than, is less than, is, is not, is greater than or equal to, or is less than or equal to the number you enter in the text box.

   d. In the box (or boxes), specify the value the property must meet.

      Note: If you are searching for a text property, you can use the text search rules described in Section F.3, "Using Text Search Rules."

   To remove the last statement in a grouping, select the grouping, and click **Remove Statement**.
6. If necessary, add more statements by repeating Step 4.
7. If necessary, add more groupings:
   - To add another grouping, select the grouping to which you want to add a subgrouping, click **Add Grouping**, then define the statements for that grouping (as described in Step 4).

     Note: You cannot add a grouping at the same level as **Grouping 1**.

   - To remove a grouping, select the grouping, and click **Remove Grouping**.

Note:

- Any groupings and statements in that grouping will also be removed.
- You cannot remove **Grouping 1**.

You might also want to limit your search by language, object types, or folders.

7.16.4 Limiting a Snapshot Query

You can limit your snapshot query to specific languages, portal repositories, objects, folders, projects, or portlets.

1. If the Snapshot Query Editor is not already open, open it now.
2. Click the **Construct Snapshot Query** page.
3. To limit your search to a specific language, under Limit Search by Document Language, select a language from the **Specify Language** list.
4. Under Specify Range of Search, select which of the repositories to search: Knowledge Directory, Portal (administrative objects), Oracle WebCenter Collaboration.

   You will see a check box for **Collaboration** only if you have this product installed.
5. Next to Repository General Settings, choose whether to search folders or documents from any source within the repositories you selected, and whether to search all subfolders within those repositories.
6. If you selected the Knowledge Directory as one of the repositories to search, specify settings under Knowledge Directory Search Settings.
   - Next to Search Results Contain, select **Knowledge Directory Folders**, and/or **Knowledge Directory Documents**.

     Note: You must select at least one of these options.

   - To restrict the search to selected folders, click **Add Document Folder**, in the Add Document Folder dialog box, select the folders to which you want to restrict your search and click **OK**.
   - To remove a folder, select it and click the Remove icon.
7. If you selected the portal as one of the repositories to search, specify settings under Portal Search Settings.
   - Next to Search Results Contain, select the portal administrative object types to include in the search, such as portlets or communities.

     Note: To select or clear all the object types, select or clear the box next to All Types.

   - To restrict the search to selected folders, click **Add Administrative Folder**, in the Add Administrative Folder dialog box, select the folders to which you want to restrict your search and click **OK**.

- To remove a folder, select it and click the Remove icon.

8. If you selected **Collaboration** as one of the repositories to search, under Restrict to Selected Collaboration Projects, click **Add Project** to select one or more Oracle WebCenter Collaboration projects to search, then click **Finish**.

Next, specify the format for your results.

7.16.5 Formatting the Results of a Snapshot Query

You can define how your snapshot query results appear. By default, results are listed in order of relevance; that is, those results that most closely match your query are listed first. You can change the order in which results are displayed, limit the number of items returned, specify a style in which the snapshot portlet will be displayed, and e-mail results to users.

1. If the Snapshot Query Editor is not already open, open it now.
2. Click the **Format Snapshot Query Result** page.
3. In the **Maximum items displayed** box, type the number of items that should appear on a page.
4. In the Order results by list, select the property type by which you want to sort results.

> **Note:** You can sort by only numeric fields. For example, you can sort your search results by Content Type ID or Object Last Modified.

5. To select the available fields for display on search results, under Query Return Fields, click **Add Query Fields**, select the fields you want to add, and click **OK**.

   The fields you add here can be selected in the administrative preferences of snapshot query portlets associated with this snapshot query. Selecting all or a subset of these fields in the administrative preferences of a particular snapshot query portlet determines what end users see in results appearing in that portlet.

6. If you want the content snapshot portlet to appear with a subscribe button that enables users to receive e-mail about search results, select **Enable e-mail subscriptions**.

> **Note:**
>
> - You must configure an external operation to send e-mail notifications for this snapshot query. See Section 7.16.7, "E-mailing the Results of a Snapshot Query."
> - Users receive the e-mail only if their e-mail addresses are available in their user profiles.

Next, preview your results.

7.16.6 Previewing the Results of a Snapshot Query

You can preview the results of a snapshot query before you save it.

1. If the Snapshot Query Editor is not already open, open it now.
2. Click the **Preview Snapshot Query Result** page.

The fields displayed in these results are the ones you added on the Format Snapshot Query Result page, under Query Return Fields. However, for each snapshot portlet associated with this query, you can select all or a subset of the available query return fields in the portlet's administrative preferences.

Next, create a snapshot portlet on the **Snapshot Portlet List** page or save the snapshot query to automatically create a snapshot portlet.

7.16.7 E-mailing the Results of a Snapshot Query

You can e-mail the results of a snapshot query to users by creating an external operation and editing SavedSearchMailer.bat for Windows or SavedSearchMailer.sh for UNIX or Linux.

Before you create an external operation to e-mail the results of a snapshot query, you must create the snapshot query and snapshot portlet.To create an external operation you must have the following rights and privileges:

- Access Administration activity right
- At least Edit access to the Snapshot Query Mailer external operation
- At least Edit access to the parent folder (the folder that will store the external operation)
- At least Select access to the job that will run this external operation or Create Jobs activity right to create a job to run this external operation

To email the results of a snapshot query:

1. If you have not already done so, edit SavedSearchMailer.bat for Windows or SavedSearchMailer.sh for UNIX or Linux to specify the settings for your mail server and customize the e-mail values.

   The saved search mailer file is located on the computer that hosts the Automation Service, in *install_dir*\scripts (for example, C:\Oracle\Middleware\wci\ptportal\10.3.3\scripts for Windows or /oracle/middleware/wci/ptportal/10.3.3/scripts for UNIX or Linux).You must replace the following argument values:

Argument	Description
SENDER	The name you want to display as the From value in the automated e-mails
MAIL_ SERVER	Your SMTP mail server
REPLYTO	The e-mail address that users can reply to from the automated e-mails

Optionally, you can replace the following argument values:

Argument	Description
USER	The name of the user you want to send the automated e-mails
PWD	The password for the user that will send the automated e-mails
MIMETYPE	The MIME type you want to use for the automated e-mails
SUBJECT	The text you want to display in the automated e-mail subject line By default the subject includes the name of the snapshot query (represented by `<search_name>`) and the name of the user receiving the results (represented by `<name>`).

Argument	Description
BODY_ HEADER	The text you want to display at the top of the automated e-mail body
BODY_ SEPARATOR	Any code you want to use to generate a separation between the header and the results
BODY_ FOOTER	The text you want to display at the bottom of the automated e-mail body

2. In the portal, click **Administration**.
3. Open the snapshot portlet for which you want to e-mail results.
4. Click the **Properties and Names** page.
5. Copy or make note of the **Object ID**, then close the snapshot portlet.
6. Open the **Intrinsic Operations** folder.
7. Select the **Snapshot Query Mailer** external operation and click the External Operation icon.
8. In the Target Folder dialog box, select the folder in which you want to store your new external operation and click **OK**.
9. Open the copy of the snapshot query mailer you just created.
10. Replace `200` in the arguments with the object ID of the snapshot query you want to e-mail.
11. Click the **Set Job** page and complete the following task:
    - Section 5.14, "Associating an Object with a Job"
12. Click the **Properties and Names** page and rename the external operation.

Set the job to run on a regular basis.

7.16.8 Creating a Snapshot Portlet to Display the Results of a Snapshot Query

You can create a snapshot portlet to display the results of a snapshot query on a portal page.

- To create a content snapshot portlet associated with this snapshot query, click **Create Content Snapshot Portlet**.

  The portlet appears under **Portlet List**, and is added to the same administrative folder as this snapshot query.

  Note:

  - If you create a content snapshot portlet manually (rather than having one automatically created when saving the snapshot query), the name of the portlet will be New Snapshot Query.
  - If you do not manually create a content snapshot portlet on this page, one will be created automatically when you save the snapshot query; the portlet will have the same name as the snapshot query.
  - To delete a snapshot portlet, you must delete it from the administrative folder that contains its associated snapshot query.

- To change the name of a snapshot portlet:
  1. Click the portlet name.

     The Portlet Editor opens.
  2. Click the **Properties and Names** page.
  3. Edit the name.
- To select the fields displayed in the results and the fields that users can search on.for a snapshot portlet, edit the administrative preferences:
  1. Click the portlet name.

     The Portlet Editor opens.
  2. Click the **Edit** button next to **Configure this Portlet**.
  3. Edit the preferences.

Users with at least Select access to this portlet can now add this portlet to their My Pages. Community administrators with at least Select access to this portlet can now add this portlet to their communities.

8

Extending Portal Services with Portlets

This chapter explains how to extend the services available through the portal, through the use of portlets.

It includes the following sections:

8.1 About Portlet Components and Features

This section describes the components and features involved in providing access to tools, service, and information with portlets:

8.1.1 Portlets

Portlets provide portal users customized tools and services as well as information. Portlets let you to integrate applications, tools, and services into your portal, while taking advantage of portal security, caching, and customization. Users can then add these portlets to their My Pages or to community pages.

Portlets can be intrinsic or remote. An intrinsic portlet consists of one or more sets of code that are located on the portal computer. This code must be installed in the correct location before an intrinsic portlet can be created. A remote portlet is a portlet hosted

by a separate remote server. When a user displays a My Page or community page that includes a remote portlet, the portal contacts the appropriate remote server to obtain updated portlet content.

Some portlets can be placed only in certain areas of the page:

- Header portlets can be added to communities, community templates, and experience definitions to change the branding of these objects by replacing a banner at the top of the page (so that it differs from the top banner displayed by the main portal).
- Footer portlets can be added to communities, community templates, and experience definitions to change the branding of these objects by replacing the banner at the bottom of the page (so that it differs from the bottom banner displayed by the main portal).
- Content canvas portlets can be added below the top banner on community pages that include a content canvas space (specified in the page layout). Content canvas portlets can display across the entire width of the page or across one or two columns. You cannot add more than one content canvas portlet per page.

8.1.2 Pagelets

Pagelets are similar to portlets; they provide customized tools, services, or information. The difference is that pagelets are created in Oracle WebCenter Pagelet Producer. You make pagelets available to portal users by creating a remote pagelet Web service, then creating a portlet based on the remote pagelet Web service.

8.1.3 Lockboxes and the Credential Vault Manager

You can provide secure portal access to existing Web applications by setting up lockboxes to store user credentials. For example, you might want to provide portal access to a secured employee benefits system. Users can enter their user authentication information through the Password Manager on the My Account page and not have to enter the information each time they access the secured application through the portal.

The lockboxes are stored in the Credential Vault Manager.

8.1.4 Portlet Web Services

Portlet Web services allow you to specify *functional* settings for your portlets, leaving the *display* settings to be set in each associated portlet. There are intrinsic portlet Web services and remote portlet Web services.

An intrinsic portlet Web service references one or more sets of code that are located on the portal computer. This code must be installed in the correct location before you can create the associated intrinsic portlet Web service.

A remote portlet Web service references services hosted by a separate remote server. These services can be hosted by a Web site or can be provided by code on a remote server. If the code is hosted by a remote server, this code must be installed before you can create the associated remote portlet Web service. When a user displays a My Page or community page that includes a remote portlet, the portal contacts the appropriate remote server to obtain updated portlet content.

8.1.5 Portlet Templates

Portlet templates allow you to create multiple instances of a portlet, each displaying slightly different information. For example, you might want to create a Regional Sales

portlet template, from which you could create different portlets for each region to which your company sells. You might even want to include all Regional Sales portlets on one page for an executive overview.

After you have created a portlet from a portlet template, there is no further relationship between the two objects. If you make changes to the portlet template, these changes are not reflected in the portlets already created with the template.

8.1.6 Portlet Bundles

Portlet bundles are groups of related portlets, packaged together for easy inclusion on My Pages or community pages. You might want to create portlet bundles for portlets that have related functions or for all the portlets that a particular group of users might find useful. This makes it easier for users to find portlets related to their specific needs without having to browse through all the portlets in your portal.

8.1.7 Portlet Content Caching

Caching some portlet content can greatly improve the performance of your portal. When you cache portlet content, the content is saved on the portal for a specified period. Each time a user requests this content—by accessing a My Page or community page that includes the cached portlet—the portal delivers the cached content rather than running the portlet code to produce the content.

When you create a portlet, you can specify whether the portlet should be cached, and if it is cached, for how long. You should cache any portlet that does not provide user-specific content. For example, you would cache a portlet that produces stock quotes, but not one that displays a user e-mail box.

If you develop portlet code, you can and should define caching parameters.

For more information on portlet caching, refer to the *Oracle Fusion Middleware Web Service Developer's Guide for Oracle WebCenter Interaction* or the documentation provided with the portlet software.

8.1.8 Portlet Preferences

Portlets can includes several different types of preferences.

Preference Type	Description	Who Can Set Them and Where
Administrative Preferences	These preferences affect everyone's view of the portlet. For example, setting which e-mail server an e-mail portlet should connect to.	They are set by the portlet creator on the Main Settings page of the Portlet Editor, or by users with administrative rights from **My Pages** > **Edit Portlet Preferences** or by clicking the edit icon in a portlet's title bar.
Personal Preferences	These preferences affect that user's view of the portlet. For example, setting how many e-mails are displayed in an e-mail portlet.	They are set by the user from **My Pages** > **Edit Portlet Preferences** or **My Communities** > **Edit Portlet Preferences**.

Preference Type	Description	Who Can Set Them and Where
Community Preferences	These preferences affect everyone's view of portlets in that community. For example, setting a specific public e-mail folder to display in an e-mail portlet, and setting a shared login/password for that folder.	These preferences are set by the community administrator on the **Portlet Preferences** page of the Community Editor. This page can include community preferences for portlets specific to that community or for other portlets. When in a community, community administrators can edit these preferences from **My Communities** > **Edit Portlet Preferences**, or by clicking the edit icon in a portlet's titlebar.
Portlet Template Preferences	These preferences affect the portlet template itself and all portlets created from that template. For example, specifying which portlet Web service a portlet uses.	These preferences are set by the portlet template creator on the **Main Settings** page of the Portlet Template Editor. If you change these preferences after portlets have been created from this template, the change will affect only new portlets. Portlets created from this template before the change was made will not be affected.

8.1.9 Portlets Available with the Portal

Some portlets (and their necessary portlet Web services and remote servers) are automatically created in the Portal Resources folder when you install the portal. There are also portlets that are available with the portal installation, but require additional steps to complete installation. For information on the additional installation steps, refer to the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Interaction for Windows* or the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Interaction for Unix and Linux*.

> **Note:** You can also create your own portlets, have a Web developer or an Oracle portlet developer create portlets for you, or download portlets from the Oracle Technology Network. For information on installing and configuring portlets provided as a software package, refer to the portlet software documentation instead of the procedures in this guide. For information on developing portlets, see the *Oracle Fusion Middleware Web Service Developer's Guide for Oracle WebCenter Interaction*.

This section describes the types of portlets and portlet templates available with the portal installation:

- Section 8.1.9.1, "Navigation Portlet"
- Section 8.1.9.2, "Branding Portlets"
- Section 8.1.9.3, "Login Portlets"
- Section 8.1.9.4, "User Profile Portlets"
- Section 8.1.9.5, "My Pages, Community Pages, and Default Profile Pages Portlets"
- Section 8.1.9.6, "Portlet Templates"

8.1.9.1 Navigation Portlet

The following navigation portlet can be used with the Portlet-Ready Navigation scheme (set in an experience definition) to provide custom navigation for your portal:

- **Navigation Tags Header Portlet**: This portlet is provided as an example of a custom header that includes navigation tags; you can customize it and use it in communities or experience definitions. This portlet is stored in the Portal Resources folder.

  Note: The Tag Navigation experience definition is also included in the portal as a convenience when you are using portlets for navigation. This experience definition uses the Portlet-Ready Navigation scheme and has the Navigation Tags Header Portlet set as its header.

8.1.9.2 Branding Portlets

The following branding portlets enable you to add custom branding to your portal pages:

- **Classic Footer Portlet**: This portlet is provided as an example of a custom footer that you can customize and use in communities or experience definitions.
- **Classic Header Portlet**: This portlet is provided as an example of a custom header that you can customize and use in communities or experience definitions.
- **Layout Footer Portlet**: This portlet is provided as an example of a custom footer that uses adaptive tags; you can customize it and use it in communities or experience definitions.
- **Layout Header Portlet**: This portlet is provided as an example of a custom header that uses adaptive tags; you can customize it and use it in communities or experience definitions.

8.1.9.3 Login Portlets

The following login portlets can be added to guest default profiles so users can log in to the portal:

- **Portal Login**: This portlet allows users to log in to the portal. You probably want to add this to all your guest users' home pages so that users can log in from the default page displayed when they navigate to your portal.
- **Tag Login Portlet**: This portlet is provided as an example of a custom login portlet that uses adaptive tags; you can customize it and add it to your guest users' home pages so that users can log in from the default page displayed when they navigate to your portal. This portlet is stored in the Portal Resources folder. For information on adaptive tags, see the Adaptive Page Layouts section of the *Oracle Fusion Middleware User Interface Customization Guide for Oracle WebCenter Framework Interaction*.

8.1.9.4 User Profile Portlets

The following user profile portlets are included on the user profile page by default:

- **Folder Expertise**: This portlet displays the folders for which the user is an expert. Administrative users with at least Edit access to the folder and at least Select access to the user can add the user to the folder as an expert through the Related Resources page of the Folder Editor, or, if users have the Self-Selected Experts

activity right, they can add themselves as experts when they are browsing folders in the Knowledge Directory. This portlet is stored in the Portal Resources folder and is displayed on the user profile page by default.

- **General Information**: This portlet displays user profile information such as name and address, but an administrative user with at least Edit access to the portlet can configure the portlet to display any information. If your portal displays a legacy layout (rather than adaptive layouts), this portlet is displayed on the user profile page by default. This portlet is stored in the Portal Resources folder.
- **Managed Communities**: This portlet displays the communities to which the user has Edit or Admin access. If your portal displays a legacy layout (rather than adaptive layouts), this portlet is displayed on the user profile page by default. This portlet is stored in the Portal Resources folder.

8.1.9.5 My Pages, Community Pages, and Default Profile Pages Portlets

The following portlets are ready to be added to My Pages, community pages, and default profile pages:

- **Job Histories Intrinsic Portlet**: This portlet displays the same job history information that is displayed on the Job History page of the Automation Service Manager. This portlet is stored in the Portal Resources folder.
- **Portal Search**: This portlet lets users search your portal and access their saved searches. Users might want to add this to their home page for easy access to their saved searches. This portlet is stored in the Portal Resources folder.
- **RSS Reader Portlet**: This portlet lets users specify an RSS or ATOM feed to display on a My Page. This portlet is stored in the Portal Resources/RSS Reader folder, but is available only if the Remote Portlet Service was installed and the RSS Reader migration package was imported.
- **RSS Community Reader Portlet**: This portlet lets community managers specify an RSS or ATOM feed to display on a community page. This portlet is stored in the Portal Resources/RSS Reader folder, but is available only if the Remote Portlet Service was installed and the RSS Reader migration package was imported.
- **User Activities**: This portlet displays a user's status history and any other recent activities that are submitted by other applications. This portlet is stored in the Activity Service folder, but is available only if the Remote Portlet Service was installed and the Activity Service migration package was imported.

  To view another user's activities, open the user's profile and look at the User Activities portlet displayed in the profile. To subscribe to e-mail notification or an RSS feed of the user's activity, click the appropriate button at the bottom of the user's User Activities portlet.
- **User Status**: This portlet lets users post their current status. This portlet is stored in the Activity Service folder, but is available only if the Remote Portlet Service was installed and the Activity Service migration package was imported.

8.1.9.6 Portlet Templates

The following portlet templates (and any necessary portlet Web services and remote servers) are created when you install the portal:

- **Community Links Portlet Template**: This template is used by the portal to create portlets that display the links saved in a Community Knowledge Directory folder. This portlet template is stored in the Portal Resources folder.

- **Content Snapshots**: This template is used by the portal to create portlets that display the results of a Snapshot Query. This portlet template is stored in the Portal Resources folder.

8.2 Working with Portlet Web Services

This section describes the following main tasks:

- Section 8.2.1, "Creating or Editing an Intrinsic Portlet Web Service"
- Section 8.2.2, "Creating or Editing a Remote Portlet Web Service"
- Section 8.2.3, "Deleting a Portlet Web Service"

It also covers the following low-level tasks:

- Section 8.2.4, "Adding Help to Portlets"
- Section 8.2.5, "Associating User Profile Information with Intrinsic Portlets"
- Section 8.2.6, "Sending General Settings from a Remote Portlet Web Service to Associated Portlets"
- Section 8.2.7, "Associating a Lockbox with a Remote Portlet Web Service"
- Section 8.2.8, "Associating a Login Form with a Remote Portlet Web Service"
- Section 8.2.9, "Adding Preference Pages to Intrinsic Portlets"
- Section 8.2.10, "Adding Preference Pages to Remote Portlets"
- Section 8.2.11, "Specifying Alternative Browsing Device Support for a Portlet Web Service"

8.2.1 Creating or Editing an Intrinsic Portlet Web Service

Before you create an intrinsic portlet Web service, you must:

- Install the portlet code on the computer that hosts the portal

To create an intrinsic portlet Web service you must have the following rights and privileges:

- Access Administration activity right
- Create Web Service Infrastructure activity right
- At least Edit access to the parent folder (the folder that will store the intrinsic portlet Web service)
- At least Select access to the remote server that the intrinsic portlet Web service will use

To edit an intrinsic portlet Web service you must have the following rights and privileges:

- Access Administration activity right
- At least Edit access to the intrinsic portlet Web service
- If you plan to change the remote server association, at least Select access to the remote server that the intrinsic portlet Web service will use

To create or edit an intrinsic portlet Web service:

1. Click **Administration**.

2. Open the Intrinsic Portlet Web Service Editor.
   - To create an intrinsic portlet Web service, open the folder in which you want to store the intrinsic portlet Web service. In the Create Object list, click **Web Service — Intrinsic Portlet**.
   - To edit an intrinsic portlet Web service, open the folder in which the intrinsic portlet Web service is stored and click the intrinsic portlet Web service name.
3. On the Main Settings page, perform tasks as necessary:
   - In the **Portlet Class Identifier** box, type the "STR_MVC_CLASS_NAME" string variable that is defined in the model for your intrinsic portlet.
   - Section 3.4.4, "Enabling and Disabling a Web Service"
4. On the Advanced Settings page, perform tasks as necessary:
   - Section 8.2.4, "Adding Help to Portlets"
   - Section 8.2.5, "Associating User Profile Information with Intrinsic Portlets"
5. On the Preferences page, perform tasks as necessary:
   - Section 8.2.9, "Adding Preference Pages to Intrinsic Portlets"
6. On the Alternative Browsing Devices page, perform tasks as necessary:
   - Section 8.2.11, "Specifying Alternative Browsing Device Support for a Portlet Web Service"
7. On the Properties and Names page, perform tasks as necessary:
   - Section 5.15, "Naming and Describing an Object"

     You can instead enter a name and description when you save this intrinsic portlet Web service.
   - Section 5.16, "Managing Object Properties" (optional)
8. On the Security page, perform tasks as necessary:
   - Section 5.17, "Setting Security on an Object"

   The default security for this intrinsic portlet Web service is based on the security of the parent folder. Administrative users with at least Select access to this intrinsic portlet Web service and the Create Portlets activity right can create portlets or portlet templates based on the Web service.
9. If you are editing an intrinsic portlet Web service, on the Migration History and Status page, perform tasks as necessary:
   - Section 5.18, "Viewing Migration History and Status for an Object"

   Note: The Migration History and Status page is not available when creating an object.

8.2.2 Creating or Editing a Remote Portlet Web Service

Before you create a remote portlet Web service, you must:

- Install the portlet code on the computer that hosts the portal or on another computer
- Create a remote server pointing to the computer that hosts the portlet code (optional, but recommended)

To create a remote portlet Web service you must have the following rights and privileges:

- Access Administration activity right
- Create Web Service Infrastructure activity right
- At least Edit access to the parent folder (the folder that will store the remote portlet Web service)
- At least Select access to the remote server that the remote portlet Web service will use

To edit a remote portlet Web service you must have the following rights and privileges:

- Access Administration activity right
- At least Edit access to the remote portlet Web service
- If you plan to change the remote server association, at least Select access to the remote server that the remote portlet Web service will use

To create or edit a remote portlet Web service:

1. Click **Administration**.
2. Open the Remote Portlet Web Service Editor.
   - To create a remote portlet Web service, open the folder in which you want to store the remote portlet Web service. In the Create Object list, click **Web Service — Remote Portlet**.
   - To edit a remote portlet Web service, open the folder in which the remote portlet Web service is stored and click the remote portlet Web service name.
3. On the Main Settings page, perform tasks as necessary:
   - Section 3.4.1, "Associating a Remote Server with a Web Service"
   - Section 3.4.2, "Specifying the Location of the Web Service Provider or Code"
   - Section 3.4.3, "Specifying Web Service Time-Out Settings"
   - Section 3.4.4, "Enabling and Disabling a Web Service"
4. On the HTTP Configuration page, perform tasks as necessary:
   - Section 3.4.5, "Specifying Caching Settings for a Web Service"
   - Section 3.4.6, "Specifying How Gatewayed Content is Handled"
   - Section 3.4.7, "Specifying What Content is Gatewayed for a Web Service"
5. On the Advanced URL Settings page, perform tasks as necessary:
   - Section 8.2.4, "Adding Help to Portlets"
   - Section 3.4.9, "Adding an Administrative Configuration Link to the Select Utility Menu"
   - Section 3.4.10, "Adding a User Configuration Link to the My Account Page"

   Note: Do not enter anything into the **Remote Migration URL** box; this box must be left blank. This feature is reserved for future use.

6. On the Advanced Settings page, perform tasks as necessary:

- Section 8.2.6, "Sending General Settings from a Remote Portlet Web Service to Associated Portlets"
- Section 3.4.12, "Sending Activity Rights from a Web Service to Associated Objects"

7. On the Authentication Settings page, perform tasks as necessary:
   - Section 8.2.7, "Associating a Lockbox with a Remote Portlet Web Service."
   - Section 3.4.13, "Specifying Authentication Settings for a Web Service"
   - Section 8.2.8, "Associating a Login Form with a Remote Portlet Web Service."
8. On the Preferences page, perform tasks as necessary:
   - Section 8.2.10, "Adding Preference Pages to Remote Portlets"
9. On the User Information page, perform tasks as necessary:
   - Section 3.4.15, "Sending User Information from a Web Service to Associated Objects"
10. On the Debug Settings page, perform tasks as necessary:
    - Section 3.4.16, "Enabling Error Tracing for a Web Service"
11. On the Alternative Browsing Devices page, perform tasks as necessary:
    - Section 8.2.11, "Specifying Alternative Browsing Device Support for a Portlet Web Service"
12. On the Properties and Names page, perform tasks as necessary:
    - Section 5.15, "Naming and Describing an Object"

      You can instead enter a name and description when you save this remote portlet Web service.
    - Section 5.16, "Managing Object Properties" (optional)
13. On the Security page, perform tasks as necessary:
    - Section 5.17, "Setting Security on an Object"

    The default security for this remote portlet Web service is based on the security of the parent folder. Administrative users with at least Select access to this remote portlet Web service and the Create Portlets activity right can create portlets or portlet templates based on the Web service.
14. If you are editing a remote portlet Web service, on the Migration History and Status page, perform tasks as necessary:
    - Section 5.18, "Viewing Migration History and Status for an Object"

    Note: The Migration History and Status page is not available when creating an object.

8.2.3 Deleting a Portlet Web Service

To delete a portlet Web service you must have the following rights and privileges:

- Access Administration activity right
- Admin access to the portlet Web service

To delete a portlet Web service:

1. Click **Administration**.
2. Navigate to the portlet Web service.
3. Select the portlet Web service you want to delete and click the delete icon.

> **Note:** Deleting a portlet Web service will break any associated portlets.

8.2.4 Adding Help to Portlets

If the portlets associated with the Web service have help, you can include a help button in the portlet title bar.

To add help to the portlets associated with a portlet Web service:

1. If the Intrinsic Portlet Web Service Editor is not already open, open it now.
2. Click the **Advanced Settings** page for an intrinsic portlet Web service or the **Advanced URL Settings** page for a remote pagelet Web service or a remote portlet Web service.
3. In the **Help Page** box, type the full URL to the help page (for example, `http://www.server.com/folder/helpfile.htm`).

> **Note:** The help page must be located on the computer hosting the Image Service.

8.2.5 Associating User Profile Information with Intrinsic Portlets

If the portlets associated with the Web service use user profile information and you intend to migrate this Web service at some time, you must specify this association in the Web service so that the user profile information is migrated with the Web service.

To associate user profile information with an intrinsic portlet Web service:

1. If the Intrinsic Portlet Web Service Editor is not already open, open it now.
2. On the left, under Edit Object Settings, click **Advanced Settings**.
3. Check the box next to **This Web Service depends on User Profile pages and sections** so the user profile information is migrated with the Web service.

8.2.6 Sending General Settings from a Remote Portlet Web Service to Associated Portlets

To specify what information the remote portlet Web service passes to associated portlets:

1. If the Remote Portlet Web Service Editor is not already open, open it now.
2. Click the **Advanced Settings** page.
3. Under Settings, specify what general information, if any, you want this Web service to pass to its associated portlets:
   - If the portlet is on a community page and you want to send the user's community security, select **Send Community ACL to Portlets**.
   - To send the ID number of the My Page or community page from which the portlet request is sent, select **Send Page ID to Portlets**.

- To send the time zone of the user from which the portlet request is sent, select **Send timezone to Portlets**.
- If this Web service requires the user to have an API session (for example, if the Web service uses the SOAP API), select **Send Login token to Portlets**; then, in the **Login Token duration** box, type the number of minutes you want the API session to last.
- To include a refresh button on the portlet, click **Show Portlet refresh button**. The refresh button appears in the title bar of portlets associated with this Web service. Users can then refresh this portlet by itself, rather than refresh the entire My Page or community that contains the portlet.
- To enable portlet session sharing, select **Share sessions with other Portlets on the same Remote Server**.
- To send the ID of the experience definition from which the portlet request is sent, select **Send Experience Definition ID to Portlets**.
- To send information on the portlet's alignment on the page from which the portlet is invoked, select **Send Portlet Alignment to Portlets**.

8.2.7 Associating a Lockbox with a Remote Portlet Web Service

A lockbox corresponds to an external Web application that users can access through the portal. To learn about lockboxes, see Section 8.6, "Working with Lockboxes."

To send credentials from a lockbox to portlets associated with a remote portlet Web service:

1. If the Remote Portlet Web Service Editor is not already open, open it now.
2. Click the **Authentication Settings** page.
3. Under Credential Vault Settings, click **Browse** to specify a lockbox for this portlet if applicable.

Note: To send credentials in portlet headers, using RSA public key/private key encryption, you must also enter the public key for RSA encryption in the remote server (on the Main Settings page) and use the IDK to provide the private key for RSA encryption (see the *Oracle Fusion Middleware Web Service Developer's Guide for Oracle WebCenter Interaction*).

8.2.8 Associating a Login Form with a Remote Portlet Web Service

If portlets associated with the Web service provide access to a remote application with a login form, specify the login form settings in the remote portlet Web service.

To associate a login form with a remote portlet Web service:

1. If the Remote Portlet Web Service Editor is not already open, open it now.
2. Click the **Authentication Settings** page.
3. Under Form Based Login, in the **Login URL** box, type the URL of the login form.
4. In the **Post URL** box, type the URL to which the login form posts.
5. Choose the credentials to be sent to the post URL:

- **None** - sends no credentials. Use this if you want to use the same user name and password for all users. If you select this, add the user name and password fields and their values under the Login Form Fields section of this page.
- **Portal** - sends the user's portal user name and password.
- **Lockbox** - sends the user's lockbox credentials for the lockbox you selected under Credential Vault Settings.

6. If you chose to send portal or lockbox credentials to the post URL, enter the names of the user name and password fields on the login form.
7. If the login form has additional fields, or you selected **N**one for the credentials to send to the post URL, add fields under Login Form Fields:
   - To add a field, click **Add Form Field**. Then enter the **Field Name** and the required **Field Value**.
   - To delete a form field, select it and click the delete icon.

8.2.9 Adding Preference Pages to Intrinsic Portlets

Some portlets might require preferences settings that are specific to that portlet. For example, you might have several portlets that use the same Web service, but can be configured to show different information based on an administrative, community manager, or user preference.

To add preference pages to an intrinsic portlet:

1. If the Intrinsic Portlet Web Service Editor is not already open, open it now.
2. On the left, under Edit Object Settings, click **Preferences**.
3. To specify the location of the logic used to display any preference pages associated with the Web service, type the "STR_MVC_CLASS_NAME" string variable that is defined in the activity space that contains the logic for your portlet preference pages:
   - **Administrative Preferences Activity Space**: These preferences are set by the portlet creator on the Main Settings page of the Portlet Editor. They affect everyone's view of the portlet.
   - **Portlet Template Preferences Activity Space**: These preferences are set by the portlet template creator on the Main Settings page of the Portlet Template Editor. They affect the portlet template itself and all portlets created from that template.

     Note: If you change these preferences after portlets have been created from the template, the change will affect only new portlets. Portlets created from the template before the change was made will not be affected.

   - **Portlet Preferences Activity Space**: These preferences are set by the user through the icon in the portlet title bar. They affect that user's view of the portlet.
   - **Community Preferences Activity Space**: These preferences are set by the community administrator on the Portlet Preferences page of the Community Editor (also accessible through the Edit Portlet Preferences option in the My

Communities menu). They affect everyone's view of the portlet in that community.

If the Web service does not have a particular type of preference page, leave that box blank. If you leave a box blank, you will not see the associated preferences link in the associated portlet or portlet editor.

8.2.10 Adding Preference Pages to Remote Portlets

Some portlets might require preferences settings that are specific to that portlet. For example, you might have several portlets that use the same Web service, but can be configured to show different information based on an administrative, community manager, or user preference.

To add preference pages to an intrinsic portlet:

1. If the Remote Portlet Web Service Editor is not already open, open it now.
2. On the left, under Edit Object Settings, click **Preferences**.
3. To specify the location of any preference pages associated with the Web service, type the path to the page (including the page name):

   Note: If you associated a remote server on the Main Settings page, you can type a relative path (/myPortlet/) or an absolute path (http://myServer/myPortlet/). If you enter an absolute path, ignore the base URL.

   - **Administrative Preferences URL**: These preferences are set by the portlet creator on the Main Settings page of the Portlet Editor. They affect everyone's view of the portlet.
   - **Portlet Template Preferences URL**: These preferences are set by the portlet template creator on the Main Settings page of the Portlet Template Editor. They affect the portlet template itself and all portlets created from that template.

     Note: If you change these preferences after portlets have been created from the template, the change will affect only new portlets. Portlets created from the template before the change was made will not be affected.

   - **Portlet Preferences URL**: These preferences are set by the user through the icon in the portlet title bar. They affect that user's view of the portlet.

     If you want to send user preferences (from either the User Configuration URL or the Portlet Preferences URL) from the Web service to associated portlets, you must specify them by name:

     – To send a user preference to the portlets associated with the Web service, type the name of the preference in the box below User Preferences.

     – To include more user preferences, click **Add User Preference**.

     – To delete a user preference, select the preference and click the delete icon.

Note: The Portlet Preferences URL differs from the User Configuration URL (specified on the Advanced URL Settings page) in the following ways:

- The Portlet Preferences URL displays a link on the Edit Portlet Preferences page, but the link displays only when the associated portlet is on the selected My Page or community page. However, the User Configuration URL displays a link on the My Account page to any user with at least Read access to the Web service.
- A user configuration page can include only user preferences. A portlet preferences page can include user preferences or portlet-specific preferences.

- **Community Preferences URL**: These preferences are set by the community administrator on the Portlet Preferences page of the Community Editor (also accessible through the Edit Portlet Preferences option in the My Communities menu). They affect everyone's view of the portlet in that community.

  If you want to send community preferences from the Web service to associated portlets, you must specify them by name:

  – To send a community preference to the portlets associated with the Web service, type the name of the preference in the box below User Preferences.

  – To include more community preferences, click **Add User Preference**.

  – To delete a community preference, select the preference and click the delete icon.

- **Session Preferences**: If you want to send session preferences from the Web service to associated portlets, you must specify them by name:

  – To send a session preference to the portlets associated with the Web service, type the name of the preference in the box below Session Preferences.

  – To include more session preferences, click **Add Session Preference**.

  – To delete a session preference, select the preference and click the delete icon.

If the Web service does not have a particular type of preference page, leave that box blank. If you leave a box blank, you will not see the associated preferences link in the associated portlet or portlet editor.

8.2.11 Specifying Alternative Browsing Device Support for a Portlet Web Service

If the portlets associated with the Web service supports alternative browsing devices, you must specify the supported devices in the Web service.

To specify alternative browsing device support for a portlet Web service:

1. If the Intrinsic Portlet Web Service Editor is not already open, open it now.
2. On the left, under Edit Object Settings, click **Alternative Browsing**.
3. Select the devices the portlet Web service supports:

- **Assistive Technology Portal**: This user interface supports assistive technology used by people with disabilities, such as screen readers, screen magnifiers, and speech recognition software.
- **Newer Phones and RIM devices**: This user interface is for users of phones that can display WML, which includes new phones and RIM Blackberry pagers.
- **Palm and Pocket PC**: This user interface is for users of personal digital assistants that can display HTML, like Palm-connected organizers and Pocket PCs.

4. If you are creating or editing a remote pagelet or remote portlet Web service and it includes a summary description of its contents, in the **Summary URL** box, type the URL to that description. This description displays when a user views portlets associated with this Web service on a wireless device.

Note: If you associated a remote server on the Main Settings page, the base URL displays to the left of the Summary URL box. You can either type a relative path, finishing the path that starts with the base URL (`/myPortlet/Summary.htm`), or you can type an absolute path, ignoring the base URL (`http://myServer/myPortlet/Summary.htm`).

8.3 Working with Remote Pagelet Web Services

This section describes the following main tasks:

- Section 8.3.1, "Creating the Oracle WebCenter Pagelet Producer Remote Server"
- Section 8.3.2, "Creating or Editing a Remote Pagelet Web Service"
- Section 8.3.3, "Deleting a Remote Pagelet Web Service"

It also covers the following low-level tasks:

- Section 8.3.4, "Selecting a Pagelet"
- Section 8.3.5, "Sending General Settings from a Remote Pagelet Web Service to Associated Portlets"
- Section 8.3.6, "Mapping Remote Pagelet Parameters to Portlet Preferences"

8.3.1 Creating the Oracle WebCenter Pagelet Producer Remote Server

Before you create the Oracle WebCenter Pagelet Producer remote server, you must:

- Install Oracle WebCenter
- Create pagelets in Oracle WebCenter Pagelet Producer

To create the Oracle WebCenter Pagelet Producer remote server you must be a member of the Administrators group.

1. Click **Administration**.
2. In the Select Utility list, click **Migration - Import**.
3. On the Package Settings page, select Web Address and type the following URL: `http://server:port/pageletadmin/pte`. Replace *`server`* with the name of the computer on which Oracle WebCenter Pagelet Producer is installed, and replace *`port`* with the port on which Oracle WebCenter Pagelet Producer runs.

4. Click **Finish**.

   The Pagelet Producer Remote Server is created in a new PageletProducer folder.

8.3.2 Creating or Editing a Remote Pagelet Web Service

Before you create a remote pagelet Web service, you must:

- Install Oracle WebCenter
- Create pagelets in Oracle WebCenter Pagelet Producer
- Create the Oracle WebCenter Pagelet Producer remote server

To create a remote pagelet Web service you must have the following rights and privileges:

- Access Administration activity right
- Create Web Service Infrastructure activity right
- At least Edit access to the parent folder (the folder that will store the remote pagelet Web service)
- At least Select access to the remote server that the pagetlet Web service will use

To edit a remote pagelet Web service you must have the following rights and privileges:

- Access Administration activity right
- At least Edit access to the remote pagelet Web service
- If you plan to change the remote server association, at least Select access to the remote server that the remote pagelet Web service will use

To create or edit a remote pagetlet Web service:

1. Click **Administration**.
2. Open the Remote Pagelet Web Service Editor.
   - To create a remote pagelet Web service, open the folder in which you want to store the remote pagetlet Web service. In the Create Object list, click **Web Service — Remote Pagelet**.
   - To edit a remote pagelet Web service, open the folder in which the remote pagelet Web service is stored and click the remote pagelet Web service name.
3. On the Main Settings page, perform tasks as necessary:

   Note: Under Server Information, you see the remote server associated with this Web service - the Pagelet Producer Remote Server. This remote server contains the information needed to connect to Oracle WebCenter Pagelet Producer. You cannot change the remote server as you can with other Web services.

   - Section 8.3.4, "Selecting a Pagelet"
   - Section 3.4.3, "Specifying Web Service Time-Out Settings"
   - Section 3.4.4, "Enabling and Disabling a Web Service"
4. On the HTTP Configuration page, perform tasks as necessary:

- Section 3.4.5, "Specifying Caching Settings for a Web Service"

5. On the Advanced URL Settings page, perform tasks as necessary:
   - Section 8.2.4, "Adding Help to Portlets"
6. On the Advanced Settings page, perform tasks as necessary:
   - Section 8.3.5, "Sending General Settings from a Remote Pagelet Web Service to Associated Portlets"
7. On the Parameter Mapping page, perform tasks as necessary:
   - Section 8.3.6, "Mapping Remote Pagelet Parameters to Portlet Preferences"
8. On the Debug Settings page, perform tasks as necessary:
   - Section 3.4.16, "Enabling Error Tracing for a Web Service"
9. On the Alternative Browsing Devices page, perform tasks as necessary:
   - Section 8.2.11, "Specifying Alternative Browsing Device Support for a Portlet Web Service"
10. On the Properties and Names page, perform tasks as necessary:
    - Section 5.15, "Naming and Describing an Object"

      You can instead enter a name and description when you save this remote pagelet Web service.
    - Section 5.16, "Managing Object Properties" (optional)
11. On the Security page, perform tasks as necessary:
    - Section 5.17, "Setting Security on an Object"

    The default security for this remote pagelet Web service is based on the security of the parent folder. Administrative users with at least Select access to this remote pagelet Web service and the Create Portlets activity right can create portlets or portlet templates based on the Web service.
12. If you are editing a remote pagelet Web service, on the Migration History and Status page, perform tasks as necessary:
    - Section 5.18, "Viewing Migration History and Status for an Object"

    Note: The Migration History and Status page is not available when creating an object.

8.3.3 Deleting a Remote Pagelet Web Service

To delete a remote pagelet Web service you must have the following rights and privileges:

- Access Administration activity right
- Admin access to the remote pagelet Web service

To delete a remote pagelet Web service:

1. Click **Administration**.
2. Navigate to the remote pagelet Web service.
3. Select the remote pagelet Web service you want to delete and click the delete icon.

Note: Deleting a remote pagelet Web service will break any associated portlets.

8.3.4 Selecting a Pagelet

To select a pagelet to make available through the Web service:

1. If the Remote Pagelet Web Service Editor is not already open, open it now. The Remote Pagelet Web Service Editor displays the Main Settings page.
2. In the Pagelet Libraries box, you see the pagelet libraries from your Oracle WebCenter Pagelet Producer deployment. Select the library that contains the pagelet you want to make available.
3. In the Pagelets box, you see the pagelets available in the library you selected in the previous step. Select the pagelet you want to make available through the Web service.

   The selected library and pagelet appear to the right of the Pagelets box.

8.3.5 Sending General Settings from a Remote Pagelet Web Service to Associated Portlets

To specify what information the pagetlet Web service passes to associated portlets:

1. If the Remote Pagelet Web Service Editor is not already open, open it now.
2. Click the **Advanced Settings** page.
3. Specify what general information, if any, you want this Web service to pass to its associated portlets:
   - If this Web service requires the user to have an API session (for example, if the Web service uses the SOAP API), select **Send Login token to Portlets**; then, in the **Login Token duration** box, type the number of minutes you want the API session to last.
   - To include a refresh button on the portlet, click **Show Portlet refresh button**. The refresh button appears in the title bar of portlets associated with this Web service. Users can then refresh this portlet by itself, rather than refresh the entire My Page or community that contains the portlet.

8.3.6 Mapping Remote Pagelet Parameters to Portlet Preferences

If the pagelet selected on the Main Settings page supports pagelet parameters, specify how users configure pagelet parameters by mapping each parameter to one or more portlet preferences.

To map pagelet parameters to portlet preferences:

1. If the Remote Pagelet Web Service Editor is not already open, open it now.
2. Click the **Parameter Mapping** page.
3. Map pagelet parameters to portlet preferences:
   - If the parameter affects the user's view of the portlet, select **Portlet Personal preference**. This allows the user to configure the parameter through the icon on the portlet title bar.

- If the parameter affects everyone's view of a portlet in a particular community, select **Portlet Community preference**. This allows the community manager to configure the parameter on the Portlet Preferences page of the Community Editor.
- If the parameter affects everyone's view of the portlet on all pages that include this portlet, select **Portlet Admin preference**. This allows the portlet creator to configure the parameter on the Main Settings page of the Portlet Editor.

Note: Portlet Personal preferences override Portlet Community preferences and Portlet Admin preferences. Portlet Community preferences override Portlet Admin preferences.

