webMethods

webMethods Portal

Administrator's Guide

VERSION 6.5.2

webMethods, Inc.
South Tower
3877 Fairfax Ridge Road
Fairfax, VA 22030
USA
703.460.2500
http://www.webmethods.com

Document ID: PRTL-AG-652-20060330

Contents

About This Guide

This guide explains how to use the Administration Dashboard to configure and manage webMethods Portal. In addition, the guide explains how to configure Portal servers and organize them into Portal clusters. The guide describes how security is implemented in webMethods Portal and how to manage it.

Document Conventions

Convention	Description
Bold	Identifies elements on a screen.
Italic	Identifies variable information that you must supply or change based on your specific situation or environment. Identifies terms the first time they are defined in text. Also identifies service input and output variables.
Narrow font	Identifies storage locations for services on the webMethods Integration Server using the convention *folder.subfolder:service*.
`Typewriter font`	Identifies characters and values that you must type exactly or messages that the system displays on the console.
UPPERCASE	Identifies keyboard keys. Keys that you must press simultaneously are joined with the "+" symbol.
\	Directory paths use the "\" directory delimiter unless the subject is UNIX-specific.
[ ]	Optional keywords or values are enclosed in [ ]. Do not type the [ ] symbols in your own code.

Additional Information

The webMethods Advantage Web site at http://advantage.webmethods.com provides you with important sources of information about webMethods components:

- **Troubleshooting Information.** webMethods provides troubleshooting information for many webMethods components in the webMethods Knowledge Base.
- **Documentation Feedback.** To provide documentation feedback to webMethods, go to the Documentation Feedback Form on the webMethods Bookshelf.
- **Additional Documentation.** All webMethods documentation is available on the webMethods Bookshelf.

webMethods

CHAPTER 1

Introduction to Portal Administration

Starting and Stopping webMethods Portal

If you are running webMethods Portal Server Configurator to create a new webMethods Portal instance or edit an existing one, you can start or stop the server from the Configurator user interface. There are other ways to start and stop webMethods Portal, described in the following sections.

Starting and Stopping on Windows

If webMethods Portal is configured on Windows computers as a service, you can use the following commands for starting and stopping.

To start webMethods Portal on a Windows host

1. Open the Control Panel and double-click the Administrative Tools icon.
2. In the Administrative Tools window, double-click the Services icon.
3. In the Services window, double-click the service named webMethods Portal Server.
4. Click **Start**.

   After a few seconds, the status changes to Started.

To stop webMethods Portal on a Windows host

1. Open the Control Panel and double-click the Administrative Tools icon.
2. In the Administrative Tools window, double-click the Services icon.
3. In the Services window, double-click the service named webMethods Portal Server.
4. Click **Stop**.

   After a few seconds, the status changes to Stopped.

Starting and Stopping from the Command Line

You can start or stop webMethods Portal at a command prompt on either Windows or UNIX computers.

To start or stop webMethods Portal

1. At a command line prompt, type the following command to move to the webMethods Portal home directory:

   ```
   cd webMethods_install_dir/Portal/server/default/bin
   ```

2 Type one the following commands:

Purpose	Operating system	Command
Start webMethods Portal in the same console window	Windows	`run.bat`
	UNIX	`run.sh`
Start webMethods Portal in a new console window	Windows	`startup.bat`
	UNIX	`startup.sh`
Stop webMethods Portal	Windows	`shutdown.bat`
	UNIX	`shutdown.sh`

For more information on controlling webMethods Portal from the command line, see "Running a Portal Server from the Command Line" on page 303.

Getting Started as webMethods Portal Administrator

The following sections describe some basic tasks you can perform to get started using webMethods Portal:

Tasks	Described here...
Log in	"Logging Into webMethods Portal" on page 19
Log out	"Logging Out of webMethods Portal" on page 20
Change your password	"Changing Your Password" on page 20

Logging Into webMethods Portal

webMethods Portal has a user interface that you access using a Web browser.