8.4 Working with Portlet Templates and Portlets

This section describes the following main tasks:

- Section 8.4.1, "Creating or Editing a Portlet Template"
- Section 8.4.2, "Deleting a Portlet Template"
- Section 8.4.3, "Creating or Editing a Portlet"
- Section 8.4.4, "Deleting a Portlet"

It also covers the following low-level tasks:

- Section 8.4.5, "Associating a Web Service with a Portlet or a Portlet Template"
- Section 8.4.6, "Editing the Portlet Template Preferences for a Portlet Template"
- Section 8.4.7, "Editing the Administrative Preferences for a Portlet"
- Section 8.4.8, "Specifying the Size, Type, and Orientation for a Portlet"
- Section 8.4.9, "Setting Security for a Portlet"
- Section 8.4.10, "Caching Portlet Content"

8.4.1 Creating or Editing a Portlet Template

Before you create a portlet template, you must:

- Install the portlet code on the computer that hosts the portal or, if your portlet does not rely on any portal code, you can instead install it on another computer
- If you installed the portlet code on a computer other than the one that hosts the portal, create a remote server to point to the remote computer
- Create a portlet Web service on which to base your portlet

To create a portlet template you must have the following rights and privileges:

- Access Administration activity right
- Create Web Service Infrastructure activity right
- At least Edit access to the parent folder (the folder that will store the portlet template)

To edit a portlet template you must have the following rights and privileges:

- Access Administration activity right
- At least Edit access to the portlet template

To create or edit a portlet template:

1. Click **Administration**.
2. Open the Portlet Template Editor.
   - To create a portlet template, open the folder in which you want to store the portlet template. In the Create Object list, click **Portlet Template**.
   - To edit a portlet template, open the folder in which the portlet template is stored and click its name.
3. On the Main Settings page, perform tasks as necessary:
   - Section 8.4.5, "Associating a Web Service with a Portlet or a Portlet Template"
   - Section 8.4.6, "Editing the Portlet Template Preferences for a Portlet Template"
   - Section 8.4.8, "Specifying the Size, Type, and Orientation for a Portlet"
4. On the Properties and Names page, perform tasks as necessary:
   - Section 5.15, "Naming and Describing an Object"
   - Section 5.16, "Managing Object Properties"
5. On the Security page, perform tasks as necessary:
   - Section 8.4.9, "Setting Security for a Portlet"

   The default security for this portlet template is based on the security of the parent folder.
6. If you are editing a portlet template, on the Migration History and Status page, perform tasks as necessary:
   - Section 5.18, "Viewing Migration History and Status for an Object"

   Note: The Migration History and Status page is not available when creating an object.

8.4.2 Deleting a Portlet Template

To delete a portlet template you must have the following rights and privileges:

- Access Administration activity right
- Admin access to the portlet template

To delete a portlet template:

1. Click **Administration**.
2. Navigate to the portlet template.
3. Select the portlet template you want to delete and click the delete icon.

8.4.3 Creating or Editing a Portlet

Note: If you copy a portlet, both the copy and the original portlet will share the same administrative preferences. Changing the preferences in one portlet changes the preferences for the other one as well. If you want each portlet to have independent administrative preferences, create a new portlet from the same Web service.

Before you create a portlet, you must:

- Install the portlet code on the computer that hosts the portal or, if your portlet does not rely on any portal code, you can instead install it on another computer
- If you installed the portlet code on a computer other than the one that hosts the portal, create a remote server to point to the remote computer
- Create a portlet Web service on which to base your portlet
- Optionally, create a portlet template on which to base your portlet

> **Note:** For information on installing portlet code, refer to the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Interaction for Windows* or the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Interaction for Unix and Linux* or the documentation that comes with your portlet.

To create a portlet you must have the following rights and privileges:

- Access Administration activity right
- Create Portlets activity right
- At least Edit access to the parent folder (the folder that will store the portlet)

To edit a portlet you must have the following rights and privileges:

- Access Administration activity right
- At least Edit access to the portlet

To create or edit a portlet:

1. Click **Administration**.
2. Open the Portlet Editor.
   - To create a portlet, open the folder in which you want to store the portlet. In the Create Object list, click **Portlet**. In the Choose Template or Web Service dialog box, select the template or Web service that provides the basic settings for your portlet and click **OK**.

     > **Note:** Use a template when possible. When you use a template, your portlet inherits the template's Web service as well as its default settings. Some Web services that are designed to work with templates might not work correctly if you bypass the template and make a new portlet directly from the Web service object.

   - To edit a portlet, open the folder in which the portlet is stored and click its name.
3. On the Main Settings page, perform tasks as necessary:
   - Section 8.4.5, "Associating a Web Service with a Portlet or a Portlet Template"
   - Section 8.4.7, "Editing the Administrative Preferences for a Portlet"
   - Section 8.4.8, "Specifying the Size, Type, and Orientation for a Portlet"
4. On the Properties and Names page, perform tasks as necessary:
   - Section 5.15, "Naming and Describing an Object"

- Section 5.16, "Managing Object Properties"

5. On the Security page, perform tasks as necessary:
   - Section 8.4.9, "Setting Security for a Portlet"

   The default security for this portlet is based on the security of the parent folder.
6. If you are editing a portlet, on the Migration History and Status page, perform tasks as necessary:
   - Section 5.18, "Viewing Migration History and Status for an Object"

   Note: The Migration History and Status page is not available when creating an object.

8.4.4 Deleting a Portlet

To delete a portlet you must have the following rights and privileges:

- Access Administration activity right
- Admin access to the portlet

To delete a portlet:

1. Click **Administration**.
2. Navigate to the portlet.
3. Select the portlet you want to delete and click the delete icon.

8.4.5 Associating a Web Service with a Portlet or a Portlet Template

1. If the Portlet Editor or the Portlet Template Editor is not already open, open it now. The editor displays the Main Settings page.
2. To establish and manage a Web service association for this portlet:
   - To associate a Web service (or to change an existing association), click **Browse**, then, in the Choose Web Service dialog box, choose the Web service you want to associate with the portlet or portlets created from the portlet template and click **OK**.

     Note: If you created the portlet from a portlet template, you can *edit* the associated Web service, but you cannot *change* it.

   - To edit the remote server, click its name.

8.4.6 Editing the Portlet Template Preferences for a Portlet Template

You can configure the portlet template preferences for a portlet template on the Main Settings page of the Portlet Template Editor.

1. If the Portlet Template Editor is not already open, open it now.
2. If the associated Web service includes portlet template preferences (specified on the Preferences page of the Portlet Web Service Editor), click **Edit** to edit the preferences.

8.4.7 Editing the Administrative Preferences for a Portlet

You can configure the administrative preferences for a portlet on the Main Settings page of the Portlet Editor.

1. If the Portlet Editor is not already open, open it now.
2. If the associated Web service includes administrative preferences (specified on the Preferences page of the Portlet Web Service Editor), click **Edit** to edit the preferences.

8.4.8 Specifying the Size, Type, and Orientation for a Portlet

You can specify the size, type, and orientation for a portlet on the Main Settings page of the Portlet Editor.

1. If the Portlet Editor is not already open, open it now and display the **Main Settings** page.
2. Specify what type of portlet this is.
   - **Narrow**: Narrow portlets can be added to narrow or wide columns. Columns extend to fit portlet content; therefore, if you choose narrow for a portlet that produces wide content, your portal might look awkward.

     If you created this portlet from a portlet template that creates narrow portlets or if you are editing an existing a narrow portlet, you can change it to a Wide portlet but not to a header, footer, or content canvas portlet.
   - **Wide**: Wide portlets can be added only to wide columns.

     If you created this portlet from a portlet template that creates wide portlets or if you are editing an existing a wide portlet, you can change it to a narrow portlet but not to a header, footer, or content canvas portlet.
   - **Header**: Header portlets can be added to communities, community templates, and experience definitions to change the branding of these objects by replacing a banner at the top of the page (so that it differs from the top banner displayed by the main portal).

     You cannot change this setting if you created this portlet from a portlet template that creates header portlets or if you are editing an existing header portlet.
   - **Footer**: Footer portlets can be added to communities, community templates, and experience definitions to change the branding of these objects by replacing the banner at the bottom of the page (so that it differs from the bottom banner displayed by the main portal).

     You cannot change this setting if you created this portlet from a portlet template that creates footer portlets or if you are editing an existing footer portlet.
   - **Content Canvas**: Content canvas portlets can be added below the top banner on community pages that include a content canvas space (specified in the page layout). Content canvas portlets can display across the entire width of the page or across one or two columns. You cannot add more than one content canvas portlet per page.

     You cannot change this setting if you created this portlet from a portlet template that creates content canvas portlets or if you are editing an existing content canvas portlet.

3. If this is a narrow or wide portlet, specify whether this portlet is a community-only portlet.
   - If you want to allow users to add this portlet to My Pages or community pages, choose **For My Pages or Community pages**.
   - If you want to allow users to add this portlet only to community pages, choose **For Community pages only**.
4. If this is a narrow or wide portlet and you do not want to display the title of this portlet when it is added to a page, select **Suppress Portlet's title bar**.

> **Note:** If this portlet includes preferences or help, suppressing the title bar will make these features unavailable in the portlet.

8.4.9 Setting Security for a Portlet

By default, a new portlet inherits the security of the parent folder, but you can change the security of each individual portlet.

1. If the Portlet Editor is not already open, open it now.
2. Click the **Security** page.
3. Specify which users and groups can access this portlet and what type of access they have:
   - To allow additional users or groups access to this portlet, click **Add Users/Groups**.
   - If this portlet can be added to My Pages and is not a header, footer, or content canvas portlet, you can force users or groups to include this portlet on their default My Pages. To do so, in the **Mandatory** list, click **Mandatory**.

> **Note:** Users and groups for which this portlet is mandatory will not be able to remove this portlet from their My Pages.

   - To specify the type of access a user or group has, in the list under the **Privilege** column, select the access type.

     For a description of the available privileges, see Section 2.5.1, "About Access Controls Lists and Access Privileges."

> **Note:** If a user is a member of more than one group included in the list, or if they are included as an individual user and as part of a group, that user gets the highest access available to her for this object. For example, if a user is part of the Everyone group (which has Read access) and the Administrators Group (which has Admin access), that user gets the higher privilege to the community: Admin.

   - To delete a user or group, select the user or group and click the Remove icon.

     To select or clear all of the user and group check boxes, select or clear the check box to the left of **Users/Groups**.
   - To see what users are included in a group, click the group name.

- To change the column used for sorting or to toggle the sort order between ascending and descending, click the column name.

  You see the Sort Ascending icon or the Sort Descending icon to the right of the column name by which the objects are sorted.

- If you chose Mandatory for any user or group, in the **Mandatory Portlet Priority** list, set this portlet's priority.

  The priority determines the portlet's placement on the My Page; portlets with higher priority display closer to the upper-left of the My Page then portlets with lower priority.

8.4.10 Caching Portlet Content

You might occasionally want to run a job to cache portlet content (for example, if the portlet takes a couple minutes to render). When the job runs, it creates a snapshot of the portlet content (in the form of a static HTML file) that can be displayed on a Web site. The file is stored in the shared files directory (for example, C:\Oracle\Middleware\wci\ptportal\10.3.3 for Windows or /oracle/middleware/wci/ptportal/10.3.3) in \StagedContent\Portlets*portletID*\Main.html. You can then create another portlet that simply displays the static HTML.

Note: The shared files directory path is set on the **Portal URL Manager** page of the Portal Settings Utility.

To run a portlet as a job you must have the following rights and privileges:

- Access Administration activity right
- Create Jobs activity right
- At least Edit access to the parent folder (the folder that will store the job)
- At least Select access to the portlet

Note:

- Because intrinsic portlets rely on the portal application, you cannot run an intrinsic portlet as a job.
- Because the content produced is static you should only run portlets that present information that is valuable when updated on a periodic basis. For example, a report portlet would be ideal to run as a job, while more interactive portlets, like application interfaces would not be appropriate.
- If the portlet includes preferences, the preferences for the user that creates the job will be used.

---

1. Click **Administration**.
2. Open the folder in which you want to store the portlet job.

Note: In order for the job to run, the folder must be registered with an Automation Service.

---

3. In the Create Object list, select **Job**.
4. On the Main Settings page, click **Add Operation**.
5. Select the portlets you want to run with this job, and click **OK**.
6. Under Schedule, select the frequency with which you want this job to run.

8.5 Working with Portlet Bundles

This section describes the following main tasks:

- Section 8.5.1, "Creating or Editing a Portlet Bundle"
- Section 8.5.2, "Deleting a Portlet Bundle"

8.5.1 Creating or Editing a Portlet Bundle

Before you create a portlet bundle, you must create the portlets you want to bundle.

To create a portlet bundle you must have the following rights and privileges:

- Access Administration activity right
- Create Web Service Infrastructure activity right
- At least Edit access to the parent folder (the folder that will store the portlet bundle)

To edit a portlet bundle you must have the following rights and privileges:

- Access Administration activity right
- At least Edit access to the portlet bundle

To create or edit a portlet bundle:

1. Click **Administration**.
2. Open the Portlet Bundle Editor.
   - To create a portlet bundle, open the folder in which you want to store the portlet bundle. In the Create Object list, click **Portlet Bundle**.
   - To edit a portlet bundle, open the folder in which the portlet bundle is stored and click its name.
3. On the Main Settings page, perform tasks as necessary:
   - To add a portlet to this bundle, click **Add Portlets**; then, in the Select Portlets dialog box, select the portlets you want to add and click **Finish**.
   - To remove a portlet, select the portlet and click the remove icon.
   - To select or clear all of the portlet check boxes, select or clear the box to the left of Portlet Names.
   - To toggle the order in which the folders are sorted (ascending/descending), click Portlet Names or click the icon to the right of that.
4. On the Properties and Names page, perform tasks as necessary:
   - Section 5.15, "Naming and Describing an Object"
   - Section 5.16, "Managing Object Properties"
5. On the Security page, perform tasks as necessary:

- Section 5.17, "Setting Security on an Object"

The default security for this portlet bundle is based on the security of the parent folder.

6. If you are editing a portlet bundle, on the Migration History and Status page, perform tasks as necessary:
   - Section 5.18, "Viewing Migration History and Status for an Object"

> **Note:** The Migration History and Status page is not available when creating an object.

8.5.2 Deleting a Portlet Bundle

To delete a portlet bundle you must have the following rights and privileges:

- Access Administration activity right
- Admin access to the portlet bundle

To delete a portlet bundle:

1. Click **Administration**.
2. Navigate to the portlet bundle.
3. Select the portlet bundle you want to delete and click the delete icon.

8.6 Working with Lockboxes

To access the Credential Vault Manager you must be a member of the Administrators Group.

You can create a lockbox for each secured application the user must access through the portal.

1. Click **Administration**.
2. In the **Select Utility** list, click **Credential Vault Manager**.
3. Create a lockbox for each secured application you will provide access to through the portal.
   - To create a new lockbox, click **New Lockbox**.

     The Lockbox Editor opens.
   - To edit an existing lockbox, click its name.

     The Lockbox Editor opens.
   - To delete a lockbox, select it and click the Remove icon.

After setting up lockboxes:

- Users must enter their login credentials through the Password Manager on the My Account page.
- To send credentials in portlet headers, using RSA public key/private key encryption, after setting up a lockbox, you must associate the lockbox with the remote portlet Web service (on the Authentication Settings page), enter the public key for RSA encryption in the remote server (on the Main Settings page), and use the IDK to provide the private key for RSA encryption (see the *Oracle Fusion Middleware Web Service Developer's Guide for Oracle WebCenter Interaction*).

8.6.1 Creating or Editing a Lockbox to Store User Credentials for External Applications

Create a lockbox for each secured application the user must access through the portal.

To access the Credential Vault Manager you must be a member of the Administrators Group.

1. Click **Administration**.
2. In the **Select Utility** list, click **Credential Vault Manager**.
3. Click **New Lockbox** or click an existing lockbox to edit it.
4. In the **Name** box, type a name for the lockbox.

   Users will see this name in a list of their external accounts when they click **Password Manager** on the **My Account** page. The name should clearly identify the external system for which users will enter their login credentials.
5. In the **Description** text box, type a description for this lockbox.

   This description displays in the Administrative Objects Directory to help other administrators understand what this object is.
6. If the system administrator did not set a mandatory object language in the portal configuration file, in the **Primary Language** list, select the language for the name and description you entered.

   If the system administrator did set a mandatory object language in the portal configuration file, you see the mandatory language instead of a list. You cannot change this setting. The name and description you entered must be in the mandatory language.

   If a localized name and description is not available in a user's selected language, the user will see the name and description in the specified primary language.
7. If you want to add localized names and descriptions:
   a. Select **Supports Localized Names**.

      The **Localized Names and Descriptions** section appears.
   b. Add or edit the localized names and descriptions:
      - To add an entry for a language, click **New Localized Name**, then, in the Name and Description dialog box, enter the localized name and/or description, select the appropriate language, and click **Finish**.
      - To edit an existing entry, click the entry you want to change, then, in the Name and Description dialog box, edit the entry as necessary, and click **Finish**.
      - To remove existing entries, select the entries you want to remove and click the Remove icon.

        To select or clear all entries, select or clear the check box to the left of **Name**.
8. Under **Lockbox Properties**, enter names for the user name and password properties for this lockbox.

   End users will see these names in the Password Manager when entering their login credentials for the external system corresponding to this lockbox.These properties will be created when you save the lockbox. After you have saved the lockbox, these properties appear as links. Click the links to edit the properties.

9

Providing Content and Services to Users through Communities

This chapter explains how to provide content and services to users through portal communities.

It includes the following sections:

9.1 About Community Components and Features

This section describes the components and features involved in providing content and services to users through communities:

9.1.1 Communities

Communities are sites within a portal designed for a specific audience or task, such as collaborative projects. The pages, portlets, layout, community preferences, and subcommunities within a community are determined by the community administrator. Although the community administrators determine which portlets are displayed in a community, a portlet itself might allow community members to change the content within each portlet.

You might have communities based on departments in your company. For example, the Marketing department might have a community containing press information,

leads volumes, a trade show calendar, and so on. The Engineering department might have a separate community containing project milestones, regulatory compliance requirements, and technical specifications.

You are automatically subscribed to communities based on your group membership. You can also join communities on your own. Some community subscriptions might be mandatory, but you can unsubscribe from those that are not. The communities you are subscribed to appear in the **My Communities** menu. Some mandatory communities might also appear as tabs in the menu area.

9.1.2 Community Menus

The community might include the following menus:

- The community menu displays all the community pages, and—if enabled by the administrator—the Community Knowledge Directory. The community pages display portlets. The Community Knowledge Directory displays the members of the community, any subcommunities of the community, and any other folders and contents the community administrator added.
- **Subcommunities** displays any subcommunities within the current community.
- **Related Communities** displays any communities that are stored in the same administrative folder as the current community.

  This menu only appears if you have access to related communities.

> **Note:** An administrative user with the Create Experience Definitions activity right can also configure a navigation scheme with customized menu options.

9.1.3 Community Templates

Each community is based on a community template. Community templates define the basic structure for the resulting communities, such as which page templates to include and, optionally, a header or footer for the community. A single community template can be used by many different communities, allowing you to keep similar types of communities looking analogous. For example, you might want all communities based on departments to look similar and contain similar content, but you might want communities based on projects to look different.

9.1.4 Page Templates

Each community page is based on a page template. Page templates define the basic structure for the resulting community pages, such as the column layout and which portlets to include. A single page template can be used by many different communities, allowing you to keep similar types of pages looking analogous. For example, you might want each department to create a community in which the first page lists the general duties of the group, the department members, and the current projects owned by the department.

9.1.4.1 Template Inheritance

When you create a community or a community page, you can decide whether to inherit the underlying community template or page template. Inheriting a template has several effects on the resulting communities and pages:

- You cannot remove objects that are included as part of the template. For example, you cannot remove pages that came from the community template and you cannot remove portlets that came from the page template.
- Any changes made to the template are inherited by the resulting communities or community pages. For example, if a page template is removed from a community template, the page is removed from any communities that inherited the template; if a portlet is removed from a page template, the portlet is removed from any pages that inherited the template.

Note: If you inherit a community template, you also inherit the included page templates.

9.1.5 Subcommunities

Subcommunities (along with community pages) allow you to create separately-secured subsections in a community, so it can have a more restrictive security than the main community. For example, you might have a Marketing Community that includes an Advertising Subcommunity. This subcommunity might have distinct owners or might be accessible to only a subset of the Marketing Community.

A subcommunity is just a community folder stored in another community folder. Therefore, the subcommunity inherits the security and design of the parent community, but you can then change these settings to suit the needs of the subcommunity. You can also change the relationships of communities and subcommunities just by rearranging the folder structure.

Note: Subcommunities can be nested 10 levels deep.

9.1.6 Community Groups and Community Portlets

With the appropriate activity rights, you can create groups and portlets inside a community without affecting portal groups or portlets. For example, you might have a group that is responsible for maintaining schedules in a specific community without making that group a portal group, or you might create a community links portlet inside a community for the convenience of community members.

Note: Community groups and community portlets are available only to the community in which they are associated. If you want to use them outside the community, you can move them from the community folder to another administrative folder.

9.1.7 Community Knowledge Directory

The Community Knowledge Directory, if enabled, displays community resources in an organizational structure that is relevant to the community (as opposed to the broader portal audience). It includes a list of community members, displayed in the **Members** folder, and a list of subcommunities, displayed in the **Subcommunities** folder. Community administrators can also create folders that contain links to relevant Web pages, community experts, portal documents, or community pages.

Note: Communities and subcommunities have separate Community Knowledge Directories.

9.1.8 Community Links Portlets

A community links portlet displays a snapshot of the links in a single Community Knowledge Directory folder. You can then add the portlet to a page in the community or invite users to add the portlet to their My Pages to provide quick access to the community resources. With the proper access privileges, you can also use the portlet to add or delete content from the associated Community Knowledge Directory folder.

9.2 Working with Community Page Templates

This section describes the following main tasks:

- Section 9.2.1, "Creating or Editing a Community Page Template"
- Section 9.2.2, "Deleting a Community Page Template"

9.2.1 Creating or Editing a Community Page Template

Community page templates define the basic structure for the resulting community pages, such as the column layout and which portlets to include. A single page template can be used by many different communities, allowing you to keep similar types of pages looking analogous. For example, you might want each department to create a community in which the first page lists the general duties of the group, the department members, and the current projects owned by the department.

Note: To create a page template you must have the following rights and privileges:

- Access Administration activity right
- Create Community Infrastructure activity right
- At least Edit access to the parent folder (the folder that will store the page template)
- At least Select access to any portlets you want to add to the page

1. Click **Administration**.
2. Open the folder in which you want to store the page template.
3. In the Create Object list, click **Page Template**.

   The Page Template Editor opens, displaying the Main Settings page.
4. Select a column layout for the page. Click **Select Page Layout**, then, in the Select Page Layout dialog box, select the layout you want and click **Finish**.

Note:

- If you intend to add a content canvas portlet (a portlet that straddles more than one column), you must select a layout that includes a dark gray section.
- Narrow portlets can display in either narrow or wide columns, but wide portlets can display only in wide columns.

5. Select portlets and position them on the page:
   - If you selected a layout that includes a section for a content canvas portlet, click **Add Content Canvas**, then, in the Content Canvas Portlets dialog box, select a content canvas portlet and click **OK**.
   - To add a portlet to the page, click **Add Portlets**, then, in the Add Portlets dialog box, select the portlets you want to add and click **Finish**.
   - To see what a portlet looks like, click **Preview** under the portlet.
   - To remove a portlet, click **Remove** under the portlet.
   - To reposition a portlet, drag the portlet to the desired position (by clicking the portlet, holding down the mouse button, and moving the mouse), then release the mouse button.

   Note: When users create pages from this template or create communities from a community template that includes this page template, they can choose to inherit the template. Inheriting the template has two effects on resulting pages, users cannot reposition or remove any portlets that are included as part of the template, and any changes to the template are mirrored in the resulting pages.

6. Optionally, specify a default name for pages created from this template:
   a. Click the **Default Page Name** page.
   b. In the **Default Page Name** box, type a name.
   c. If the system administrator did not set a mandatory object language in the portal configuration file, in the **Primary Language** list, select the language for the name you entered.

      If the system administrator did set a mandatory object language in the portal configuration file, you see the mandatory language instead of a list. You cannot change this setting. The name you entered must be in the mandatory language.

      If a localized name is not available in a user's selected language, the user will see the name in the specified primary language.
   d. If you want to add default names for other languages, select **Supports Localized Names**, then, in the **Localized Names and Descriptions** section, add or edit the localized names:
      – To add an entry for a language, click **New Localized Name**, then, in the Name and Description dialog box, enter the localized name and/or description, select the appropriate language, and click Finish.

- To edit an existing entry, click the entry you want to change, then, in the Name and Description dialog box, edit the entry as necessary, and click Finish.
- To remove existing entries, select the entries you want to remove and click the Remove icon.

  To select or clear all entries, select or clear the check box to the left of **Name**.

9.2.2 Deleting a Community Page Template

To delete a page template you must have the following rights and privileges:

- Access Administration activity right
- Admin access to the page template

To delete a page template:

1. Click **Administration**.
2. Navigate to the page template.
3. Select the page template you want to delete and click the delete icon.

Note: The page template will be removed from any associated community templates.

9.3 Working with Community Pages

This section describes the following main tasks:

- Section 9.3.1, "Creating a Community Page"
- Section 9.3.2, "Editing a Page in the Flyout Page Editor"
- Section 9.3.3, "Deleting a Community Page"

9.3.1 Creating a Community Page

You can create different pages in a community to categorize information for your community audience. For example, you might have a project community that includes a page for each department that is involved in the project.

To create a community page you must have the following rights and privileges:

- If you are creating the page from the Administrative Objects Directory or from the Community Editor, you must have the Access Administration activity right and at least Select access to the page template on which the page will be based
- At least Edit access to the community
- At least Select access to any portlets you want to add to the page

There are several ways to create a community page:

- Section 9.3.1.1, "Creating a Community Page with One Click"
- Section 9.3.1.2, "Creating a Community Page From the Administrative Objects Directory"
- Section 9.5.5, "Creating a Community Page From the Community Editor"

9.3.1.1 Creating a Community Page with One Click

You can create a new community page with one click.

To create a community page you must have the following rights and privileges:

- At least Edit access to the community
- At least Select access to any portlets you want to add to the page

1. Display the community to which you want to add a page.
2. Click **Create Page**.

   The new page is created.
3. To add portlets to the page, click **Edit Page**.

9.3.1.2 Creating a Community Page From the Administrative Objects Directory

You can create a community page from the Administrative Objects Directory.

To create a community page you must have the following rights and privileges:

- Access Administration activity right
- At least Edit access to the community
- At least Select access to the page template on which the page will be based
- At least Select access to any portlets you want to add to the page

1. Click **Administration**.
2. Open the community folder to which you want to add the page.
3. In the Create Object list, click **Page**.

   The New Page dialog box opens.
4. Select the page template on which you want to base this page, and click **OK**.
5. Specify whether you want to inherit the template, and click **OK**.

   Note: If you inherit the template, you cannot reposition or remove portlets that are included as part of the template, and any changes made to the template are mirrored in the page you create.

   The Standard Page Editor opens.
6. Select a column layout for the page.

   Note:

   - If you intend to add a content canvas portlet (a portlet that straddles more than one column), you must select a layout that includes a dark gray section.
   - Narrow portlets can display in either narrow or wide columns, but wide portlets can display only in wide columns.
7. Select portlets and position them on the page:

- If you selected a layout that includes a section for a content canvas portlet, click **Add Content Canvas**, then, in the Content Canvas Portlets dialog box, select a content canvas portlet and click **OK**.
- To add a portlet to the page, click **Add Portlets**, then, in the Add Portlets dialog box, select the portlets you want to add and click **Finish**.
- To create a portlet and add it to the page, click **Create Portlets**. On the Choose Portlet Template page, select a Portlet Template, click **Next >>**, and complete the Portlet Editor.
- To see what a portlet looks like, click **Preview** under the portlet.
- To remove a portlet, click **Remove** under the portlet.
- To reposition a portlet, drag the portlet to the desired position (by clicking the portlet, holding down the mouse button, and moving the mouse), then release the mouse button.

9.3.2 Editing a Page in the Flyout Page Editor

You can rename a page, add portlets, recommend portlets, and reposition portlets while viewing the page.

Click **Edit Page**. The Flyout Page Editor appears, enabling you to perform the following actions:

> **Note:** The Flyout Page Editor appears only if you are viewing an adaptive page layout (not a legacy page layout).

- To rename the page, in the **Change Page Name** box, type the new name.
- To add a portlet to the page, under the portlet name, click **Add to Page**.

  A placeholder for the portlet is added to the page below the Flyout Page Editor.
- To remove a portlet, under the portlet name, click **Remove**, or click in the portlet's title bar.
- To see what a portlet looks like, under the portlet name, click **Preview**.

  From the Preview Portlet page you can perform the following actions:
  - To add the portlet to your page and close the preview, click **Add this portlet**.
  - To view a description of the portlet, click **View Description**. When you are finished, click **Close**.
  - To return to the list of portlets without adding the portlet to your page, click **Close**.
- To view a list of the portlets in a portlet bundle, under the bundle name, click **Open**.
- To add all the portlets from a bundle, under the bundle name, click **Add**.

  A placeholder for each portlet is added to the page below the Flyout Page Editor.

> **Note:** You can remove a portlet added as part of a bundle by clicking the Remove icon in the portlet's title bar.

- To search for portlets and portlet bundles, in the **Search for Portlets** box, type the text you want to search for and click **Search**.

  For searching tips, see Section F.3, "Using Text Search Rules."

  To remove your search criteria, click **Search** again.
- To change the sort order of portlets, in the **Sort By** list, select an option: Item Name Ascending, Item Name Descending, Date Modified Ascending, Date Modified Descending.
- To page through the list of portlets, click **<< Previous**, **Next >>**, or a particular page number.
- To browse through administrative folders, click **Browse All Folders**.

  Note: This link displays folders that might not contain portlets or portlet bundles.

  To view the portlets and portlet bundles in a folder, click the folder name.
- To reposition a portlet, in the area under the Edit Page section, drag the portlet to the desired position (by clicking the portlet, holding down the mouse button, and moving the mouse), then release the mouse button.

  Each column on the page is represented by a gray box. To change the column structure, click **Go to Advanced Editor**, then click **Select Page Layout**.
- To close the Flyout Page Editor, click **Close**, or, in the Edit Page section, click the Close icon or **Close Editor**.

9.3.3 Deleting a Community Page

To delete a community template you must have the following rights and privileges:

- Access Administration activity right
- Admin access to the community page

To delete a community page:

1. Click **Administration**.
2. Navigate to the community page.
3. Select the community page you want to delete and click the delete icon.

Note: You can also delete a page from within the Community Editor.

9.4 Working with Community Templates

This section describes the following main tasks:

- Section 9.4.1, "Creating or Editing a Community Template"
- Section 9.4.2, "Deleting a Community Template"

It also covers the following low-level tasks:

- Section 9.4.3, "Managing Page Templates in a Community Template"

9.4.1 Creating or Editing a Community Template

Before you create a community template, you must:

- Create any page templates you want to add to this community template
- Create any header and footer portlets you want to add to the community template

To create a community template you must have the following rights and privileges:

- Access Administration activity right
- Create Community Infrastructure activity right
- At least Edit access to the parent folder (the folder that will store the community template)
- At least Select access to any page templates you want to add to this community template
- At least Select access to any header and footer portlets you want to add to the community template

To create a community template you must have the following rights and privileges:

- Access Administration activity right
- At least Edit access to the community template
- If you plan to change the page templates included in the community template, at least Select access to the page templates
- If you plan to change the header or footer portlets used in the community template, at least Select access to the header and footer portlets

To create or edit a community template:

1. Click **Administration**.
2. Open the Community Template Editor.
   - To create a community template, open the folder in which you want to store the community template. In the Create Object list, click **Community Template**.
   - To edit a community template, open the folder in which the community template is stored and click the community template name.
3. On the Main Settings page, perform tasks as necessary:
   - Section 9.4.3, "Managing Page Templates in a Community Template"
4. On the Header and Footer page, perform tasks as necessary:
   - Section 9.5.9, "Managing the Header and Footer in a Community or Community Template"
5. On the Properties and Names page, perform tasks as necessary:
   - Section 5.15, "Naming and Describing an Object"

     You can instead enter a name and description when you save this community template.
   - Section 5.16, "Managing Object Properties" (optional)
6. On the Security page, perform tasks as necessary:
   - Section 5.17, "Setting Security on an Object"

The default security for this community template is based on the security of the parent folder. Administrative users with at least Select access to this community template and the Create Communities activity right can create communities based on the template.

7. If you are editing a community template, on the Migration History and Status page, perform tasks as necessary:
   - Section 5.18, "Viewing Migration History and Status for an Object"

   Note: The Migration History and Status page is not available when creating an object.

9.4.2 Deleting a Community Template

To delete a community template you must have the following rights and privileges:

- Access Administration activity right
- Admin access to the community template

To delete a community template:

1. Click **Administration**.
2. Navigate to the community template.
3. Select the community template you want to delete and click the delete icon.

9.4.3 Managing Page Templates in a Community Template

To add page templates to a community template you need at least Select access to the page templates.

To manage page templates in a community template:

1. If the Community Template Editor is not already open, open it now and display the Main Settings page.
2. Manage the page templates in the community template:
   - To add a page template, click **Add Page Templates**, then, in the Add Page Templates dialog box, select the page templates you want to add to this community template and click **OK**.
   - To remove a page template, select the template and click the Remove icon.

     To select or clear all of the page template check boxes, select or clear the box to the left of **Page Template Names**.

     Note: If you remove a page template, the associated page will be removed from any communities that inherit the changes in this template. It might take up to 15 minutes for this occur.

   - To change the order in which the pages will appear in the communities created from this template, use the arrow icons to the right of the page templates.
     - To move a page to the top of this list, click the Move to Top icon.
     - To move a page up one space in this list, click the Move Up icon.

- To move a page down one space in this list, click the Move Down icon.
- To move a page to the bottom of this list, click the Move to Bottom icon.

Note: If you change the order of the pages, and communities have previously been created from this community template, the page order will change in all of the communities derived from this community template.

9.5 Working with Communities

This section describes the following main tasks:

- Section 9.5.1, "Creating or Editing a Community"
- Section 9.5.2, "Deleting a Community"

It also covers the following low-level tasks:

- Section 9.5.3, "Applying a Community Template to a Community"
- Section 9.5.4, "Setting the Community Home Page and Ordering Community Pages"
- Section 9.5.5, "Creating a Community Page From the Community Editor"
- Section 9.5.6, "Deleting a Page from a Community"
- Section 9.5.7, "Enabling or Disabling the Community Knowledge Directory"
- Section 9.5.8, "Inviting Users to the Community"
- Section 9.5.9, "Managing the Header and Footer in a Community or Community Template"
- Section 9.5.10, "Creating a Subcommunity"
- Section 9.5.11, "Creating a Community Group"
- Section 9.5.12, "Setting Community Preferences for Portlets"
- Section 9.5.13, "Creating a Community Portlet"
- Section 9.5.14, "Setting Security on a Community"

9.5.1 Creating or Editing a Community

Before you create a community, you must:

- Create the community template on which this community will be based
- Create the page templates on which your community pages will be based
- Create any portlets you want to add to the community pages

To create a community you must have the following rights and privileges:

- Access Administration activity right
- Create Communities activity right
- At least Edit access to the parent folder (the folder that will store the community)
- At least Select access to the community template on which this community will be based

- At least Select access to any page templates you will use to create community pages
- At least Select access to any portlets you want to add to the community pages

To create a community you must have the following rights and privileges:

- Access Administration activity right
- At least Edit access to the community
- If you plan to change the community template on which the community is based, at least Select access to the template
- If you plan to add pages to the community, at least Select access to the page templates you will use to create new pages
- If you plan to add portlets to any community pages, at least Select access to the portlets

To create or edit a community:

1. Click **Administration**.
2. Open the Community Editor.
   - To create a community, open the folder in which you want to store the community. In the Create Object list, click **Community**.
   - To edit a community, open the folder in which the community is stored and click the community name.
3. On the Community Pages page, complete the following tasks:
   - Section 9.5.3, "Applying a Community Template to a Community"
   - Section 9.5.4, "Setting the Community Home Page and Ordering Community Pages"
   - Section 9.5.5, "Creating a Community Page From the Community Editor"
   - Section 9.5.6, "Deleting a Page from a Community"
   - Section 9.5.7, "Enabling or Disabling the Community Knowledge Directory"
   - Section 9.5.8, "Inviting Users to the Community"
4. On the Header and Footer page, perform tasks as necessary:
   - Section 9.5.9, "Managing the Header and Footer in a Community or Community Template"
5. On the Subcommunities page, perform tasks as necessary:
   - Section 9.5.10, "Creating a Subcommunity"
6. On the This Community's Groups page, perform tasks as necessary:
   - Section 9.5.11, "Creating a Community Group"
7. On the Portlet Preferences page, perform tasks as necessary:
   - Section 9.5.12, "Setting Community Preferences for Portlets"
8. On the This Community's Portlets page, perform tasks as necessary:
   - Section 9.5.13, "Creating a Community Portlet"
9. On the Properties and Names page, perform tasks as necessary:
   - Section 5.15, "Naming and Describing an Object"

You can instead enter a name and description when you save this community.

- Section 5.16, "Managing Object Properties" (optional)

10. On the Security page, perform tasks as necessary:
    - Section 9.5.14, "Setting Security on a Community"

    The default security for this community is based on the security of the parent folder.
11. If you are editing a community, on the Migration History and Status page, perform tasks as necessary:
    - Section 5.18, "Viewing Migration History and Status for an Object"

    Note: The Migration History and Status page is not available when creating an object.

9.5.2 Deleting a Community

To delete a community you must have the following rights and privileges:

- Access Administration activity right
- Admin access to the community

To delete a community:

1. Click **Administration**.
2. Navigate to the community.
3. Select the community you want to delete and click the delete icon.

Note: Deleting a community also deletes the community's pages, subcommunities, groups, and portlets.

9.5.3 Applying a Community Template to a Community

Each community is based on a community template. Community templates define the basic structure for the resulting communities, such as which page templates to include and, optionally, a header or footer for the community. A single community template can be used by many different communities, allowing you to keep similar types of communities looking analogous. For example, you might want all communities based on departments to look similar and contain similar content, but you might want communities based on projects to look different.

1. If the Community Editor is not already open, open it now.
2. In the Community Templates section, click **Select Community Template**.

Note: If you are editing an existing community, the button says **Change Community Template**. Before changing the template, note the following:

- Any pages from the old community template that are not part of the new community template will be removed.
- If you have set special headers and footers for your community, switching to a community template that enforces a header or footer will remove your header or footer.

The Community Templates dialog box opens.

3. Select a template and click **OK**.
4. If you do not want this community to inherit future changes to the template, clear the box next to **Inherit the Template**.

   If you select to inherit changes, any change applied to the community template affects the community. For example, if a page is removed from the community template, the page will be removed from this community as well. Additionally, if you inherit changes, you cannot delete pages associated with the template, but you can add new pages and change the order of the pages.
5. Click **OK**.

9.5.4 Setting the Community Home Page and Ordering Community Pages

The order in which pages are displayed in the Community Pages list is the order in which the page links will display to users. By default, the first page you add to a community, whether directly or through a community template, will be the home page of your community.

If the Community Editor is not already open, open it now.

- To change the home page, move the desired page to the top of the Community Pages list by clicking the Move to Top icon to the far right of the page name.
- To move a page up one space in this list, click the Move Up icon.
- To move a page down one space in this list, click the Move Down icon.
- To move a page to the bottom of this list, click the Move to Bottom icon.

9.5.5 Creating a Community Page From the Community Editor

You can create a community page while creating or editing a community.

To create a community page you must have the following rights and privileges:

- Access Administration activity right
- At least Edit access to the community
- At least Select access to the page template on which the page will be based
- At least Select access to any portlets you want to add to the page

1. If the Community Editor is not already open, open it now.
2. Click **New Page**.

   The New Page dialog box opens.

3. Select the page template on which you want to base this page, and click **OK**.
4. Specify whether you want to inherit the template, and click **OK**.

   Note: If you inherit the template, you cannot reposition or remove portlets that are included as part of the template, and any changes made to the template are mirrored in the page you create.

   The Standard Page Editor opens.
5. Select a column layout for the page. Click **Select Page Layout**, then, in the Select Page Layout dialog box, select the layout you want and click **Finish**.

   Note:

   - If you intend to add a content canvas portlet (a portlet that straddles more than one column), you must select a layout that includes a dark gray section.
   - Narrow portlets can display in either narrow or wide columns, but wide portlets can display only in wide columns.
6. Select portlets and position them on the page:
   - If you selected a layout that includes a section for a content canvas portlet, click **Add Content Canvas**, then, in the Content Canvas Portlets dialog box, select a content canvas portlet and click **OK**.
   - To add a portlet to the page, click **Add Portlets**, then, in the Add Portlets dialog box, select the portlets you want to add and click **Finish**.
   - To create a portlet and add it to the page, click **Create Portlets**. On the Choose Portlet Template page, select a Portlet Template, click **Next >>**, and complete the Portlet Editor.
   - To see what a portlet looks like, click **Preview** under the portlet.
   - To remove a portlet, click **Remove** under the portlet.
   - To reposition a portlet, drag the portlet to the desired position (by clicking the portlet, holding down the mouse button, and moving the mouse), then release the mouse button.

9.5.6 Deleting a Page from a Community

You can delete any page that is not inherited from the community template.

To delete a community page, you must have at least Edit access to the community.

1. If the Community Editor is not already open, open it now.
2. Select the page you want to delete and click the Remove icon.

   Note: You can only delete pages that say **No** in the **From Community Template** column. If you chose to inherit changes from the community template, pages that are part of that template say **Yes** in the **From Community Template** column and cannot be deleted.

The page is deleted from the community folder.

9.5.7 Enabling or Disabling the Community Knowledge Directory

To enable the Community Knowledge Directory:

1. If the Community Editor is not already open, open it now.
2. Clear the box next to **Disable Community Knowledge Directory**.

You can only enable or disable the Community Knowledge Directory from this page; to modify the folders and objects in the Community Knowledge Directory, navigate to the community, display the Community Knowledge Directory, and click **Edit**.

9.5.8 Inviting Users to the Community

To invite users to your community:

1. If the Community Editor is not already open, open it now.
2. At the top left of the page, click **Send To Others**.
3. In the dialog box, copy the text, then click **Close**.
4. In your e-mail application, paste the text into an e-mail message and send it.

   When other portal users click the URL in your e-mail, the community opens. If a user does not have permission to see the community, an error message is displayed.

9.5.9 Managing the Header and Footer in a Community or Community Template

You can add header and footer portlets to communities to control what community members see at the top and bottom of the pages in the community.

To add a header or footer you must have the following privileges:

- At least Edit access to the community or community template
- At least Select access to the header and footer portlets you want to add

To manage the header and footer for the community or community template:

1. If the Community Editor or Community Template Editor is not already open, open it now.
2. Click the **Header and Footer** page.
3. Manage the header and footer portlets:
   - To add or change the header, under Community Header, click **Browse**, then, in the Select a Header dialog box, select the header you want, and click **OK**.
   - To add or change the footer, under Community Footer, click **Browse**, then, in the Select a Footer dialog box, select the footer you want, and click **OK**.
   - To remove the header, under Community Header, click **Remove**.
   - To remove the footer, under Community Footer, click **Remove**.
   - (For community templates only) To use experience definition headers and footers, select **Force community to use header and footer from experience definition**.

     This forces communities created from this template to use the header and footer from the experience definition rather than from this template or from

the community itself. Because users might be assigned to different experience definitions with different headers and footers, if you select this option, communities created from this template might display different headers and footers to different users.

Note: This setting does not display in the Community Editor or in the User Profile Manager.

9.5.10 Creating a Subcommunity

Subcommunities, which can be nested 10 levels deep, allow you to have differently secured subsections in a community. For example, you might have a Marketing community that contains the Advertising Subcommunity. The Advertising Subcommunity could have distinct owners; or only a subset of the Marketing community might be entitled to see the Advertising Subcommunity.

To create a subcommunity:

1. If the Community Editor is not already open, open it now.
2. On the left, under Edit Community Settings, click **Subcommunities**.
3. Click **Create Subcommunity**.
4. Complete the Community Editor.

   The new subcommunity you create is stored in the parent community folder.

Note: You can also create a subcommunity by navigating to the parent community folder and, from the Create Object drop-down list, selecting **Community**.

9.5.11 Creating a Community Group

A group is a set of portal users to whom you grant specific access privileges. You can create community groups without affecting portal groups. You create community groups so that you can easily assign responsibilities to community members. For example, you might have a group that is responsible for maintaining schedules in the community.

To create a group available only to this community:

1. If the Community Editor is not already open, open it now.
2. On the left, under Edit Community Settings, click **This Community's Groups**.
3. Click **Create Group**.
4. Complete the Group Editor.

   The new group you create is stored in the parent community folder.

Note:

- You can also create a group for this community by navigating to the parent community folder and, from the Create Object drop-down list, selecting **Group**.
- Groups created in the Community Editor are only available within the community.
- To make a community group available in other areas of the portal, move the group to a non-community administrative folder.

9.5.12 Setting Community Preferences for Portlets

Some portlets have community preferences. You can set these preferences to control the portlet content displayed in the community. You can also hide the title bar of specific portlets in a community.

To create a group available only to this community:

1. If the Community Editor is not already open, open it now.
2. On the left, under Edit Community Settings, click **Portlet Preferences**.

   If a portlet in the community has community preferences, the edit icon appears in the Community column.
3. Click the edit icon and set any community preferences available for the portlet.
4. If you can preview the portlet, the name of the portlet will appear as a link. To preview the portlet, click its name.
5. Portlets can be displayed with or without title bars. Sometimes, a portlet is registered to suppress its title bar. If the portlet allows a title bar to be shown, a check box appears in the Display Title bar column. Clearing this check box suppresses the title bar for this portlet on this page.

Note: Certain features of a portlet (such as online help) might be unavailable from the community page if the title bar is suppressed.

9.5.13 Creating a Community Portlet

You can create portlets that can be used only in a specific community.

To create a portlet available only to this community:

1. If the Community Editor is not already open, open it now.
2. On the left, under Edit Community Settings, click **This Community's Portlets**.
3. Click **Create Portlet**.
4. Choose a portlet template and click **Next>>**, then complete the Portlet Editor.

   The new portlet you create is stored in the parent community folder.

Note:

- You can also create a portlet for this community by navigating to the parent community folder and, from the Create Object drop-down list, selecting **Portlet**.
- Portlets created in the Community Editor are only available within the community.
- To display these portlets to community users, you must add these portlets to the appropriate community page.
- To make a community portlet available to other communities, move the portlet to a non-community administrative folder.

9.5.14 Setting Security on a Community

By default, a new community inherits the security of the parent folder, but you can change this security.

1. Open the Community Editor by creating a new community or editing an existing community.
2. Click the **Security** page.
3. Specify which users and groups can access this community and what type of access they have:
   - To allow additional users or groups access to this community, click **Add Users/Groups**.
   - To specify whether this community is mandatory, select an option in the **Mandatory** list:

     By default communities are **Not Mandatory**.

     – To force users or groups to be members of this community, select **Mandatory**.

     – To force users or groups to be members of this community and add a tab to the portal banner for this community, select **Mandatory with Tab**.

     Note: Users and groups for which this community is mandatory will not be able to unsubscribe from this community, that is, this community will always be available in their My Communities menu.

   - To specify the type of access a user or group has, in the list under the **Privilege** column, select the access type.

     For a description of the available privileges, see Section 2.5.1, "About Access Controls Lists and Access Privileges."

     Note: If a user is a member of more than one group included in the list, or if they are included as an individual user and as part of a group, that user gets the highest access available to her for this object. For example, if a user is part of the Everyone group (which has Read access) and the Administrators Group (which has Admin access), that user gets the higher privilege to the community: Admin.

- To delete a user or group, select the user or group and click the Remove icon.

  To select or clear all of the user and group check boxes, select or clear the check box to the left of **Users/Groups**.

- To see what users are included in a group, click the group name.
- To change the column used for sorting or to toggle the sort order between ascending and descending, click the column name.

  You see the Sort Ascending icon or the Sort Descending icon to the right of the column name by which the objects are sorted.

- If you chose Mandatory with Tab for any user or group, in the **Mandatory Tab Priority** list, set this community tab's priority.

  The priority determines the order in which tabs display in the portal banner: tabs with higher priority display before tabs with lower priority.

10 Managing Search

This chapter describes how to implement search for documents that reside in the Knowledge Directory, in communities, or in the collection of crawled links.

It includes the following sections:

- Section 10.1, "About Tagging Engine Integrated Search"
- Section 10.2, "Customizing Search Service Behavior"
- Section 10.3, "About Grid Search"
- Section 10.4, "About the Search Update Job"
- Section 10.5, "About Providing Search Access to External Repositories with Federated Searches"

10.1 About Tagging Engine Integrated Search

Tagging Engine integrated search is the portal's banner and advanced search utilizing the Tagging Engine search service to return search results. This integration provides the benefits of the Tagging Engine to the portal search experience. Tag search lets you search for items and people by creating queries that contain tag references. An item or person is returned in your search results when a tag you search for is associated with that item or person.

However, Tagging Engine integrated search limits the search options for text and dates to "contains" and "is" searches.

10.2 Customizing Search Service Behavior

This section discusses the following topics:

- Search Result Types
- Search Results Sorting Options
- Best Bets and Top Best Bets
- How Banner Field Settings Affect Search Results
- Spell Correction for Searches
- The Search Thesaurus
- Customizing Categorization of Search Results

10.2.1 Search Result Types

You can limit your search to particular types of objects.

Result Type	Description
Documents	Returns documents from the portal Knowledge Directory.
Knowledge Directory Folders	Returns folders from the portal Knowledge Directory.
Users	Returns portal users.
Communities	Returns communities.
Community Pages	Returns pages in a community
Portlets	Returns portlets.
Collaboration Items	Returns documents, discussions, and task lists from Oracle WebCenter Collaboration.
Publisher Items	Returns documents from Publisher.

10.2.2 Search Results Sorting Options

You can specify how your search results are sorted.

Option	Description
Relevance	Displays your results according to how closely they match your search query. **Note**: Best bets are only shown in search results when sorting by relevance.
Last Modified Date	Displays your results in the order in which they were most recently edited. The result that was modified most recently will display first.
Folder	Groups your results by the folders in which they are stored and displays a list of the folders that contain search results.
Object Type	Groups your results by type of object (such as documents, users, communities, or portlets) and displays a list of the types of objects returned by your search.

10.2.3 Best Bets and Top Best Bets

Best bets associate specific search phrases (specified by an administrative user with the Access Search Results Manager activity right) with a set of search results. When end users enter a search query that matches a best bet search phrase, the best bet results appear as the first results in the relevance-ranked result list. Additionally, users can choose to go directly to the highest ranking best bet, the top best bet, instead of seeing the normal search results. For example, the top best bet for the term “HR” might be the Human Resources community. If users use the top best bet feature, they go directly to the Human Resources community instead of seeing all search results for the term “HR.”

Note:

- Best bets are not case-sensitive.
- Best bets apply only to the portal banner search box and search portlet. Best bets are not used by other portal search interfaces, such as advanced search or object selection search.
- Users go to the top best bet (for example, a community) only if they have at least Read access to it. If they do not, they see the list of search results to which they do have access.
- The phrase "Best Bet" appears next to each best bet result to inform the user that the result has been judged especially relevant to the query.

10.2.3.1 Creating Best Bets

Best bets associate specific search phrases (specified by an administrative user with the Access Search Results Manager activity right) with a set of search results. When end users enter a search query that matches a best bet search phrase, the best bet results appear as the first results in the relevance-ranked result list. Additionally, users can choose to go directly to the highest ranking best bet, the top best bet, instead of seeing the normal search results. For example, the top best bet for the term "HR" might be the Human Resources community. If users use the top best bet feature, they go directly to the Human Resources community instead of seeing all search results for the term "HR."

To access the Search Results Manager you must have the following rights:

- Access Administration activity right
- Access Utilities activity right
- Access Search Results Manager activity right

Note:

- Best bets are case-insensitive.
- You can create hundreds of best bets, each mapping to a maximum of 20 results.
- Since best bets are handled by the Search Service and are not managed portal objects, best bets do not migrate from development to production environments; you must re-create them in the production environment.

1. Click **Administration**.
2. From the **Select Utility** list, select **Search Results Manager**.
3. Launch the Best Bet Editor by clicking **New Best Bet**.
4. Complete the best bet settings as described in the online help.

Users who search for the phrase you specified now see the best bets you created. Users can go directly to the top best bet by using the top best bet operator (>) in their search or by clicking rather than **Search**.

Note: For information on how to enable this button using the Search tag, see the *Oracle Fusion Middleware Web Service Developer's Guide for Oracle WebCenter Interaction*.

10.2.4 How Banner Field Settings Affect Search Results

When a user enters a query into a search box in the portal, the portal searches the properties specified on the Banner Fields page of the Search Results Manager and ranks those results based on the specified weighting settings.

Note: Banner field settings apply to all searches: search from the portal banner, advanced search, object selection search, and any other portal search interfaces.

The default banner field properties are Name, Description, and Full-Text Content. However, you can also add other properties, such as Keyword, Department, or Author, to further refine the search results.

Another way of controlling the search results is by modifying the relevance weight for banner field properties. Overweighting a property increases its relevancy ranking; and underweighting it decreases it. For example, you can manipulate the search to first return documents whose content matches the search string (by overweighting the Full-Text Content property) followed by documents whose name matches the search string (by underweighting the Name property). When users type widgets, documents with widgets in the content appear first in a relevance-ranked search result; they are followed by documents or files with widgets in their names.

10.2.4.1 Controlling Search Results with Banner Fields and Weighting

When a user enters a query into a search box in the portal, the portal searches the properties specified on the Banner Fields page of the Search Results Manager and ranks the results based on the specified weighting settings. The default banner field properties are Name, Description, and Full-Text Content, with a high weight applied to Name. However, you can add other properties (such as Keyword, Department, or Author) and change the weighting to further refine the search results.

To access the Search Results Manager you must have the following rights:

- Access Administration activity right
- Access Utilities activity right
- Access Search Results Manager activity right

Note: Since banner field settings are a Search Service setting and not managed portal objects, the settings do not migrate from development to production environments; you must re-create them in the production environment.

1. Click **Administration**.
2. From the **Select Utility** list, select **Search Results Manager**.
3. Click the **Banner Fields** page.

The Banner Fields page displays the properties that the portal searches. The following information is displayed for each banner field.

Column	Description
Property	The property on the search banner.
Percent Weight	The proportion of the weight assigned to the property field.
Weight	The relevance ranking of the property field. Type in a weight for each property field. If you want to attach more weight to a particular property field, increase the weight number.

4. Add, edit, or delete banner fields to improve search results.
   - To add a new property field and set its weight:
     a. Click **Add Field**.

        New fields appear.

     b. From the **Property** list, select the property field you want to add.

     c. Set the weight by typing a number in the text box in the **Weight** column.
   - To delete a property field, select it and click the Delete icon.
   - To remove any customizations you have made, click **Restore Defaults**.
   - To change the weight of a property field, type a number in the text box in the **Weight** column.

     The values in the **Percent Weight** column are automatically updated when you change the value in the **Weight** column.

10.2.5 Spell Correction for Searches

Automatic spell correction is applied to the individual terms in a banner search when the terms are not recognized by the Search Service. Spell correction is not applied to quoted phrases.

For example, if a user queries for `portel server` but the term "portel" is unknown to the Search Service, items matching the terms "portal" and "server" would be returned instead. The same applies to Internet Style mode and query operators mode. So, for instance, a search for `portel <NEAR> server` would return documents containing the terms "portal" and "server" in close proximity, but only if there are no matches for "portel" and "server" in close proximity.

Automatic spell correction is enabled by default. You can disable it from the Search Results Manager in the administrative portal user interface. Users can disable spell correction on a per-search basis by using the <WORD> operator.

10.2.5.1 Enabling and Disabling Spell Correction for Searches

Automatic spell correction is applied to the individual terms in a banner search when the terms are not recognized by the Search Service. Spell correction is not applied to quoted phrases.

To access the Search Results Manager you must have the following rights:

- Access Administration activity right
- Access Utilities activity right

- Access Search Results Manager activity right

> **Note:** Spell correction is enabled by default.

1. Click **Administration**.
2. From the **Select Utility** list, select **Search Results Manager**.
3. Click the **Thesaurus and Spell Correction** page.
4. Enable or disable spell correction.
   - To enable spell correction, select the **Apply Spell Correction** check box.
   - To disable spell correction, clear the **Apply Spell Correction** check box.

10.2.6 The Search Thesaurus

The Search Service enables you to create a thesaurus (or synonym list), load it into the server, and enable thesaurus expansion for all user queries. Thesaurus expansion allows a term or phrase in a user's search to be replaced with a set of custom related terms before the actual search is performed. This feature improves search quality by handling unique, obscure, or industry-specific terminology.

For example, with conventional keyword matching, a search for the term "web applications" might not return documents that discuss portlets or Web services. However, by creating a thesaurus entry for "web applications," it is possible to avoid giving users zero search results because of differences in word usage. The entries allow related terms or phrases to be weighted for different contributions to the relevance ranking of search results. For example, "web applications" is not really a synonym for Web services, so a document that actually contains Web applications should rank higher than one that contains Web services.

The entries are lower-case, comma-delimited lists of the form:

```
web applications,portlets,web services[0.5]
```

In this example, the number `[0.5]` corresponds to a nondefault weighting for the phrase `web services`.

Thesaurus entries can be created to link closely related terms or phrases, specialized terminology, obsolete terminology, abbreviations and acronyms, or common misspellings. The expansion works by simply replacing the first term in an entry with an OR query consisting of all the terms or phrases in the entry. The weights are then taken into consideration when matching search results are ranked.

The thesaurus expansion feature is best used for focused, industry- or domain-specific examples. It is not intended to cover general semantic relationships between words or across languages, as with a conventional paper thesaurus. Although the Search Service thesaurus expansion can definitely improve search quality, adding entries for very general or standard terms can actually degrade search quality if it leads to too many search result matches.

10.2.6.1 About the Thesaurus File

The thesaurus is a comma-delimited file, in which each line represents a single thesaurus entry.

The first comma-delimited element on a line is the name of the thesaurus entry. The remaining elements on that line are the search tokens that should be treated as

synonyms for the thesaurus entry. Each synonym can be assigned a weight that determines the amount each match contributes to the overall query score. For example, a file that contains the following two lines defines thesaurus entries for couch and dog:

```
couch,sofa[0.9],divan[0.5],davenport[0.4]
dog,canine,doggy[0.85],pup[0.7],mutt[0.3]
```

Searches for `couch` generate results with text matching terms couch, sofa, divan, and davenport. Searches for `dog` generate results that have text matching terms dog, canine, doggy, pup, and mutt. In the example shown, the term dog has the same contribution to the relevance score of a matching item as the term canine. This is equivalent to a default synonym weighting of 1.0. In contrast, the presence of the term pup contributes less to the relevance score than the presence of the term dog, by a factor of 0.7 (70%).

The example thesaurus entries constitute a complete comma-delimited file. No other information is needed at the beginning or the end of the file. Entries can also contain spaces. For example, a file that contains the following text creates a thesaurus entry for New York City:

```
new york city,big apple[0.9],gotham[0.5]
```

Searches for the phrase “new york city” will return results that also include results containing “big apple” and “gotham.” Thesaurus expansion for phrase entries only occurs for searches on the complete phrase, not the individual words that constitute the phrase. Similarly, the synonym entries are treated as phrases and not as individual terms. So while a search for “new york city” returns items containing “big apple” and “gotham,” a search for new (or for york, or for city, or for “new york”) will not. Conversely, an item that contains big or apple but not the phrase “big apple” will not be returned by a search for “new york city.”

Comma-delimited files support all UTF8-encoded characters; they are not limited to ASCII. However, punctuation should not be included. For example, if you want to make ne'er-do-well a synonym of wastrel, replace the punctuation with whitespace:

```
wastrel,ne er do well[0.7]
```

This matches documents that contain ne'er-do-well, ne er do well or some combination of these punctuations and spaces (such as ne'er do well). If you want your synonym to match documents that contain neer-do-well, which does not separate the initial ne and er with an apostrophe, you must include a separate synonym for that, such as:

```
wastrel,ne er do well[0.7],neer do well[0.7]
```

Comment lines can be specified by beginning the line with a “#”:

```
# furniture entries
couch,sofa[0.9],divan[0.5],davenport[0.4]
#chair,stool[5.0]
# animal entries
dog,canine[0.9],doggy[0.85],pup[0.7],mutt[0.3]
```

In this example, the Search Service parses two thesaurus entries: couch and dog. There will be no entry for chair.

These examples are of entries that contain only ASCII characters. This utility supports non-ASCII characters as well, as long as they are UTF8-encoded.

> **Note:** Some editors, especially when encoding UTF-8, insert a byte order mark at the beginning of the file. Files with byte order marks are not supported, so remove the byte order mark before running the customize utility.

A CDF thesaurus file can have at most 50,000 distinct entries (lines). Each entry can have at most 50 comma-delimited elements (including the name of the entry). If either of these limits are exceeded, the customize utility will exit with an appropriate error message.

10.2.6.2 Creating and Implementing the Synonym List for the Thesaurus

After you create the file, you load it into the Search Service.

1. Create a comma-delimited, UTF-8 file containing the desired thesaurus entries.

   For details on how to format entries, see Section 10.2.6.1, "About the Thesaurus File."

   > **Note:** Thesaurus entries must be in lower-case.

2. Stop the Search Service.

   The comma-delimited file is converted to a binary format in the next step. The conversion removes and replaces certain files used by the Search Service, and this removal and replacement cannot be done while the Search Service is running.

3. At a command prompt, run the customize utility.

   The utility must be run from a command prompt, taking command-line arguments for the thesaurus file and the path to the Search Service installation:

   ```
   customize -r thesaurus_file SEARCH_HOME
   ```

   Replace *thesaurus file* with the path to the thesaurus file and replace *SEARCH_HOME* with the root directory of the Search Service installation.

   For example, if your thesaurus file is located in \temp and your Search Service was installed in the default

   ```
   location, type:
   customize -r \temp\thesaurus.cdf C:\Oracle\Middleware\wci\ptsearchserver\10.3.3
   ```

   The files in `SEARCH_HOME\common` are removed and replaced by files of the same name, though their contents now represent the mappings created by the customize utility.

4. Restart the Search Service.

   The files produced by the customize utility are loaded when the Search Service starts.

If you have not already done so, you must enable the thesaurus in the Search Results Manager.

10.2.6.3 Enabling the Search Thesaurus

The Search Service enables you to create a thesaurus (or synonym list), load it into the server, and enable thesaurus expansion for all user queries. Thesaurus expansion

allows a term or phrase in a user's search to be replaced with a set of custom related terms before the actual search is performed. This feature improves search quality by handling unique, obscure, or industry-specific terminology.

To access the Search Results Manager you must have the following rights:

- Access Administration activity right
- Access Utilities activity right
- Access Search Results Manager activity right

1. Click **Administration**.
2. From the Select Utility list, select **Search Results Manager**.
3. Click the **Thesaurus and Spell Correction** page.
4. Select **Use the Thesaurus**.

If you have not already done so, you must create the synonym list in the database.

10.2.6.4 Reverting to the Default Thesaurus Mappings

The customize utility has a command-line mode for reverting to the set of mappings files that shipped with the Search Service (removing any thesaurus customizations).

1. Stop the Search Service.
2. At a command prompt, run the customize utility.

   The utility must be run from a command prompt, taking a command-line argument for the path to the Search Service installation:

   ```
   customize -default SEARCH_HOME
   ```

   Replace *SEARCH_HOME* with the root directory of the Search Service installation.

   For example, if your Search Service was installed in the default location, type:

   ```
   customize -default C:\Oracle\Middleware\wci\ptsearchserver\10.3.3
   ```

   The files in `SEARCH_HOME\common` are removed and replaced with the original thesaurus file contents.
3. Restart the Search Service.

   The files produced by the customize utility are loaded when the Search Service starts.

If you no longer want to use thesaurus expansion, disable the thesaurus in the Search Results Manager.

10.2.7 Customizing Categorization of Search Results

Users can use the Sort By list on the search results page to sort results by object type or by folder location in the Knowledge Directory or Administrative Objects Directory. You can customize this list to include additional categories relevant for your users. For example, if you use a property in your portal documents named Region, you can customize the Sort By list to include Sort By Region: New England, Midwest, and so forth.

The first issue to consider when assessing whether categorizing search results by a particular property is a good idea is whether the property will be defined for a substantial percentage of all search results. For instance, if 90% of search results do not have the property defined, then when categorizing by that property, most everything

will fall under “All Others”, and the categorization will not be very useful. For that reason, as a rule of thumb it is not generally recommended to add a custom categorization option for a property which is undefined for more than half of all documents and administrative objects.

The other issue to consider is whether the values for the property will make reasonable category titles. In order for categorization to work well for a property, each value should be a single word or a short noun phrase, for example, New England, Midwest, Product Management, Food and Drug Administration, and so forth. The values should not be full sentences or long lists of keywords, for example, “This content crawler crawls the New York Times finance section”. The entire contents of the property value for each item will be considered as a single unit for the purposes of categorization, so it will look odd if a full sentence is returned as a category title.

The first step in the process of adding a new categorization option is to ensure that documents and objects include the property you want to use to sort by category. See Section 7.5.2, "Mapping Source Document Attributes to Portal Properties Using the Global Document Property Map" and Section 7.5.3, "Associating Properties with Portal Objects Using the Global Object Property Map."

You must also ensure that the property that defines the category for sorting has the following configuration:

- Supported for use with documents
- Visible in the user interface
- Searchable
- Mandatory

  Since the search results categorization will only be valuable if there are many items with defined values for the property, and will be of maximum value if everything has a value for the property.
- Named appropriately

10.3 About Grid Search

Grid search consists of shared files (for example, C:\Oracle\Middleware\wci\cluster for Windows or /oracle/middleware/wci/cluster for UNIX or Linux) and search nodes. When you start the Search Service, it looks at the cluster.nodes file in the shared files location to determine the host, port, and partition of each node in the cluster. It monitors and communicates the availability of the search nodes and distributes queries appropriately.

The Search Service also automatically repairs and reconciles search nodes that are out of sync with the cluster. At startup, nodes will check their local TID against the current cluster checkpoint and index queues. If the current node is out-of-date with respect to the rest of the cluster, it must recover to a sufficiently current transaction level (at or past the lowest cluster node TID) before servicing requests for the cluster. Depending upon how far behind the local TID is, this operation may require retrieval of the last-known-good checkpoint data in addition to replaying queued index requests.

Although the Search Service performs many actions automatically to keep your cluster running properly, there are some maintenance and management tasks you perform manually to ensure quality search in your portal.

10.3.1 About Checkpoints

A checkpoint is a snapshot of your search cluster that is stored in the cluster folder (for example, C:\Oracle\Middleware\wci\cluster for Windows or /oracle/middleware/wci/cluster for UNIX or Linux), a shared repository available to all nodes in the cluster. When initializing a new cluster node, or recovering from a catastrophic node failure, the last known good checkpoint will provide the initial index data for the node's partition and any transaction data added since the checkpoint was written will be replayed to bring the node up to date with the rest of the cluster.

You manage checkpoints on the Checkpoint Manager page of the Search Cluster Manager. You can perform the following actions with the Checkpoint Manager:

- Manually create an individual checkpoint or schedule checkpoints to be automatically created on a periodic basis.
- Restore your search collection from a checkpoint.

Since checkpoint data is of significant size, limit the number of checkpoints maintained by the system. Specify how many checkpoints to keep on the Settings page of the Search Cluster Manager.

10.3.2 About Search Cluster Topology

Your search cluster is made up of one or more partitions, each of which is made up of one or more nodes. As your search collection becomes larger, the collection can be partitioned into smaller pieces to facilitate more efficient access to the data. As the Search Service becomes more heavily used, replicas of the existing partitions, in the form of additional nodes, can be used to distribute the load. Additional nodes also provide fault-tolerance; if a node becomes unavailable, queries are automatically issued against the remaining nodes.

Note: If a partition becomes unavailable, the cluster will continue to provide results; however, the results will be incomplete (and thus indicated in the query response).

You manage the partitions and nodes in your search cluster on the Topology Manager page of the Search Cluster Manager. You can perform the following actions with the Topology Manager:

- Add or delete a node.
- Repartition the cluster (add or delete partitions).

Note: Adding a partition to the cluster requires redistributing of potentially hundreds of thousands of documents.

- Assign a node to a different partition.

10.3.3 About Search Logs

Search logs are kept for the search cluster as well as for each node in the search cluster. The cluster logs are stored in the \cluster\log folder, for example, C:\Oracle\Middleware\wci\cluster\log for Windows or /oracle/middleware/wci/cluster/log for UNIX or Linux. The cluster logs include

cluster-wide state changes (such as cluster initialization, node failures, and node recoveries), errors, and warnings.

The node logs are stored in the node's logs folder, for example, C:\Oracle\Middleware\wci\ptsearchserver\10.3.3\node1\logs for Windows or /oracle/middleware/wci/ptsearchserver/10.3.3/node1/logs for UNIX or Linux. There are two kinds of node logs: event logs and trace logs. Event logs capture major node-local state changes, errors, warnings, and events. Trace logs capture more detailed tracing and debugging information.

There are several ways to view the logs:

- You can open the log file in a text reader.
- You can view search logging through PTSpy.
- You can set up another OpenLog listener to receive logging information.

A new cluster log is created with each new checkpoint. The log that stores all activity since the last checkpoint is called cluster.log. When a new checkpoint is created, the cluster.log file is saved with the name checkpoint.log, for example, 0_1_5116.log.

10.3.4 About the Command Line Admin Utility

The Command Line Admin Utility lets you to perform the same functions you can perform in the Search Cluster Manager as well as change the run level of the cluster and purge and reset the search collection.

The Command Line Admin Utility is located in bin\native folder in the Search Service installation folder (for example, C:\Oracle\Middleware\wci\ptsearchserver\10.3.3\bin\native\cadmin.exe for Windows or /oracle/middleware/wci/ptsearchserver/10.3.3/bin/native/cadmin for UNIX or Linux). Invoking the command with no arguments displays a summary of the available options:

```
% $RFHOME/bin/native/cadmin
Usage: cadmin <command> [command-args-and-options] [--cluster-home <CLUSTER_HOME>]
```

This Command Line Admin Utility lets you perform the following actions:

- Section 10.3.4.2, "Requesting Search Cluster Status for a Particular Node"
- Section 10.3.4.1, "Requesting Search Cluster Status"
- Section 10.3.4.3, "Changing the Run Level of the Cluster"
- Section 10.3.5.1, "Purging the Search Collection"
- Section 10.3.4.4, "Initiating a Cluster Checkpoint"
- Section 10.3.4.5, "Reloading from a Checkpoint"
- Section 10.3.4.6, "Changing Cluster Topology"
- Section 10.3.4.7, "Aborting a Checkpoint or Reconfiguration Operation"

10.3.4.1 Requesting Search Cluster Status

You can use the Command Line Admin Utility to view the status of your search cluster.

The Command Line Admin Utility is located in bin\native folder in the Search Service installation folder (for example, C:\Oracle\Middleware\wci\ptsearchserver\10.3.3\bin\native\cadmin.exe for

Windows or /oracle/middleware/wci/ptsearchserver/10.3.3/bin/native/cadmin for UNIX or Linux).

- Run the status command to display the status of the cluster.

```
% cadmin status --cluster-home=/shared/search
```

  By default, the status command displays a terse, one-line summary of the current state of the cluster:

```
2005-04-22 13:54:13 checkpoint_xxx 0/1/198 0/1/230 impaired
```

- Run the status command with the verbose flag to display the full set of information, including the status of every node in the cluster.

```
% cadmin status --verbose --cluster-home=/shared/search

2005-04-22 13:54:13 /shared/search checkpoint_xxx
cluster-state: impaired
cluster-tid: 0/1/198 0/1/230
partition-states: complete impaired
node p0n0: 0 192.168.1.1 15244 0/1/198 0/1/460 run
node p0n1: 0 192.168.1.2 15244 0/1/198 0/1/460 run
node p1n0: 1 192.168.1.3 15244 0/1/198 0/1/230 run
node p1n1: 1 192.168.1.4 15244 0/1/100 0/1/120 offline
```

- Run the status command with the period flag to repeatedly emit status requests at a specified interval.

```
% cadmin status --period=10 --count=5

2005-04-22 13:54:13 checkpoint_xxx 0/1/198 0/1/230 impaired
2005-04-22 13:54:23 checkpoint_xxx 0/1/198 0/1/230 impaired
2005-04-22 13:54:33 checkpoint_xxx 0/1/198 0/1/230 impaired
2005-04-22 13:54:43 checkpoint_xxx 0/1/198 0/1/230 impaired
2005-04-22 13:54:53 checkpoint_xxx 0/1/400 0/1/428 complete
```

10.3.4.2 Requesting Search Cluster Status for a Particular Node

You can use the Command Line Admin Utility to request information about specific nodes within the cluster.

The Command Line Admin Utility is located in bin\native folder in the Search Service installation folder (for example, C:\Oracle\Middleware\wci\ptsearchserver\10.3.3\bin\native\cadmin.exe for Windows or /oracle/middleware/wci/ptsearchserver/10.3.3/bin/native/cadmin for UNIX or Linux).

- Run the nodestatus command to display the status of a particular node.

```
% cadmin nodestatus p0n0 p1n0
```

  This displays the same type of information that is displayed as part of the verbose cluster status request:

```
node p0n0: 0 192.168.1.1 15244 0/1/198 0/1/460 run
node p1n0: 1 192.168.1.3 15244 0/1/198 0/1/230 run
```

- Run the nodestatus command with the period flag to repeatedly emit status requests at a specified interval.

```
% cadmin nodestatus p0n0 p1n0 --period=10
```

```
2005-04-22 13:54:13 p0n0 0 192.168.1.1 15244 0/1/198 0/1/460 run
2005-04-22 13:54:13 p1n0 0 192.168.1.1 15244 0/1/198 0/1/460 run
2005-04-22 13:54:23 p0n0 0 192.168.1.1 15244 0/1/198 0/1/460 run
2005-04-22 13:54:23 p1n0 0 192.168.1.1 15244 0/1/198 0/1/460 run
```

10.3.4.3 Changing the Run Level of the Cluster

You can use the Command Line Admin Utility to modify the run level of the cluster, or of individual nodes within the cluster. For example, you might want to place nodes in standby mode before changing cluster topology or shutting them down.

Transitioning from standby to any of the operational modes (recover, readonly, stall, run) will validate the node's state against the cluster state and will trigger a checkpoint restore if one is warranted. Transitions to readonly or offline modes are also potentially useful: readonly mode halts incorporation of new index data on a node; offline mode will cause the search server to exit.

The Command Line Admin Utility is located in bin\native folder in the Search Service installation folder (for example, C:\Oracle\Middleware\wci\ptsearchserver\10.3.3\bin\native\cadmin.exe for Windows or /oracle/middleware/wci/ptsearchserver/10.3.3/bin/native/cadmin for UNIX or Linux).

- To set run level of p0n0 and p1n0 to standby, run:

  ```
  % cadmin runlevel standby p0n0 p1n0
  ```

- To set run level of the entire cluster to run (affects only non-offline nodes), run:

  ```
  % cadmin runlevel run
  ```

10.3.4.4 Initiating a Cluster Checkpoint

A checkpoint is a snapshot of your search cluster that is stored in the cluster folder (for example, C:\Oracle\Middleware\wci\cluster for Windows or /oracle/middleware/wci/cluster for UNIX or Linux), a shared repository available to all nodes in the cluster. When initializing a new cluster node, or recovering from a catastrophic node failure, the last known good checkpoint will provide the initial index data for the node's partition and any transaction data added since the checkpoint was written will be replayed to bring the node up to date with the rest of the cluster.

The Command Line Admin Utility is located in bin\native folder in the Search Service installation folder (for example, C:\Oracle\Middleware\wci\ptsearchserver\10.3.3\bin\native\cadmin.exe for Windows or /oracle/middleware/wci/ptsearchserver/10.3.3/bin/native/cadmin for UNIX or Linux).

10.3.4.5 Reloading from a Checkpoint

You can use the Command Line Admin Utility to reload your cluster from a saved checkpoint.

1. Run the restore command:

   ```
   % cadmin restore
   ```

Since restoring from a checkpoint is a time-consuming process, the admin utility displays its progress.

Example 10–1 Output from Restoring from a Checkpoint

```
Restoring cluster from \\cluster_home\checkpoint_xxx
Node p0n0 retrieving data
Node p0n1 retrieving data
0%..10%..20%..30%..40%..50%..60%..70%..80%..90%..100%
Node p0n0 restarted
Node p0n1 restarted
Restoration complete
```

10.3.4.6 Changing Cluster Topology

You can use the Command Line Admin Utility to add or remove nodes from the search cluster or repartition the search cluster.

The Command Line Admin Utility is located in bin\native folder in the Search Service installation folder (for example, C:\Oracle\Middleware\wci\ptsearchserver\10.3.3\bin\native\cadmin.exe for Windows or /oracle/middleware/wci/ptsearchserver/10.3.3/bin/native/cadmin for UNIX or Linux).

1. Run the topology command:

   ```
   % cadmin topology new.nodes
   ```

2. Change the cluster.nodes file:

   - To add new nodes to the search cluster (for failover capacity), install a new node, and edit the cluster.nodes file to include the node as a peer on an existing partition.

     Issue a "soft reset" to the cluster through the command line utility, which causes all nodes to re-examine the cluster topology file and thus recognize the new node. When the new node receives a soft reset, it recognizes that it must catch up to the rest of the cluster and begins the automated index recovery process from the last checkpoint.

   - To repartition the cluster, edit the number of partitions in the cluster.nodes file. You will be asked to confirm the action and the admin utility will confirm that a checkpoint exists before performing the repartitioning operation.

Since changing cluster topology can be a time-consuming process, the admin utility displays its progress.

Example 10–2 Output from Adding and Removing Nodes

```
Current topology:
<contents of current cluster.nodes file>
New topology:
<contents of new.nodes file>
Nodes to add: p0n2, p1n2, p2n2
Nodes to remove: p0n0, p1n0, p2n0
Is this correct (y/n)? y
Applying changes…
p0n2 has joined
p2n0 has left
...
Changes applied successfully
```

Example 10–3 Output from Repartitioning the Cluster

```
Current topology:
<contents of current cluster.nodes file>
New topology:
<contents of new.nodes file>
Nodes to add: p3n0, p3n1
Is this correct (y/n)? y
CAUTION: the requested changes require repartitioning the search collection
The most recent checkpoint is checkpoint_xxx from 2004-04-22 16:00:00
Is this correct (y/n)? y
Repartitioning from 3 partitions into 4
0%
5%
<progress messages>
100%
Repartitioning successful
Applying changes…
p0n2 has joined
p2n0 has left
...
Changes applied successfully
```

If the repartition fails, the search collection leaves the cluster in its original state, if at all possible, and provides information about the failure. The cluster.nodes file is rolled back to the previous state after making sure that the last-known good checkpoint refers to an un-repartitioned checkpoint directory.

10.3.4.7 Aborting a Checkpoint or Reconfiguration Operation

You can abort a long-running checkpoint or cluster reconfiguration operation by exiting from the command line utility.

- To exit from the command line utility, press CTRL+C.

  The cluster will be restored to its state before attempting the checkpoint or topology reconfiguration.

  In the case of a checkpoint operation, the utility sends a "checkpoint abort" command to the checkpoint coordinator to cleanly abort the checkpoint create/restore operation.

  In the case of a cluster reconfiguration, the utility restores the original cluster.nodes file and initiates a soft restart of the affected cluster nodes to restore the cluster to its previous configuration.

10.3.5 Purging and Rebuilding the Search Collection

You can purge and rebuild the contents of the search collection. You might want to do this in a dire situation where the contents of the cluster are corrupted beyond repair and good checkpoints are not available for recovery.

1. Put all cluster nodes in standby mode.
2. Purge the collection.
3. Rebuild the collection.
4. If your portal deployment includes Oracle WebCenter Collaboration, rebuild the Oracle WebCenter Collaboration index.

10.3.5.1 Purging the Search Collection

You can purge the contents of the search collection. You might want to purge the cluster in staging or development systems, or if you want to clean out the search collection without re-installing all the nodes. Purging (and rebuilding) the search collection may also be useful in a dire situation where the contents of the cluster are corrupted beyond repair and good checkpoints are not available for recovery.

As a safeguard against purging the collection by accident, all cluster nodes must be in standby mode.

The Command Line Admin Utility is located in bin\native folder in the Search Service installation folder (for example, C:\Oracle\Middleware\wci\ptsearchserver\10.3.3\bin\native\cadmin.exe For Windows or /oracle/middleware/wci/ptsearchserver/10.3.3/bin/native/cadmin for UNIX or Linux).

By default, the checkpoints and index queue are left in place, enabling you to rebuild the local index on a node where the archive appears to be corrupted. You can add a flag to the command to remove the checkpoints.

- To purge the search collection, but keep checkpoints:

  ```
  % cadmin purge
  ```

  As a safeguard against purging the collection by accident, you must confirm the action before the purge command is sent out.The purge command causes a node to generate empty archive collections (document, spell, and mappings) and perform a soft-restart to load them into memory. Before reloading, the admin utility updates the checkpoint files in the shared repository to prevent the nodes from automatically reloading from an existing checkpoint.

- To purge the search collection and delete existing checkpoints:

  ```
  % cadmin purge --remove-checkpoints
  ```

Sometimes the purge command does not work properly, where it fails to purge the index files. During this scenario the search file structure gets tainted and the Search Service will not start. If this occurs you receive an error similar to this:

```
Failed Unexpected exception while sending PURGE to searchserver01, Error during
parsing: Failed -- purge failed on streetfighter01 This node should be shutdown,
purged, and restarted manually.
```

At this point you will not be able to shut down, purge, or restart the Search Service. You must re-run the Oracle WebCenter Interaction installer. Select only the Search Service option and choose overwrite.

If you are purging the collection to correct a problem (for example if your collection was corrupted or you had to reinstall the Search Service), your next step is to rebuild the collection.

10.3.5.2 Rebuilding the Search Collection

Your search index might get out of sync with your database if, during a crawl, the Search Service became unavailable or a network failure prevented an indexing operation from completing. Another possibility is that a Search Service with empty indexes was swapped into an existing portal with pre-existing documents and folders.

To rebuild the search collection you must have the following rights:

- Access Administration activity right

- Access Search Results Manager activity right

The Search Service Manager lets you specify when and how often the Search Update Agent repairs your search index. Rather than synchronizing particular objects, the repair synchronizes all objects in the database with the search index. Searchable objects in the database are compared with IDs in the search index. If an object ID in the database is not in the search index, the Search Update Agent attempts to re-index the object; if an ID in the search index is not in the database, the Search Update Agent removes the object from the search index.

Run the Search Update Agent for purposes of background maintenance or complete repopulation of the search index.

1. Configure the Search Service to repair itself.
   a. Click **Administration**.
   b. From the Select Utility list, choose **Search Service Manager**.
   c. Under Search Repair Settings, change **Next Repair Date** to a time in the past.
   d. Click **Administration** again.
2. Wait one minute for the setting to update.
3. Run one of the Search Update jobs in verbose mode.
   a. Open the **Intrinsic Operations** folder.
   b. Open one of the Search Update jobs.

      The Job Editor opens.
   c. Change the Logging Level to **Verbose** and click **Finish**.

      Note: Make note of the logging mode before you change it, so that you can change it back after the repair is complete.

   d. Select the job you just edited and click **Run Once**.

      By running the job this way, you avoid having to go back into the job and revert to the previous schedule settings.
4. Ensure that the job is running in repair mode.
   1. Open the job you just created; it should be called something like Search Update 1 — Run Once.

      The Job Editor opens.
   2. Click the **Job History** page.
   3. Click the job name.

      The job log opens.
   4. Ensure that the job is running in repair mode.

      The second line of the job log should be similar to this:

      ```
      Mar 1, 2008 9:10:02 AM- PTIndexer.ctor : Indexing will extract at most
      1000000 encoded bytes of text from each document.
      ```

      About half-way down the first page of the log you should see a message that should be similar to this:

```
Mar 1, 2008 9:10:02 AM- Search Update Agent is repairing the directories...
```

5. Reinstall the Search Service and select **Overwrite the existing search index**. For details on installing the Search Service, refer to the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Interaction for Windows* or the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Interaction for Unix and Linux*.

10.3.5.3 Rebuilding the Oracle WebCenter Collaboration Search Collection

Rebuilding reconciles data between the Oracle WebCenter Collaboration database and Search Service index. Since this is a lengthy and computationally expensive process, use the rebuild operation only when absolutely necessary.

To access the Collaboration Administration Utility you must have the following rights:

- Access Administration activity right
- Access Utilities activity right
- Manage Collaboration activity right

1. Click **Administration**.
2. In the Select Utility list, click **Collaboration Administration**.
3. Click the **Search Service** page.
4. Click **Rebuild Search Collection**.

10.4 About the Search Update Job

The Search Update job performs the following actions on the search index: updates the index, releases expired locks on users and objects, and repairs the search index according to the Search Service Manager repair settings.

The Search Update job is located in the Intrinsic Operations administrative folder. The default frequency of the Search Update job is one hour, which is suitable for most portal deployments. If your search index is very large, the Search Update Agent might not be able to finish in one hour, so you should edit the frequency of the job.

10.4.1 How the Search Index is Updated

As users create, delete, and change objects in the portal, the search index gets updated. In some cases, the portal updates the search index immediately; in other cases, the search is not updated until the next time the Search Update Agent runs.

The following table describes the cases in which the search index is updated immediately (I) or updated by the Search Update Agent (SU).

Object	Create	Delete	Move	Change Name or Description	Change Other Properties
Document	I	SU	SU	I	I
Directory Folder	I	SU	SU	I	SU
Administrative Folder	I	I	I	I	I
Administrative Object	I	I	I	I	I

Note: If the Knowledge Directory preferences are set to use the search index to display browse mode, changes will not display until the Search Update Agent runs. The Knowledge Directory edit mode and the Administrative Object Directory display objects according to the database, and therefore show changes immediately.

10.5 About Providing Search Access to External Repositories with Federated Searches

Federated searches allow you to establish search relationships with other sources (including other portals, Web sites, or custom databases). Federated searches provide end users a single interface and unified result set for searches over multiple Oracle WebCenter Interaction portals, as well as parallel querying of external internet and intranet-based search engines.

There are incoming and outgoing federated searches:

- An incoming federated search allows other Oracle WebCenter Interaction portals to search your portal.
- An outgoing federated search enables users of your portal to search other Oracle WebCenter Interaction portals or other external repositories.

10.5.1 Search Web Services

Search Web services allow you to specify general settings for your remote search repository, leaving the security settings to be set in the associated outgoing federated searches, enabling you to segregate access to your search repository through multiple outgoing federated searches.

If there is a non-portal repository to search, Oracle or another vendor might have written a search Web service to access it. If not, Oracle provides an IDK that enables you to write your own search Web services in Java or .NET. For details, refer to the *Oracle Fusion Middleware Web Service Developer's Guide for Oracle WebCenter Interaction*.

Note: The settings for outgoing federated search objects will often be specific to the search Web services that implement the searches. In these cases, the Web services themselves provide the configuration options as Service Configuration Interface (SCI) pages.

10.5.2 Portal-to-Portal Searches

One Oracle WebCenter Interaction portal can request and/or serve content to another Oracle WebCenter Interaction portal. When you install the portal, the Public Access incoming federated search is created. This allows other Oracle WebCenter Interaction portals to search this portal as the Guest user.

To allow other search relationships, you must create new incoming or outgoing federated searches. Whether your portal is requesting or serving content, you and the other administrators involved must agree upon the following issues before establishing federated searches:

- Which portals will serve content?
- Which portals will request content?
- What portal identification name and password will be used to identify the portals?

For every request issued, the requesting portal sends an ID and password to identify itself to the serving portal. You must enter the same ID and password in both the requesting portal's outgoing federated search and the serving portal's incoming federated search.

- What content from the serving portal will be available to the requesting portal?

  If both portals share a common external database of users, such as an LDAP server or Active Directory domain, and those users have been imported into both portals, grant the shared users access to the appropriate content on the serving portal. This provides the greatest degree of content security without requiring any additional administrative work.

  If the portals do not share a database of user information, users from the requesting portal must impersonate users from the serving portal. Because impersonation is specified on a group basis (that is a group from the requesting portal is set to impersonate a user from the serving portal), you should create a different serving portal user for each requesting portal group that needs access to different content in the serving portal.

  Note: You should create new serving portal users specifically for impersonation, then communicate the user names and what they can access to the administrator of the requesting portal.

  The serving portal can also allow unauthenticated users to search the portal as the Guest user.

After you and the other administrators involved have determined how this relationship will work, you are ready to establish your incoming or outgoing federated searches.

For an example of how requesting portal users can impersonate serving portal users to gain access to secured content, see Section 10.5.6, "Example of Impersonating Serving Portal Users."

To learn how multiple portals accessing the same user repository can share content, see Section 10.5.3, "Building a Composite Portal with Federated Searches."

10.5.3 Building a Composite Portal with Federated Searches

Multiple portals accessing the same user repository can share content. All portals involved in the relationship must import the same users and groups from a single user repository.

There are two scenarios for building a composite portal:

- Multiple content portals each possess links to a large number of documents. A single user can visit the separate content portals, always with the same user name and password, and always receive access to the correct content.

  In this scenario, each portal acts as both a serving and a requesting portal.

- One portal is set up as a master portal rather than a content portal. Through this master portal, users can access content from the various content portals.

  In this scenario, the master portal acts as the requesting portal, and the content portals act as the serving portals.

- On each serving portal, the administrator creates an incoming federated search that includes the authentication sources that the serving portals share with the requesting portals.

  All users making requests to a serving portal must be imported into the portal through one of these common authentication sources.

- On each requesting portal, the administrator creates an outgoing federated search for each content portal, selecting **No** for **Send portal authentication**.

  Users will make the requests using their own user accounts.

10.5.4 Allowing Other Portals to Search Your Portal

An incoming federated search allows other Oracle WebCenter Interaction portals to search your portal.

Before you create an incoming federated search, you must:

- Agree upon a portal identification name and password with the administrator of the requesting portal.
- If the users from the requesting portal do not exist in your portal, create one or more portal users that can be impersonated by users of the requesting portal.

To create an outgoing federated search you must have the following rights and privileges:

- Access Administration activity right
- Create Federated Searches activity right
- At least Edit access to the parent folder (the folder that will store the federated search)
- If the users from the requesting portal do not exist in your portal, at least Select access to the authentication sources or groups that include the impersonated users

1. Click **Administration**.
2. Open the folder in which you want to store the federated search.
3. In the **Create Object** list, click **Federated Search - Incoming**.
4. In the **Portal identification name** box, type the agreed upon name.
5. In the **Portal identification password** box, type the agreed upon password.
6. In the **Password confirmation** box, type the password again.
7. In the **Served links are valid for** box, type the minimum number of minutes or which these results should be cached.

   After a requesting portal issues a search of your portal, the links returned by the search are stored for at least as long as you specify here. After this period has elapsed, the user on the requesting portal might must re-issue the search.
8. To allow unauthenticated users to search the portal as a guest, click the **Allow unauthenticated users to search as the Guest user** box.
9. If the users from the requesting portal do not exist in your portal, select the authentication sources or groups that include the impersonated users.

   Incoming search requests include the name of a local portal user (that is, a user from the serving portal) to impersonate during the search. The request is honored

only if the impersonated user is a member of one of the authentication sources or one of the groups you specify.

- To add an authentication source, click **Add Authentication Source**, in the Choose Authentication Sources dialog box, select an authentication source, and click **OK**.
- To add a group, click **Add Group**, in the Choose Groups dialog box, select a group, and click **OK**.
- To delete an authentication source or a group, select it and click the Remove icon.

  To select or clear all of the authentication source or group boxes, select or clear the box to the left of **Authentication Sources** or **Groups**.
- To toggle the order in which the authentication sources or groups are sorted, click **Authentication Sources** or **Groups**.

10.5.5 Providing Search Access to External Repositories with Outgoing Federated Searches

An outgoing federated search enables users of your portal to search other Oracle WebCenter Interaction portals or other external repositories.

Before you create an outgoing federated search, you must:

- Create a search Web service.
- Agree upon a portal identification name and password with the administrator of the serving portal.
- If your portal users do not exist in the serving portal, work with the serving portal user to determine the serving portal users that can be impersonated and what they can access.

To create an outgoing federated search you must have the following rights and privileges:

- Access Administration activity right
- Create Federated Searches activity right
- At least Edit access to the parent folder (the folder that will store the federated search)
- If your portal users do not exist on the serving portal, at least Select access to the groups that must impersonate serving portal users

1. Click **Administration**.
2. Open the folder in which you want to store the federated search.
3. In the **Create Object** list, click **Federated Search - Outgoing**.

   The Choose Web Service dialog box opens.
4. Select the Web service that provides the basic settings for your outgoing federated search and click **OK**.

   The Outgoing Federated Search Editor opens, displaying the Portal to Portal Settings page.
5. If you are not searching another Oracle WebCenter Interaction portal, leave **No** selected.

If you are searching another Oracle WebCenter Interaction portal:

a. Next to **Send portal authentication**, select **Yes**.

b. In the **Portal identification name** box, type the agreed upon name.

c. In the **Portal identification password** box, type the agreed upon password.

d. In the **Password confirmation** box, type the password again.

e. If your portal users do not exist on the serving portal, under **User Name Aliasing**, map groups from your portal to users from the serving portal that they can impersonate:

Note: When a requesting user tries to search a serving portal, the requesting portal examines the list of mapped groups from the top down; the first group in the list to which the requesting user belongs is used to determine what serving portal user the requesting user will impersonate. Therefore, groups with high levels of security should be mapped first (at the top of the list), so that requesting users are granted the highest level of security available to them.

- Click **Add Group**, in the Select Group dialog box, select the groups you want to add and click **OK**.
- To the far right of the group, click the Edit icon.
- In the **Use this user name alias** column box, type the name of the serving portal user whom you want this group of requesting users to impersonate.
- Click the Save icon to save the mapping.

  To delete a group, select it and click the Remove icon. To select or clear all of the group boxes, select or clear the box to the left of **Members of this group**.

After the administrator of the serving portal has set up the incoming federated search, your users can use federated search to search content from the other portal.

10.5.6 Example of Impersonating Serving Portal Users

This example shows how a search relationship might be set up between two separate portals.

The fictional company *Servicor* wants to share content with its fictional partner *Requesticon*. In this case, Servicor's portal is the serving portal, and Requesticon's portal is the requesting portal.

10.5.6.1 Configuring the Serving Portal

First, the administrator of the Servicor portal creates two portal users: *Requesticon Engineer* and *Requesticon Executive*. Both of these users are added to the portal group named *Requesticon Visitors*.

These users are then individually granted access to appropriate content on the Servicor portal. Requesticon Engineer is granted Read access to the *Engineering*, *QA*, and *Product Management* folders of the Servicor Knowledge Directory. Requesticon Executive is granted Read access to the *Servicor Market* and *Investor Relations* folders.

The administrator of the Servicor portal then sets up an incoming federated search. On the Main Settings page of the Incoming Federated Search Editor, the Servicor

administrator includes the *WCI Authentication Source* and the group *Requesticon Visitors*. The WCI Authentication Source is included because the Requesticon Engineer and the Requesticon Executive users were both created in the portal; had they been imported through another authentication source, then *that* authentication source would must be included instead. The Requesticon Visitors group is included here to prevent users of the requesting portal from attempting to impersonate any user other than Requesticon Engineer or Requesticon Executive.

With the serving portal configured this way, only requests issued by Requesticon Engineer and Requesticon Executive are answered, and only appropriate content is visible.

10.5.6.2 Configuring the Requesting Portal

On the Main Settings page of the Outgoing Federated Search Editor, the administrator of the Requesticon portal selects **Yes** for **Send portal authentication**. Then, under User Name Aliasing, the Requesticon administrator maps the group *Executives* to the Servicor user named *Requesticon Executive* and the group *Engineers* to the Servicor user named *Requesticon Engineer*. This way, all users that are members of the Engineers group impersonate Requesticon Engineer when issuing requests, and all users that are members of the Executives group issue requests as Requesticon Executive.

> **Note:** The Requesticon Engineer and Requesticon Executive exist only in the Servicor portal, not in the Requesticon portal; these users were created specifically for impersonation by Requesticon users.

When a requesting user tries to search a serving portal, the requesting portal examines the list of mapped groups from the top down; the first group in the list to which the requesting user belongs is used to determine what serving portal user the requesting user will impersonate. Therefore, groups with high levels of security should be mapped at the top of the list. The requesting portal administrator made sure to add the Executives group *before* the Engineers group so that if any user on the requesting portal is a member of both the Executives group and the Engineers group, then that user will impersonate the Requesticon Executive user. Being an executive, this user is likely to be granted access to more content.

10.6 Working with Search Web Services

This section describes the following main tasks:

- Section 10.6.1, "Creating or Editing a Search Web Service"
- Section 10.6.2, "Deleting a Search Web Service"

It also covers the following low-level task:

- Section 10.6.3, "Sending General Settings from a Search Web Service to Associated Federated Searches"

10.6.1 Creating or Editing a Search Web Service

Before you create a search Web service, you must:

- Install the search provider on the computer that hosts the portal or on another computer
- Create a remote server pointing to the computer that hosts the search provider (optional, but recommended)

To create a search Web service you must have the following rights and privileges:

- Access Administration activity right
- Create Web Service Infrastructure activity right
- At least Edit access to the parent folder (the folder that will store the search Web service)
- At least Select access to the remote server that the search Web service will use

To edit a search Web service you must have the following rights and privileges:

- Access Administration activity right
- At least Edit access to the search Web service
- At least Select access to the remote server that the search Web service will use

To create or edit a search Web service:

1. Click **Administration**.
2. Open the Search Web Service Editor.
   - To create a search Web service, open the folder in which you want to store the search Web service. In the Create Object list, click **Web Service — Search**.
   - To edit a search Web service, open the folder in which the search Web service is stored and click the search Web service name.
3. On the Main Settings page, complete the following tasks:
   - Section 3.4.1, "Associating a Remote Server with a Web Service"
   - Section 3.4.2, "Specifying the Location of the Web Service Provider or Code"
   - Section 3.4.3, "Specifying Web Service Time-Out Settings"
   - Section 3.4.4, "Enabling and Disabling a Web Service"
4. On the HTTP Configuration page, perform tasks as necessary:
   - Section 3.4.6, "Specifying How Gatewayed Content is Handled"
   - Section 3.4.7, "Specifying What Content is Gatewayed for a Web Service"
5. On the Advanced URL Settings page, perform tasks as necessary:
   - Section 3.4.8, "Adding a Service Configuration Page to a Web Service Editor"
   - Section 3.4.9, "Adding an Administrative Configuration Link to the Select Utility Menu"
   - Section 3.4.10, "Adding a User Configuration Link to the My Account Page"
6. On the Advanced Settings page, perform tasks as necessary:
   - Section 10.6.3, "Sending General Settings from a Search Web Service to Associated Federated Searches"
   - Section 3.4.11, "Specifying Encoding Style for a Web Service"
7. On the Authentication Settings page, perform tasks as necessary:
   - Section 3.4.13, "Specifying Authentication Settings for a Web Service"
8. On the Preferences page, perform tasks as necessary:
   - Section 3.4.14, "Sending User Preferences from the Web Service to Associated Objects"

9. On the User Information page, perform tasks as necessary:
   - Section 3.4.15, "Sending User Information from a Web Service to Associated Objects"
10. On the Debug Settings page, perform tasks as necessary:
   - Section 3.4.16, "Enabling Error Tracing for a Web Service"
11. On the Associated Objects page, perform tasks as necessary:
   - Section 3.4.17, "Viewing Objects Associated with a Web Service"
12. On the Properties and Names page, perform tasks as necessary:
   - Section 5.15, "Naming and Describing an Object"

     You can instead enter a name and description when you save this search Web service.
   - Section 5.16, "Managing Object Properties" (optional)
13. On the Security page, perform tasks as necessary:
   - Section 5.17, "Setting Security on an Object"

   The default security for this search Web service is based on the security of the parent folder. Administrative users with at least Select access to this search Web service and the Create Federated Searches activity right can create federated searches based on the Web service.
14. If you are editing a search Web service, on the Migration History and Status page, perform tasks as necessary:
   - Section 5.18, "Viewing Migration History and Status for an Object"

   Note: The Migration History and Status page is not available when creating an object.

10.6.2 Deleting a Search Web Service

To delete a search Web service you must have the following rights and privileges:

- Access Administration activity right
- Admin access to the search Web service

To delete a search Web service:

1. Click **Administration**.
2. Navigate to the search Web service.
3. Select the search Web service you want to delete and click the delete icon.

   Note: Deleting a search Web service will break any associated federated searches.

10.6.3 Sending General Settings from a Search Web Service to Associated Federated Searches

To specify what information the search Web service passes to associated federated searches:

1. If the Search Web Service Editor is not already open, open it now.
2. Click the **Advanced Settings** page.
3. Under Settings, specify what general information, if any, you want this Web service to pass to its associated federated searches:
   - To send the language of the user from which the search request is sent, select **Send Locale to service**.
   - To send the time zone of the user from which the search request is sent, select **Send timezone to Portlets**.
   - If this Web service requires the user to have an API session (for example, if the Web service uses the SOAP API), select **Send Login token to Portlets**; then, in the **Login Token duration** box, type the number of minutes you want the API session to last.
   - To send the ID of the experience definition from which the portlet request is sent, select **Send Experience Definition ID to Portlets**.

11

Automating Administrative Tasks

This chapter describes the steps you take to set up the Automation Service and schedule jobs that perform routine portal administration tasks.

It includes the following sections:

11.1 About Jobs

Jobs allow you to schedule portal management operations. A job is a collection of related operations. Each operation is one task, such as a crawl for documents, an import of users, or one of the system maintenance tasks.

You must run jobs to perform the following actions:

- Import or synchronize users and groups through an authentication source
- Import or refresh documents through a content crawler
- Perform external operations
- Run and store content for some portlets
- Import user information through a profile source
- Move or copy content through a smart sort (the portal creates and runs the job automatically)

11.2 About Portal Agents

The portal comes with several operations that can only be accessed through the jobs with which they are associated. These special operations are referred to as agents.

The following agent jobs are stored, by default, in the Intrinsic Operations portal folder:

- The Audit Log Management Agent job archives old audit messages into files and deletes old audit files.

  The Audit Log Management Agent job also archives and deletes audit files according to the schedule set in the Audit Manager utility.
- The Bulk Subscriptions Agent job subscribes users in bulk to the communities and portlets you specify in the Bulk Add editor.
- The Document Refresh Agent job performs background maintenance on your Knowledge Directory, such as refreshing document links and properties, and deleting expired documents.
- The Dynamic Membership Update Agent job updates dynamic portal group memberships.
- The Search Update Agent job makes sure the search collection is synchronized with the database. You can run multiple instances of this job at the same time.

  The Search Update Agent job also repairs the search index according to the frequency set in the Search Service Manager utility.
- The Weekly Housekeeping Agent job performs weekly housekeeping on your system, such as deleting expired invitation codes and old job logs and removing community members who no longer have access to a community.

11.3 About Running Scripts Through the Portal with External Operations

An external operation enables you to run shell scripts (for example, .sh or .bat files) through the portal and schedule these actions through portal jobs. For example, you might want to create a script that queries documents, pings portal servers, e-mails snapshot query results to users, or runs some other custom job, then create an external operation that points to the script, and use a job to run the script on a specified schedule.

11.3.1 External Operations Created Upon Installation

When you install the portal, there are two working example external operations that are created in the Intrinsic Operations portal folder:

- **Bulk Subscriber**: This external operation subscribes users to communities and groups when you use bulk add.
- **Snapshot Query Mailer**: This is a sample external operation that e-mails the results of snapshot queries to users.

  For more information on this external operation, see Section 7.16.7, "E-mailing the Results of a Snapshot Query."

11.4 Working with External Operations

This section describes the following tasks:

11.4.1 Creating or Editing External Operations

To create an external operation you must have the following rights and privileges:

- Access Administration activity right
- Create External Operations activity right
- At least Edit access to the parent folder (the folder that will store the external operation)
- At least Edit access to the job that will run this external operation

To edit an external operation you must have the following rights and privileges:

- Access Administration activity right
- At least Edit access to the external operation
- If you plan to change the job that will run this external operation, at least Edit access to the job

---

Note:

- Because the standard error output from the command or script is captured to the job log, avoid the use of new shells, redirects, and pipes.
- Passing arguments to `cmd` or `start` in shell programs might disable the time-out mechanism.
- When you are extending scripts in the External Operation Editor, carefully consider all potential effects of the scripts. Ensure that your script does not introduce a security risk.

To create or edit an external operation:

1. Click **Administration**.
2. Open the External Operation Editor.
   - To create an external operation, open the folder in which you want to store the external operation. In the Create Object list, click **External Operation**.
   - To edit an external operation, open the folder in which the external operation is stored and click the external operation name.
3. In the **Operating System Command** box, type the relative path and file name of the script enclosed in quotes (“).

> **Note:** All external operation scripts must reside in the scripts directory of each of the Automation Services that will run them. The scripts directory is located on the computer that hosts the Automation Service, in the Oracle WebCenter Interaction installation directory (for example, C:\Oracle\Middleware\wci\ptportal\scripts for Windows or /oracle/middleware/wci/ptportal/scripts for UNIX or Linux). The Automation Service will not run any scripts that are not in this directory.

The following tokens in the command line will be substituted:

- names of environment variables surrounded with percent signs (%)
- `<user_id>`
- `<security_token>`
- `<job_id>`
- `<operation_id>`
- `<last_job_runtime>`

Expanded tokens that contain spaces or special characters which are not surrounded with quotes (“) are enclosed in quotes automatically.

4. In the **Time-out in seconds** box, type the number of seconds after which, if this operation is still running, you want the job to stop.

   If you do not want to set a time-out, leave this setting at **0** (infinite).

To run this operation, you must associate it with a job and schedule the job to run.

11.4.2 Deleting an External Operation

To delete an external operation you must have the following rights and privileges:

- Access Administration activity right
- Admin access to the external operation

To delete an external operation:

1. Click **Administration**.
2. Navigate to the external operation.
3. Select the external operation you want to delete and click the delete icon.

11.5 Working with Automation Services and Jobs

This section describes the following main tasks:

- Section 11.5.1, "Starting the Oracle WCI Automation Service"
- Section 11.5.2, "Registering Automation Services"
- Section 11.5.3, "Registering Job Folders with Automation Services"
- Section 11.5.4, "Creating or Editing a Job"
- Section 11.5.5, "Deleting a Job"

It also covers the following low-level tasks:

11.5.1 Starting the Oracle WCI Automation Service

The Automation Service runs as a Windows service or a daemon. Ensure the Oracle WCI Automation Service is configured to start automatically when you start your system. For information on configuring the Oracle WCI Automation Service to start automatically, see the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Interaction for Windows* or the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Interaction for Unix and Linux*.

11.5.2 Registering Automation Services

Before you can run jobs, you must register any computers hosting Automation Services and register job folders with those Automation Services. The primary Automation Service is registered when you install the Automation Service and execute the related database scripts described in the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Interaction for Windows* or the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Interaction for Unix and Linux*.

To access the Automation Service Utility you must be a member of the Administrators Group.

To register automation services:

1. Click **Administration**.
2. In the Select Utility list, click **Automation Service**.
3. Click **Add Automation Service**.

   The Register Automation Service dialog box opens.
4. Type the name of the computer that hosts the Automation Service.

   Use the host name only (for example, automationserver1), not the fully qualified domain name.
5. Type the network address that identifies the computer.
6. Click **Finish**.

The new Automation Service appears in the list. To the right of each Automation Service, you can see if the server is online or offline and when the job folders associated with the server were last updated.

You must assign job folders to this Automation Service before you can run jobs with it.

11.5.3 Registering Job Folders with Automation Services

Jobs can run only if the folder in which they are stored is assigned to an Automation Service. All of the jobs in a folder are run by one or more Automation Services. If multiple Automation Services are associated with a single folder, the Oracle WCI Automation Service assigns jobs according to the resources available on each Automation Service.

To access the Automation Service Utility you must be a member of the Administrators Group.

Note: You must register each folder separately. An Automation Service does not monitor child folders of registered folders.

To register a job folder with an automation service:

1. Click **Administration**.
2. In the Select Utility list, click **Automation Service**.
3. Click the name of the Automation Service to run the jobs.

   The Register Folders Editor opens.
4. Click **Add Folder**.

   The Add Job Folder dialog box opens.

The job folder appears in the list. Under each registered job folder, you can see the jobs stored in that folder and the next time each job is scheduled to run.

- To edit a job, click its name.
- To remove a job folder, select the folder and click the Remove icon.

  To select or clear all of the folder check boxes, select or clear the box to the left of **Folders**.

11.5.4 Creating or Editing a Job

When you create portal objects that require related jobs, the object editor includes a page to configure and schedule the related job. If you want to create additional jobs independently of the object editors, follow the instructions in this section.

Before you can run jobs, you must:

- Confirm that the Oracle WCI Automation Service is running on the Automation Service computer. If it is not running, start it now, as described in Section 11.5.1, "Starting the Oracle WCI Automation Service."
- Register the Automation Service with the portal, as described in Section 11.5.2, "Registering Automation Services."
- Assign administrative folders to the registered Automation Services, as described in Section 11.5.3, "Registering Job Folders with Automation Services."

To create a job you must have the following rights and privileges:

- Access Administration activity right
- Create Jobs activity right
- At least Edit access to the parent folder (the folder that will store the job)

- At least Select access to any objects or operations you want to add to the job

To edit a job you must have the following rights and privileges:

- Access Administration activity right
- At least Edit access to the job
- If you plan to change the objects or operations associated with the job, at least Select access to those objects or operations

To create or edit a job:

1. Click **Administration**.
2. Open the Job Editor.
   - To create a job, open the folder in which you want to store the job. In the Create Object list, click **Job**.

     Note: The folder in which you store the job must be registered with an automation service to run the job.

   - To edit a job, open the folder in which the job is stored and click its name.
3. On the Main Settings page, perform tasks as necessary:
   - Section 11.5.6, "Adding Operations to a Job"
   - Section 11.5.7, "Scheduling a Job to Run"
   - Section 11.5.8, "Setting a Timeout Period for a Job"
   - Section 11.5.9, "Setting a Job to Ignore Errors"
   - Section 11.5.10, "Setting the Logging Level for a Job"
   - Section 11.5.11, "Saving Job Checkpoints"
4. On the Job History page, perform tasks as necessary:
   - Section 11.5.12, "Viewing Job Status and Job Logs"
   - Section 11.5.14, "Aborting In-Process Jobs"
5. On the Properties and Names page, perform tasks as necessary:
   - Section 5.15, "Naming and Describing an Object"

     You can instead enter a name and description when you save this remote pagelet Web service.

   - Section 5.16, "Managing Object Properties" (optional)
6. On the Security page, perform tasks as necessary:
   - Section 5.17, "Setting Security on an Object"

   The default security for this job is based on the security of the parent folder. Administrative users with at least Select access to this job can associate objects with the job.
7. If you are editing a remote pagelet Web service, on the Migration History and Status page, perform tasks as necessary:
   - Section 5.18, "Viewing Migration History and Status for an Object"

Note: The Migration History and Status page is not available when creating an object.

11.5.5 Deleting a Job

To delete a job you must have the following rights and privileges:

- Access Administration activity right
- Admin access to the job

To delete a job:

1. Click **Administration**.
2. Navigate to the job.
3. Select the job you want to delete and click the delete icon.

11.5.6 Adding Operations to a Job

To associate an operation with a job:

1. If the Job Editor is not already open, open it now.
2. Under Add an Operation, perform the following actions:
   - To run operations with this job, click **Add Operation**; then, in the Select Job Operations dialog box, select the operations you want to add and click **OK**.
   - Each time this job runs, each of these operations is executed, in order, starting at the top of this list. Because the operations run in the order listed (one operation must complete before another begins), you might have to change this order. For example, you might want to run an authentication source operation to import new users and then run a profile source operation to import profile information for those new users.

     To change the order of operations, perform the following actions:

     – To move an operation to the top of this list, click the move to top icon.

     – To move an operation up one space in this list, click the move up icon.

     – To move an operation down one space in this list, click the move down icon.

     – To move an operation to the bottom of this list, click the move to bottom icon.
   - To remove an operation, select the operation and click the remove icon.

     To select or clear all of the operation check boxes, select or clear the check box to the left of **Operations**.

11.5.7 Scheduling a Job to Run

To schedule a job to run:

1. If the Job Editor is not already open, open it now.
2. Under Schedule, specify when you want this job to run:
   - If you do not want to run this job, leave the default setting (**Unscheduled**).
   - If you want to run this job immediately, choose **Run Once - Now**.

- If you want to run this job at a specified date and time, choose **Run Once**. By default, the date and time are set to the current date and time. To change this setting, type a different date and time in the appropriate boxes. To choose the date from a calendar, click the calendar icon. After this job completes, it resets itself to **Unscheduled**.
- If you want to run this job on a regular basis, choose **Run Periodically**.

  In the **Next** boxes, type a date and time you want to start running this job on this schedule. To choose the date from a calendar, click the calendar icon.

  In the **Every** box, type a number and, in the drop-down list, choose a period.

  In the **Do not run after** boxes, type a date and time you want to stop running this job on this schedule. To choose the date from a calendar, click the calendar icon.

  If there are particular times during weekdays that you do not want this job to run, select **Suspension Times for Content Crawler Jobs** and select the beginning and end of the suspension times in the **From** and **To** drop-down lists, respectively. You might want to avoid running long, resource-intensive jobs during normal business hours so you do not slow down other jobs.

Note: The suspension times do not affect crawler jobs that start before the beginning of the suspension time and are still running when the suspension time begins. Crawler jobs that are already running when the suspension time begins will continue normally.

11.5.8 Setting a Timeout Period for a Job

If you want this job to be stopped if it does not complete in a specific amount of time, you can set a timeout period for the job. If the job does not complete in the specified time, the portal asks the job to stop processing. If the job does not respond to this request within ten minutes, the portal forcibly stops the job.

To set a timeout period for a job:

1. If the Job Editor is not already open, open it now.
2. In the **Timeout** period box, type a number and, in the drop-down list, choose a period.

11.5.9 Setting a Job to Ignore Errors

By default, if an operation fails, the remaining operations associated with the job are not attempted. If you want the portal to attempt to run the other operations even if one operation fails, you can set the job to ignore errors.

To set a job to ignore errors:

1. If the Job Editor is not already open, open it now.
2. Select **Ignore errors and run all operations**.

11.5.10 Setting the Logging Level for a Job

To set the logging level for a job:

1. If the Job Editor is not already open, open it now.

2. In the Logging Level drop-down list, choose the amount of information you want to record in the job history logs:
   - **Silent**: no information is logged.
   - **Low**: only significant process information is logged.
   - **Normal**: high-level process information and outcomes are logged.
   - **Verbose**: All process information is logged. This level of logging will affect the performance of the portal, and should therefore be used only temporarily (for example, to troubleshoot a problem).

11.5.11 Saving Job Checkpoints

If this job includes content crawler operations that process information for long periods, you might want to record periodic notes in the log to show that the job is still running (you can view the job log for this job in the Job History page of this editor or for all in-process jobs through the Job History page of the Automation Service Manager).

Note: This setting only applies to content crawler operations.

To save checkpoints for a job:

1. If the Job Editor is not already open, open it now.
2. Select **Save checkpoints every** and, in the box, type the number of minutes you want to wait between checkpoints.

11.5.12 Viewing Job Status and Job Logs

You can view a history for a job as well as the logs from each job on the Job History page of the Job Editor. You can view the same information for all jobs on the Job History page of the Automation Service Utility.

To view status and logs through the Job Editor you must have the following rights and privileges:

- Access Administration activity right
- At least Edit access to the job

To view status and logs through the Automation Service Utility you must be a member of the Administrators group.

To view job status and logs:

1. Click **Administration**.
2. Access the **Job History** page.
   - To access the Job History page through the Job Editor, open the folder in which the job is stored and click its name. Click **Job History** page.
   - To access the Job History page through the Automation Service Utility, in the Select Utility list, click **Automation Service**. Click **Job History** page.
3. View the history of jobs that have run and the logs for individual jobs.
   - To view the detailed job log for a job, click the name of the job.

     The log appears in a dialog box.

- To search the log, in the job log dialog box, enter a search term (using wildcards such as *) and click **Search Log**.
- To limit the histories displayed on this page, in the **View** and **to** boxes, type the earliest and latest dates for which you want to view job histories and click **>>**.

  To choose the date from a calendar, click the Calendar icon.
- To remove the filter clear the **View** and **to** boxes and click >>.
- To refresh the job history data, click the Refresh icon.
- To download a text file version of a detailed job log, click the Download icon to the far-right of the job name; when asked to open or save the file, click **Save**, specify a location in which to save the file, and click **Save** again.

11.5.12.1 Job History Information

The Job History page provides information about in-process and completed jobs.

Column	Description
Job Name	Displays the name of the job. Click the job name to view the detailed job log.
Server	Displays the name of the Automation Service that ran the job.
Next Run	Displays the next date and time the job is scheduled to run.
Start	Displays the starting date and time for the last time the job ran.
Finish	Displays the ending date and time for the last time the job ran.
Status	Displays what happened when the job ran last: ■ **Succeeded** indicates that the job was able to complete. ■ **Failed** (in red text) indicates that the job experienced errors and was not able to complete. ■ **In Process** indicates that the job is running now. ■ **Interrupted** indicates that the job was terminated unexpectedly. ■ **Suspended** indicates that the job stopped before completing its work and will resume its work at the next scheduled run time.

11.5.13 Deleting Job Histories

On the Job History page of the Automation Service Utility, you can delete job histories from the database.

> **Note:** You cannot delete job histories from the Job Editor.

To access the Automation Service Utility you must be a member of the Administrators group.

1. Click **Administration**.
2. In the Select Utility list, click **Automation Service**.
3. Click **Job History** page.
4. To delete job histories from the database, in the **Delete to** box, type the latest date for which you want to delete histories and click **>>**.

   To choose the date from a calendar, click the Calendar icon.

Any histories with this date or an earlier date are deleted from the database.

11.5.14 Aborting In-Process Jobs

You can stop a job that is processing on the Job History page of the Job Editor of the Automation Service Utility.

To abort an in-process job through the Job Editor you must have the following rights and privileges:

- Access Administration activity right
- At least Edit access to the job

To abort an in-process job through the Automation Service Utility you must be a member of the Administrators group.

To abort an in-process job:

1. Click **Administration**.
2. Access the **Job History** page.
   - To access the Job History page through the Job Editor, open the folder in which the job is stored and click its name. Click **Job History** page.
   - To access the Job History page through the Automation Service Utility, in the Select Utility list, click **Automation Service**. Click **Job History** page.
3. To cancel a job, select the job and click **Abort**.

Note: You cannot cancel jobs that have already completed. The check boxes next to completed jobs are unavailable (grayed out).

12

Migrating, Backing-Up, and Restoring Your Portal

This chapter describes the steps you take to migrate (export and import), back up, and restore portal objects.

It includes the following sections:

12.1 About Object Migration

Object migration lets you copy resources from one portal to another. You might want to do this for several reasons. You might have multiple portals to handle a global deployment or you might want to create multiple portals to separate development, testing, and production.

You can copy resources from one portal to another by creating migration packages, which can be used to:

- Export objects created in a development portal and import them to your production portal when they have been properly tested.
- Import portal objects to install new features on your portal. For example, you might want to install a portlet suite and register those portlets in your portal.

There are several things you can do to make migration as easy and effective as possible:

- Keep source and target portals as similar as possible to reduce the mapping required.
- Create migration packages as soon as possible after approving objects. The object settings in a migration package are those present at package creation, not those present at object approval. Creating migration packages soon after approval minimizes the chance that object settings have changed since approval.
- You can selectively import objects in a migration package, so if you want to import content crawlers and communities separately, you can import a package twice, and select different objects each time you import it.

Note: User preferences for associated with add-on products, such as Oracle WebCenter Collaboration, are not migrated with the user.

The Migration - Export utility in the portal lets you create migration packages. To import objects from a migration package, you use the Migration - Import utility.

Migration Feature	Description
Portal objects that can be included in the package	All objects
Oracle WebCenter Collaboration information	Can migrate Oracle WebCenter Collaboration information
Requests and approval	Users with at least Edit access to objects can request migration, but only members of the Administrators group can approve objects for migration. An administrator selects approved objects to add to a migration package, and can also add object to the package without making a migration request. Users with the Access Utilities activity right can check the status of their migration requests.
Creating a migration package	Only users with the Access Utilities activity right can create a migration package. An administrator can add objects that do not have migration requests to a migration package (bypassing the request and approval process).
Object dependencies	Dependencies always maintained. Dependent objects can be included in a migration package, but do not must be.
Unique universal identifiers (UUIDs) and their effect on subsequent importing migration packages	By default UUIDs are maintained, so that subsequent migrations overwrite previously migrated objects. However, if you do not want to overwrite previously migrated objects, you have the option of creating a new instance of the same object, with a new UUID.

12.2 Migrating Objects

This section describes the following tasks:

- Section 12.2.1, "Requesting That an Object Be Migrated"
- Section 12.2.2, "Approving Objects for Migration"
- Section 12.2.3, "Creating a Migration Package in the Portal"
- Section 12.2.4, "Creating a Migration Package Using the Command Line Tool"
- Section 12.2.5, "Importing Objects in the Portal"
- Section 12.2.6, "Importing Objects Using a Command Line Tool"

12.2.1 Requesting That an Object Be Migrated

You can request that an object be added to a migration package to be exported to another portal.

> **Note:** You must have at least Edit access to the object for which you want to request migration.

1. Search for the object or click **Administration** and navigate to the object.
2. Select the object and click the Migrate icon.
3. In the Script Prompt dialog box, describe why you want this object migrated and click **OK**.

To view the status of your migration request, open the object's editor and click the **Migration History and Status** page. Under **Migration Status**, you see whether your request is waiting for approval, has been approved, or has been rejected, as well as your comments and any comments from the portal administrator approving or rejecting the object.

12.2.2 Approving Objects for Migration

When users want an object to be migrated, they submit a migration request. A portal administrator can then approve the request, and the object is added to the migration package.

There are two ways to approve objects for migration: in the object's editor or using the Approve Objects for Migration Utility.

- To approve a single object requested for migration, use the object's editor.

  See Section 5.18, "Viewing Migration History and Status for an Object."

- To approve all objects requested for migration, use the Approve Objects for Migration Utility.

  See Section 12.2.2.2, "Approving Objects for Migration Through the Administrative Utility."

12.2.2.1 Approving an Object for Migration

When users want an object to be migrated, they submit a migration request. A portal administrator can then approve the request, and the object is added to the migration package.

1. Open the object's editor by creating a new object or editing an existing object.
2. Click the **Migration History and Status** page.

   Under Migration Status, you see whether this object has been requested for migration, and, if so, whether it is waiting for approval, has been approved, or has been rejected.
3. If you are a member of the Administrators group, and you want to add this object to the migration package to be migrated to another portal, select **Approve this object for migration**.

> **Note:** Users who are not members of the Administrators group do not see this option.

After approving objects for migration, you can use the Migration - Export Utility to create a migration package.

12.2.2.2 Approving Objects for Migration Through the Administrative Utility

When users want an object to be migrated, they submit a migration request. A portal administrator can then approve the request, and the object is added to the migration package.

To use the Approve Objects for Migration Utility you must be a member of the Administrators Group.

12.2.3 Creating a Migration Package in the Portal

You can create a migration package that includes portal resources as well as Oracle WebCenter Collaboration information.

To create a migration package, you must be a member of the Administrators group.

1. Click **Administration**.
2. In the Select Utility list, click **Migration - Export**.
3. On the Portal Resources page, perform tasks as necessary:
   - Section 12.2.3.2, "Selecting Objects to Export in a Migration Package"
4. On the Package Settings page, perform tasks as necessary:
   - Section 12.2.3.1, "Specifying a Name, Description, and Contact for a Migration Package"
5. On the Add Existing Package Resources page, perform tasks as necessary:
   - Section 12.2.3.3, "Adding Resources from Another Migration Package"
6. Click **Finish**.

   A status message is displayed as the migration package is being created. When the migration package is created, you can download it to your desktop.

   Note: If you are also migrating Oracle WebCenter Collaboration objects, those will be written to a .zip file on the computer where Oracle WebCenter Collaboration is installed. You must move this file from this location to the target location.

You can now use the migration package to import the migrated resources into another portal.

12.2.3.1 Specifying a Name, Description, and Contact for a Migration Package

You must specify a name, description, and contact person for a migration package.

To create a migration package, you must have at least Edit access to the objects you want to add to the package.

1. If the Migration — Export Utility is not already open, open it now.
2. Click the **Package Settings** page.
3. In the **Package name** box, type the name for the package file that will be created when you click **Finish** (this file is given a .pte extension).

4. In the **Package description** box, type a description that clarifies the purpose of this export package to other portal administrators.
5. In the **Publisher name** box, type the person to contact with any questions about this export package.

12.2.3.2 Selecting Objects to Export in a Migration Package

You can select objects to export on the Portal Resources page of the Migration — Export Utility.

To create a migration package, you must have at least Edit access to the objects you want to add to the package.

1. If the Migration — Export Utility is not already open, open it now and display the **Portal Resources** page.
2. Under **Resources**, select the objects you want to add and what you want to export.
3. To select individual objects, select the type of object from the **Select Resources** list, then, in the dialog box, select the objects you want to add and click **OK**.
4. To add all objects that have been approved for migration, click **Add All Approved**.
5. If the object is a folder and you want to export the folder's contents, select **Export Contents**.
6. To export the object's dependencies, select **Export Dependencies**.

   Dependencies are any other objects that are required by the object you are exporting.
7. To remove an object, select the object and click the Remove icon.

   To select or clear all of the object check boxes in a column, select or clear the check box above the column.
8. To toggle the sort order of the objects, click **Resources**.
9. Under **Export Settings**, select the check box if you also want to export parent folders of objects you marked for Export Dependencies.

   If you do not select this option, only references to those parent folders will be exported.

12.2.3.3 Adding Resources from Another Migration Package

You can add objects from an existing migration package to the package you are creating on the Add Existing Package Resources page of the Migration — Export Utility.

To create a migration package, you must have at least Edit access to the objects you want to add to the package.

> **Note:** If the portal settings on an object in the existing migration package have changed since the package was created, the current portal settings on the object will be exported.

1. If the Migration — Export Utility is not already open, open it now and display the **Add Existing Package Resources** page.

2. Under Migration Package, specify the package from which you want to add objects.
   - To browse to a package on your computer or in your network, click **Browse**, select the migration package file (a .pte file), and click **Open**.
   - To get the package from a Web address, select **Web Address** and type the URL to the package.

     If you must enter login credential to access the Web address, type the information in the **Username** and **Password** boxes.
3. Click **Load Package**.

> **Note:** Only objects that are currently in the portal will be displayed on the **Portal Resources** page.

Select resources from this package on the **Portal Resources** page.

12.2.4 Creating a Migration Package Using the Command Line Tool

You can create a migration package to export portal objects from one portal to be imported into another portal.

> **Note:** You cannot export Oracle WebCenter Collaboration objects using the command line tool. To export those objects, use the Migration - Export Utility in the portal. See Section 12.2.3, "Creating a Migration Package in the Portal."

1. Log in to the host computer for the portal as the user who owns the portal installation.
2. Use the command `ptmigration.bat` (for Windows) or `./ptmigration.sh` (for UNIX) with the following parameters:

   ```
   ./ptmigration.sh [username] [password] -export [migration_package_name] [log_file_name] <-exportdependencies>
   ```

   Where the parameters are as follows:

Parameter	Description
migration_package_name	Required. The name and path of the migration package to be created
log_file_name	Required. The name and path of the log file to be created. The path to the log file must be different from that of the migration package.
-exportdependencies	Optional. Use this parameter to export any additional objects upon which the objects you are exporting depend.

3. Press ENTER.

   All objects approved for migration are exported into the migration package. The migration utility updates the migration status in the source portal.

12.2.5 Importing Objects in the Portal

You can import objects from another portal using the Migration — Import Utility.

Before you import a migration package (.pte file), place the package to a location that is accessible over your network.

Notes:

- If you are also importing Oracle WebCenter Collaboration objects, you must place the .zip file in the same location as the .pte file.
- If you are importing a migration package created with a previous version of Oracle WebCenter Interaction and the migration package includes users, you must either manually edit the user's password in the administrative user interface or you must export the users and import them again. Previously passwords were saved as clear text and are therefore not supported in the current version.

To import a migration package you must be a member of the Administrators group.

1. Click **Administration**.
2. In the Select Utility list, click **Migration - Import**.
3. On the Package Settings page, perform tasks as necessary:
   - Section 12.2.5.1, "Specifying the Location and Import Settings for the Migration Package"
4. Click the **Unresolved Dependencies** page and complete the following task:
   - Section 12.2.5.3, "Resolving Import Dependencies"

   Note: This page appears only if there is an unresolved dependency.
5. On the Portal Resources page, perform tasks as necessary:
   - Section 12.2.5.2, "Selecting Objects to Import from a Migration Package"
6. Click **Finish**.

   A status message is displayed as the migration package is being created. When the migration package is created, you can download it to your desktop.

12.2.5.1 Specifying the Location and Import Settings for the Migration Package

To import objects you specify the location of the migration package and what you want you want to import.

To import a migration package, you must have at least Edit access to the objects you want to add to the package.

1. Under Migration Package, specify the package from which you want to add objects.
   - To browse to a package on your computer or in your network, click **Browse**, select the migration package file (a .pte file), and click **Open**.
   - To get the package from a Web address, select **Web Address** and type the URL to the package.

If you must enter login credential to access the Web address, type the information in the **Username** and **Password** boxes.

2. Click **Load Package**.
3. Under Import Settings, select options for import.

Option	Description
Import ACLs	Select this to import the Access Control Lists (user and group security settings) for all the objects you are importing.
Overwrite Remote Servers	Specifies that existing remote server objects should be overwritten by remote server objects in the migration package. The default is that existing remote servers are not overwritten.
Remember Dependency Settings	Select this if, on subsequent imports, you want the objects you are now importing to retain the new dependencies that you select in the importing portal. (You select new dependencies on the Unresolved Dependencies page.)
Always Create New Object Instances (Create Duplicates of Existing Objects)	Select this if you want to create new object instances instead of overwriting objects that may already exist on the importing portal.

12.2.5.2 Selecting Objects to Import from a Migration Package

You can select objects to import on the Portal Resources page of the Migration — Import Utility.

To import a migration package, you must have at least Edit access to the objects you want to add to the package.

This page displays the objects contained in the migration package you loaded. All objects will be imported when you click **Finish**, unless you remove them.

1. If the Migration — Import Utility is not already open, open it now.
2. Click the **Portal Resources** page.
3. Remove objects you do not want to import by selecting them and clicking the Remove icon.

If there are objects to import from Oracle WebCenter Collaboration, you can choose those objects on the **Collaboration Resources** page.

12.2.5.3 Resolving Import Dependencies

If any of the objects you are importing depend on resources that are not included in the package, those missing resources are listed on the Unresolved Dependencies page of the Migration — Import Utility. For example, in your migration package you may have a portlet that depends on a Web service, which is not included in the package. You can resolve those dependencies by pointing to existing objects in your portal.

To create a migration package, you must have at least Edit access to the objects you want to add to the package.

Note: This page appears only if there is an unresolved dependency.

1. If the Migration — Import Utility is not already open, open it now.
2. Click display the **Unresolved Dependencies** page.

   Any missing resources are displayed in the Dependency column. The associated object in the migration package is listed under each missing dependency.
3. Click the Edit icon beside the dependency.
4. Select a replacement object from this portal and click **OK**.

   The replacement object is displayed in the Replacement column.

12.2.6 Importing Objects Using a Command Line Tool

You can import objects from another portal with a migration package.

1. Copy the migration package to the target portal host computer.
2. Log in to the host computer for the portal as the user who owns the portal installation.
3. Use the command `ptmigration.bat` (for Windows) or `./ptmigration.sh` (for UNIX) with the following parameters:

   ```
   ptmigration.bat [username] [password] -import [migration package name] [log
   file name] <-noacl> <-overwriteremoteservers> <-createnewobjectinstances>
   ```

   Where the parameters are as follows:

Parameter	Description
migration package name	Required. The name and path of the migration package to be created
log file name	Required. The name and path of the log file to be created. The path to the log file must be different from that of the migration package.
-noacl	Optional. Use this parameter if you do not want to import the Access Control Lists (security data) associated with the objects you are importing.
-overwriteremoteservers	Optional. Specifies that existing remote server objects should be overwritten by remote server objects in the migration package. The default is that existing remote servers are not overwritten.
-createnewobjectinstances	Optional. Use this parameter if you want to create new object instances instead of overwriting objects that may already exist on the importing portal.

4. Press ENTER.

   All the objects in the migration package are imported. The imported objects are located in the same folders on the target portal as on the source portal. Objects with missing dependencies will be skipped and not imported. Check the migration log to see which ones were skipped.

12.3 Backing Up the Portal

You can back up your system without taking it offline.

1. Back up your database according to your database vendor documentation and best practices.

2. Create a snapshot of your search collection and back it up to another location or tape backup.
3. Back up your document repository files and log files to another location or tape backup.

12.4 Restoring the Portal

1. Stop the Web service on all computers hosting the portal application.
2. Stop the Oracle WCI Automation Service on all computers hosting Automation Services.
3. Stop the Oracle WCI Search service.
4. If you must rebuild your portal database, use your database software to restore from a previously saved database.
5. Replace your search collection with backups as close as possible to the time of the database backup you are using.

Your database backup might not exactly match your search collection backup, so the restored database and search collection will be out of sync. To correct this, rebuild the search collection.

12.5 Rebuilding the Search Collection

Your search index might get out of sync with your database if, during a crawl, the Search Service became unavailable or a network failure prevented an indexing operation from completing. Another possibility is that a Search Service with empty indexes was swapped into an existing portal with pre-existing documents and folders.

To rebuild the search collection you must have the following rights:

- Access Administration activity right
- Access Search Results Manager activity right

The Search Service Manager lets you specify when and how often the Search Update Agent repairs your search index. Rather than synchronizing particular objects, the repair synchronizes all objects in the database with the search index. Searchable objects in the database are compared with IDs in the search index. If an object ID in the database is not in the search index, the Search Update Agent attempts to re-index the object; if an ID in the search index is not in the database, the Search Update Agent removes the object from the search index.

Run the Search Update Agent for purposes of background maintenance or complete repopulation of the search index.

1. Configure the Search Service to repair itself.
   a. Click **Administration**.
   b. From the Select Utility list, choose **Search Service Manager**.
   c. Under Search Repair Settings, change **Next Repair Date** to a time in the past.
   d. Click **Administration** again.
2. Wait one minute for the setting to update.
3. Run one of the Search Update jobs in verbose mode.
   a. Open the Intrinsic Operations folder.

b. Open one of the Search Update jobs.

The Job Editor opens.

c. Change the Logging Level to **Verbose** and click **Finish**.

Note: Make note of the logging mode before you change it, so that you can change it back after the repair is complete.

d. Select the job you just edited and click **Run Once**.

By running the job this way, you avoid having to go back into the job and revert to the previous schedule settings.

4. Ensure that the job is running in repair mode.

a. Open the job you just created; it should be called something like Search Update 1 — Run Once.

The Job Editor opens.

b. Click the **Job History** page.

c. Click the job name.

The job log opens.

d. Ensure that the job is running in repair mode.

The second line of the job log should be similar to this:

```
Mar 1, 2008 9:10:02 AM- PTIndexer.ctor : Indexing will extract at most
1000000 encoded bytes of text from each document.
```

About half-way down the first page of the log you should see a message that should be similar to this:

```
Mar 1, 2008 9:10:02 AM- Search Update Agent is repairing the directories...
```

5. Reinstall the Search Service and select **Overwrite the existing search index**. For details on installing the Search Service, refer to the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Interaction for Windows* or the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Interaction for Unix and Linux*.

A

Configuring Portal Settings

This appendix contains a detailed description of the Oracle WebCenter Configuration Manager and for Oracle WebCenter Interaction configuration files that you can edit to customize your installation.

It includes the following sections:

A.1 Oracle WebCenter Configuration Manager

Oracle WebCenter Configuration Manager enables you to manage the configuration settings of Oracle WebCenter products through a user interface rather than having to edit .xml files.

This section includes the following sections:

A.1.1 Activity Service Settings

This section describes the settings in the Activity Service section of the Configuration Manager.

Page	Setting	Description
Activity Service Database	Vendor	Database vendor
	Host	Name of the computer that hosts the database
	User name	Name of the database user
	Password	Password for the database user; this value is not displayed
	Port	Port number on which the database services requests
	Minimum pooled database connections	Minimum number of pooled connections for the database
	Maximum pooled database connections	Maximum number of pooled connections for the database
	SID (Oracle Only)	SID for the database (applies only to Oracle databases)
	Database Name (MSSQL Only)	Name of the database (applies only to Microsoft SQL Server databases)
Application Settings	HTTP enabled	Enables/disables HTTP as the application's web protocol
	HTTP port	Port on which the application listens for HTTP requests
	HTTPS enabled	Enables/disables HTTPS as the application's web protocol
	HTTPS port	Port on which the application listens for HTTPS requests
General	Apply Tag Filtering	Enables/disables tag filtering
	Email Template Location	File location for the email notification template
	Portal URL	Location of the Portal Server; this setting enables the portal to generate links
Logging	Server	Application name that will uniquely identify log messages sent from this application Logging Utilities will use this string to determine the location from which log messages originate. The application name can be any string that meets the following restrictions: it must not be empty, it must not exceed 128 in length, and it may only contain non-white-space visible ASCII characters and the space character. Most Oracle WebCenter Interaction products follow the naming convention *product_name.machine_name.user_name*.
	Local only	Limits broadcast of this application's logging messages to only the computer on which this application is installed
WCI Directory	Authentication provider	Provider type (ALI Directory, generic LDAP, or Active Directory)
	Host	Name of the computer that hosts the Directory Service
	Port	Port number on which the Directory services requests

Page	Setting	Description
	Principal	Distinguished name of the Directory administrator, for example `uid=administrator,ou=users,dc=bea,dc=com`
	Credential	Password for the principal
	SSL enabled	Enables/disables SSL
WCI Notification Service	URL	Fully-qualified URL (protocol, domain name, and port) used to connect to the Notification Service
	Timeout (milliseconds)	Number of milliseconds that clients wait before the notification request is terminated
	Host	Name of the computer that hosts the Notification Service
WCI Security Database	Vendor	Database vendor
	Host	Name of the computer that hosts the database
	User name	Name of the database user
	Password	Password for the database user; this value is not displayed
	Port	Port number on which the database services requests
	Minimum pooled database connections	Minimum number of pooled connections for the database
	Maximum pooled database connections	Maximum number of pooled connections for the database
	SID (Oracle Only)	SID for the database (applies only to Oracle databases)
	Database Name (MSSQL Only)	Name of the database (applies only to Microsoft SQL Server databases)
WCI Security Identity Services	Key service file path	File path to the keystore file on the server
	Key service default alias	Keystore alias
	Key service passphrase	Keystore passphrase; this value is not displayed
WCI Security Login Tokens	Default token type	Type of Login Token used by default by ALUI Security Only use ALUI if your Directory is pointed at ALI Directory.
	Token expiration time in minutes	Token expiration time, in minutes
	Message authentication code seed value	Seed value used to create MAC signatures used to authenticate Login Tokens This should match the MAC seed for any external systems expected to consume the tokens created by ALUI Security, or to create tokens to be consumed by ALUI Security. For portal tokens, this value should match the "login token root key" in the PTSERVERCONFIG table in the portal database.

A.1.2 Automation Service Settings

This section describes the settings in the Automation Service section of the Configuration Manager.

Page	Setting	Description
Crawler Settings	Web Crawler file timeout (seconds)	Web file crawler timeout
	SOAP file timeout (seconds)	SOAP timeout for crawlers
General	Server name	Name that should be used to identify this Automation Service; this is typically the name of the host computer
	Port	Port number used by the Automation Service
Logging	Server	Application name that will uniquely identify log messages sent from this application Logging Utilities will use this string to determine the location from which log messages originate. The application name can be any string that meets the following restrictions: it must not be empty, it must not exceed 128 in length, and it may only contain non-white-space visible ASCII characters and the space character. Most ALI products follow the naming convention *product_name.machine_name.user_name*.
	Local only	Limits broadcast of this application's logging messages to only the computer on which this application is installed
Portal Database	Vendor	Database vendor
	Host	Name of the computer that hosts the database
	User name	Name of the database user
	Password	Password for the database user; this value is not displayed
	Port	Port number on which the database services requests
	Minimum pooled database connections	Minimum number of pooled connections for the database
	Maximum pooled database connections	Maximum number of pooled connections for the database
	SID (Oracle Only)	SID for the database (applies only to Oracle databases)
	Database Name (MSSQL Only)	Name of the database (applies only to Microsoft SQL Server databases)

A.1.3 Content Upload Service Settings

This section describes the settings in the Content Upload Service section of the Configuration Manager.

Page	Setting	Description
Application Settings	HTTP enabled	Enables/disables HTTP as the application's web protocol
	HTTP port	Port on which the application should listen for HTTP requests
	HTTPS enabled	Enables/disables HTTPS as the application's web protocol

Page	Setting	Description
	HTTPS port	Port on which the application should listen for HTTPS requests
Document Repository Service	Host	Name of the computer that hosts the Document Repository Service
	Port	Port number on which the Document Repository services requests
	Override host name and port with this URL	Overrides the above settings Ignored if blank. An example value is: `http://localhost:8020/dr`

A.1.4 Document Repository Settings

This section describes the settings in the Document Repository section of the Configuration Manager.

Page	Setting	Description
Application Settings	HTTP enabled	Enables/disables HTTP as the application's web protocol
	HTTP port	Port on which the application should listen for HTTP requests
	HTTPS enabled	Enables/disables HTTPS as the application's web protocol
	HTTPS port	Port on which the application should listen for HTTPS requests

A.1.5 LDAP IDS Service Settings

This section describes the settings in the LDAP IDS Service section of the Configuration Manager.

Page	Setting	Description
Application Settings	HTTP enabled	Enables/disables HTTP as the application's web protocol
	HTTP port	Port on which the application should listen for HTTP requests
	HTTPS enabled	Enables/disables HTTPS as the application's web protocol
	HTTPS port	Port on which the application should listen for HTTPS requests

A.1.6 Portal Service Settings

This section describes the settings in the Portal Service section of the Configuration Manager.

Page	Setting	Description
Analytics Communication	Enabled	Select this option if you want the portal to pass information to Oracle WebCenter Analytics.

Page	Setting	Description
Crawler Settings	Web Crawler file timeout (seconds)	Enter the number of seconds you want a Web crawler to try to get to a Web page before it times out.
	SOAP file timeout (seconds)	Enter the number of seconds you want a remote crawler to try to get to a document before it times out.
Gateway	Gateway Enabled	Select this option if you want to allow portal content to be gatewayed.
	Gateway temporary directory	Enter the full path to the directory where temporary files will be stored.
	Gateway max upload (in bytes)	Enter the maximum file size allowed for uploads.
	Gateway min upload (in bytes)	Enter the minimum file size allowed for uploads.
	Gateway min streamable (in bytes)	Enter the minimum size of streamable content.
	Gateway temporary file pool size	Enter a value that is greater than the number of ASP/JAVA worker threads for the portal.
Logging	Server	Application name that will uniquely identify log messages sent from this application Logging Utilities will use this string to determine the location from which log messages originate. The application name can be any string that meets the following restrictions: it must not be empty, it must not exceed 128 in length, and it may only contain non-white-space visible ASCII characters and the space character. Most ALI products follow the naming convention *product_name.machine_name.user_name*.
	Local only	Limits broadcast of this application's logging messages to only the computer on which this application is installed
Main Portal Settings	Web home directory	Enter the directory for the Portal's JAR files.
	Image Server base URL	Enter the base URL for the Portal's Image Server.
	Image Server secure base URL	Enter the base URL for the Portal Image Server running HTTPS.
	Image Server connection URL	Enter the base URL that is used when the Portal Server connects to the Image Server to retrieve JSRegistry information. In many configurations this URL is the same as the Image Server Base URL.
	Image Server connection URL timeout (seconds)	Enter the timeout for the Image Server Connection URL, in seconds. -1 means do not check during startup. Note that if this is invalid, your portal will not work.
	Administrative Portal base URL	Enter the base URL to the Administrative Portal. It is required that absolute URL be used in Security Mode 3.
	Temporary file home directory	Enter the temporary files directory to be used by the portal. This should not be Web accessible.
	Internal SSO LoginToken timeout (minutes)	
Portal Database	Vendor	Database vendor
	Host	Name of the computer that hosts the database

Page	Setting	Description
	User name	Name of the database user
	Password	Password for the database user; this value is not displayed
	Port	Port number on which the database services requests
	Minimum pooled database connections	Minimum number of pooled connections for the database
	Maximum pooled database connections	Maximum number of pooled connections for the database
	SID (Oracle Only)	SID for the database (applies only to Oracle databases)
	Database Name (MSSQL Only)	Name of the database (applies only to Microsoft SQL Server databases)
Portal International Settings	Locale	Enter the default locale for users. Setting it to the string "UseBrowser" causes the portal to derive the locale from the browser's language settings and store it as the user's locale.
	Time Zone (numeric value)	Enter the default time zone for the user. If it is -1 then the time zone of the computer on which Portal is deployed is used.
	Mandatory Object Language	This setting allows the administrator to set the language for all new objects. If it is blank, the user creating the object can choose the language for the object. If it is not blank, the value will be used as the language for all new and edited objects. The value should be a locale string (for example, it should match the name of a folder under the msgs directory.)
Portal System Properties	Server name	Enter the name of the portal server or virtual load-balanced server (for example, the main load balanced server name: portal.mycompany.com).
	Machine name	Enter the computer name (for example, the physical name of the individual portal server computer behind the load-balancer: portalserver1243).
	Performance comments	This setting specifies whether the performance comments in the HTML source are enabled. 0 means the comments and stacktraces are disabled. 1 means the comments and stacktraces are enabled. 2 means the comments are enabled but stacktraces are disabled. 3 means the comments are disabled but stacktraces are enabled.
	Debugging mode	This setting specifies whether debugging features are enabled. This is disabled by default. You can enable this to debug portal startup issues, especially if you have made customizations to XML files. Make sure to set to disable debugging when you are done troubleshooting. 1 means debugging is enabled. 0 means debugging is disabled.

Page	Setting	Description
	Doctype specification	1: none, 2: HTML 3.2, 3: HTML 4.0 Transitional, 4: HTML 4.0 Frameset, 5: HTML 4.0 Strict. It is unlikely that you would want to set one global doctype for the portal. Generally, you would set the doctype on a particular page through legacy or adaptive page layouts. For information on creating adaptive layouts, see the Adaptive Page Layouts section of the *Oracle Fusion Middleware User Interface Customization Guide for Oracle WebCenter Framework Interaction*. Neither the portal nor any other Oracle WebCenter Interaction product has been verified to support either the transitional or strict document type specification on a global level. By default the portal does not include a specific doctype declaration in its HTML because doing so would limit the display of portlets in which the doctypes were invalid or inconsistent with the portals declared doctype. If you are confident that all your portlets adhere to a particular doctype you can set that document type here.
	Adaptive layout mode	Enter a numeric value indicating whether page and/or portlet layout modes are enabled. Both are enabled by default. 0 means layout mode is disabled. 1 means page and portlet layout modes are enabled. 2 means page layout mode is only enabled. 3 means portlet layout mode is only enabled.
	Virtual directory path	Enter the virtual directory path. It is typically /portal/.
	HTTP entry point	Enter the portal main Servlet mapping name. This has to be the same has the mapping name for HTTPInterpreter in web.xml. It is typically server.pt.
	HTTP Port	Enter the port number for the Portal running HTTP.
	HTTP Secure Port	Enter the port number for the Portal running HTTPS.
	SSO virtual directory path	Enter the SSO Virtual directory path. It is typically /portal/.
	SSO servlet name	Enter the SSO Servlet mapping name. This has to be the same has the mapping name for SSOLoginPage in web.xml. It is typically SSOServlet.
	Database connection timeout	Enter the amount of time in seconds before a database connection times out. The value has to be between 0 and 1500 (15 minutes). Default is 30 seconds.
	Read Access To Editors	Enable this to allow users read access to object editors they have READ/SELECT access to. Otherwise, no user is allowed to view the object's editor without EDIT permissions on that object.
Service Settings	Enabled	If enabled, searches are performed via the Tagging Engine; if disabled, searches are performed via the Search Service.
	Pathways Server Cache Timeout	This setting controls how often Portal checks to see if the Tagging Engine has been migrated into Portal. This controls whether or not Tagging Engine integration is enabled.

Page	Setting	Description
	Ensemble Server Cache Timeout	This setting controls how often Portal checks to see if the Pagelet Producer has been migrated into Portal. This controls whether or not Pagelet Producer integration is enabled.

A.1.7 RSS Reader Settings

This section describes the settings in the RSS Reader section of the Configuration Manager.

Page	Setting	Description
Application Settings	HTTP enabled	Enables/disables HTTP as the application's web protocol
	HTTP port	Port on which the application should listen for HTTP requests
	HTTPS enabled	Enables/disables HTTPS as the application's web protocol
	HTTPS port	Port on which the application should listen for HTTPS requests
Logging	Server	Application name that will uniquely identify log messages sent from this application Logging Utilities will use this string to determine the location from which log messages originate. The application name can be any string that meets the following restrictions: it must not be empty, it must not exceed 128 in length, and it may only contain non-white-space visible ASCII characters and the space character. Most ALI products follow the naming convention *product_name.machine_name.user_name*.
	Local only	Limits broadcast of this application's logging messages to only the computer on which this application is installed
Portlet Configuration	Domain List for Login Tokens	Comma separated list of domain/computer names used to determine which RSS feeds need the portal login token. Domain names need to be prefaced with a * (for example `*.example.com`), while individual computer names should not start with * (for example `portal.portal-host.com`). These will be matched against the host name from the feed URL, not including the port or scheme (for example `portal.example.com`, not `https://portal.example.com:8080`). An example value might look like this: `*.example.com, portal.portal-host.com`.

A.1.8 Search Admin UI Service Settings

This section describes the settings in the Search Admin UI Service section of the Configuration Manager.

Page	Setting	Description
Application Settings	HTTP enabled	Enables/disables HTTP as the application's web protocol

Page	Setting	Description
	HTTP port	Port on which the application should listen for HTTP requests
	HTTPS enabled	Enables/disables HTTPS as the application's web protocol
	HTTPS port	Port on which the application should listen for HTTPS requests

A.1.9 Search Server Settings

This section describes the settings in the Search Server section of the Configuration Manager.

Page	Setting	Description
Search Node	Search Server Port	TCP port which Search Server listens for incoming requests
	Cluster Home Directory	Fully-qualified path to the shared cluster directory
	Document Token Cache Size (in tokens)	Number of tokens in the document token cache
	Spell Token Cache Size (in tokens)	Number of tokens in the spell token cache
	Mapping Token Cache Size (in tokens)	Number of tokens in the mapping token cache
	Index Cache Size (in bytes)	Size (in bytes) of the index cache
	Docset Cache Size (in bytes)	Size (in bytes) of the docset cache

A.1.10 Search Service Settings

This section describes the settings in the Search Service section of the Configuration Manager.

Page	Setting	Description
Application Settings	Port	Port number on which the Search Service listens for requests
	Thread Pool Size	Number of threads to use for the communication and processing of requests between the Search Service and client applications
	Memory Report Interval (seconds)	Reporting time interval for reports of JVM memory usage (seconds) If the interval is 0 or less, no memory reporting is reported.
Logging	Server	Application name that will uniquely identify log messages sent from this application Logging Utilities will use this string to determine the location from which log messages originate. The application name can be any string that meets the following restrictions: it must not be empty, it must not exceed 128 in length, and it may only contain non-white-space visible ASCII characters and the space character. Most ALI products follow the naming convention *product_name.machine_name.user_name*.

Page	Setting	Description
	Local only	Limits broadcast of this application's logging messages to only the computer on which this application is installed
Search Server	Search Host	Name of the computer that hosts the Search Server
	Search Port	Port number on which the Search Server services requests

A.1.11 Tagging Service Settings

This section describes the settings in the Tagging Service section of the Configuration Manager.

Page	Setting	Description
Activity Service	Host	Name of the computer that hosts the Activity Service
	Port	Port number on which the Activity Server services requests
	Timeout (milliseconds)	Number of milliseconds that clients wait before the Activity Service request is terminated
Administrative Credentials	User name	User name of an administrative user for Oracle WebCenter Interaction
	Password	Password for the administrative user
Analytics	Enabled	Enable Oracle WebCenter Analytics communication
	Enabled	Enable clustering
	Collector hostname	Name of the computer that hosts the Analytics collector
	Collector port	Port number on which the Analytics collector services requests
	Logging level	The level of detail for logged information
	Enable console logging	Enable/disable console logging
Application Settings	HTTP enabled	Enables/disables HTTP as the application's web protocol
	HTTP port	Port on which the application should listen for HTTP requests
	HTTPS enabled	Enables/disables HTTPS as the application's web protocol
	HTTPS port	Port on which the application should listen for HTTPS requests
Content Sources	Web Content Source ID	Object ID of the Portal Web Content Source
	Enable Portal Upload	Enable/disable uploading documents to the portal
	Portal Upload Content Source ID	Object ID of the Portal Upload Content Source
	Portal Upload Service URL	Server URL for the Portal Upload Service

Page	Setting	Description
Logging	Server	Application name that will uniquely identify log messages sent from this application Logging Utilities will use this string to determine the location from which log messages originate. The application name can be any string that meets the following restrictions: it must not be empty, it must not exceed 128 in length, and it may only contain non-white-space visible ASCII characters and the space character. Most ALI products follow the naming convention *product_name.machine_name.user_name*.
	Local only	Limits broadcast of this application's logging messages to only the computer on which this application is installed
Portal Database	Vendor	Database vendor
	Host	Name of the computer that hosts the database
	User name	Name of the database user
	Password	Password for the database user; this value is not displayed
	Port	Port number on which the database services requests
	SID (Oracle Only)	SID for the database (applies only to Oracle databases)
	Database Name (MSSQL Only)	Name of the database (applies only to Microsoft SQL Server databases)
Search Service	URL	Name of the computer that hosts the Search Service
	Timeout (milliseconds)	number of milliseconds that the Rank Engine waits before the search request is terminated
Tagging Service Database	Vendor	Database vendor
	Host	Name of the computer that hosts the database
	User name	Name of the database user
	Password	Password for the database user; this value is not displayed
	Port	Port number on which the database services requests
	Minimum pooled database connections	Minimum number of pooled connections for the database
	Maximum pooled database connections	Maximum number of pooled connections for the database
	SID (Oracle Only)	SID for the database (applies only to Oracle databases)
	Database Name (MSSQL Only)	Name of the database (applies only to Microsoft SQL Server databases)
WCI Directory	Authentication provider	Provider type (ALI Directory, generic LDAP, or Active Directory)
	Host	Name of the computer that hosts the Directory
	Port	Port number on which the Directory services requests
	Principal	Distinguished name of the directory administrator, for example `uid=administrator,ou=users,dc=bea,dc=com`

Page	Setting	Description
	Credential	Password for the principal; the value is not displayed
	SSL enabled	Enable/disable SSL
WCI Notification Service	URL	Fully-qualified URL (protocol, domain name, and port) used to connect to the Notification Service
	Timeout (milliseconds)	Number of milliseconds that clients wait before the notification request is terminated
WCI Security Database	Vendor	Database vendor
	Host	Name of the computer that hosts the database
	User name	Name of the database user
	Password	Password for the database user; this value is not displayed
	Port	Port number on which the database services requests
	Minimum pooled database connections	Minimum number of pooled connections for the database
	Maximum pooled database connections	Maximum number of pooled connections for the database
	SID (Oracle Only)	SID for the database (applies only to Oracle databases)
	Database Name (MSSQL Only)	Name of the database (applies only to Microsoft SQL Server databases)
WCI Security Identity Services	Key service file path	File path to the keystore file on the server
	Key service default alias	Keystore alias
	Key service passphrase	Keystore passphrase; this value is not displayed
WCI Security Login Tokens	Default token type	Type of Login Token used by default by ALUI Security Only use ALUI if your Directory is pointed at ALI Directory.
	Token expiration time in minutes	Token expiration time, in minutes
	Message authentication code seed value	Seed value used to create MAC signatures used to authenticate Login Tokens This should match the MAC seed for any external systems expected to consume the tokens created by ALUI Security, or to create tokens to be consumed by ALUI Security. For portal tokens, this value should match the "login token root key" in the PTSERVERCONFIG table in the portal database.
Web Authentication	User name	HTTP Basic Authentication user name Along with the password, this is used by the Tagging Engine to securely identify requests as originating from the portal. This does not need to be the user name of a portal user. These credentials must match the credentials defined in the Administrator's Basic Authentication Information section of the Tagging Engine Remote Server object's properties in the portal.
	Password	Password for the HTTP Basic Authentication user

A.1.12 UCM Content Service Settings

This section describes the settings in the UCM Content Service section of the Configuration Manager.

Page	Setting	Description
Application Settings	HTTP enabled	Enables/disables HTTP as the application's web protocol
	HTTP port	Port on which the application should listen for HTTP requests
	HTTPS enabled	Enables/disables HTTPS as the application's web protocol
	HTTPS port	Port on which the application should listen for HTTPS requests

A.1.13 WCI API Service Settings

This section describes the settings in the WCI API Service section of the Configuration Manager.

Page	Setting	Description
Application Settings	HTTP enabled	Enables/disables HTTP as the application's web protocol
	HTTP port	Port on which the application should listen for HTTP requests
	HTTPS enabled	Enables/disables HTTPS as the application's web protocol
	HTTPS port	Port on which the application should listen for HTTPS requests
Crawler Settings	Web Crawler file timeout (seconds)	Web file crawler timeout
	SOAP file timeout (seconds)	SOAP timeout for crawlers
Logging	Server	Application name that will uniquely identify log messages sent from this application Logging Utilities will use this string to determine the location from which log messages originate. The application name can be any string that meets the following restrictions: it must not be empty, it must not exceed 128 in length, and it may only contain non-white-space visible ASCII characters and the space character. Most ALI products follow the naming convention *product_name.machine_name.user_name*.
	Local only	Limits broadcast of this application's logging messages to only the computer on which this application is installed
Portal Database	Vendor	Database vendor
	Host	Name of the computer that hosts the database
	User name	Name of the database user
	Password	Password for the database user; this value is not displayed
	Port	Port number on which the database services requests

Page	Setting	Description
	Minimum pooled database connections	Minimum number of pooled connections for the database
	Maximum pooled database connections	Maximum number of pooled connections for the database
	SID (Oracle Only)	SID for the database (applies only to Oracle databases)
	Database Name (MSSQL Only)	Name of the database (applies only to Microsoft SQL Server databases)
WCI Service General	Image Service Connection URL	URL that the SOAP API Service uses to contact the Image Service
	Session Duration	Length of time sessions are valid for (in minutes) when calling RemoteSessionFactory.getExplicitLoginContext(user,password)

A.1.14 WCI Directory Settings

This section describes the settings in the WCI Directory section of the Configuration Manager.

Page	Setting	Description
LDAP Listener Settings	Host name	Name of the computer that hosts the LDAP listener
	Port number	Port number on which the LDAP listener services requests
WCI Directory Database	Vendor	Database vendor
	Host	Name of the computer that hosts the database
	User name	Name of the database user
	Password	Password for the database user; this value is not displayed
	Port	Port number on which the database services requests
	Minimum pooled database connections	Minimum number of pooled connections for the database
	Maximum pooled database connections	Maximum number of pooled connections for the database
	SID (Oracle Only)	SID for the database (applies only to Oracle databases)
	Database Name (MSSQL Only)	Name of the database (applies only to Microsoft SQL Server databases)

A.1.15 WCI Notification Service Settings

This section describes the settings in the WCI Notification Service section of the Configuration Manager.

Page	Setting	Description
Administrative Credentials	User name	Name of an administrative user for Oracle WebCenter Interaction

Page	Setting	Description
	Password	Password for the administrative user (optional)
Application Settings	HTTP enabled	Enables/disables HTTP as the application's web protocol
	HTTP port	Port on which the application should listen for HTTP requests
	HTTPS enabled	Enables/disables HTTPS as the application's web protocol
	HTTPS port	Port on which the application should listen for HTTPS requests
Email Notifications	Character Encoding	Scheme to use when encoding text in notifications
	SMTP Relay Host(s)	Comma separated list of SMTP mail servers used to send email notifications (for example `myserver.domain.com,myserver2.domain.com`)
	SMTP Port	Port that will be used when connecting to the specified mail servers
	From Display Name	Name that notifications will appear to be from
	From Email Address	Email address that will be used to send email addresses as specified in the FROM field (for example `administrator@myserver.domain.com`)
	Mail Server Connection Timeout (ms)	Number of milliseconds, that the Notification Service will keep an inactive connection to the mail server before timing out
	SMTP Server Requires Authentication	Specifies whether the SMTP relay server requires a valid user name and password in order to send email
	User Name	User name to use when authenticating with the SMTP server
	Password	Password to use when authenticating with the SMTP server; the value is not displayed
External Database	Should connect	Specifies whether this optional database connection is enabled
General Settings	Host Name	Fully-qualified name of the host of the Notification Service This value is used to construct URLs that are used when the service is not using the WCI binary gateway (for example: `myserver.domain.com`)
	Host Port	Port that the Notification Service web application is running on This value is used to construct URLs that are used when the service is not using the WCI binary gateway
	Data Location	Location on the Notification Service server where all persisted data will be stored This value is used for the embedded database and the JMS message queue (for example `c:\bea\alui\cns\1.0`)
	WebCenter Interaction URL	Base URL of Oracle WebCenter Interaction This URL used as the basis for constructing gateway links (for example `http://portal_server:8080/portal/server.pt`)

Page	Setting	Description
	Oracle WCI API Service URL	URL of the SOAP API Service This URL is available on the Portal URL Manager page of the Portal Settings Utility in portal administration (for example `http://portal_server:11905/ptapi/services/QueryInterfaceAPI`)
	Port	Port that client applications use to bind to interfaces exposed by the Notification Service
	Enable Debug Logging to Console	Forces the Notification Service to log all events, regardless of log level, directly to the console
Identity Services	Key service file path	File path to the keystore file on the server
	Key service default alias	Keystore alias
	Key service passphrase	Keystore passphrase; this value is not displayed
Internal Database	Embedded Database Name	Name of the embedded database Spaces are not allowed.
Logging	Server	Application name that will uniquely identify log messages sent from this application Logging Utilities will use this string to determine the location from which log messages originate. The application name can be any string that meets the following restrictions: it must not be empty, it must not exceed 128 in length, and it may only contain non-white-space visible ASCII characters and the space character. Most ALI products follow the naming convention *product_name.machine_name.user_name*.
	Local only	Limits broadcast of this application's logging messages to only the computer on which this application is installed
Login Tokens	Default token type	Type of Login Token used by default by ALUI Security Only use ALUI if your Directory is pointed at ALI Directory.
	Token expiration time in minutes	Token expiration time, in minutes
	Message authentication code seed value	Seed value used to create MAC signatures used to authenticate Login Tokens This should match the MAC seed for any external systems expected to consume the tokens created by ALUI Security, or to create tokens to be consumed by ALUI Security. For portal tokens, this value should match the "login token root key" in the PTSERVERCONFIG table in the portal database.
Message Processing Thread Pool	Maximum Pool Size	Specifies the most threads that will be used to handle processing inbound JMS messages that have been successfully received
	Maximum Pool Size	Specifies the most threads that will be used to handle processing outbound notifications
	INotificationSession Queue Size	Specifies the size of the JMS queue that handles remote method calls for INotificationSession
	INotificationManager Queue Size	Specifies the size of the JMS queue that handles remote method calls for INotificationManager

Page	Setting	Description
Notification Templates	Base URL	Base URL of the Image Service (for example `http://myserver.domain.com/imageserver`)
	Cache Templates	Determines whether remote templates should be cached or retrieved with every request This option should always be checked unless running in a development environment.
	Cache Interval (seconds)	Determines how often the file modification time is checked (in seconds) A value of 0 disables checking.
RSS Feeds	Enable Basic Authentication	Require aggregators to send basic authentication encoded user credentials in order to access feeds
	Gateway RSS Feed URLs	Encode the RSS Feed URLs to go through the portal gateway
	Feed Removal Age	Age (in days) when old feed items are automatically removed
Security Database	Datastore enabled	Indicates whether the StoredService is enabled
	Database Name	Name of the database
User and Group Directory	Authentication provider	Provider type (ALI Directory, generic LDAP, or Active Directory)
	Host	Name of the computer that hosts the Directory
	Port	Port number on which the Directory services requests
	Principal	Distinguished name of the directory administrator, for example `uid=administrator,ou=users,dc=bea,dc=com`
	Credential	Password for the principal; the value is not displayed
	SSL enabled	Enable/disable SSL

A.2 Configuring Portal Settings Using the Portal Utility

The Portal Settings Utility enables you to manage portal settings for user creation, login, portal URLs, and debug settings.

> **Note:** The Image Service location is not managed through the Portal Settings Utility. For information on managing the Image Service location, see Section A.3, "Updating the Image Service Location."

To access the Portal Setting Utility you must be a member of the Administrators Group.

1. Click **Administration**.
2. From the Select Utility list, choose **Portal Settings**.
3. On the User Settings Manager page, perform tasks as necessary:
   - If you want to enable any user to create a new account for your portal, select **Allow creation of Self Registered Users**.

     New users are given the Default Profile settings.

- If you have users who access the portal through mobile devices, you might want to enable numeric login to make logging in easier. To enable numeric login, select **Allow numeric Login for mobile devices**.
- If you want to automatically assign a numeric user name when a new user is created (through importation, manual creation, or self-registration), select **Auto-assign numeric Login IDs for new Users**.

Note: When you are manually creating a user, the Mobile Device Authentication page does not display a numeric ID; the numeric ID is not assigned until you save the user. To view the automatically generated numeric ID, click the new user's name to open the User Editor and click the Mobile Device Authentication page.

- Automatically lock user accounts after failed login attempts, as described in Section 6.2.3.1, "Automatically Locking User Accounts."
- Manage password rules, as described in Section A.2.1, "Configuring Password Management."
- To update the login token key, click **Update**.

  Login tokens are used by many internal processes for authentication. For security purposes, you should occasionally update the key used to generate login tokens.

  The frequency at which you need to do this depends on portal usage and your company's required level of security. For a portal that gets moderate usage, you should only need to update the key twice a year.

Note:

- When you update the key, outstanding tokens become invalid, but the portal issues new keys when the process is refreshed. For this reason, you should try to update the token during low-usage times.
- In general, users should not notice when you update the key. However, users that have the portal remember their password need to reset this option the next time they login to the portal.

---

4. On the Portal URL Manager page, perform tasks as necessary:

Caution: You should not change these URLs unless you move the associated portal server.

- If the base URL of your portal changed, edit the value in the **Primary Web Server URL** box.
- If the base URL to your gateway changed, edit the value in the **Display Files URL** box.This URL is used to construct document links. The links go through the gateway.

Note: The portal Web server uses a URL that is generated from the settings in your portal configuration file.

- If the URL to your SOAP listener changed, edit the value in the **Soap Server URL** box. This URL is passed to portlets that communicate through SOAP, so the portlets know where to post information.
- If the file path to store the stored content portlet changed, edit the value in the **Shared Files Path** box.The htm files generated by the job that runs the portlet are deposited in this folder.

5. On the General Settings page, perform tasks as necessary:
   - To troubleshoot any conflicts arising from experience rules affecting the user, select **Enable Experience Rules Debug Mode**. It enables users to display experience rules debug messages on their My Pages. When you enable this mode, the debug option is available when the user clicks **My Account**, then **Display Options**, then **Advanced Settings**. This debug page is only visible if you enable experience rules debug mode.
   - To troubleshoot portlet errors, select **Enable Portlet Errors Debug Mode**. When you enable this debug mode, end users see additional error information if there is a problem with a portlet.
6. Click **Finish**.

A.2.1 Configuring Password Management

You can configure rules for passwords. The create/manage password user interface displays the applicable password rules. Next to each rule is an icon showing whether the password has met the rule requirement. Password hints appear to the right of the password field to assist the user in typing in a valid password.

Note:

- Password management applies only to user accounts created through the portal (not those managed through an authentication source).
- Password strength checking is done only when users create or change their passwords. If a rule is changed, the rule will not affect existing passwords.

1. If the Portal Settings Utility is not already open, open it now.
2. In the **Minimum Password Length** box, type the minimum number of characters required for passwords. The default is 7.
3. If you want passwords to require at least one number, select **Passwords Require a Number**. This option is disabled by default.
4. If you want passwords to require at least one upper case letter and one lower case letter, select **Passwords Require Upper and Lower Case**. This option is disabled by default.
5. If you want passwords to require at least one punctuation character, select **Passwords Require Punctuation**. This option is disabled by default.

6. If you want to make sure that passwords do not include the user ID, select **Passwords Cannot Include the User ID**. This option is enabled by default.
7. In the **Password Reuse History** box, type the number of times a user must change passwords before an old password can be reused. If this option is set to 0 (the default setting) passwords can always be reused.

   Note: This value must be set to a number between 0 and 12.

8. In the **Password Expiration** box, type the number of days before a password expires. If this option is set to 0 (the default setting) passwords never expire.

   If a user's password expires, the user is redirected to the Change Password page until the user changes the password (the user is locked out of the rest of the portal).

   Note: The passwords for intrinsic Administrator user, guest users, and default profile users do not expire.

9. In the **Password Expiration Warning** box, type the number of days before a password expires that you want to warn a user to change the password. If this option is set to 0 (the default setting) users receive no warning.

   At the specified number of days before expiration, the user is redirected to the Change Password page.

A.3 Updating the Image Service Location

If you change the location of your Image Service, you must update the location in the Imageserver Server remote server object:

1. Log in to the portal as an administrator.
2. Click **Administration**.
3. Open the **Portal Resources** folder.
4. Expand the **Remote Server** section.
5. Click **Imageserver Server** to open the object.
6. Update the **Base URL** location.

A.4 Modifying the portalconfig.xml File

If your configuration requirements change after initial deployment, you can modify the portalconfig.xml configuration file located in the *install_dir*/settings/portal directory. Replace *install_dir* the Oracle WebCenter installation directory, for example, C:\Oracle\Middleware\wci or /oracle/middleware/wci for Windows or /oracle/middleware/wci for UNIX or Linux.

A.4.1 URLMapping

The URL mapping determines the portal base URL according to the requested URL from the request object. The portal base URL is the base URL for every single link and redirection. For example, if your portal base URL is:

http://portal.company.com/portal/server.pt, then the link to the default My Page would be: http://portal.company.com/portal/server.pt?space=MyPage.

You can add as many entries as you want to the mapping. Mapping URLs should start with http:// or https:// and end with the HTTP entry point name (unless it's the default value, "*").

> **Note:** If requests will come from both an http URL and an https URL you must create a separate mapping for each one. Then map each of these request URLs to an application URL and a secure application URL.

- ApplicationURL0: In SecurityModes 2 and 3, ApplicationURL should be set to the same value as SecureApplicationURL. In mode 0, ApplicationURL0 might be equal to "*". In this case, the Application Base URL will be the URL from the Request object.
- SecureApplicationURL0: In SecurityMode 0, SecureApplicationURL is not used. In modes 2 and 3, SecureApplicationURL0 might be equal to "*". In this case, the Application Base URL will be the URL from the request object.

A.4.2 PersonalSettings

The following configuration parameters apply to personal settings.

Parameter	Description
Greeting	The default greeting for the user. If a user wishes to override this greeting, then they can do so by changing their personal settings.
Accessibility	The default portal interface type. ■ 1: Assistive Technology Portal (508 Compliant) ■ 2: Low Bandwidth Portal ■ 3: Standard Portal
OverrideGuestAccessStyle	Override the guest user access style (from the DB) with the Accessibility value above. ■ 0: The portal will use the DB value. ■ 1: The portal will override the DB value with the value from this file.

A.4.3 CachedSettings

The following configuration parameters apply to cached settings.

Add entries for personal settings that should be cached on the http session of each user. Personal settings that are not included in this list will be retrieved from the portal every time they are requested. Settings that are on this list are obtained from the portal on login and are cached for the duration of the user's http session.

> **Note:** AccessStyle, Locale, and TimeZone should always be cached by the server.

Users can customize these settings by clicking **My Account** in the portal interface.

The following settings are cached by default:

Parameter	Description
Greeting	Stores the personalized greeting that displays on the portal banner when the user logs into the portal.
AccessStyle	Stores the user display option.
Locale	Stores the preferred language of the portal interface. Portlet names and content display in the selected language only if the language is supported by the portlets. It also stores the format for portal entries (including search requests). For example, if the user chose British English, the portal displays and expects dates in the DD/MM/YYYY format (whereas in American English, the portal displays and expects dates in the MM/DD/YYYY format).
TimeZone	Stores the time zone of the user.
PortletTimeout	Stores the maximum time to wait for a portlet to load.
CollapsedGadgets	Stores which portlets were minimized by the user.
COMCollapsedGadgets	Stores which portlets in the community page were minimized by the user.
MyPageRefreshRate	Stores the refresh rate of user My Pages.

A.4.4 Authentication

The following configuration parameters apply to authentication.

Parameter	Description
AllowGuestAccess	Allow the guest user to access the portal. If guest access is not allowed, the portal will always prompt for login information.
GuestRedirectToLogin	If the guest user does not specify a space in the URL query string, this setting determines the initial page the user sees. Users can navigate to different portal pages by including `space=xxxx` strings in the URL query string. For example, if the user were to type: `http://MYSERVER/portal/server.pt?space=MyPage`, the user will be directed to the My Page (the access privileges of that page will be in effect). However, if the user did not include a `space=xxxx` string in the query string (that is, the user only typed: `http://MYSERVER/portal/server.pt`), the portal directs them to a default page, depending on the GuestRedirectToLogin setting and the experience definition settings, as follows: ■ 0: The portal will redirect the guest user to the home page defined in the current experience definition (usually a My Page or community page). ■ 1: The portal will redirect the guest user to the login page as defined in the current experience definition.
RedirectOnLogout	After logging out the user is redirected to a default page as follows: ■ 0: The portal will redirect the guest user to the home page defined in the current experience definition (usually a My Page or community page). ■ 1: The portal will redirect the guest user to the login page as defined in the current experience definition.

Parameter	Description
AuthTokenExpiration	This setting enables you to set how long the portal remembers your login password after doing an HTTP Basic Authentication for WebDav. The value should be formatted in minutes and is defaulted to 30 minutes. Entering 0 will disable the cookie from being set.
AllowDefaultLoginPageAuthSource	Controls the use of the default authentication source for portals (that do not use single sign-on) on the login page and Login Portlet. It also lets you configure the authentication source list.

DefaultAuthSourcePrefix	Sets the default authentication source prefix that will be prepended to the login name when users log in to your system, unless they select another authentication source from the list on the login page. In the case of SSO, this is the authentication source category for all of your SSO users.
	
	You can use AuthSourcePrefix tags to order the items in the authentication source list. Entries in the list should look like the following:
	
	`<AuthSourcePrefix[i] value="Auth Source Prefix">`
	`</AuthSourcePrefix[i]>`
	
	Where [i] is replaced with the items' order in the list (starting with 1).
	
	To include the WCI Authentication Source in the list, simply make an entry with “WCI Authentication Source” as the value. The WCI Authentication Source is for users who are created in the portal, manually, through invitations, or through the Create an Account page. For example, to include the WCI Authentication Source as the third item in the list, use the following tag:
	
	`<AuthSourcePrefix3 value="WCI Authentication Source">`
	`</AuthSourcePrefix3>`
	
	Authentication source prefixes in the ordered list are displayed first in the list and are followed by any authentication sources not included in the ordered list.
	
	Authentication Source Modes:
	
	■ 0: This is the default mode. In this mode the portal does not use the default authentication source, and the list has no special ordering.
	
	■ 1: In this mode the portal uses the default authentication source, and the list is hidden, but there is a link users can click to show the list. This lets users select a nonstandard authentication source.
	
	To use this mode, you must turn off the caching on the Login Portlet or disable the Login Portlet and set the `DefaultAuthSourcePrefix` tag to the prefix of the authentication source that is the default for all users.
	
	■ 2: In this mode the portal uses the default authentication source, and the list is shown with the default authentication source selected.
	
	To use this mode, you must turn off the caching on the Login Portlet or disable the Login Portlet and set the `DefaultAuthSourcePrefix` tag to the prefix of the authentication source that is the default for all users.
	
	■ 3: In this mode the portal uses the default authentication source, and the list is unavailable.

Parameter	Description
AllowAutoConnect	Setting for saving passwords in cookies. ■ 0: Turns off the option of saving passwords in a cookie. ■ 1: Users will see a "Remember my password" check box on the login page of your portal. Passwords are saved as cookies for users that select this check box, which lets users who navigate to your portal be logged in automatically.
SSOVendor	Sets the single sign-on configuration. For information on SSO, see Deploying Single Sign-On.
CaptureBasicAuthenticationForPortlets	Determines whether to capture basic authentication information (login and password) and store it in the session (to send to portlets). The basic authentication information cannot be captured when users select "Remember my password" to login through a cookie. ■ 0: The authentication information will not be stored in the session. ■ 1: The authentication information will be stored in the session.
RememberPassword	This setting enables you to set how long the portal remembers your login password. The value should be formatted in minutes. The default is one week.
BrowserLoginTokenExpiration	This setting enables you to set whether the portal caches a login token in a browser session cookie that will expire when the browser is closed. Entering 0 will disable the cookie from being set, and is the default value. Entering a positive number controls how long the login token will remain valid. Note that the cookie is only valid as long as the browser is open, so if the user closes their browser, the login token will be removed. The login token expiration is an upper limit if they don't close their browser. A reasonable value for this would be 600 minutes (one workday). The value should be formatted in minutes. **Note**: The BrowserLoginTokenExpiration setting is only active when AllowAutoConnect is set to 1.

A.4.5 Security

The following configuration parameter applies to security.

Parameter	Description
SecurityMode	This setting determines which pages will use SSL encryption. You must install a digital certificate and enable SSL on your Web server before changing the default value of 0. **Note**: Changing the security mode affects the URL Mapping. For more information, see Chapter A, "Configuring Portal Settings." ■ 0: The portal does not check the security of incoming requests. In mode 0, ApplicationURL0 and SecureApplicationURL0 may be equal to "*". In this case, the Application Base URL will be the base URL from the Request object. ■ 1: Selected pages that involve sensitive information such as passwords use SSL, while other pages are sent unencrypted for better performance. Only pages of Activity Spaces listed in SecureActivitySpaces.xml (which is located in the same folder as portalconfig.xml) are sent through HTTPS. The portal verifies that links and redirections to Secure Activity Spaces uses HTTPS. If a secure Activity Space were requested through a non-secure URL, the portal would redirect the same request to HTTPS. If XPRequest.GetRequestURL() equals URLFromRequest0, ApplicationURL0 and SecureApplicationURL0 might both be the Application Base URL, depending on the security of the Activity Space. You must install a digital certificate and enable SSL on your Web server. ■ 2: Every page uses SSL.The portal verifies that every single incoming request uses HTTPS. If it does not, the portal will redirect this request to HTTPS. This setting is best for very secure applications where performance is not a major concern. If the URL from the Request object equals URLFromRequest0, SecureApplicationURL0 will be the Application Base URL. URLFromRequest0 has to be equal to "*". This is the default entry. It will be used if no mapping entry matched the URL from the Request object. You must install a digital certificate and enable SSL on your Web server. ■ 3: Select this mode if you are using an SSL Accelerator. Because the portal is behind an SSL Accelerator, the security of the incoming requests is not verified. The portal trusts every request from the SSL Accelerator. All the links and redirections are in HTTPS. If URL from the Request object equals URLFromRequest0, SecureApplicationURL0 will be the Application Base URL. URLFromRequest0 has to be equal to "*". This is the default entry. It will be used if no mapping entry matched the URL from the Request object. You must install a digital certificate and enable SSL on your Web server.

A.4.6 Documents

The following configuration parameters apply to documents.

Parameter	Description
NewDocumentTime	The number of days that a document or folder displays "new" after its name.
DocumentLastUpdated	The number of days that a document displays "updated" after its name.
OpenNewWindow	The default setting for the open in new window preference. ■ 0: The document opens in the same window. ■ 1: The document opens in a new window. Users can override this setting by changing their personal preferences.
SubFolderBrowseThroughSearch	This parameter sets the Subfolder Browsing source. ■ 0: Subfolder browsing is driven through the database. ■ 1: Subfolder browsing is driven through search. **Note**: Database driving browsing may often be faster for subfolders, while search may be faster for documents.

A.4.7 Crawlers

The following configuration parameter applies to content crawlers.

Parameter	Description
MaxWebCrawlRadius	The setting for the maximum number of links away from the target page to crawl. For example, if you select 1, the content crawler attempts to import every page directly linked to the target page; if you select 2, the content crawler attempts to import every page directly linked to the target page, and every page directly linked to those linked pages. This setting corresponds to the **Crawl Radius** list in the Web Content Crawler Editor. The default maximum is 4, which means the list allows a crawl radius of 1 to 4.

A.4.8 Search

The following configuration parameter applies to search.

Parameter	Description
NumSearchResultsPerPage	The default number of search results to show per search results page.

A.4.9 Style

The following configuration parameter applies to style.

Parameter	Description
StyleSheetName	The name for the portal's default stylesheet.

A.4.10 Communities

The following configuration parameters apply to communities.

Parameter	Description
DefaultCommunityID	Configure this setting only if your navigation scheme is Tabbed Section Left Vertical Navigation or if you use a custom navigation scheme that uses the IPluggableNavModelRO.GetDefaultCommunity() method. In these cases, the setting specifies the ID of the default community to display when a user clicks the **Community** tab.
CommKnowledgeDirLinksPerPage	The number of links to display on one screen in the community Knowledge Directory.

A.4.11 Administration

The following configuration parameters apply to administration.

Parameter	Description
IsAdminSite	Determines whether the computer is an administrative portal or a browsing-only portal. ■ 0: Sets the computer into a browsing-only portal. ■ 1: Sets the computer into a browsing and administrative portal.
AdminObjectsPerPage	Determines the number of administrative objects of a single type (for example, content crawlers or content sources) allowed to display on one screen. This controls the number of items displayed on the administrative interface. The default is 10.
MaxResultsToDisplay	This setting is currently used only by Group editor, to set the maximum number of users to display.

A.4.12 Invitations

The following configuration parameter applies to invitations.

Parameter	Description
IsInvitationURLSecure	Sets the security of the invitation URL. **Note**: Use a secure URL only if you disable http. ■ 0: Unsecure. The URL uses http://. You can use an unsecure invitation URL with any security mode, so long as you do not disable http or have http URLs redirect to https. ■ 1: Secure. The URL uses https://. If the SecurityMode setting in your portalconfig.xml file does not allow http, you must select this mode.

A.4.13 Gateway

The following configuration parameter applies to gatewayed URLs.

Parameter	Description
PutUserIDInURL	This setting controls if the user ID should be part of the gateway URLs or not. ■ 0: User ID in the gateway URL is always set to 0. ■ 1: User ID in the gateway URL contains real user ID. **Note**: HTTP caching proxies will work better if userid is not part of the URL.

A.4.14 Navigation

The following configuration parameter applies to navigation.

Parameter	Description
intMyPortletPrefButtonInPortletHeader	This setting controls if the My Portlet Preference button on is displayed in portlet headers. ■ 0: Button is displayed. ■ 1: Button is not displayed.

A.5 Customizing the Tokens in Friendly URLs

By default, the portal areas are represented by the following tokens in friendly URLs: mypage, community, user, directory, document, and gw. However, the system administrator can change these tokens to fit the needs of the company.

1. Open the following file in a text editor: *install_dir*\settings\portal\FriendlyURLs.xml.

   For example: C:\Oracle\Middleware\wci\settings\portal\FriendlyURLs.xml for Windows or /oracle/middleware/wci/settings/portal/FriendlyURLs.xml for UNIX or Linux

2. Edit the `<key>` values as desired.

   You can change the following tokens:

   - `mypage` — represents a My Page object
   - `community` — represents a community object
   - `user` — represents a user
   - `directory` — represents a Knowledge Directory folder
   - `document` — represents a document
   - `gw` — represents gatewayed object

   For example, you might change the token for directory to "folder" as in the following code:

```
<FriendlyURLMapping>
<key>folder</key>
<classId>17</classId>
</FriendlyURLMapping>
```

   This would mean that users could access Knowledge Directory folders through a friendly URL in the format: *http://portal.company.com/portal/server.pt*/folder/*object_name*/*object_id*

A.5.1 Disabling Friendly URLs

By default, you can direct users to portal areas with simple URLs, referred to as friendly URLs. However, you can disable friendly URLs for your deployment if you want to.

1. Open the following file in a text editor: *install_dir*\settings\portal\FriendlyURLs.xml.

For example: C:\Oracle\Middleware\wci\settings\portal\FriendlyURLs.xml for Windows or /oracle/middleware/wci/settings/portal/FriendlyURLs.xml for UNIX or Linux.

2. Comment out any FriendlyURLMapping you want to disable.

   For example, you can disable friendly URLs for Knowledge Directory folders by commenting out the following code:

```
<!--
<FriendlyURLMapping>
    <key>directory</key>
    <classId>17</classId>
</FriendlyURLMapping>
-->
```

A.5.2 Friendly Gateway URLs

Gatewayed content is displayed with an URL that makes it easy to read and extract information from.

Gatewayed URLs include several tokens to help to determine where the gatewayed content came from.

Here is an example of a part of a gatewayed URL: `../gw/ws2000_c230_u1/..`

- The first part of the gateway URL is the gateway token — `gw`

  Note: The system administrator can customize this token in the FriendlyURLs.xml file. For information on customizing friendly URL tokens, see Section A.5, "Customizing the Tokens in Friendly URLs."

- The second part of the URL specifies where the content came from:
  - If the content came from a Web service, like in our example, you see `ws` followed by the Web service ID.
  - If the content came from a portlet, you see `pt` followed by the portlet ID.
- The remaining parts of the URL specify any additional parameters, separated with underscores (_):
  - If there is a community parameter, you see `c` followed by the community ID.
  - If there is a page parameter, you see `p` followed by the page ID.
  - If there is a preference parameter, you see `r` followed by the preference ID.
  - If there is a user parameter, you see `u` followed by the user ID.

A.6 About Fine-Tuning the Search Service Configuration

The installer sets most Search Service configuration parameters to useful defaults. In addition to the default configuration file, the *install_dir*/ptsearchserver/10.3.3/config directory includes template configuration files for Search Service deployments.

The templates include settings appropriate for a number of operating systems and RAM configurations. RAM determines the recommended maximum number of documents in the search collection, and this collection size determines many of the settings in the template configuration files. Examine the contents of these files, choose

the one appropriate for your deployment, and rename the template node.ini (the active configuration file).

> **Note:** If the Search Service component resides on the same host computer as other portal components, consider using a template tuned for a smaller amount of memory to prevent system paging that adversely affects Search Service performance.

In some cases you might be able to further improve performance by modifying some values in the node.ini file. This section includes the following sections that describe the parameters in node.ini:

- Default Search Service Parameters
- Optional Search Service Parameters

A.6.1 Default Search Service Parameters

The following parameters appear in node.ini by default.

Parameter	Description
RFINDEX	Directory used to store Search Service index files. By default, the installer puts these files in the *install_dir*/ptsearchserver/10.3.3/index subdirectory. The directory should have sufficient space for the collection you are indexing. You should not change this parameter unless you move your index files or are instructed to do so by customer support.
RFPORT	Port that the Search Service uses for communication with other processes (mainly the portal). The installer prompts for this port number during installation. This value displays in the Search Service Manager, on the Host Settings page. If you change this value in node.ini, you must also change the value in the Search Service Manager or the portal will malfunction.
RF_MAPPING_TOKEN_CACHE_SIZE	Specifies the size of the cache of mapping tokens. These tokens represent thesaurus and Best Bets entries read from the mappings collection. The default value is 5000. This parameter is chosen in the configuration file templates to reflect the expected number of tokens associates with the maximum supported collection size. The value of this parameter does not have a large effect on Search Service performance. Each cache element is 120 bytes, so the default mapping cache will occupy 600 kilobytes of memory.
RF_LOG_VERBOSITY	Numeric parameter that determines how much information is logged in the Search Service logs. Values range from 0 to 5. The default is 3 (high verbosity). You generally do not must change this parameter. We recommend you not set this below 3. If RF_LOG_VERBOSITY is set below 3, the reports generated by the Search Log Analysis external operation (and viewable on the Search Results Manager) will not contain all of the information needed to support log analysis.

Parameter	Description
RF_DOCUMENT_ TOKEN_CACHE_SIZE	Numeric parameter that specifies the size of the cache of document tokens. These tokens are words from the actual indexed content in the Search Service. The default value is 250000. This parameter has a significant effect on Search Service indexing and query performance, with larger values providing better performance. This parameter is chosen in the configuration file templates to reflect the expected number of tokens associates with the maximum supported collection size. Each cache element is 120 bytes, so the default document token cache occupies 29 megabytes of memory.
RF_SPELL_TOKEN_ CACHE_SIZE	Numeric parameter that specifies the size of the cache of spelling tokens. These tokens are word fragments from the spelling data derived from the indexed content. The default value is 250000. This value does not must be larger than the number of tokens in the spell collection, and it does not must exceed the value in the configuration file templates provided in the config directory. This parameter has a significant effect on indexing performance, spell checking, and wild card queries. If these operations seem particularly slow, you can increase the value specified by this parameter. In practice, values larger than 1000000 provide diminishing return while consuming significant amounts of memory. Each cache element is 120 bytes, so the default spell cache occupies 29 megabytes of memory.
RF_INDEX_CACHE_ BYTES	Numeric parameter specifying the size of the index cache in bytes. The default value is 78643200 (75 megabytes). The value of this parameter has a significant effect on Search Service query performance. The index and docset (see RF_DOCSET_CACHE_ BYTES) caches should be made as large as possible while leaving sufficient memory available for the Search Service's other needs.
RF_DOCSET_CACHE_ BYTES	Numeric parameter specifying the size of the document cache in bytes. The default value is 2614400 (25 megabytes). The value of this parameter has a significant effect on Search Service query performance. The index and docset (see RF_INDEX_CACHE_ BYTES) caches should be made as large as possible while leaving sufficient memory available for the Search Service's other needs.

A.6.2 Optional Search Service Parameters

Optionally, if advised by customer support, you can add the following values to the node.ini file.

Parameter	Description
RFLOG	Directory where the Search Service writes its logs. The default is the SearchServerInstall/logs subdirectory. Edit this value only if you change this directory; the new directory must exist and must be writable by the Search Service.
RF_HIGH_PRIORITY	If this parameter is set to any value, Search Service attempts to increase its process priority over that of other processes. This is not normally necessary, but might be useful on a computer where other processes compete for resources with the Search Service.
RF_MAX_WILDCARD_ EXPANSIONS	When a user enters a query that uses a wildcard (for example, “plum*”), this parameter determines the maximum number of terms into which the wildcard is expanded (for example, plum, plums, plumber). The default is 100 terms. This limit keeps overly general queries (“*ing”) from expanding into a huge number of terms and consuming too much time and memory. In large installations, you might must increase this value.

Parameter	Description
RF_MAX_QUERY_ MSECS	Maximum time, in milliseconds, for user queries. The default is 10000 (ten seconds). After processing the query for this much time, the Search Service returns results it has found so far. You might want to lower the value of this parameter if end users complain that ten seconds is too long to wait for query results.
RF_MAX_TOTAL_ RESULTS	Maximum number of results returned by a query. The default is 10000. You do not generally must change this parameter because the portal displays fewer results than the Search Service maximum.
RF_MAX_NUM_ STATIC_ARCHIVES	Maximum number of static archives per collection created in the index directory. The default is 50; meaning that there will be up to 50 archive.NNN.docset files (where NNN is a number), archive.NNN.index files, and so on. There can also be up to 50 spell.NNN.docset files, spell.NNN.index files, and so forth. You do not generally must change this parameter; the only reason might be an operating system (such as Solaris 2.6) that does not allow the Search Service to use enough file descriptors to open all the files at once. Lowering this number causes archive merges to use more memory and disk space.
RF_QUERY_THREADS	Number of threads to dedicate to query processing. The default is 8. You might must increase this parameter if your Search Service is under heavy load. The value should represent the expected number of simultaneous queries. If this value is too low, incoming queries will wait on a queue for the next free query thread and users will experience longer query times (possibly several seconds).
RF_QUERY_QUEUE_ SIZE	When all Search Service query threads (see RF_QUERY_ THREADS) are busy, incoming query requests are placed on a queue to wait for the next available query thread. This parameter determines the length of that queue. The default value is 20 and usually does not must be changed. Should the query queue ever become full, additional query requests are rejected and a message is written to the Search Service logs. If this happens, you can increase RF_QUERY_QUEUE_SIZE.
RF_INDEX_THREADS	Number of threads to dedicate to indexing requests. The default is 2. You might must increase this parameter if the indexing performance of your Search Service is too low. However, devoting additional system resources to indexing will reduce query performance. Ideally, the value of RF_INDEX_THREADS should not exceed the number of CPUs on the system.
RF_INDEX_QUEUE_ SIZE	When all Search Service index threads (see RF_INDEX_THREADS) are busy, incoming index requests are placed on a queue to wait for the next available index thread. This parameter determines the length of that queue. The default value is 20. To estimate a good value, add the number of threads in all content crawlers that might be running simultaneously (you can request up to four threads when setting up a content crawler). To be conservative, make your estimates high. If this parameter is too low, content crawlers can fill the index queue and the Search Service rejects additional index requests until the queue has room for more requests. **Note**: It is better to schedule nonoverlapping crawls than to set a high value for RF_INDEX_QUEUE_SIZE; consider changing the crawl schedule before modifying this parameter.
RF_HANDSHAKE_ THREADS	Number of threads to dedicate to servicing incoming socket connections. The default is 5. This value should never must be changed.

Parameter	Description
RF_HANDSHAKE_QUEUE_SIZE	Socket connections from Search Service clients are placed on this queue to await acknowledgment by one of the handshake threads (see RF_HANDSHAKE_THREADS). This parameter determines the length of that queue. The default value is 20. Once successfully acknowledged, the connections are assigned to either the query or index queue. Under exceptionally high loads, this queue might fill up and the Search Service will reject new connections until the queue has room for more requests. Should this happen, you can increase the value of this parameter.
RF_TOKEN_LEXICON_REBUILD_LIMIT	Maximum lexicon size, measured in number of tokens, to rebuild automatically. If the Search Service detects that the lexicon was closed improperly, the lexicon is rebuilt as part of the startup process. This can be time consuming. The default value is 400000, ensuring that the rebuild requires no more than a few minutes. Larger lexicons needing repair must be rebuilt with the standalone examinearchive utility. You might change the value or set it to zero to allow automatic rebuild of arbitrarily large lexicons. **In Windows Systems:** Setting this value too large can result in error dialogs being posted by the Windows Service Control Manager when the Search Service is run as a Windows service and a lexicon rebuild is performed. These error dialogs indicate that the service is failing to start in a timely manner. They can be disregarded.
RF_USE_DATA_FILE_CACHE	Numeric parameter indicating whether the Search Service should use caches when accessing index and document data. A value of zero disables the caches and causes the Search Service to use memory-mapping. A nonzero value activates the caches. The default value is 1. We strongly recommend you do not change this value. This parameter serves as the master on/off switch for RF_INDEX_CACHE_BYTES, RF_DOCSET_CACHE_BYTES, RF_INDEX_CACHE_MAX_PAGES_PER_BLOCK, and RF_DOCSET_CACHE_MAX_PAGES_PER_BLOCK. When RF_USE_DATA_FILE_CACHE is zero, these other parameters have no effect. Disabling the caches for small search collections (less than 1 gigabyte of data) might provide a slight improvement in performance depending upon the amount of available physical memory on the Search Service host. In memory-mapped mode, the Search Service fails if the index and document data, plus the Search Service's internal data structures should exceed 2 or 3 gigabytes (depending upon the operating system configuration).
RF_REQUIRED_DISK_SPACE	Amount of disk space (in KB) required to start a dynamic index merge. When merging dynamically indexed data into the search collection, the Search Service verifies that this amount of free space is available on the volume containing the search collection. If the space is not available, the merge process aborts, the Search Service enters read-only mode, and further dynamic indexing requests are rejected. The default value for this parameter is 40000 and should not must be changed.

When you modify cache settings, keep the following important values and relationships in mind:

- An RF_DOCSET_CACHE_BYTES:RF_INDEX_CACHE_BYTES ratio of 1:3 has been empirically determined to provide near-optimal cache performance for typical search collections.
- Token cache entries occupy 108 (32-bit platforms) or 120 (64-bit platforms) bytes.

- Reasonable values for RF_MAPPING_TOKEN_CACHE_SIZE are 500 to 10000.
- For performance reasons, document offsets and index offsets data is accessed through memory-mapping, regardless of the setting of RF_USE_DATA_FILE_CACHE in the node.ini file meaning that the memory footprint of a running Search Service depends on the size of the search collection, and this consideration has been calculated in the settings for the configuration file templates in the config directory. The amount of memory needed for these mappings can be calculated approximately as (Size of *.docsetOffsets files in bytes) + 0.006 * (Size of *.index and *.key.index files in bytes).
- Leave sufficient address space (and, ideally, physical RAM) available for the number of query and index threads. Allow 10 MB per query thread (see RF_QUERY_THREADS) and 50 MB per index thread (see RF_INDEX_THREADS).

B

Logging Features

This chapter describes the logging features available with Oracle WebCenter Interaction.

It includes the following sections:

B.1 About the Logging Features

Oracle WebCenter Interaction has several logging features available to help you monitor the health of your portal and troubleshoot any problems you might have.

- Job logs: If you must troubleshoot a problem with an authentication source, content crawler, or operation, you can view the logs for the job associated with that object. To view a job log, open the job and click the Job Logs page. For more information, see Section 11.5.12, "Viewing Job Status and Job Logs."
- The System Health Monitor is an administrative portal tool that provides real-time access to performance information on remote servers, custom objects, and Oracle WebCenter Interaction services. To access the System Health Monitor, go to portal administration and click **Select Utility**, then **System Health Monitor**. For details, see the portal online help.
- Log files: Each Oracle WebCenter Interaction component has its own log files. For example, the portal's log file is located in *install_dir*\ptportal\10.3.3\settings\logs.
- Logging Spy: Logging Spy (formerly PTSpy) is the primary log message receiver for Oracle WebCenter Interaction's logging framework. A GUI-based application for displaying log messages as they stream in from the portal and other log message senders.
- Logger: Logger runs as an unattended background process that receives log messages from the Oracle WebCenter Interaction logging framework and uses the Log4J framework to write messages to a disk file or other repository.
- Console Logger: Console Logger is similar to the Logger, but runs in a console window instead of in an unattended background process. Console Logger uses the Log4J console appender to display log messages in the console window.

B.2 Logging Levels

There are eight logging severity levels:

Table B–1 Logging Levels

Severity Level	Description	Logging Spy Color Code
Info	Normal but significant event.	black
Action	Significant action between Info and Warning.	black
Function	Brackets the beginning and ending of function and puts bracketed message in context.	black
Performance	A millisecond timestamp (e.g., operation X took # milliseconds) for costly tunable operations.	green
Warn	Minor problem.	pink
Debug	Most common and numerous log call, used for detailed call tracing and parameter logging.	gray
Error	Major problem affecting application function.	red
Fatal	Blocking problem.	white on red

Verbose logging levels can be intrusive. Use the Debug logging level only if you are actively debugging; this level of logging will affect the performance of the portal.

B.3 Logging Spy

Logging Spy (formerly PTSpy) is the primary log message receiver for Oracle WebCenter Interaction's logging framework. Logging Spy displays log messages from the portal and other Oracle WebCenter Interaction products and services. It provides additional features including fine-grained filtering, saved log file display, error highlighting, find, and sort.

To launch Logging Spy in Windows, click **Start**, **Programs**, **Oracle**, **WebCenter Logging Utilities**, then **Logging Spy**. (The shortcut location is configured during installation. If you changed the default, use the location you chose.)

The default path to launch Logging Spy in UNIX and Linux is: *install_dir*/ptlogging/10.3.3/bin/PTSpy.sh

The buttons below the menus invoke the following features:

- **Open Existing Log File**: Loads a *.spy log file into the log buffer for review.
- **Save File**: Saves the contents of the log buffer to a *.spy log file for later review.
- **Copy Selection**: Copies the selected log message lines into the system clipboard as text. Click the mouse over a line to select it. Use shift+up arrow or shift+down arrow to extend the selection.
- **Clear Log**: Clears the contents of the log buffer.
- **Set Filters**: Invokes the Filter Settings dialog box to change the visibility of various log levels and components.
- **Start/Stop Logging**: A toggle button to start or stop logging. Stopping logging may be useful when many messages are flowing and you want to concentrate on a set of messages already captured by Logging Spy.

To configure which applications to log and which logging levels to retrieve:

1. Click **Set Filters** to open the Filter Settings dialog.
2. To add a new application, click **Edit**, then **Add Message Sender**.
3. In the Add Message Sender dialog box, select the logging application name of the sender from which you wish to receive log messages and click **OK**.

   Most Oracle WebCenter Interaction components use the naming convention productname.computername.username. If you do not see an application name for your sender, see the instructions in Section B.6, "Logging FAQ."

The message sender is displayed as a top node in the Filter Settings dialog. If Logging Spy detects the application on the network, the application components will appear as sub-nodes in the Filter Settings dialog. Under each component sub-node are eight sub-nodes for the eight logging levels. For information on logging levels, see Section B.2, "Logging Levels."

By default, the Warn, Error, Fatal and Action logging levels are enabled for all components. To change these settings, click the corresponding checkbox or use the Edit menu to make changes that affect multiple components. To revert all components to the default settings, click Edit | Reset Filters. Click Apply or OK to save your changes. (The default settings are defined in an XML configuration file called ptspy.xml. The format of ptspy.xml is similar to that of ptLogger.xml. For information on ptLogger.xml, see Section B.4.1, "Configuring Logger (ptLogger.xml).")

The Logging Spy interface displays enabled logging messages from all application components in the order they are received. The view can be filtered by a range of parameters, including component and severity level (Type).

The state of the logging receiver is displayed in the bottom right of the Spy window:

- Not receiving: The logger is stopped and is not receiving messages.
- Receiving autoscroll on: The default state of the receiver is to display all messages in the window and scroll as new messages are received.
- Receiving Messages: Click the highlighted line to start auto-scrolling. Last received message ID: ##: If you click on a logging message line to view a specific message, the receiver stops scrolling. New messages are still added to the bottom of the display. To reactivate auto-scroll, click the selected line again.
- Not displaying some received messages: If you sort the view by a specific column, the receiver only displays the existing messages, ordered by the selected column. New messages are buffered. To reset the window and view all messages, click any logging message line in the window twice.

To view the full text of a logging message, copy the line to a text editor. To select the entire line, click CTRL+C. To select the message text only, click CTRL+M. (To paste the text in the text editor, click CTRL+V.)

If you do not see any messages from your sender, see the instructions in Section B.6, "Logging FAQ." This page also explains how to configure the memory allowance for Logging Spy.

B.4 Logger

Logger runs as an unattended background process that receives log messages from the Oracle WebCenter Interaction logging framework and uses the Log4J framework to write the messages to a disk file or other repository. Log4J is an open source logging solution from Apache that comes bundled with a wide variety of solutions for dealing with logging messages. In Log4J terminology, these solutions are called appenders. By

taking advantage of Log4J appenders, Logger is also able to deal with log messages in a wide variety of ways.

The primary use of Logger is to save log messages to a disk file, but it can also be used in more exotic ways, such as sending log messages to an e-mail system. This can all be done without any coding, simply by modifying the ptLogger.xml configuration file and adding Log4J appender elements as explained below. The default location for the log files produced by Logger is *install_dir*\ptlogging\logs.

B.4.1 Configuring Logger (ptLogger.xml)

Logger uses an XML configuration file called ptLogger.xml (*install_dir*\settings\ptlogging). This configuration file specifies which servers the logger should receive messages from, and which Log4J appender(s) should be used for the log messages from each server. Each server can be associated with one or more appenders. You can also specify that only messages at certain logging levels from a given server should be sent to an appender.

The specification for the ptLogger.xml file is as follows.

The root level xml node must be `<configuration>`. Under `<configuration>` there are two types of nodes: `<appender>` and `<filters>`. There may be zero or more of any of these nodes and they may appear in any order. The syntax and semantics of each node is defined below.

An `<appender>` node defines the settings for a specific Log4J appender, and must follow the format specified in the Log4J specification, as shown in the example below.

```
<appender class="org.apache.log4j.RollingFileAppender"
name="CollabRollingLogFile">
     <layout class="com.plumtree.openlog.log4jbridge.MyPatternLayout" />
     <!-- The output file name -->
<param name="File" value="c:/collab.log" />
     <!-- The maximum size of each file -->
<param name="MaxFileSize" value="10MB" />
     <!-- The maximum number of files to keep around -->
<param name="MaxBackupIndex" value="1" />
</appender>
```

- The `class` attribute specifies the Java class of the appender. In this example, the attribute is "org.apache.log4j.RollingFileAppender," so the Rolling File Appender is being specified. This is the appender used most often by the Logger. The purpose of the Rolling File Appender is to save log messages to a disk file with control over the size of the file. When the file gets too big, a new log file will be started. (Logging messages can be forwarded to any Log4J appender.)
- The `name` attribute specifies a user-defined name. It is important to specify a unique and meaningful name for each appender. In the example above, the name is "CollabRollingLogFile" indicating that this appender will be used to save log messages from Oracle WebCenter Collaboration. This name is used in the <filters> node to associate the appender with a server.
- The `layout` element specifies the Java class to use for the layout. This value should never be changed. Every appender node must use the layout class com.plumtree.openlog.log4jbridge.MyPatternLayout.
- The `<param>` node with attribute `name="File"` specifies the location of the output file. The value attribute should contain the full path to the desired output file.

- The <param> node with attribute name="MaxFileSize" specifies how large the file is allowed to grow before a new log file is started. See the Log4J documentation for details.
- The <param> node with attribute name="MaxBackupIndex" specifies how many backup log files to keep. See the Log4J documentation for details.

A <filters> node is used to specify a log message sender from which Logger should receive messages and the appender to which messages should be channeled. The filters node defines which logging levels are enabled for each component in the sending application, as shown in the examples below.

```
<filters server="collab.Foo-w2k.BarryF" appender="CollabRollingLogFile"
enabled="true" restrict-to-local="false" >

<component-defaults>
<level enabled="false" value="Debug" />
<level enabled="false" value="Info" />
<level enabled="false" value="Warning" />
<level enabled="true" value="Error" />
<level enabled="true" value="Fatal" />
<level enabled="false" value="Action" />
<level enabled="false" value="Performance" />
<level enabled="false" value="Function" />
</component-defaults>

<component name="Documents">
<level enabled="false" value="Debug" />
<level enabled="true" value="Info" />
<level enabled="true" value="Warning" />
<level enabled="true" value="Error" />
<level enabled="true" value="Fatal" />
<level enabled="true" value="Action" />
<level enabled="false" value="Performance" />
<level enabled="false" value="Function" />
</component>

</filters>

<filters server="collab.Foo-w2k.BarryF" appender="EmailAppender" enabled="true" >

<component name="Documents">
<level enabled="false" value="Debug" />
<level enabled="false" value="Info" />
<level enabled="false" value="Warning" />
<level enabled="true" value="Error" />
<level enabled="true" value="Fatal" />
<level enabled="false" value="Action" />
<level enabled="false" value="Performance" />
<level enabled="false" value="Function" />
</component>

</filters>
```

The <filters> node has two required attributes (server and appender), two optional attributes (enabled and restrict-to-local).

- The server attribute (required) is the application name of the log message sender from which Logger should receive log messages. Typically a log message sender will read its application name from a configuration file at start-up. The application name can be any string that meets the following restrictions: it must be no longer

than 128 characters and non-empty, it may only contain non-white-space visible ASCII characters and the space character. Most Oracle WebCenter Interaction products follow the naming convention [product-name].[computer-name].[user-name].

- The appender attribute (required) is the name of the appender node to which Logger will send messages. This attribute must reference the name attribute from an existing <appender> node (described above). The first node in the example above references the CollabRollingLogFile appender node defined above. The second node uses an appender called "EmailAppender," so there must be an <appender> node named "EmailAppender" somewhere in the ptLogger.xml file.
- The enabled attribute (optional) offers a convenient way to disable a server without deleting the entire <filters> node. If the attribute is omitted, the value defaults to true. If the attribute is set to false, the server is temporarily disabled; no log messages from this server will be received.
- The restrict-to-local attribute (optional) enables you to restrict the scope of the filter messages it sends out to the local computer. If the attribute is omitted, the value defaults to false. If the attribute is set to true, the Logger assumes that the log message sender resides on the same computer on the network; no messages will be sent over the network. If you do not know whether the log message sender will reside on the same computer as Logger, the value of this attribute should be set to false.

Each node has zero or more `<component>` sub-nodes and an optional `<component-defaults>` sub-node.

- Each `<component>` sub-node has eight `<level>` sub-nodes and one required name attribute. The value of the name attribute is the name of one of the components from the server. (A component is a named sub-part of an application. For example, Oracle WebCenter Collaboration uses components named Documents, Discussions, Tasks, Calendar, Search, UI, Infrastructure, and Miscellaneous. The portal uses over 100 different components.) The eight `<level>` sub-nodes correspond to the eight logging levels: Debug, Info, Warning, Error, Fatal, Action, Performance, and Function.

  Each `<level>` sub-node has two required attributes: `enabled` and `value`.

  - The `value` attribute is required defines the logging level (Debug, Info, Warning, Error, Fatal, Action, Performance, or Function). As noted above, a <component> node must have eight <level> sub-nodes, one for each logging level.
  - The `enabled` attribute sets whether a specific logging level is enabled. Its value must be set to either true or false. If a logging level is disabled (`enabled="false"`), messages in that category will not be sent to the receiver.
- The `<component-defaults>` sub-node (optional) has eight `<level>` sub-nodes that follow the syntax described above. The values of the `<level>` sub-nodes in the `<component-defaults>` sub-node apply to all components of the application other than the ones explicitly defined in a `<component>` node.

If you do not see any messages from your sender in the logging file, see the instructions in Section B.6, "Logging FAQ."

B.4.2 Starting Logger

In Windows, Logger is a service. Start and stop the service by clicking **Start**, **Programs**, **Oracle**, **WebCenter Logging Utilities**, then **Logger Start** or **Logger Stop**.

In UNIX and Linux, Logger is a daemon. Start and stop the daemon using the shell script *install_dir*/ptlogging/10.3.3/bin/ptLogger.sh. To start the daemon, use the command: `ptLogger.sh start`. To stop the daemon, use the command: `ptLogger.sh stop`.

B.5 Console Logger

Console Logger is similar to Logger, except that it runs in a console window. Console Logger uses the Log4J console appender to display logging messages in a console window. Console Logger has limited use; in most cases, it is preferable to use Logging Spy.

Console Logger uses an XML configuration file called consolelogger.xml. The format for consolelogger.xml is identical to that of ptLogger.xml (see Section B.4.1, "Configuring Logger (ptLogger.xml)"). Console Logger ships with one `<appender>` node in consolelogger.xml:

```
<appender class="org.apache.log4j.ConsoleAppender" name="Console">
<layout class="com.plumtree.openlog.log4jbridge.MyPatternLayout" />
</appender>
```

This node uses the Log4J Console Appender which, as the name implies, sends log messages to the console. It is possible to add additional <appender> nodes to consolelogger.xml as with ptLogger.xml, but this approach is uncommon.

B.5.1 Starting Console Logger

To run Console Logger in Windows, execute *install_dir*\ptlogging\10.3.3\bin\consoleLogger.bat.

To run Console Logger in UNIX, execute *install_dir*/ptlogging/10.3.3/bin/consoleLogger.sh.

B.6 Logging FAQ

The following troubleshooting information provides solutions for common problems with logging configuration.

B.6.1 Logging Spy

Q: The application I need does not appear in the list of senders in the Add Message Sender dialog box.

A: First, ensure that the message sender is running. Then check the following:

- If the message sender is running on a different computer, confirm that the sender is configured to allow remote spying. The message sender will have a logging configuration setting named restrictToLocalHost, or something similar. The value of this setting must be set to False to allow remote spying. For details, see the documentation for the message sender.

- If the message sender is running on a computer on a different subnet, confirm that the network routers are configured to allow UDP multicast traffic between the message sender computer and the Logging Spy computer.
- If the message sender or Logging Spy runs on a Microsoft Windows computer, the problem might be due to a known issue on some versions of the Windows operating system. The problem shows up when a Microsoft Windows computer has more than one network adapter installed. This is common if the Microsoft Windows computer has VM Ware installed. There are several workarounds:
  - Install an appropriate hotfix or service pack for the Microsoft Windows operating system. See the Microsoft support page for this issue at `http://support.microsoft.com/?kbid=827536`.
  - Alternatively, you can remove the additional network adapters. Disable the VMWare adapters. (Go to Control Panel | Network and Dial-Up Connections, right-click on each connection and disabling it.) Get the properties for your Local Area Connection and disable the VMWare Network Bridge.

Q: Where are the messages from my sender? Logging Spy does not display messages from my application.

A: First, go through troubleshooting steps above. In Logging Spy, check the filter settings for the message sender. By default, only Error, Warning, Fatal, and Action are enabled. It is possible that the log message sender is not sending any messages at those logging levels. Try enabling Debug and see if you receive any messages.

Q: How do I increase the amount of memory allotted to Logging Spy?

A: Logging Spy will collect and display log messages until it detects that it is running low on memory. At this point it will refuse to accept messages and will display an alert. This is true both when Spy is displaying messages that are streaming in, and when Spy is displaying messages from a .spy log file. To increase the amount of memory available to Logging Spy, follow the steps below.

Windows:

1. Edit the ptspy.lap file located in *install_dir*/ptlogging/10.3.3/bin.
2. Locate the following line: `-Xmx256m`

   The number in this line defines the maximum megabytes of memory available to Logging Spy (256 by default as shown above).
3. Set this number to the desired level. As a first step we recommend doubling the number to 512 (**`-Xmx512m`**).
4. Save the file and restart Logging Spy.

UNIX:

1. Edit the ptspy.sh file located in *install_dir*/ptlogging/10.3.3/bin.
2. Locate the following line: `JAVA_MEM_OPTS="-Xms32m -Xmx256m"`

   The second number indicates the maximum megabytes of memory available to Logging Spy (256 by default as shown above).
3. Set this number to the desired level. As a first step we recommend doubling the number to 512 (**`JAVA_MEM_OPTS="-Xms32m -Xmx512m"`**).
4. Save the file and restart Logging Spy.

B.6.2 Logger

Q: Where are the messages from my sender? Logger is not recording messages from my message application.

A: First, go through troubleshooting steps under the first question above. If you are not receiving any messages in a log file from a given message sender, ensure that the Logger Service/Daemon is running. Check the Logger internal diagnostic file at *install_dir*/ptlogging/logs/ptlogger.out. You should see messages of the form `"Starting the Logger service...", "--> Wrapper Started as Service","OpenLog: verbosity level = 2", "Logger: Successfully read configuration file at: C:\Program Files\Oracle\Middleware\wci\ptlogging\10.3.3\bin\..\..\..\settings\ptlogging\ptLogger.xml"`.

Check the Logger configuration file: *install_dir*/settings/ptlogging/ptLogger.xml. Ensure that there are appropriate `<filters>` and `<appender>` nodes in the configuration file for the message sender from which you are trying to receive messages. For more information, see Section B.4, "Logger."

C

Using the Counter Monitoring System

This chapter describes how to use the Counter Monitoring System to view real time statistical data on your portal, reported by various performance counters.

It includes the following sections:

- Section C.1, "About Counter Monitoring"
- Section C.2, "Key Performance Counters"
- Section C.3, "Using Windows Perfmon to View Counter Data"

C.1 About Counter Monitoring

The Counter Monitoring System collects information from various performance counters for portal applications and exposes them for diagnosis and review. This system can be used to examine counters from any Oracle WebCenter application that resides on a remote host, provided the two computers are on a network in which they can reach each other through UDP.

With the Counter Monitoring System you can:

- Set up counter logging files in your desired format to view counter information.
- Use the Counter Monitoring console to request specific counter data in real time.
- If you use a Windows system, use the Windows Perfmon utility to view portal counter data.

C.2 Key Performance Counters

The Counter Monitoring System collects information from various performance counters for portal applications and exposes them for diagnosis and review. This system can be used to examine counters from any Oracle WebCenter application that resides on a remote host, provided the two computers are on a network in which they can reach each other through UDP.

The following table lists the key counters provided with the portal. Each category of performance has one or more instances. Each instance in a category can be monitored with the counters for that category.

Category	Instances	Counters
Cache Many UI objects and pages have their own individual cache systems. Cache counters track each individual cache.	CommunityInfoCache - The cache for a PT Community GuestLoginInfoCache - The cache for a Guest Login HTTP_CACHE - The cache for HTTP requests, for remote portlets or Web services PreferenceCache - The cache for any preference page SubportalInfoCache - The cache for any experience definition	Size - The number of items currently in the cache MaxSize - The maximum number of items in the cache before it gets flushed NumSearches - Increments every time the cache is accessed NumHits - Increments every time a cache is accessed and cached contents are found NumInserts - Increments every time a cache is accessed and no cached contents are found
Opendb_SQLstats Database statistics for OpenDB	SQLSelectStats - SQL queries that are "SELECT" statements	NumOperations - The number of SQL operations that occurred
OpenHTTPLowLevelNetwork Counter Basic HTTP information, including usage, connections, transactions	Total - There is one instance per remote host. Total aggregates all of the statistics.	BytesReceived - Number of bytes received from the remote host BytesSent - Number of bytes sent to the remote host OpenConnections - The number of open connections to remote hosts
OpenHTTPHttpLevelstatistics HTTP requests statistics	Total - There is one instance per remote host. Total aggregates all of the statistics.	RequestsActive - The number of HTTP requests that are active RequestsProcessed - The number of HTTP requests that have been processed
portalpages Statistics related to portal pages	NA - Single instance	CommunityPages - How many times a community page was hit LoginsFailure - How many times a user login attempt failed LoginsSuccessful - How many times users logged in MyPages - How many times a My Page was hit TotalHits - How many times any portal page was hit TotalOpensessions - How many open sessions there are currently

C.3 Using Windows Perfmon to View Counter Data

The Counter Monitoring System integrates with the Windows Perfmon application. Once you start the portal, the Perfmon adaptor will add Oracle WebCenter counters to the list of possible counters to monitor. You can then start Perfmon (or any other

monitoring application that works with Windows Performance Counters) and see Oracle WebCenter counters in the list of available counters.

1. Click **Start** > **Run**.
2. Type perfmon.exe and click **OK**.

> **Note:** In Perfmon, the category name is prefixed by the context name. The context name is set in the `context` element in the configuration.xml file (in *install_dir*\settings).

The Perfmon adaptor adds a few percentage points of overhead to overall system performance, so you might want to disable it after viewing the counter data. In *install_dir*\settings\configuration.xml, set `opencounters:perfmon-enabled` to `false`.

D

Localizing Your Portal

This chapter describes how you can internationalize and localize your portal.

It includes the following sections:

- Section D.1, "Localizing Object Names and Descriptions"
- Section D.2, "Localization Manager XML"
- Section D.3, "About the Locale Map"
- Section D.4, "About Search Service Internationalization Support"

D.1 Localizing Object Names and Descriptions

You can localize object names and descriptions, so that users see the names and descriptions in their chosen language. For example, if you have an object called “Engineering,” you could add “Ingénierie” as the localized entry for French. A user viewing the French user interface would see the Ingénierie as the object name, as well as any other names and descriptions localized into French.

There are two ways to localize object names and descriptions: in the object's editor or using the Localization Manager.

- To localize the name and description for a single object, use the object's editor.

  See Section D.1.1, "Localizing the Name and Description for an Object."

- To localize all object names and descriptions, use the Localization Manager.

  See Section D.1.2, "Localizing All Object Names and Descriptions."

D.1.1 Localizing the Name and Description for an Object

You can localize object names and descriptions, so that users see the names and descriptions in their chosen language. For example, if you have an object called “Engineering,” you could add “Ingénierie” as the localized entry for French. A user viewing the French user interface would see the Ingénierie as the object name, as well as any other names and descriptions localized into French.

Note:

- You can localize names and descriptions into only the languages supported by the portal.
- You cannot localize names and descriptions for users.
- You can localize the names and descriptions for all objects at the same time using the Localization Manager.

1. Open the object's editor by creating a new object or editing an existing object.
2. Select **Supports Localized Names**.

   The **Localized Names and Descriptions** section appears.
3. Add or edit the localized names and descriptions:
   - To add an entry for a language, click **New Localized Name**, then, in the Name and Description dialog box, enter the localized name and/or description, select the appropriate language, and click **Finish**.
   - To edit an existing entry, click the entry you want to change, then, in the Name and Description dialog box, edit the entry as necessary, and click **Finish**.
   - To remove existing entries, select the entries you want to remove and click the Remove icon.

     To select or clear all entries, select or clear the check box to the left of **Name**.

D.1.2 Localizing All Object Names and Descriptions

You can localize object names and descriptions, so that users see the names and descriptions in their chosen language. For example, if you have an object called "Engineering," you could add "Ingénierie" as the localized entry for French. A user viewing the French user interface would see the Ingénierie as the object name, as well as any other names and descriptions localized into French.

To access the Localization Manager you must be a member of the Administrators Group.

Although you can supply localized names and descriptions on an object-by-object basis through the object editor, you might find it more efficient to edit all objects at the same time through the Localization Manager. The Localization Manager enables you to download an .xml file that includes the names and descriptions for all objects that support localized names. You can then edit the .xml file and upload it back into the portal.

Note:

- You must configure each object to allow localization before downloading the .xml file.
- You can localize names and descriptions into only the languages supported by the portal.
- You cannot localize names and descriptions for users.
- You can localize each object individually using the object's editor.

1. Click **Administration**.
2. In the Select Utility list, click **Localization Manager**.
3. Export the names and descriptions for all portal objects that support localization by clicking **Download**, and saving the XML file to your computer.
4. Open the file with a text editor, add or edit localized values for the objects, and save your changes.

   For example, to edit the French term for Everyone, you might

   ```
   make the following change:
   <target language="fr">Tous</target>
   ```

5. Return to the Localization Manager, and click **Browse**.
6. Navigate to the exported file and click **Open**.
7. Upload and apply your changes to the portal by clicking **Upload**.

D.2 Localization Manager XML

Each localized object is represented by an entry in the Localization Manager XML file.

```
<segment classid="2" itemid="51" stringid="0">
  <source language="en">Everyone</source>
  <target language="de" />
  <target language="en" />
  <target language="es" />
  <target language="fr" />
  <target language="it" />
  <target language="ja" />
  <target language="ko" />
  <target language="pt" />
  <target language="zh" />
  </segment>
```

The first line displays information about the object entry:

- The classid represents the object type (in this example, a group).
- The itemid represents the object ID in the portal database.
- The stringid is “0” for the object name and “1” for the object description.

The second line displays the primary language term (in this example, the primary language is English and the term is Everyone).

The remaining lines display the available languages.

Value	Language
de	German
en	English
es	Spanish
fr	French
it	Italian
ja	Japanese
ko	Korean

Value	Language
nl	Dutch
pt	Portuguese
zh	Simplified Chinese
zh-tw	Traditional Chinese

D.3 About the Locale Map

A Locale Map allows you to create custom mappings for locales supported by Oracle WebCenter Interaction. For example, since Traditional Chinese is used in Hong Kong, you might want to map the Hong Kong locale to the Traditional Chinese locale so that if users select Hong Kong as their locale in the portal or their browser, the portal displays Traditional Chinese.

The Locale Map is stored in the i18n folder of the installation directory (for example, *install_dir*\10.3.3\i18n\LocaleMap.xml).

To create the mapping from the Hong Kong locale to the Traditional Chinese locale, you add the following mapping to the LocaleMap.xml file:

```
<Mapping>
  <from>zh-hk</from>
  <to>zh-tw</to>
</Mapping>
```

D.4 About Search Service Internationalization Support

The portal provides support for 61 languages. The portal uses Unicode characters to store and retrieve text, and the system has access to linguistic rules for multiple languages during full-text indexing. This makes it possible to have documents of different languages within the same search collection, with significantly improved results. The user interface handles text using the UTF-8 encoding, so search results are always displayed correctly, if the appropriate fonts are available to the Web browser.

Some languages supported by the portal include support for word stemming and compound decomposition. This additional information is used to enhance results of the full-text index. For a list of supported languages, including which have enhanced support, see Chapter D, "Localizing Your Portal."

D.4.1 Crawling International Document Repositories

Web and file content crawlers are associated with a specific language. All documents processed by a content crawler are indexed using the linguistic rules appropriate for the specified language. For optimal results, create a separate content crawler to handle documents of different languages. For most European languages, mixing languages within a single crawl will not render the content unsearchable; however, word stemming and decomposition information stored in the documents will be missing for languages other than the content crawler's designated language. Avoid indexing Asian language documents with a content crawler configured for a European language, as special tokenization rules are required for processing the Asian languages.

D.4.2 Submitting International Documents to the Knowledge Directory

When you use the Submit Document utility to add documents to the Knowledge Directory, you specify the document language by choosing from a pop-up list of the

supported languages. As with content crawlers, this language should be set to the actual language of the document for optimal results. Correct specification of language is particularly crucial for proper indexing of Asian language content.

E

Deploying Single Sign-On

This appendix describes how to deploy Single Sign-On (SSO) capabilities in the portal environment.

It includes the following sections:

- Section E.1, "About SSO"
- Section E.2, "Configuring an SS0 Authentication Provider for Use with the Portal"
- Section E.3, "Configuring the Portal for SSO"
- Section E.4, "Common SSO Questions"

E.1 About SSO

SSO is an authentication system that permits users to access multiple servers in a domain through a single point of entry. When SSO is deployed in the portal, user sessions are authenticated transparently by an SSO service against authentication sources commonly deployed in the enterprise, such as LDAP or Microsoft Active Directory.

To deploy SSO in your portal, configure the following resources so that they can share user and domain authentication information:

1. SSO Authentication Server. See Section E.2, "Configuring an SS0 Authentication Provider for Use with the Portal."
2. Remote server. See Section 3.3.1, "Creating or Editing a Remote Server."
3. Authentication web service. See Section 6.8.1, "Creating or Editing an Authentication Web Service."
4. Authentication source. See Section 6.9.4, "Creating a Single Sign-On Authentication Source."
5. Portal. See Section E.3, "Configuring the Portal for SSO."

E.2 Configuring an SS0 Authentication Provider for Use with the Portal

This section describes how to configure authentication servers to protect the portal. The following topics provide configuration details for supported and unsupported servers:

- Section E.2.1, "Configuring Oracle Single Sign-On,"
- Section E.2.2, "Configuring the Windows Integrated Authentication Service"
- Section E.2.3, "Configuring Netegrity SiteMinder"

- Section E.2.4, "Configuring an Oblix Authentication Provider"
- Section E.2.5, "Integrating With Other Authentication Providers"

Caution: You configure the SSO authentication server to protect the portal. You do not need to configure the SSO server to protect the Image Service. If you do, communication between the portal and Image Service can result in errors. The Image Service contains only static public content that ships with every portal installation. No data specific to users or to your organization is ever stored on the Image Service.

E.2.1 Configuring Oracle Single Sign-On

Follow these steps to configure Oracle Single Sign-On for your SSO deployment:

1. Install the following software as described in the associated documentation:
   - Oracle Internet Directory or Oracle Virtual Directory (or any other LDAP server supported by Oracle WebCenter Interaction)
   - Oracle Http Server (OHS)
   - Apache Tomcat
   - Oracle WebCenter Interaction
   - Oracle WebCenter Identity Service for LDAP
   - Oracle Single Sign-On
2. Enable proxy support in Oracle HTTP Server:
   a. In a text editor, open httpd.conf. By default, this file is located in *OHS_install_dir*\ohs\conf.
   b. Add the following lines:

```
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_connect_module modules/mod_proxy_connect.so
LoadModule proxy_http_module modules/mod_proxy_http.so
```

   c. At the end of the configuration file, add the following parameter (this will forward all requests to OHS to the application server hosting the portal):

```
ProxyPass /portal/ http://portal_host_name:port/portal/
ProxyPassReverse /portal/  http://portal_host_name:port/portal/
```

   d. Save the file.
   e. Restart the Oracle HTTP Server.
3. Edit the URL mappings in portalconfig.xml, so that Oracle WebCenter Interaction creates links using the FQDN and port number of the Oracle HTTP Server:
   a. In a text editor, open portalconfig.xml. By default, this file is located in File is usually located in the following directory: *portal_install_dir*\settings\portal.
   b. In the `URL Mappings` section, edit the `default` to look like the following (this assumes a security mode 0 for Oracle WebCenter Interaction):

```
<setting name="URLFromRequest0">
  <value xsi:type="xsd:string">*</value>
</setting>
```

```
<setting name="ApplicationURL0">
  <value xsi:type="xsd:string">http://ohs_host_fqdn:ohs_
port/portal/server.pt</value>
</setting>
<setting name="SecureApplicationURL0">
  <value xsi:type="xsd:string">https://ohs_host_fqdn:ohs_
port/portal/server.pt</value>
</setting>

<clients>
  <client name="portal"/>
</clients>
```

c. Save the file.

d. Restart the Tomcat instance hosting Oracle WebCenter Interaction for the changes to take effect.

Note: You might also need to update the `AdminSiteBaseURL` value in the configuration.xml file (located in *portal_install_dir*/settings) to point to the FQDN of the OHS host.

---

4. Create an authentication source, connecting to the same LDAP server used by the Oracle Single Sign-On:

   a. Perform the steps described in Section 6.9.4, "Creating a Single Sign-On Authentication Source," selecting the LDAP authentication Web service, specifying connection information for the LDAP server used by Oracle Single Sign-On.

   b. Run the authentication source job to synchronize the users and groups.

   c. Confirm that one of the synchronized users can log in to the portal.

5. Configure settings in portalconfig.xml to enable SSO, specifying information about headers and cookies being generated by the Oracle Single Sign-On policies you configured:

   a. In a text editor, open portalconfig.xml. By default, this file is located in File is usually located in the following directory: *portal_install_dir*\settings\portal.

   b. Set the `DefaultAuthSourcePrefix` value to the Authentication Source Category you specified when you created the authentication source.

   c. Configure the following settings:

```
<setting name="SSOVendor">
  <value xsi:type="xsd:integer">6</value>
</setting>
<setting name="AllowDefaultLoginPageAuthSource">
  <value xsi:type="xsd:integer">2</value>
</setting>
<setting name="DefaultAuthSourcePrefix">
  <value xsi:type="xsd:string">Authentication_Source_Category</value>
</setting>
<setting name="CookiePath">
  <value xsi:type="xsd:string">/</value>
</setting>
<setting name="CookieDomain">
  <value xsi:type="xsd:string">.my.company.com</value>
</setting>
```

```
<setting name="SSOCookieIsSecure">
  <value xsi:type="xsd:integer">0</value>
</setting>
```

d. Uncomment the configuration block located underneath the `portal:SSOVendor` component, and configure to look like the following:

```
<component name="portal:SSOVendor"
type="http://www.plumtree.com/config/component/types/portal/ssovendor">

  <setting name="NameHeader">
    <value xsi:type="xsd:string">uid</value>
  </setting>
  <setting name="PrefixHeader">
    <value xsi:type="xsd:string"/>
  </setting>
  <setting name="PasswordHeader">
    <value xsi:type="xsd:string"/>
  </setting>
  <setting name="Cookie">
    <value xsi:type="xsd:string"/>
  </setting>
  <setting name="SecureHeader">
    <value xsi:type="xsd:string"/>
  </setting>
  <setting name="LogoutURL">
    <value xsi:type="xsd:string">Partner_Single_Sign-Off_URL?p_done_
url=Landing_URL</value>
  </setting>

  <clients>
    <client name="portal"/>
  </clients>
</component>
```

Note:

- The `NameHeader` value will be used in the Oracle Single Sign-On policy configuration, and should correspond to the User Name Attribute specified during the creation of the authentication source. You can instead have Oracle WebCenter Interaction try to get the name of the authenticated user from a server variable by changing the `UseRemoteUser` value to `1`. For example:

```
<component name="portal:SSOVendor"
type="http://www.plumtree.com/config/component/types/portal/sso
vendor">

  <setting name="UseRemoteUser">
    <value xsi:type="xsd:integer">1</value>
  </setting>

</component>
```

- Replace *`Partner_Single_Sign-Off_URL`* with the sign-off URL shown in the Partner Application Setting of Oracle WebCenter Interaction in Oracle Single Sign-On.
- Replace *`Landing_URL`* with the URL of the page on which you want the user to land after Oracle Single Sign-On sign off. This value is usually the same as Apache reverse proxy Oracle Single Sign-On login URL for Oracle WebCenter Interaction.

e. Save the file.

f. Restart the Tomcat instance hosting Oracle WebCenter Interaction for the changes to take effect.

6. Create a new partner application in Oracle Single Sign-On for Oracle WebCenter Interaction:

a. Navigate to the Oracle Single Sign-On administrative user interface.

b. Click **Login** and log in as orcladmin with the password you created when you installed Oracle Single Sign-On.

c. Click **Single Sign-On Server Administration**.

d. Click **Administer Partner Applications**.

e. Click **Add Partner Application**.

f. Type a name for the partner application.

g. In the **Home URL** box, type `http://`*`portal_url`*.

h. In the **Success URL** box, type `http://`*`portal_url`*`/osso_login_success`.

i. In the **Logout URL** box, type `http://`*`portal_url`*`/osso_logout_success`.

j. Leave **end date** blank.

k. Click **OK**.

7. Create an osso.conf file:

a. Click the pencil icon next to the partner application you created.

b. Create a text file with the following text, replacing the variables with the settings from the Oracle Single Sign-On user interface:

```
sso_server_version=v1.4
cipher_key=Encryption_Key
site_id=Site_ID
site_token=Site_Token
login_url=Single_Sign-On_URL
logout_url=Single_Sign-Off_URL
cancel_url=http://portal_url
```

Note: The cancel_url should point to where you want the user to end up if they click **Cancel** instead of logging in.

c. Save this file to: \ohs\conf\osso\osso.conf.txt.

d. Open a command prompt and cd to the folder.

e. Run the following command: `..\..\bin\apobfuscate.exe osso.conf.txt osso.conf`

Running the command generates an obfuscated copy of the config file used by mod_osso. In a production deployment, delete osso.conf.txt to avoid storing the cipher key in clear text.

8. Configure OHS:

a. Open \ohs\conf\httpd.conf in a text editor.

b. Confirm that the following line exists and is not commented out:

```
Include the mod_osso configuration file
include "OHS_install_dir\ohs\conf\mod_osso.conf"
```

c. Comment out the default auth modules:

```
#LoadModule auth_module modules/mod_auth.so
#LoadModule auth_anon_module modules/mod_auth_anon.so
#LoadModule auth_dbm_module modules/mod_auth_dbm.so
```

d. Save the file.

e. Open mod_osso.conf in a text editor.

f. Add the following lines:

```
LoadModule osso_module modules/mod_osso.so

<IfModule mod_osso.c>
  OssoConfigFile conf/osso/osso.ensemble.conf
  OssoIpCheck off
  OssoIdleTimeout off
  <Location /authenticateWithApplicationServer>
      require valid-user
      AuthType Basic
  </Location>
</IfModule>
```

g. Save the file.

h. Restart OHS.

E.2.2 Configuring the Windows Integrated Authentication Service

Follow these steps to configure the Windows Integrated Authentication (WIA) service (formerly known as Windows NT LAN Manager (NTLM)) for your SSO deployment:

1. Open the IIS Internet Service Manager.
2. In the left pane, expand the Web server folder and then its portal virtual directory subfolder; right-click the sso folder and choose **Properties**.
3. Click the **Directory Security** tab.
4. In the Anonymous access and authentication control group, click the **Edit** button.
5. In the Authenticated Access group, select the **Integrated Windows Authentications** box. Leave the remaining boxes unselected.
6. Click **OK** to accept changes to Directory Security settings.
7. Click **OK** to accept changes to Properties.

Note: In the portal environment where SSO via WIA is deployed, Internet Explorer users are not prompted for a user name and password when they attempt to log into the portal Web site if the following provisions have been made by the client

---

- The user must be logged into a Windows NT domain as a user that has rights to access the portal.
- An HTTP proxy must not reside between the client computer and the portal Web site.
- Internet Explorer must be configured to recognize the portal Web site as a local intranet site. If the site is not in the local intranet zone by default, add it from the browser. From the Tools menu, choose **Security**, then **Local Intranet**. Click **Sites**. Click **Advanced**. Add the address for the portal Web site.

Note:

- Netscape Navigator versions prior to 7.1 are not supported. For Netscape Navigator 7.1 (and later), users are prompted for user name and password when they attempt to log in to the portal Web site.
- In the portal environment where SSO via WIA is deployed, the portal does not pass user passwords as Basic Authentication Headers to remote servers.

E.2.3 Configuring Netegrity SiteMinder

Follow these basic steps to configure Netegrity SiteMinder Policy Server for use with the portal:

1. Configure the Netegrity SiteMinder Policy Server. See Section E.2.3.1, "Configuring Netegrity SiteMinder Policy Server."
2. Configure Netegrity SiteMinder Web Agent. See the section that applies to the version of SiteMinder you run:

- Section E.2.3.2, "Configuring Netegrity SiteMinder Web Agent 4.6 or 5.5"
- Section E.2.3.3, "Configuring Netegrity SiteMinder Web Agent 5.5 SP3 or 6.0 on Windows"
- Section E.2.3.4, "Configuring Netegrity SiteMinder Web Agent 5.5 SP3 or 6.0 on UNIX or Linux"

E.2.3.1 Configuring Netegrity SiteMinder Policy Server

To configure SiteMinder Policy Server for your deployment:

1. Install the server as described in Netegrity documentation.
2. Open the SiteMinder administrative tool and log in as a user that can create objects.
3. (For 5.5, 5.5 SP3, or 6.0.2.5) Create a host conf object:
   a. In the left pane, click **Host Conf Object**.
   b. In the right pane, right-click the **Default Host Configuration Object** and choose **Duplicate Configuration Object**.
   c. In the **Name** box, type a host name, such as `policyserver`.
   d. In the Configuration Values group, double-click the **policyserver** object and use the controls to set the IP address for the policy server address and the three ports, typically 44441, 44442, 44443. For example, type `10.1.140.124,44441,44442,44443`.
   e. Click **Apply** and then **OK**.
4. Create an agent:
   a. In the left pane, right-click **Agents** and choose **Create Agent**.
   b. In the **Name** box, type the name of the portal.
   c. (For 4.6 only) In the address box, type the IP address of the portal or use SiteMinder controls to perform DNS lookup.
   d. (For 4.6 only) In the shared secret box, type a string that matches one to be set on the Web Agent host.
   e. Click **Apply** and then **OK**.
5. (For 5.5, 5.5 SP3, or 6.0.2.5) Create an Agent Conf Object:
   a. In the left pane, click **Agent Conf Objects**.
   b. In the right pane, right-click the type of server that approximates the default settings (for example, IISDefaultSettings or ApacheDefaultSettings) and choose **Duplicate Configuration Object**.
   c. In the **Name** box, type a descriptive name for the object, typically the host name followed by the configuration object name, for example `PortalServerIISDefaultSettings` or `PortalServerApacheDefaultSettings`.
   d. In the Configuration Values group, double-click **DefaultAgentName**; uncomment the parameter (remove the leading #) and specify as its value the name of the agent you created.
   e. (For 5.5 SP3 or 6.0.2.5) In the Configuration Values group, double-click **BadURLChars** and modify its value to the following: `//,./,/.,/*,*.,~,\`

f. (For 5.5 SP3 or 6.0.2.5) In the Configuration Values group, configure **LogAppend**, **LogConsole**, **LogFileName**, **LogLevel**, and **Logfile** to your preferences. For details, refer to the online help.

g. Click **Apply** and then **OK**.

6. Create a user directory:

   a. In the left pane, right-click **User Directories** and choose **Create User Directory**.

   b. In the **Name** box, type a descriptive name for the object, for example `Iplanet`.

   c. In the **NameSpace** box, choose the appropriate namespace, for example:

      WinNT. If you choose WinNT, specify the Windows NT domain name in the **Windows Domain** text box.

      LDAP. If you choose LDAP, specify the IP address and port number for the server that hosts the LDAP user directory and use the LDAP Search and LDAP User DN Lookup group controls to configure search and lookup according to the conventions and examples described in the context-sensitive online help for the Netegrity administration tool.

   d. Click **Apply**.

   e. To display user groups that have been imported into the Policy Server, click **View Contents**.

   f. To verify that users have been imported, click **Search** and query LDAP for specific users.

   g. Click **Apply** and then **OK**.

7. Create a policy domain:

   a. In the left pane, right-click **Policy Domain** and choose **Create Policy Domain**.

   b. In the **name** box, type a descriptive name for the domain, for example `Portal`.

   c. In the **add directory** box, specify the User Directory you created.

   d. Click **Apply** and then **OK**.

8. Create a realm:

   a. In the left pane, click the **Domains** tab.

   b. Right-click the domain created above and choose **Create Realm**.

   c. In the **name** box, type a descriptive name for the realm, for example `SSO`.

   d. In the Resource group, from the Agent drop-down list box, select the agent you created.

   e. In the **Resource Filter** box, type `/portal/sso` for 4.6 or 5.5 or type `/portal/SSOServlet` for 5.5 SP3 or 6.0.2.5, which is the directory the portal uses to authenticate against SSO services.

   f. In the Authentication Scheme box, choose **Basic Authentication**.

   g. Click **Apply** and then **OK**.

9. Create a rule for the realm:

a. In the left pane, expand the policy domain tree so it displays named realms; right-click the realm you created and choose **Create Rule under Realm**.

b. In the **name** box, type a descriptive name for the rule, for example `Allow Access`.

c. In the Realm and Resource group, choose the realm created above; in the resource box, specify `/*`.

d. In the Allow/Deny and Enable/Disable group, enable the rule and set it to **Allow Access** when the rule fires.

e. In the Action box, click **Web Agent Actions** and then **GET**, **POST**, and **PUT**.

f. Click **Apply** and then **OK**

10. Create a policy for the realm:

a. Under the domain created above, right-click **Policies** and choose **Create Policy**.

b. In the **Name** box, type a descriptive name for the Policy, for example `Normal Case`.

c. Click the **Users** tab and use the controls to add users or groups for whom this policy applies.

d. Click the **Rules** tab and use the **Add/Remove Rules** button to add the rule you created above.

e. Click **Apply** and then **OK**.

E.2.3.2 Configuring Netegrity SiteMinder Web Agent 4.6 or 5.5

To configure SiteMinder Web Agent 4.6 or 5.5 for your deployment:

1. Install the Web Agent setup program on the same host as the portal.
2. When setup is complete, you are prompted to complete the Web Agent Configuration Wizard. If you choose to run the wizard at a different time, from the **Start** menu, choose **Programs**, then **SiteMinder**, then **Web Agent Configuration Wizard** to open the wizard.
3. When the wizard prompts for components to configure, choose **IIS**.
4. Click **Configure**.
5. In the **Policy Server** box, type the name of the Policy Server you set up.
6. In the **Agent name** box, type the name of the agent you created.
7. In the **Cookie domain** box, type the fully qualified domain name for which you want the authentication cookie to be forwarded. For example, if you specify `.company.com`, the cookie enables access to all domains that end in company.com.
8. In the **IIS Proxy User Name and Password** box, type a user name and password to run the SiteMinder ISAPI filter on IIS. This user must have administrator rights on the IIS host.
9. In the **Shared Secret** box, type a string that exactly matches the name of the Agent object you created on the Policy Server.
10. Open the IIS Web Management Console. From the **Start** menu, choose **Programs**, then **SiteMinder**, then **IIS**, then **WebManagement Console**.
11. Click the **Settings** tab, and select **Enable Web Agent** and **Enable Policies**.

12. Click the **Single Sign On** tab. Select **Require Cookies** and clear the other two boxes. Set the **Cookie Domain** to the fully qualified domain name for which you want the cookie to be forwarded. For example if you specify `.company.com`, the cookie enables access to all domains that end in company.com.
13. Restart IIS to apply the modified settings.

E.2.3.3 Configuring Netegrity SiteMinder Web Agent 5.5 SP3 or 6.0 on Windows

To configure SiteMinder Web Agent 5.5 SP3 or 6.0 on Windows for your deployment:

1. Install the Web Agent setup program on the same host as the portal.
2. When setup is complete, you are prompted to complete the Web Agent Configuration Wizard. If you choose to run the wizard at a different time, from the **Start** menu, choose **Programs**, then **SiteMinder**, then **Web Agent Configuration Wizard** to open the wizard.
3. When prompted, specify the settings you configured in the previous section for the following objects: Policy Server IP Address and Host Configuration Object name.
4. In the *siteminder_webagent_install_location*\IIS\bin\WebAgent.conf file, set the `EnableWebAgent` parameter to `yes`.

E.2.3.4 Configuring Netegrity SiteMinder Web Agent 5.5 SP3 or 6.0 on UNIX or Linux

To configure SiteMinder Web Agent 5.5 SP3 or 6.0 on UNIX or Linux for your deployment:

1. If you have not done so already, on the host computer for the portal, install Apache HTTPd.
2. On the portal host computer, install:

   Either these components:

   - SiteMinder Web Agent 5.5
   - SiteMinder Web Agent 5.5 Quarterly Maintenance Release (QMR) 6
   - SiteMinder Web Agent 5.5 QMR 6 CR007

   Or these components:

   - SiteMinder Web Agent 6.0
   - SiteMinder Web Agent 6.0 Quarterly Maintenance Release (QMR) 2
   - SiteMinder Web Agent 6.0 QMR 2 CR005

   For details on installing Netegrity SiteMinder components, refer to the Netegrity Customer Care Web site and Netegrity SiteMinder documentation.

   For an example of installing the SiteMinder Web Agent, Web Agent QMR, and hotfix, see Knowledge Base article DA_236222, "Netegrity Siteminder 5.5 Web Agent Installation Tips."
3. Invoke the SiteMinder configuration utility, for example, from the command-line, enter: `./nete-wa-config`.
4. When prompted, enter your preferences but be sure to specify the settings you configured in the previous section for the following objects: Policy Server IP Address and Host Configuration Object name.

5. When prompted, enter the location for the Apache Web server root directory, for example, `/opt/httpd/`.
6. Source the Netegrity environment script. From the command-line, enter: `source /opt/netegrity/siteminder/webagent/nete_wa_env.sh`.
7. Modify the Apache Web server httpd.conf configuration file to enable the SiteMinder Web Agent. The lines in the following excerpt show an httpd.conf file that enables the SiteMinder Web Agent:

```
...
LoadModule sm_module /opt/netegrity/siteminder/webagent/lib/mod2_sm.so

...
# SSO Configuration
SmInitFile /opt/httpd/conf/WebAgent.conf
Alias /siteminderagent/pwcgi/ "/opt/netegrity/siteminder/webagent/pw"
<Directory "/opt/netegrity/siteminder/webagent/pw">
        Options Indexes MultiViews ExecCGI
        AllowOverride None
        Order allow,deny
        Allow from all
</Directory>

Alias /siteminderagent/pw/  "/opt/netegrity/siteminder/webagent/pw"
<Directory "/opt/netegrity/siteminder/webagent/pw">
        Options Indexes MultiViews ExecCGI
        AllowOverride None
        Order allow,deny
        Allow from all
</Directory>

Alias /siteminderagent/  "/opt/netegrity/siteminder/webagent/samples/
<Directory "/opt/netegrity/siteminder/webagent/samples/">
        Options Indexes MultiViews
        AllowOverride None
        Order allow,deny
        Allow from all
</Directory>

##SITEMINDER .exe ##
AddHandler cgi-script .exe

##SITEMINDER .fcc ##
AddHandler smformsauth-handler .fcc

##SITEMINDER .scc ##
AddHandler smadvancedauth-handler .scc

##SITEMINDER .ccc ##
AddHandler smcookieprovider-handler .ccc

...
```

   The lines that configure SiteMinder Web Agent must be *before* lines that include a Web application server configuration file, such as oracle.conf.
8. Modify the following settings in /opt/httpd/conf/WebAgent.conf:
   - Ensure: `enablewebagent="YES"`
   - Add: `ServerPath="/opt/httpd/conf/httpd.conf"`

9. Restart the Apache Web server.

E.2.4 Configuring an Oblix Authentication Provider

Follow these basic steps to configure the Oblix components for use with the portal:

1. Install and configure the Oblix suite 6.5, 7.0, or 7.0.4.
2. Configure Oblix Access Server for the portal. See the section that applies to the Web server you use:
   - Section E.2.4.1, "Configuring Oblix Access Server for a Portal Running on Tomcat"
   - Section E.2.4.2, "Configuring Oblix Access Server for a Portal Running on IIS"
3. Install and configure a corresponding Oblix Webgate for Apache. See Section E.2.4.3, "Configuring Oblix WebGate for Apache."
4. If necessary, configure Oblix WebGate to work with remote servers. See Section E.2.4.4, "Configuring Oblix WebGate to Work with Remote Servers."

E.2.4.1 Configuring Oblix Access Server for a Portal Running on Tomcat

Follow these basic steps to configure Oblix Access Server for use with a portal running on Tomcat:

1. Install Oblix suite 6.5, 7.0, or 7.0.4. Each Oblix suite includes the following components: COREid, WebPass, Access Server, and Access Manager.

   For information on installing Oblix products, refer to Oblix product documentation.
2. Open NetPoint Access Manager, typically http://oblix_access_server:port/access/oblix.
3. Create a policy domain:
   a. In the left pane, click **Create Policy Domain**.
   b. Type a descriptive name for the policy domain and click **Save**.
   c. Click **Modify**.
   d. Enable the policy domain and click **Save**.
4. Create an HTTP resource:
   a. Click the **Resources** tab and then click **Add**.
   b. In the Resource drop-down list, choose **HTTP**.
   c. In the URL-prefix drop-down list, choose the backslash (/) and type `portal`.
   d. Click **Save**.
5. Create a policy:
   a. Click the **Policies** tab and then click **Add**.
   b. In the **Name** box, type a descriptive name for the policy, for example `allow access`.
   c. In the Resource Type drop-down list, choose **HTTP**.
   d. In the Resource Operations group, click **GET** and **POST**.
   e. In the Resource group, select **all**.

f. In the **URL Pattern** field, enter `{SSOServlet[;!]*,SSOServlet/.../*,SSOServlet}`.

   URLS that contain the string "SSOServlet" and other variations of "SSOServlet" will be forced to authenticate. Without a URL pattern, Oblix issue an authentication prompt for all requests, however, this would prevent portal Guest functionality.

g. Leave the other fields blank and click **Save**.

6. Create an authorization rule for everyone. The Oblix server parses the rule to send the user name attribute to the portal, enabling the user to log in as a known user with user-defined roles, privileges, views, and so forth.

   a. Click the **Authorization Rules** tab, and then click **Add**.

   b. In the **name** box, type a descriptive name for the rule, for example `Allow Everyone`.

   c. Enable the rule and click **Save**.

   d. Click the **Allow Access** sub-tab and then click **Add** to display controls for adding users or groups to allow access to this resource.

   e. Add appropriate users and groups. Any user/group that needs access to the portal should be included here. Change the Role to **Anyone** and click **Save**.

   Note: The name of the user displayed here does not necessarily match the name you enter during Oblix login.

7. Create a default rule:

   a. Click **Default Rules** tab, then click **Add**.

   b. Click the **Authentication Rule** sub-tab, and enter a **Name** and **Description**.

   c. In the Authentication Scheme drop-down menu, select **NetPoint None Authentication**. This authentication scheme is created automatically by the Oblix installation.

   d. Click **Save**.

   e. Click the **Authorization Expression** sub-tab, and click **Add**.

   f. Click the **Expression** sub-sub-tab, and add the Allow Everyone Rule you created previously (or select the rule by the name you gave it). You must click **Add** so that the name appears in the Authorization Expression box.

   g. Click the **Actions** sub-sub-tab, then click **Add**.

   h. Under Authorization Success, fill in the last line of fields:

      For **Type**, enter a descriptive name such as `headerVar`.

      For **Name**, enter `UID`.

      For **Return Attribute**, enter the value of the UID header sent to portal. Typically, this value is `UID` if using LDAP or `samaccountname` if using Active Directory.

   i. Click **Save**.

8. Create an authorization rule for the policy you created:

   a. Click the **Policies** tab.

b. Click the name of the policy created above to select it.

c. Click the **Authentication Rule** sub-tab and add a method appropriate to your configuration, for example, Basic over LDAP.

> **Note:** Basic over LDAP is a rule created during Oblix installation. If it is not available, Oblix was not installed properly.

d. Click **Save**.

E.2.4.2 Configuring Oblix Access Server for a Portal Running on IIS

Follow these basic steps to configure Oblix Access Server for use with a portal running on IIS:

1. Install Oblix suite 6.5, 7.0, or 7.0.4. Each Oblix suite includes the following components: COREid, WebPass, Access Server, and Access Manager.

   For information on installing Oblix products, refer to Oblix product documentation.

2. Open NetPoint Access Manager, typically http://oblix_access_server:port/access/oblix.

3. Create a policy domain:

   a. In the left pane, click **Create Policy Domain**.

   b. Type a descriptive name for the policy domain and click **Save**.

   c. Click **Modify**.

   d. Enable the policy domain and click **Save**.

4. Create an HTTP resource:

   a. Click the **Resources** tab and then click **Add**.

   b. In the Resource drop-down list, choose **HTTP**.

   c. In the URL-prefix drop-down list, choose the backslash (/) and type the path to the SSO virtual directory in the adjacent text box, for example, `portal/sso` for typical Oracle WebCenter Interaction deployments.

   > **Note:** Do not enter the full path to the server.

   d. Click **Save**.

5. Create a policy:

   a. Click the **Policies** tab and then click **Add**.

   b. In the **Name** box, type a descriptive name for the policy, for example `allow access`.

   c. In the Resource Type drop-down list, choose **HTTP**.

   d. In the Resource Operations group, click **GET** and **POST**.

   e. In the Resource group, select the resource you created (in this example, /portal/sso).

   f. Leave the other fields blank and click **Save**.

6. Create an authorization rule. The Oblix server parses the rule to send the user name attribute to the portal, enabling the user to log in as a known user with user-defined roles, privileges, views, and so forth.
   a. Click the **Authorization Rules** tab, and then click **Add**.
   b. In the **name** box, type a descriptive name for the rule, for example `Forward User Name`.
   c. Enable the rule and click **Save**.
   d. Click **Actions**, then click **Add**.
   e. Under Authorization Success, fill in the last line of fields:

      For **Type**, enter a descriptive name such as `headerVar`.

      For **Name**, enter `UID`.

      For **Return Attribute**, enter the name of the attribute used by the authentication source to map to the user name in the user directory. For example, IPlanet LDAP uses the `uid` attribute by default. Other LDAP repositories, and Active Directory, use `cn` or `samaccountname` by default.

      Note: Do not configure an action to return a value.

   f. Click **Save**.
   g. Click the **Allow Access** sub-tab and then click **Add** to display controls for adding users or groups to allow access to this resource.
   h. Add appropriate users and groups. Any user/group that needs access to the portal should be included here.
   i. Click **Save**.
7. Create an authorization rule for the policy you created:
   a. Click the **Policies** tab.
   b. Click the name of the policy created above to select it.
   c. Click the **Authentication Rule** sub-tab and add a method appropriate to your configuration, for example, Basic over LDAP.

      Note: Basic over LDAP is a rule created during Oblix installation. If it is not available, Oblix was not installed properly.

   d. Click **Save**.
   e. Click the **Authorization Expression** sub-tab, then click **Add**.
   f. In the Select the Authorization Rule box, choose the rule you created above.
   g. Click **Save**.

E.2.4.3 Configuring Oblix WebGate for Apache

Use the version of Oblix WebGate that is compatible with your Oblix suite. For example, if you use Oblix NetPoint 6.5, configure Oblix WebGate 6.5; if you use Oblix COREid 7.0, use Oblix WebGate 7.0.

To set up Oblix WebGate for Apache:

1. On the host computer for the portal, install the version of Apache required by Oblix WebGate:
   - For WebGate 6.5, install Apache 1.3.
   - For WebGate 7.0 or 7.0.4, install Apache 1.3 or Apache 2.0.
2. On the host computer for the portal, install Oblix WebGate for Apache. For details, refer to Oblix documentation.
3. On the host computer for the portal, on the Web application server to which the portal application is deployed, modify the Web application server setting to turn off URL rewrites.

   For information about modifying the Web application server to turn off URL rewrites, refer to the Web application server documentation or Knowledge Base article DA_239501, "Configuring Web Application Servers to not Rewrite URLs."

E.2.4.4 Configuring Oblix WebGate to Work with Remote Servers

To enable SSO token delegation to a remote tier, for all remote portlet servers that have WebGate installed, turn off IP validation in the WebGate configuration file:

1. Open the ../netpoint/webcomponent/access/oblix/apps/webgate/webgatestatic.lst file.
2. At the beginning of the file, set IPValidation to false. The beginning of the file should look something like this:

```
BEGIN:vCompoundList
DenyOnNotProtected:false
CachePragmaHeader:no-cache
CacheControlHeader:no-cache
IPValidation:false
```

3. Save the webgatestatic.lst file, and restart the remote server. You do not need to restart the portal.

E.2.5 Integrating With Other Authentication Providers

Oracle WebCenter Interaction does not provide out of the box integrations with other authentication vendors. However you can integrate with other vendors using the following SSO configuration options:

- BasicSSO. We recommend that you implement SSO for unsupported authentication servers using the BasicSSO method whenever possible.

  Follow these basic steps for the BasicSSO method:

  1. Install and configure your authentication server as described in your vendor's documentation.
  2. Create a remote server. See Section 3.3.1, "Creating or Editing a Remote Server."
  3. Create an authentication Web service. See Section 6.8.1, "Creating or Editing an Authentication Web Service."
  4. Create an authentication source. See Section 6.9.4, "Creating a Single Sign-On Authentication Source."
  5. Follow special configuration requirements for BasicSSO described in Section E.3.1, "Modifying the Portal Configuration for BasicSSO."

- CustomSSO. We recommend that you implement SSO for unsupported authentication servers using the BasicSSO method whenever possible. Use CustomSSO only if BasicSSO is not sufficient to implement the SSO solution needed for your deployment.

  Follow these basic steps for the CustomSSO method:

  1. Install and configure your authentication server as described in your vendor's documentation.
  2. Create a remote server. See Section 3.3.1, "Creating or Editing a Remote Server."
  3. Create an authentication Web service. See Section 6.8.1, "Creating or Editing an Authentication Web Service."
  4. Create an authentication source. See Section 6.9.4, "Creating a Single Sign-On Authentication Source."
  5. Follow special configuration requirements for CustomSSO described in Section E.3.5, "Modifying the Portal Configuration for CustomSSO Service."

  For information on developing CustomSSO integration code, see "Developing Custom SSO Objects to Integrate Third-Party SSO Servers with the Portal: DA_217750," which is available from the Knowledge Base of the Support Center.

E.3 Configuring the Portal for SSO

This section describes how to modify the portal configuration to enable SSO in the following cases:

- Section E.3.1, "Modifying the Portal Configuration for BasicSSO"
- Section E.3.2, "Configuring Integration with WIA"
- Section E.3.3, "Modifying the Portal Configuration for Integration with Netegrity Authentication Servers"
- Section E.3.4, "Modifying the Portal Configuration for Integration with Oblix Authentication Servers"
- Section E.3.5, "Modifying the Portal Configuration for CustomSSO Service"

Note: You must configure the appropriate SSO settings described in this section on each portal server for which you want to deploy SSO.

E.3.1 Modifying the Portal Configuration for BasicSSO

Oracle WebCenter Interaction provides a built-in BasicSSO service that enables integration with any authentication server. To configure the BasicSSO service, you configure portalconfig.xml so the portal can derive authentication information from the authentication source you created, as described in Section 6.9.4, "Creating a Single Sign-On Authentication Source."

E.3.1.1 Configuring portalconfig.xml

Configure settings in the portalconfig.xml file, as described in the following table and subsequent example.

Table E–1 SSO Settings in portalconfig.xml

Setting	Values

SSOVendor	`<setting name="SSOVendor">`
	`<value xsi:type="xsd:integer">50</value>`
	`</setting>`

DefaultAuthSourcePrefix	This setting can be omitted if the value of the PrefixHeader setting matches the Authentication Source Category string you configured for your remote or LDAP authentication source.
	Otherwise, set the value of this setting to the Authentication Source Category string.
	For example, if your Authentication Source Category string is `HQ`, set DefaultAuthSourcePrefix to HQ, as shown in the following example:
	`<setting name="DefaultAuthSourcePrefix">`
	`<value xsi:type="xsd:string">HQ</value>`
	`</setting>`

CookiePath	Set this value to `/`. Specify a different setting only if your SSO authentication server requires a different convention.
	Example:
	`<setting name="CookiePath">`
	`<value xsi:type="xsd:string">/</value>`
	`</setting>`

CookieDomain	Set this value to the fully qualified domain name for which you want the cookie to be forwarded. For example, if you specify `.company.com`, the cookie enables access to all domains that end in company.com.
	The string must start with a period (.) and include a minimum of two periods.
	Example:
	`<setting name="CookieDomain">`
	`<value xsi:type="xsd:string">.plumtree.com</value>`
	`</setting>`

SSOCookieIsSecure	Set this value to `0` or `1`.
	0 (the default) specifies the connection to the remote server does not require SSL for the cookie to be forwarded.
	1 specifies SSL is required.
	Example:
	`<setting name="SSOCookieIsSecure">`
	`<value xsi:type="xsd:integer">0</value>`
	`</setting>`

The following example configuration enables BasicSSO:

```
<setting name="SSOVendor">
     <value xsi:type="xsd:integer">50</value>
</setting>
<setting name="DefaultAuthSourcePrefix">
     <value xsi:type="xsd:string"/>
```

```
</setting>
<setting name="CookiePath">
     <value xsi:type="xsd:string">/</value>
</setting>
<setting name="CookieDomain">
     <value xsi:type="xsd:string">.it.company.com</value>
</setting>
<setting name="SSOCookieIsSecure">
     <value xsi:type="xsd:integer">0</value>
</setting>
```

Next, modify the settings of the `<portal:SSOVendor>` component in the portalconfig.xml file, as described in the following table and subsequent example.

Table E–2 <portal:SSOVendor> Component

Setting	Values
NameHeader	Set this value to the name of the user name header your authentication server sends to the portal. The value must be a legal header name. If you want the user name extracted from the Base64-decoded Authentication Header, specify `Authorization`. `<NameHeader>` requires a valid value if `<UseRemoteUser>` is not specified or is set to `0`.
PrefixHeader	Set this value to the name of the header containing an authentication source prefix if one is required by remote portlets to authenticate login. If you want the prefix extracted from the Base64-decoded Authentication Header, specify `Authorization`. `<PrefixHeader>` can be set to an empty string but must be present in portalconfig.xml.
PasswordHeader	Set this value to the name of the header containing a password if one is required by remote portlets to authenticate login. If you want the password extracted from the Base64-decoded Authentication Header, specify `Authorization`. `<PasswordHeader>` can be set to empty string but must be present in portalconfig.xml.

Cookie	Set this value to the name of a header containing a cookie if one is required by remote portlets to authenticate login.
	To specify multiple values, separate values with semi-colons (;). For example:
	`<setting name="Cookie">`
	`<value xsi:type="xsd:string">ssocookie1;ssocookie2</value>`
	`</setting>`
	You configure cookie attributes in the portalconfig.xml file. For information, see Section E.3.1.1, "Configuring portalconfig.xml."

SecureHeader	Set this value to the name of a header that should not be forwarded to remote portlets. The value you specify is understood as a prefix: headers that start with this value are not forwarded. To specify multiple values, separate values with semi-colons (;).

Table E–2 (Cont.) <portal:SSOVendor> Component

Setting	Values

UseRemoteUser	To extract the name of the authenticated user from a server variable instead of a user name header, set the value to 1. For example:
	`<setting name="UseRemoteUser">`
	`<value xsi:type="xsd:integer">1</value>`
	`</setting>`
	For Java implementations, the server variable is REMOTE_USER. In .NET, the variable is AUTH_USER.
	By default, this value is set to 0 (false).
	If `<NameHeader>` is not specified, the value of `<UseRemoteUser>` must be set to `1`.

The following example configuration summarizes settings for BasicSSO:

```
<component name="portal:SSOVendor"
type="http://www.plumtree.com/config/component/types/portal/ssovendor">
<setting name="NameHeader">
     <value xsi:type="xsd:string">pt_user</value>
</setting>
<setting name="PrefixHeader">
     <value xsi:type="xsd:string">pt_domain</value>
</setting>
<setting name="PasswordHeader">
     <value xsi:type="xsd:string">pt_password</value>
</setting>
<setting name="Cookie">
     <value xsi:type="xsd:string">PTSSOCookie</value>
</setting>
<setting name="SecureHeader">
     <value xsi:type="xsd:string">authorization</value>
</setting>
<setting name="LogoutURL">
     <value xsi:type="xsd:string"/>
</setting>
<clients>
     <client name="portal"/>
</clients>
</component>
```

To extract the name of the authenticated user from a server variable instead of a user name header:

```
<component name="portal:SSOVendor"
type="http://www.plumtree.com/config/component/types/portal/ssovendor">
<setting name="UseRemoteUser">
     <value xsi:type="xsd:integer">1</value>
</setting>
</component>
```

E.3.2 Configuring Integration with WIA

Oracle WebCenter Interaction provides built-in integration with WIA. Instead of configuring BasicSSO service, follow the procedures in this section to configure SSO integration with WIA.

If you specify the Windows NT domain name as the name for the Authentication Source Category when you set up your authentication source (as described in Section 6.9.4, "Creating a Single Sign-On Authentication Source"), you need only configure settings in portalconfig.xml.

E.3.2.1 Configuring portalconfig.xml

Configure settings in the portalconfig.xml file, as described in the following table and subsequent example.

Table E–3 SSO settings in portalconfig.xml for configuring integration with WIA

Setting	Value

SSOVendor	`<setting name="SSOVendor">`
	`<value xsi:type="xsd:integer">5</value>`
	`</setting>`

DefaultAuthSourcePrefix	This setting can be omitted if you set the Authentication Source Category value to the appropriate Windows NT domain name when you configure your remote authentication source. For example, if your Windows domain name is USA and your Authorization Source Category string is USA, this setting can be empty. If you set the Authentication Source Category to a value other than the Windows NT domain name, specify that string. For example, if your Authentication Source Category string is HQ, set DefaultAuthSourcePrefix to HQ, as shown in the following example:
	`<setting name="DefaultAuthSourcePrefix">`
	`<value xsi:type="xsd:string">HQ</value>`
	`</setting>`
	Additionally, set:
	`<setting name="UseDomain">`
	`<value xsi:type="xsd:integer">0</value>`
	`</setting>`

The following example configuration enables integration with WIA:

```
<setting name="SSOVendor">
     <value xsi:type="xsd:integer">5</value>
</setting>
<setting name="DefaultAuthSourcePrefix">
     <value xsi:type="xsd:string"/>
</setting>
```

Next (if applicable) modify the settings of the <portal:SSOVendor> component in the portalconfig.xml file, as described in the following table and subsequent example.

Table E–4 <portal:SSOVendor> Settings

Setting	Values

UseDomain	If you set the Authentication Source Category to the Windows NT domain name, you do not need to configure this setting. If you set the Authentication Source Category to a value other than the Windows NT domain name, set the value to `0`.
	`<setting name="UseDomain">`
	`<value xsi:type="xsd:integer">0</value>`
	`</setting>`
	Additionally, configure the `<DefaultAuthSourcePrefix>` setting in portalconfig.xml, as described in Section E.3.2.1, "Configuring portalconfig.xml."

The following example configuration summarizes settings that can be configured for integration with WIA:

```
<component name="portal:SSOVendor"
type="http://www.plumtree.com/config/component/types/portal/ssovendor">
<setting name="UseDomain">
     <value xsi:type="xsd:integer">0</value>
</setting>
</component>
```

E.3.3 Modifying the Portal Configuration for Integration with Netegrity Authentication Servers

Oracle WebCenter Interaction provides built-in integration with Netegrity authentication servers. Instead of configuring BasicSSO service, follow the procedures in this section to configure SSO integration with a Netegrity authentication server.

Configure settings in the portalconfig.xml file, as described in the following table and subsequent example.

Table E–5 SSO Settings in portalconfig.xml

Setting	Values

SSOVendor	`<setting name="SSOVendor">`
	`<value xsi:type="xsd:integer">2</value>`
	`</setting>`

DefaultAuthSourcePrefix	Set this value to a string that matches the value you entered for Authentication Source Category when you configured your authentication source. For example, if your Authentication Source Category string is HQ, set DefaultAuthSourcePrefix to HQ, as shown in the following example:
	`<setting name="DefaultAuthSourcePrefix">`
	`<value xsi:type="xsd:string">HQ</value>`
	`</setting>`

Table E–5 (Cont.) SSO Settings in portalconfig.xml

Setting	Values

CookiePath	Set this value to `/`. Specify a different setting only if your SSO authentication server requires a different convention.
	Example:
	`<setting name="CookiePath">`
	`<value xsi:type="xsd:string">/</value>`
	`</setting>`

CookieDomain	Set this value to the fully qualified domain name for which you want the cookie to be forwarded. For example, if you specify `.company.com`, the cookie enables access to all domains that end in company.com.
	The string must start with a period (.) and include a minimum of two periods.
	Example:
	`<setting name="CookieDomain">`
	`<value xsi:type="xsd:string">.company.com</value>`
	`</setting>`

SSOCookieIsSecure	Set this value to `0` or `1`.
	0 (the default) specifies the connection to the remote server does not require SSL for the cookie to be forwarded.
	1 specifies SSL is required.
	Example:
	`<setting name="SSOCookieIsSecure">`
	`<value xsi:type="xsd:integer">0</value>`
	`</setting>`

The following example enables integration with a Netegrity authentication server:

```
<setting name="SSOVendor">
     <value xsi:type="xsd:integer">2</value>
</setting>
<setting name="DefaultAuthSourcePrefix">
     <value xsi:type="xsd:string">HQ</value>
</setting>
<setting name="CookiePath">
     <value xsi:type="xsd:string">/</value>
</setting>
<setting name="CookieDomain">
     <value xsi:type="xsd:string">.company.com</value>
</setting>
<setting name="SSOCookieIsSecure">
     <value xsi:type="xsd:integer">0</value>
</setting>
```

E.3.4 Modifying the Portal Configuration for Integration with Oblix Authentication Servers

Oracle WebCenter Interaction provides built-in integration with Oblix authentication servers. Instead of configuring BasicSSO service, follow the procedures in this section to configure SSO integration with an Oblix authentication server.

> **Note:** By default, the portal expects the Oblix server to forward the user name header named uid. If you configure your Oblix server to forward a user name header with a different name, you must configure your SSO implementation as BasicSSO service. For information about BasicSSO service, see Section E.3.1, "Modifying the Portal Configuration for BasicSSO."

Configure settings in the portalconfig.xml file, as described in the following table and subsequent example.

Table E–6 SSO Settings in portalconfig.xml

Setting	Values

SSOVendor	`<setting name="SSOVendor">`
	`<value xsi:type="xsd:integer">3</value>`
	`</setting>`

DefaultAuthSourcePrefix	Set this value to a string that matches the value you entered for Authentication Source Category when you configured your authentication source. For example, if your Authentication Source Category string is HQ, set DefaultAuthSourcePrefix to HQ, as shown in the following example:
	`<setting name="DefaultAuthSourcePrefix">`
	`<value xsi:type="xsd:string">HQ</value>`
	`</setting>`

CookiePath	Set this value to `/`. Specify a different setting only if your SSO authentication server requires a different convention.
	Example:
	`<setting name="CookiePath">`
	`<value xsi:type="xsd:string"/>/</value>`
	`</setting>`

CookieDomain	Set this value to the fully qualified domain name for which you want the cookie to be forwarded. For example, if you specify `.company.com`, the cookie enables access to all domains that end in company.com.
	The string must start with a period (.) and include a minimum of two periods.
	Example:
	`<setting name="CookieDomain">`
	`<value xsi:type="xsd:string">.company.com</value>`
	`</setting>`

Table E–6 (Cont.) SSO Settings in portalconfig.xml

Setting	Values

SSOCookieIsSecure	Set this value to `0` or `1`.
	0 (the default) specifies the connection to the remote server does not require SSL for the cookie to be forwarded.
	1 specifies SSL is required.
	Example:
	`<setting name="SSOCookieIsSecure">`
	`<value xsi:type="xsd:integer">0</value>`
	`</setting>`

The following example enables integration with an Oblix authentication server:

```
<setting name="SSOVendor">
     <value xsi:type="xsd:integer">3</value>
</setting>
<setting name="DefaultAuthSourcePrefix">
     <value xsi:type="xsd:string">HQ</value>
</setting>
<setting name="CookiePath">
     <value xsi:type="xsd:string">/</value>
</setting>
<setting name="CookieDomain">
     <value xsi:type="xsd:string">.company.com</value>
</setting>
<setting name="SSOCookieIsSecure">
     <value xsi:type="xsd:integer">0</value>
</setting>
```

E.3.5 Modifying the Portal Configuration for CustomSSO Service

Oracle WebCenter Interaction supports custom integration with unsupported authentication servers for which you have developed integration code. For information on developing integration code, see "Developing Custom SSO Objects to Integrate Third-Party SSO Servers with the Portal: DA_217750."

Instead of configuring BasicSSO service, follow the procedures in this section to configure integration with your CustomSSO service.

Configure settings in the portalconfig.xml file, as described in the following table and subsequent example.

Table E–7 SSO Settings in portalconfig.xml

Setting	Values

SSOVendor	Set this value to 100 or above.
	`<setting name="SSOVendor">`
	`<value xsi:type="xsd:integer">100</value>`
	`</setting>`

Table E–7 (Cont.) SSO Settings in portalconfig.xml

Setting	Values

CustomSSOClass	Set this value to the fully qualified class name for the object you developed to integrate an SSO authentication server with the portal.
	Example:
	`<setting name="CustomSSOClass">`
	`<value xsi:type="xsd:string">com.company.portaluiinfrastructure.sso.integrations.SSOTest</value>`
	`</setting>`

CustomSSOAssembly	(.NET only) Set this value to the name of the assembly that contains the .NET class you specified with the CustomSSOClass setting.
	Example:
	`<setting name="CustomSSOAssembly">`
	`<value xsi:type="xsd:string"/>portaluiinfrastructure</value>`
	`</setting>`

DefaultAuthSourcePrefix	Set this value to a string that matches the value you entered for Authentication Source Category when you configured your authentication source. For example, if your Authentication Source Category string is HQ, set DefaultAuthSourcePrefix to HQ, as shown in the following example:
	`<setting name="DefaultAuthSourcePrefix">`
	`<value xsi:type="xsd:string">HQ</value>`
	`</setting>`

CookiePath	Set this value to `/`. Specify a different setting only if your SSO authentication server requires a different convention.
	Example:
	`<setting name="CookiePath">`
	`<value xsi:type="xsd:string"/>/</value>`
	`</setting>`

CookieDomain	Set this value to the fully qualified domain name for which you want the cookie to be forwarded. For example, if you specify `.company.com`, the cookie enables access to all domains that end in company.com.
	The string must start with a period (.) and include a minimum of two periods.
	Example:
	`<setting name="CookieDomain">`
	`<value xsi:type="xsd:string"/>.company.com</value>`
	`</setting>`

Table E–7 (Cont.) SSO Settings in portalconfig.xml

Setting	Values

SSOCookieIsSecure	Set this value to `0` or `1`.
	0 (the default) specifies the connection to the remote server does not require SSL for the cookie to be forwarded.
	1 specifies SSL is required.
	Example:
	`<setting name="SSOCookieIsSecure">`
	`<value xsi:type="xsd:integer">0</value>`
	`</setting>`

The following example uses CustomSSO to enable integration with an unsupported authentication server on a .NET platform:

```
<setting name="SSOVendor">
     <value xsi:type="xsd:integer">100</value>
</setting>
<setting name="CustomSSOClass">
     <value
xsi:type="xsd:string">com.company.portaluiinfrastructure.sso.integrations.SSOTest<
/value>
</setting>
<setting name="CustomSSOAssembly">
     <value xsi:type="xsd:string">portaluiinfrastructure</value>
/setting>
<setting name="DefaultAuthSourcePrefix">
     <value xsi:type="xsd:string">HQ</value>
</setting>
<setting name="CookiePath">
     <value xsi:type="xsd:string">/</value>
</setting>
<setting name="CookieDomain">
     <value xsi:type="xsd:string">.company.com</value>
</setting>
<setting name="SSOCookieIsSecure">
     <value xsi:type="xsd:integer">0</value>
</setting>
```

The following example uses CustomSSO to enable integration with an unsupported authentication server on a Java platform:

```
<setting name="SSOVendor">
     <value xsi:type="xsd:integer">100</value>
</setting>
<setting name="CustomSSOClass">
     <value
xsi:type="xsd:string">com.company.portaluiinfrastructure.sso.integrations.SSOTest<
/value>
</setting>
<setting name="DefaultAuthSourcePrefix">
     <value xsi:type="xsd:string">HQ</value>
</setting>
<setting name="CookiePath">
     <value xsi:type="xsd:string">/</value>
</setting>
<setting name="CookieDomain">
     <value xsi:type="xsd:string">.company.com</value>
```

```
</setting>
<setting name="SSOCookieIsSecure">
     <value xsi:type="xsd:integer">0</value>
</setting>
```

E.4 Common SSO Questions

This section contains links to common SSO questions and the answers.

- Section E.4.5, "Why Can't I Access the Portal Through SSOLogin.aspx or the SSOServlet?"
- Section E.4.7, "How Can I Debug My SSO Deployment?"
- Section E.4.3, "Does the Portal with SSO Support Guest User Sessions?"
- Section E.4.6, "Why Do Users Get JavaScript Errors and Portal Menus Fail to Load if I Configure the SSO Authentication Server to Protect the Image Service Virtual Directory?"
- Section E.4.4, "How Can I Change Login Credentials From an SSO Session?"
- Section E.4.2, "Why Isn't the SSO Cookie Forwarded to Remote Servers or Portlets?"
- Section E.4.1, "Why Doesn't SSO Work for a Particular User?"
- Section E.4.9, "How Do I Configure Reverse Proxy with My SSO Deployment Using Apache HTTP Server?"
- Section E.4.10, "How Do I Configure Reverse Proxy with My SSO Deployment Using a Java Application Server?"
- Section E.4.8, "How Do I Configure Reverse Proxy with My SSO Deployment Using Oblix Netpoint Access Server (versions 6.1.1 or 6.5) with an Apache WebGate?"

E.4.1 Why Doesn't SSO Work for a Particular User?

Examine the following settings or events to diagnose the cause of this problem:

- In portalconfig.xml, the user name prefix must match the value for the Authentication Source Category set in the authentication source portal object. Ensure these strings are identical.
- Use Oracle WebCenter Logging Spy to see if the SSO authentication server is passing the user name to the portal. If you see an error message in red type that indicates `SSO integration returned a null user name. Exiting SSOLoginPage`, then there is something wrong with the configuration. Ensure that you have configured the authentication server correctly to forward the user name after authentication to the portal.

E.4.2 Why Isn't the SSO Cookie Forwarded to Remote Servers or Portlets?

Examine the following settings or events to diagnose the cause of this problem:

- In portalconfig.xml, ensure the value of the <CookieDomain> element begins with a period.
- In portalconfig.xml, ensure the value of the <CookiePath> element is the standard value, `<CookiePath value="/"/>`, or otherwise is a reasonable value.

- In the authentication server, ensure the value of the cookie object enables the cookie to be forwarded.
- Examine the configurations for the authentication server and the portal to ensure fully qualified domain names are specified for all servers.
- If you are unable to diagnose the problem with these methods, use a TCP tracing tool to see the value returned by the SSO provider. The path and domain must match the values for <CookiePath> and <CookieDomain> in portalconfig.xml.

E.4.3 Does the Portal with SSO Support Guest User Sessions?

Guests can access the portal while SSO is enabled. Guest access is controlled by the `AllowGuestAccess` setting in the `Authentication` section of portalconfig.xml. When guest access is disabled, users can browse the portal without logging in. When users click **Log In** in the portal banner or when they attempt to visit a page for which the guest user does not have access, the portal redirects them to the SSO login page, and they are prompted by the SSO product for their login credentials.

If users already have an SSO cookie from another application, they still browse the portal as the guest user until they click **Log In**. At which point, they are logged in without entering their user name and password.

Guest access can be enabled or disabled independently from SSO. If guest access and SSO are both disabled, users have to log in before accessing any part of the portal.

E.4.4 How Can I Change Login Credentials From an SSO Session?

If you must log in as Administrator or other portal user from within an SSO session, you can perform the following steps:

1. Click **Log Off** in the portal banner.

   This logs you out of the portal and takes you to the portal login page, as if SSO were disabled.

2. From this page you can log in as a non-SSO user or you can browse the portal as guest.
3. When you want to log back in as an SSO user, click **Log In** in the portal banner.

   You are automatically logged in to the portal in an SSO session.

E.4.5 Why Can't I Access the Portal Through SSOLogin.aspx or the SSOServlet?

The first time you access the portal after you deploy SSO, you must access the portal from the main portal URL: http://*servername*/portal/server.pt.

If you try to access the portal through /portal/sso/SSOLogin.aspx (.NET) or /portal/SSOServlet (Java), your request fails and the following error appears in Oracle WebCenter Logging Spy trace logs: `The SSO Login Page was unable to retrieve the request URL from the session. Will use a relative redirect to return to the main page.`

E.4.6 Why Do Users Get JavaScript Errors and Portal Menus Fail to Load if I Configure the SSO Authentication Server to Protect the Image Service Virtual Directory?

The portal and other Oracle WebCenter products, such as Oracle WebCenter Collaboration, periodically send HTTP requests to the Image Service to check the version of the JavaScript components stored on the Image Service. These requests are

not associated with a particular user's session and do not send an SSO cookie or other credentials. If the Image Service is protected by your SSO solution, the request from the portal is blocked from checking the JavaScript versions. As a result, the portal cannot load the proper JavaScript files and end users encounter JavaScript errors and possibly other errant behavior. To resolve this problem, do not configure your SSO authentication server to protect the Image Service, but only the portal. You do not must protect the Image Service as it contains only static public content that ships with every portal installation. No data specific to users or to your organization is ever stored on the Image Service.

E.4.7 How Can I Debug My SSO Deployment?

The portal provides built-in trace statements that are useful for debugging SSO integration. For example, when a user attempts to log in using SSO, the contents of all headers are traced. To enable this tracing, turn on all tracing for the **Portal UI - Infrastructure** component.

E.4.8 How Do I Configure Reverse Proxy with My SSO Deployment Using Oblix Netpoint Access Server (versions 6.1.1 or 6.5) with an Apache WebGate?

1. Install Oblix NetPoint Access Server, including NetPoint Access Manager, NetPoint COREid, and Oblix Apache WebGate. WebGate must be installed on the same server as the Apache HTTP server. For detailed instructions, refer to Oblix documentation.
2. Use Oblix Access Manager to create the portal protection policy. For detailed instructions, refer to Oblix documentation.
3. Configure Oblix NetPoint Access Server. For detailed instructions, see Configuring an Oblix Authentication Provider.
4. Configure the Apache HTTP server for reverse proxy. For detailed instructions, see the procedures that follow these steps.
5. Configure the portal for SSO. For detailed instructions, see Configuring the Portal for SSO.
6. Configure the portal application server for reverse proxy. For detailed instructions, see the procedures following these steps.
7. Restart services to apply configuration modifications.

E.4.9 How Do I Configure Reverse Proxy with My SSO Deployment Using Apache HTTP Server?

1. Install the version of the Apache HTTP server recommended by the Oblix Installation Guide.

   For Netpoint 6.5, Oblix recommends the latest version of the Apache, v1.3 line. The configuration described in this example has been tested with version v1.3.29.
2. Turn on the proxy module inside of the Apache configuration.

   To do so, edit *apache_install_dir*/conf/httpd.conf to uncomment the lines titled `LoadModule proxy_module modules/mod_proxy.so` and `AddModule mod_proxy.c`. (To uncomment a line, remove the pound symbol (#) at the beginning of the line).
3. Configure Apache to act as a reverse proxy for your portal.

To do so, add lines similar to the following example at the end of httpd.conf:

```
ProxyRequests Off
ProxyPass /portal http://your_portal_server.domain.com:7001/portal
ProxyPassReverse /portal http://your_portal_server.domain.com:7001/portal
```

This example configuration redirects requests from the Apache Web server (http://proxy_server.domain.com:80/portal/xyz) to the portal application server (http://your_portal_server.domain.com:7001/portal/xyz). You must specify the fully qualified domain name here and for all other times you type in the server names. For more information on Apache reverse proxy, see http://httpd.apache.org/docs/mod/mod_proxy.html.

4. Start or restart the Apache HTTP server.

E.4.10 How Do I Configure Reverse Proxy with My SSO Deployment Using a Java Application Server?

1. Open *install_dir*/ptportal/10.3.3/settings/config/portalconfig.xml for editing.
2. Configure the <URLMapping> element so that it is similar to the following example:

```
<URLFromRequest0 value="*"/>
<ApplicationURL0 value="http://proxy_server.domain.com/portal/server.pt"/>
<SecureApplicationURL0 value="*"/>
```

3. Replace `proxy_server.domain.com` with the fully qualified domain name for the Apache HTTP server.
4. Configure the <SSOVirtualDirectoryPath> element so that it is similar to the following example:

```
<SSOVirtualDirectoryPath value="http://proxy_server.domain.com/portal/"/>
```

5. Replace `proxy_server.domain.com` with the fully qualified domain name for the Apache HTTP server.
6. Restart the application server.

F

Default Behavior of Search Service

This appendix describes the default behavior of the portal searches, including search syntax and text search rules.

It includes the following sections:

F.1 About the Different Types of Search

The portal provides banner and advanced search tools for typical and advanced users, respectively. The fundamental search syntax and behavior are the same in banner and advanced search, but banner search adds automatic broadening, ranking features, and syntax correction. The following table specifies the search type implemented in the search tools available through different areas of the portal.

Portal Area	Search Type	Description
Banner search	Banner	Searches the following portal objects: banner fields, the Knowledge Directory, portlets, communities, users, Oracle WebCenter Collaboration items, and Publisher items.
Advanced search	Advanced	Allows composition of complex queries on specific document or object properties. Allows searches on date fields as well as text fields. Allows restriction to specific object type. Advanced search also enables searching of all (or any combination of) indexable portal objects, including many which are not searched in banner search, such as content crawlers, jobs, and Web services.

Portal Area	Search Type	Description
Federated Search	n/a	Federated search enables you to query multiple search Web services and receive collated results. Portal search can be included as one of the search services. The portal search option from this page behaves similarly to banner search, except only documents in the Knowledge Directory are searched. Spell correction, Best Bets, and other customizations made with the Search Results Manager do not apply.
Object selection	Banner	Search functionality enables end users to search for portlets when adding portlets to pages or search for communities when joining communities.
Administrative object search	Banner	Administrators can search the Administrative Objects Directory, optionally filtering by folder and object type. Search for specific kinds of portal objects is also integrated into the creation of various kinds of administrative objects. For instance, when creating a remote content crawler, the administrator is presented with the option of searching the available content source objects.
Filters	Advanced	Filters enable you to create an advanced search query that documents must match to be allowed into a particular folder in the Knowledge Directory.
Snapshot Query	Advanced	A search query that enables you to specify conditions for searching portal objects and, optionally, display the results in a Content Snapshot Portlet and/or e-mail the results to users. You can limit your search by language, object type, folder, property, and text conditions.

F.2 Elements of Search Syntax

There are several syntax elements that work together in search.

F.2.1 About Operator Modes

The Search Service parses queries to determine which operator modes to use for the query.

F.2.1.1 Bag of Words Mode

If the query does not include any search operators (+/-, AND, OR, NEAR, and so on), the Search Service parses the query in Bag of Words mode. Each word in the query must be present in all of the search results; the Boolean AND operator is implicit.

F.2.1.2 Query Operators Mode

If the query includes query operators, the Search Service parses the query in Query Operators mode.

Query operators AND, OR, NOT, and NEAR are spotted without any special marking (for example, cat AND dog), but all other operators must be surrounded by angle brackets (for example, <WORD>) to be recognized as having special meaning.

A query that contains three or more terms and an operator is parsed as if the terms on each side of the operator were quoted phrases.

Example: `Search Service and Notification`

This query is parsed as: `"Search Service" AND Notification`

Search operators are localized for the following European languages: English, Danish, Dutch, Finnish, French, German, Italian, Norwegian (Bokmal), Norwegian (Nynorsk), Portuguese, and Spanish. If you put angle brackets around the operators, the English versions are also recognized. For example, in the Spanish locale, the following queries are equivalent: `perro Y gato`, `perro <AND> gato`, and `perro gato`. However, `perro AND gato` is not equivalent in the Spanish locale, because AND is not surrounded by angle brackets.

Anything enclosed in angle brackets but not recognized as one of the supported operators is ignored.

F.2.1.3 Internet Style Mode

If the query includes operators common to internet search engines such as AltaVista and Google, the Search Service parses the search in Internet Style mode. All terms preceded by a plus (+) are required. All terms preceded by a minus (-) are excluded. If at least one term is preceded by a +, then any "plain" terms not preceded by a + or - are used to boost ranking of results, but are not required. For example, consider the following query: `+dog -cat bird`

This query returns documents that contain dog but do not contain cat, and ranks documents with both dog and bird highest. Compare this to a similar query: `bird -cat`

This query returns documents that contain bird but do not contain cat. Absent any + terms, the plain term bird is treated as a required term.

F.2.1.4 Search String Operators

Operator	Description	Example Search Text	Example Search Results
<AND> Alternative: AND, & (ampersand)	Connects two terms that must both be included in each item returned.	holiday <AND> schedule	Holiday Schedule
<OR> Alternative: OR, ACCRUE, ANY, | (vertical bar), , (comma)	Connects two terms where at least one must be included in each item returned.	holiday <OR> vacation	Holiday Schedule, Christmas Holiday Party, Scheduling Vacation
<NOT> Alternative: NOT, AND NOT	Term must not appear in items returned.	holiday <NOT> vacation	Holiday Schedule, Christmas Holiday Party
<NEAR/N> Alternative: NEAR	Terms must appear within N words of each other, regardless of order, in items returned.	early <NEAR/10> retirement	Plan early for your retirement
<ORDER>	Both terms must appear in items returned, and the first term must precede the second term.	song <ORDER> bird	song bird (not bird song)
<WORD>	Turns off stemming, alternate case, and spell correction.		

Operator	Description	Example Search Text	Example Search Results
<PHRASE> Alternative: Surround terms in " (double quotes)	Both terms must appear sequentially, in a phrase in items returned.		
<SENTENCE>	Same as <NEAR/10>.		
<PARAGRAPH>	Same as <NEAR/50>.		
+ (plus)	Term must appear in the items returned.		
- (minus)	Term must not appear in the items returned.		
* (asterisk)	The wildcard specifies that the result must match 0 or more characters at the beginning or end of a word.	sub*	subdirectory, subject, subjective
> (right angle bracket)	The top best bet operator brings the user directly to the top best bet for a term, such as a community, document, or portlet.	>HR	You are navigated to the HR Community.

There are certain circumstances in which a user can unintentionally invoke a more advanced search mode by inadvertently using operators. Examples include the following queries:

Query	Equivalent to...
The young and the restless	“the young” <AND> “the restless”
File not found	file <AND> <NOT> found
Error -217439239	Error <AND> <NOT> 217439239

In each of these examples, enclosing the query in double quotes yields the desired effect.

F.2.2 Precedence and Parentheses

The Internet Style mode operators '+' and '-' take precedence over the other search operators. For example, `+big dog <order> cat` matches all documents that contain the term big, boosting the ranking of any documents that contain any of the three terms dog, or cat.

Within query operators mode, the operators have the following precedence classes, from greatest to least:

1. NEAR, ORDER, PHRASE, SENTENCE, PARAGRAPH
2. NOT
3. AND
4. OR

Parentheses can be used to override operator precedence. The following two queries are equivalent (the parentheses do not effect the semantics of the search).

- `a and b near c or d`
- `(a and (b near c)) or d`

This search matches documents that meet one of two conditions:

- The document contains the term d
- The document contains the terms a, b, and c, with b and c in close proximity

On the other hand, the parentheses in the following query override the default operator precedence:

```
a and b near (c or d)
```

This search matches documents containing the terms a and b and either c or d, where b is in close proximity to c or d.

F.2.3 Punctuation

Punctuation is treated specially in searches.

The following rules describe the interpretation of punctuation characters.

- Quotation marks are always interpreted as operators signifying a quoted phrase. It is therefore impossible to search for a quotation mark (there is no escape character, such as a backslash, which would remove the special significance of the quotation marks).
- All other punctuation loses any special operator significance inside of quotation marks. (The same holds for all operators, such as AND.)
- Outside of quotation marks, punctuation either has significance as an operator, or it is ignored. The following punctuation has special operator significance outside of quotation marks:
  - Left and right angle brackets(<>) enclose operators, as in <NEAR>
  - Comma (,) is treated as OR
  - Ampersand (&) is treated as AND
  - Vertical bar (|) is treated as OR
  - Plus (+) and minus (-) are interpreted as Internet Style syntax
  - Asterisk (*) is interpreted as a wildcard character
- Punctuation is always split apart from adjoining alpha-numeric characters. For example, an advanced search for `bag-of-words` matches documents containing the three tokens bag, of, and words.
- Underscore is treated as punctuation, meaning you must enclose a term containing an underscore in quotes to get an exact match (for example, `"HOST_NAME"` matches HOST_NAME, but without the quotes, it also matches HOST NAME).

  Symmetrical punctuation tokenization takes place on text stored in the index, so the explosion of a query term such as bag-of-words does not prevent the search from matching a document containing the phrase bag-of-words.

Note: ■Terms generated by wildcard expansion are not stemmed.

- Wildcard expansion is performed internally by replacing each pattern with a limited list of terms that match the pattern before actually executing the query. Very broad wildcard expressions might therefore return a partial list of results.

F.2.4 Case Sensitivity

All searches are case-insensitive, except when the <WORD> operator is used.

Table F–1 Case Sensitivity Examples

Query	Matches
`Oracle`	Items containing Oracle, oracle, or any other case variant.
`"Search Service"`	Items containing the phrase Search Service or any other case variant.
`<WORD> Oracle`	Items containing Oracle, but not oracle or ORACLE.

F.2.5 Stemming

Word stemming is applied to all individual terms in the search query, except within quoted phrases, or when the <WORD> operator is used. The stemming of query terms means that a query term will match documents containing morphological variants of that term. For example, a search for `dogs AND go` would match a document containing the terms dog and went. (This example applies to English; stemming employs language-specific information and depends on the user's locale and the language used to index the document.)

Note:

- Terms generated by wildcard expansion are not stemmed.
- Stemming is not applied to terms within a quoted phrase.

F.2.6 Wildcards

The wildcard operator (*) is used to search for partial matches (prefixes, suffixes, and substrings) of indexed terms.

Wildcard expansion is performed internally by replacing each pattern with a limited list of terms that match the pattern before actually executing the query. Very broad wildcard expressions might therefore return a partial list of results.

Note:

- Terms generated by wildcard expansion are not stemmed.
- Wildcards cannot be used within quoted phrases.

Table F–2 Wildcard Examples

Search Type	Query	Matches
prefix	`cat*`	Finds all documents containing terms that start with cat, such as caterpillar.
suffix	`*cat`	Finds all documents with terms that end in cat, such as tomcat.
substring	`*cat*`	Finds all documents with terms that contain cat, such as tomcats. Mid-string wildcard expressions must contain at least three characters (for example, *abc* is legal but *bc* is not).

F.2.7 Quoted Phrases

A quoted phrase in the user search query matches only documents that contain the given sequence of terms. For instance, a search for `"big dog"` will not match a document that contains the terms big and dog if it does not contain the phrase big dog.

Note:

- Stemming is not applied to terms within a quoted phrase.
- Wildcards cannot be used within quoted phrases.

F.2.8 Thesaurus Expansion

Thesaurus expansion allows a term or phrase in a user's search to be replaced with a set of custom related terms before the actual search is performed. This feature improves search quality by handling unique, obscure, or industry-specific terminology.

Thesaurus expansion has the following characteristics:

- It is applied to each term in a banner search.
- It is applied in all three search modes (Internet Style, Query Operators, and Bag of Words).
- It is not applied to quoted phrases.
- If a term is expanded by a thesaurus entry, then it is not eligible for automatic spelling correction.
- Unlike automatic spell correction, which is applied only as a fallback when the non-corrected terms do not match any documents, thesaurus expansion is always applied to all individual search terms.

F.2.9 How Language Settings Apply to Search

Documents and portal objects are indexed with a language setting that determines how word breaking and stemming are applied. When a user issues a search query, word breaking and stemming are applied according to the user account locale settings. Search results are best when the language used for the search matches the language of the documents being searched. However, searches are normally applied to documents in all languages. Cross-language searches do not benefit from localized stemming and word breaking, but can still return useful results.

The advanced search page offers the ability to restrict searches to a particular language.

- The user account search preferences give the option of returning only documents that were indexed using the language of the locale.
- Portal objects can have localized names and descriptions. Banner searches are performed against the default object names and descriptions and the names and descriptions of the locale.

When searching portal content through the Search box in the portal banner, the text of the query is processed using the language setting of the user interface. If the portal interface is German, the query is tokenized and stemmed using German language rules, providing optimal search results for documents indexed using German linguistic rules.

If the search collection contains documents in other languages, you can still retrieve them with a query using the appropriate text (assuming the user interface permits entry of the necessary characters). Typing English words into the search box of a portal using a German interface applies German linguistic rules to the query text. Because English stemming is not used, the query is not able to match alternate English word forms; however, English language documents containing the entered words are retrieved.

Although you can enter Asian language text into a European language search box (if a compatible character encoding is used), you should limit the text to a single word or manually separate words with white space to be able to match Asian content in the search collection.

The Advanced Search page provides additional functionality for searching in a multi-language document collection. A pop-up list allows the user to select the language to use for query processing. Linguistic rules for tokenizing and stemming the selected language are used when processing the query text.

The query operators recognized by Simple Search and Advanced Search are sensitive to the language setting. For example, the AND operator can be specified as "UND" when the query is processed as German. Localized operators are available for the following languages: English, Danish, Dutch, Finnish, French, German, Italian, Norwegian (Bokmal), Norwegian (Nynorsk), Portuguese, and Spanish. All other languages use English operators.

F.2.9.1 Search Service Language Support

The portal provides support for 61 languages.

Of the languages supported by the portal, the following languages include support for word stemming and compound decomposition. This additional information is used to enhance results of the full-text index.

- Chinese (Simplified)
- Chinese (Traditional)
- Czech
- Danish
- Dutch
- English
- Finnish
- French
- German

- Greek
- Hungarian
- Italian
- Japanese
- Korean
- Norwegian (Bokmal)
- Norwegian (Bokmal)
- Polish
- Portuguese
- Russian
- Spanish
- Swedish
- Turkish

The following languages are supported at a reduced level.

- Afrikaans
- Albanian
- Arabic
- Basque
- Belarusian
- Bengali
- Bulgarian
- Catalan
- Cornish
- Croatian
- Esperanto
- Estonian
- Faeroese
- Gallegan
- Hebrew
- Hindi
- Icelandic
- Indonesian
- Irish
- Kalaallisut
- Konkani
- Latvian
- Lithuanian

- Macedonian
- Maltese
- Manx
- Marathi
- Persian
- Romanian
- Serbian
- Serbian-Croatian
- Slovak
- Slovenian
- Swahili
- Tamil
- Telugu
- Thai
- Ukranian
- Vietnamese

F.3 Using Text Search Rules

When you search for text, you generally can just type the text you are looking for (the search string). However, there are a few rules you should be aware of:

Note: Search strings are case-insensitive; that is, uppercase A is the same as lowercase a.

- To find objects or documents containing all terms in your search string, separate your terms with spaces.

  This is the same as using AND.

- To find objects or documents containing one or more of the terms in your search string, separate your terms with commas.

  This is the same as using OR.

- To search for an exact phrase, type quotation marks (“) around the phrase.
- To specify that a term must be included in each result, type a plus (+) in front of the term.
- To exclude a term from the results, type a minus (-) in front of the term.

Note:

- Do not include a space after the plus or minus.
- Do not use the plus or minus in the same search with other search string operators.

F.4 Search Examples

The descriptions of searches below do not include any of the query expansion or ranking techniques that are employed in banner search. Except where otherwise noted, all matches are case-insensitive.

Query	Expected Behavior
Dog	Searches for documents containing any stem variant of Dog.
<WORD> Dog	Searches for documents containing Dog as specified exactly with no stemming or lowercasing. This is the only case-sensitive form of search.
Big <PHRASE> Dog	Searches for documents containing the exact phrase big dog without stemming.
“Big Dog”	Same as Big <PHRASE> Dog.
cat AND dog	Searches for documents containing stem variants of cat and dog. Equivalent to cat <AND> dog.
cat <ALL> dog	Same as cat AND dog.
cat OR dog	Searches for documents containing stem variants of cat or dog.
cat, dog	Same as cat OR dog.
cat <ANY> dog	Same as cat OR dog.
cat <ACCRUE> dog	Same as cat OR dog.
cat NOT dog	Searches for documents containing stem variants of cat but not containing stem variants of dog.
cat AND NOT dog	Same as cat NOT dog.
cat NEAR dog	Finds stem variants of cat occurring near dog (default is within 25 words).
cat NEAR/15 dog	Finds stem variants of cat within 15 words of dog.
cat <ORDER><NEAR/15> dog	Finds stem variants of cat within 15 words before dog. Can also use more convenient syntax cat <ORDER NEAR/15> dog.
cat <ORDER> dog	Finds stem variants of cat anywhere before dog.
cat <SENTENCE> dog	Finds stem variants of cat within 10 words of dog.
cat <PARAGRAPH> dog	Finds stem variants of cat within 50 words of dog.
cat <XYZ> dog	Finds stem variants of cat and dog. The unsupported operator XYZ is ignored.
cat*	Finds all documents containing terms that start with cat, such as caterpillar.
*cat	Finds all documents with terms that end in cat such as tomcat.
cat	Finds all documents with terms that contain cat such as tomcats. Mid-string wildcard expressions must contain at least three characters (for example, *abc* is legal but *bc* is not).
dog *	Finds documents containing stem variants of dog. The singleton wildcard is treated as stray punctuation.
dog cat bird	Finds documents containing stem variants of all three terms, dog, cat, and bird. (Bag of Words mode)

Query	Expected Behavior
big dog AND bird	Finds documents containing the phrase big dog, and stem variants of the term bird. (Query Operators mode with implicit phrase construction)
dog cat +bird	Finds documents containing stem variants of bird. The rank is boosted for documents containing stem variants of dog or cat. The words dog and cat are not joined into a phrase in Internet Style mode.
+dog -cat bird	Finds documents that contain stem variants of dog but do not contain stem variants of cat, and ranks documents with both dog and bird highest.
bird -cat	Finds documents that contain stem variants of bird but do not contain stem variants of cat.
bag-of-words	Searches for documents containing stem variants of the three terms: bag, of, and words. Punctuation marks are treated as spaces when quotation marks are not present.
“Mr. Jones”	Searches for the phrase mr. jones. Punctuation marks are considered part of the search string if they are included within quoted phrases.

F.5 How Search Results Are Ranked

Search results are ranked according to relevance, by default. There are several factors that determine relevance.

F.5.1 How Term Frequency Factors in Relevance

The number of times a query term (or its stemmed and case variant forms) appears in a searchable item has a large influence on the relevance ranking of the item. All other things being equal, items which contain more instances of a query term will rank higher than items containing fewer instances. This is known as term-frequency-based ranking.

F.5.2 About Metadata (Field) Weighting

Banner searches are performed across several document fields, and some fields are weighted higher than other fields, so that, for instance, a match on an object name ranks higher than a match on an object description. By default, the fields searched are name, description, and full-text content.

F.5.3 How Phrases and Proximity Factor in Relevance

In banner search, Bag of Words mode employs special relevancy ranking features which emphasize phrase and proximity matches with the search phrase, even though the user did not employ quotes or proximity operators.

The search phrase terms are used to generate three queries:

1. All words joined together as a single phrase
2. Stem variants of all words and all quoted phrases <ORDER><NEAR> each other
3. Stem variants of all words and all quoted phrases joined together with AND

The three queries combined with the OR operator into a single query, and the relevance ranking are designed to ensure that the results from group 1 always rank above group 2, which rank above group 3.

For example, if you enter `"san francisco" hotels`, the following queries would be generated:

- "san francisco hotels"
- "san francisco" <ORDER><NEAR> hotels
- "san francisco" AND hotels

The search results pages for banner and advanced search allow you to sort the search results by last-modified date, folder, or object type.

F.6 About Banner Search Behavior

Banner search adds some special features to increase the chances that a search will return relevant results.

Banner search has several characteristics:

- In banner search, if a user search query causes syntax errors in Internet Style mode or query operators mode, it is automatically retried in Bag of Words mode to be as forgiving as possible of user error. For example, if you enter dog and, this query would cause a syntax error in Query Operators mode, because it is missing the right-hand operand to and. The query would then be passed to Bag of Words mode, which would attach no special operator significance and would therefore retrieve documents containing dog and and.
- Term proximity can boost the relevancy ranking in banner search.
- Automatic spelling correction is applied only in banner search.

F.7 About Advanced Search Behavior

Advanced search behavior is intended to support complex, precise queries. Therefore it generally does not employ the automatic broadening features of banner search, such as broad cross-field searching or automatic spell correction. Stemming, however, is applied in advanced search.

The Text Search portion of advanced search will search across name, description and full text content. Additional property criteria are applied only to the fields specifically selected in each criterion.

User queries that cause syntax errors in Internet Style mode or Query Operators mode will display an error message in the user interface; the search will not fall back to Bag of Words mode.

G

Oracle WebCenter Console for Microsoft SharePoint

This appendix describes Oracle WebCenter Console for Microsoft SharePoint, which allows you to crawl and index items from a Microsoft Office SharePoint Server (MOSS) or Windows SharePoint Services (WSS) site or site collection. It also allows you to crawl a list of MOSS or WSS sites specified by an RSS feed.

> **Note:** For information on setting up Oracle WebCenter Console for Microsoft SharePoint content sources, crawlers, and jobs, see Section 7, "Managing Portal Content," or *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Interaction for Windows*.

This appendix includes the following sections:

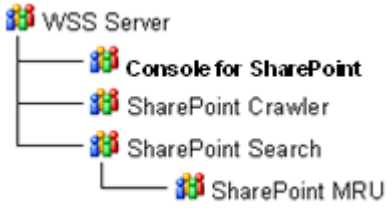
- Section G.1, "Representing Microsoft SharePoint Items in the Portal"
- Section G.2, "Accessing Microsoft SharePoint Items and the Console for SharePoint Community"
- Section G.3, "Opening Microsoft SharePoint Documents"
- Section G.4, "Customizing Oracle WebCenter Console for Microsoft SharePoint Portlets"

G.1 Representing Microsoft SharePoint Items in the Portal

Microsoft SharePoint items crawled into the portal are represented as standard portal folders and documents, and can be viewed and accessed like any other document that has been imported into the portal. The SharePoint crawler does apply some special properties to Microsoft SharePoint items to help differentiate them from other items.

G.1.1 Microsoft SharePoint Site Structure and Portal Knowledge Directory Folders

Assume your Microsoft SharePoint site is structured as depicted below. In addition to the subsites represented by each node, each site by default also contains announcements, discussions, documents, events, and tasks.



If the crawler was set to mirror folder structure of the Microsoft SharePoint site, each Microsoft SharePoint site is represented as a folder with the prefix **[Site]**, differentiating folders representing Microsoft SharePoint sites from folders representing Microsoft SharePoint list types. Each **[Site]** folder contains subfolders for each list type found on that Microsoft SharePoint site. For example, all documents in the **SharePoint Crawler** site are located in the **Shared Documents** folder under the **[Site] SharePoint Crawler** site folder.

If the crawler is configured not to mirror the source folder structure, all of the items will be stored in the same folder. Microsoft SharePoint site or list item type subfolders will not be created.

G.1.2 Microsoft SharePoint Items and Portal Documents

In addition to crawling in document properties, the SharePoint crawler adds special SharePoint specific properties to Microsoft SharePoint content crawled into the portal. This facilitates searching for Microsoft SharePoint items in the portal. The properties added are:

- **WSS Document URL** – The URL of the item in the Microsoft SharePoint site.
- **WSS Icon** – Used to display appropriate SharePoint icon in the portal.
- **WSS Last Modified** – The date and time the Microsoft SharePoint item was last modified in Microsoft SharePoint.
- **WSS Object Type** – The type of Microsoft SharePoint item represented by this document.
- **WSS Property Page URL** – The URL of the properties page of the item in the Microsoft SharePoint site. This value is the same as the WSS Document URL for all Microsoft SharePoint items except for documents.
- **WSS Site** – The name of the host Microsoft SharePoint site.

G.2 Accessing Microsoft SharePoint Items and the Console for SharePoint Community

Microsoft SharePoint items crawled into the portal can be accessed using standard portal methods, such as browsing the Knowledge Directory or using search. If a user runs a general search in the portal, they will see Microsoft SharePoint items along with results from other sources.

The Console for SharePoint community is provided to allow users to run simple searches that return only Microsoft SharePoint items.

G.2.1 Console for SharePoint Community

The Console for SharePoint community contains portlets to search and access Microsoft SharePoint items. It is meant as a starting point to access Microsoft SharePoint resources; however, the Oracle WebCenter Console for Microsoft SharePoint portlets are not bound to the Console for SharePoint community. The portlets can be used in any community or user My Page.

The Console for SharePoint community can be customized like any other portal community.

G.2.2 SharePoint Search Portlet

The SharePoint Search portlet allows users to enter a search term and returns the results in the portlet body itself.

- The portlet displays 10 results at a time.
- The icon to the far left identifies the type of Microsoft SharePoint item that is returned.
- The Name column displays the name of the document as stored in the portal.
- The Site column displays the Microsoft SharePoint site where the source item is stored.
- The details icon always points to the properties page of the Microsoft SharePoint item regardless of the click-through setting of the associated content source or portlet itself.
- The **Next>>** link at the bottom right pages to the next 10 results.

G.2.2.1 Opening Microsoft SharePoint Items Through the Portlet

When users click on the name of a Microsoft SharePoint item in the portlet, the Microsoft SharePoint item is opened using the WSS Document URL property. How the Microsoft SharePoint item is finally displayed is controlled by MOSS or WSS and not the portal. Security is also handled by the interaction of the browser and MOSS or WSS and is not controlled by the portal or portlet.

Note: This portlet does not follow the Document Display Options setting in My Account -> Display Options. This is to mimic the behavior of WSS and MOSS more closely.

G.2.2.1.1 SharePoint Search Portlet and Overriding Click-through Options If the SharePoint Search portlet is accessed through a community, the portlet can be configured to override the clickthrough behavior specified in the SharePoint content source and set by the crawler. This can be set in the portlet's community preferences.

Since this a community preference, the setting can be different for each community where this portlet is used. This setting only applies when the portlet is accessed from a community: if the portlet is on a My Page, it will follow the setting on the documents' content source.

G.2.2.1.2 Customizing the SharePoint Search Portlet The SharePoint Search portlet is essentially a pre-concerted advanced search portlet that allows end users to specify the actual search term. These search settings can be configured via the administrative preferences of the SharePoint Search portlet. The search settings can be modified to meet the specific needs of the deployment.

While most of the criteria that can be specified are the same as in an advanced search, the default WSS Site criteria is special to this portlet. The criteria "**WSS Site Contains Text**" indicates that only items where the value WSS Site is not blank are returned. The SharePoint crawler automatically populates the WSS Site property during import. Non-SharePoint items will not have the WSS Site value populated. If this criteria is removed, searches from this portlet will return non-SharePoint items as well.

Results can be narrowed even further by adding criteria such as WSS Object Type. For example, if the criteria "**WSS Object Type Contains Document**" is added, only Microsoft SharePoint documents will be returned.

Administrative preferences are specific to an instance of a portlet, and can be different for different copies of the portlet. For example, if there are five copies of the portlet object, they can all be configured to search based on different criteria.

G.2.2.2 Most Recently Used SharePoint Items Portlet (MRU)

The Most Recently Used SharePoint Items portlet displays the last ten items that were accessed by a specific user through all SharePoint Search portlets or the MRU portlet itself. The last item accessed will be placed at the top of the list. The portlet displays the last ten items accessed by the current user, not by all users who access Microsoft SharePoint items through the portal.

- The portlet displays the last ten items accessed.
- The icon to the far left identifies the type of Microsoft SharePoint item that was accessed.
- The Name column displays the name of the document as stored in the portal.
- The Site column displays the Microsoft SharePoint site where the source item is stored.
- The details icon always points to the properties page of the Microsoft SharePoint item regardless of the click-through setting of the associated content source or portlet itself.

Clickthrough behavior is determined by the content source. The clickthrough behavior overrides settings of the SharePoint Search portlet do not apply to the MRU portlet.

> **Note:** This portlet does not follow the Document Display Options setting in My Account -> Display Options. This is to mimic the behavior of WSS and MOSS more closely.

Even though there can be more than one SharePoint Search portlet, there should only be one MRU portlet. The MRU portlet will display the last items accessed by a user from all SharePoint Search portlets.

G.3 Opening Microsoft SharePoint Documents

The portal allows the clickthrough behavior for Microsoft SharePoint documents to be either directly to the document itself or to the properties page of the document.

The default clickthrough behavior of SharePoint content sources is to open the Microsoft SharePoint item's properties page. The properties page gives the end user more information and functions than opening the document directly. The SharePoint properties page gives access to the following options:

- The document can be opened and edited by clicking on the Name link.

- The document properties can be edited, the document deleted, discussion can be started, etc.
- Version information is displayed, for example user, time, and so on.
- The WSS Site and the folder that the document is located is displayed.
- The URL to go directly to the document is available in the address bar of the browser.

The drawback to clicking through to this page is that it requires an extra click by the end user to view the document.

The benefit to opening the document directly on clickthrough from the SharePoint Search or MRU portlet is that documents are displayed immediately. The drawback is that it is more difficult to determine where the document is located (which folder in which site) or perform the actions available from the properties page.

A compromise could be to set the SharePoint content source to open to the properties page and set SharePoint Search portlets to open documents directly. This allows users to access Microsoft SharePoint items from the Knowledge Directory or general search and still get the necessary Microsoft SharePoint object information. Users who access the document from the SharePoint Search portlet open the document directly and can access the properties by clicking the details icon on the portlet results.

G.4 Customizing Oracle WebCenter Console for Microsoft SharePoint Portlets

The UIs of the Oracle WebCenter Console for Microsoft SharePoint portlets can be controlled by a custom stylesheet that is loaded with the banner in the Console for SharePoint community. The styles that control the portlets are:

```
/* column controls */
.MRUIconColumn {width: 25px;}
.MRUNameColumn {width: 70%;}
.MRUSiteColumn {width: 30%}
.MRUPropColumn {width: 20px;}

.SearchIconColumn {width: 25px;}
.SearchNameColumn {width: 70%;}
.SearchSiteColumn {width: 30%;}
.SearchPropColumn {width: 20px;}
```

While it is not possible to add new columns, it is possible to remove columns by changing the styles. For example, to remove the "Site" column, replace the value {width: 30%} to {display: none} for that style.

The stylesheet is located in the following folder:

PT_HOME\ptimages\imageserver\sharepoint\private\css

You can copy the styles to your custom style sheets for use in areas where the Console for SharePoint banner is not used.