To log into webMethods Portal

1 Access the webMethods Portal Login page by entering a URL in a Web browser:

`http://host:port`

where:

- *host* is the host name of the machine on which webMethods Portal is installed.

- *port* is the port on which webMethods Portal listens for incoming requests. The default port for webMethods Portal is 8080.

For example, if the host name is `rubicon.company.com` and it uses the default port (8080), type the following URL:

```
http://rubicon.company.com:8080
```

2 In the **User Name** field of the Login page, type the webMethods Portal administrator user name: `PortalAdmin`.

Note: When logging in, the value you specify in the user name is case insensitive. However, after logging in, webMethods Portal uses the case of the user name that is defined in your user account. For example, if the user account is defined as "PortalAdmin," you can log in using "portaladmin." When webMethods Portal needs to use the user name, for example, for HTTP authentication, it uses the version defined in the user account, which is "PortalAdmin."

3 In the **Password** field type the portal administrator password, which by default is `admin`.

Important! To keep webMethods Portal secure, you should change the default portal administrator password. For instructions about how to change the password, see "Changing Your Password" on page 20.

4 Click **Login**.

After you log in, Portal displays the portal administrator home page.

Logging Out of webMethods Portal

Perform the following procedure to log out of webMethods Portal.

To log out of webMethods Portal

Click the **Logout** link, which is located at the top of all Portal pages.

Changing Your Password

Change your password by editing the fields on the **User Information** tab of your profile.

To change your password

1 Click the **My Profile** link, which is located at the top of all Portal pages.

2 On the **User Information** tab, type your new password in the **Password** field.

3 In the **Confirm Password** field, type your new password again for confirmation.

4 Click **Apply**.

Introduction to the Administration Dashboard

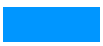
webMethods Portal includes an Administration Dashboard that allows portal administrators to efficiently manage their portal deployments. It also delivers a powerful framework that allows portal administrators to selectively delegate specific administrative functions to other administrators or IT staff. The Administration Dashboard provides one-stop access to all of the following administrative functions that are typically needed to manage a portal deployment:

- **Portal Analysis:** contains administrative portlets for monitoring your portal deployment, viewing log files for troubleshooting, and analyzing portal usage patterns to optimize portal performance.
- **Portal Configuration:** contains administrative portlets for managing and configuring portal components, such as the underlying portal directory, data sources, installed components, events, and so forth.
- **Portal Content:** contains administrative portlets for managing the portal's content management system.
- **Portal User Interface:** contains administrative portlets for managing the look-and-feel of your portal deployment. This category includes the following portlets: Shell Administration, Skin Administration, and Start Page Administration.
- **Portal User Management:** contains administrative portlets for managing portal users and delegated administrators, as well directory services.

This chapter describes these categories in more detail.

Accessing the Administration Dashboard

Note: You must have Administrative credentials to access the Administration Dashboard.



To access the Administration Dashboard from the default Administrator's Start page

1 Log in to webMethods Portal using an account with Administrator credentials. This displays the portal Start page.

2 Click the Administration link from the navigation menu at the top of the page.

3 Click the Administration Dashboard folder from the Start page.

The Administration Dashboard User Interface

The Administration Dashboard provides a list of administrative categories with a series of portlets for managing a Portal server instance. Select one of the administration categories to view the portlets that are available for each main category.

The following tables describes the portlets available on the Administration Dashboard. Details on how to use each of the portlets are available in later sections of this book.

Portal Analysis

Name	Description
Logging Configuration	Controls logging for the Portal server. You can set thresholds for individual categories of logging information. In addition, you can set the collector threshold for the View Logging Messages portlet. See "Controlling Portal Logging" on page 150.
Session Monitor	Enables you to monitor real-time user activity for a portal deployment and send status messages to active portal users by means of e-mail. For active users, a portal administrator can view a user's profile information and send the user e-mail directly from within this portlet. See "Monitoring Real-Time User Activity" on page 156.
View Logging Messages	Allows you to search for the occurrence of log messages that have been collected by the Logging Collector. In the View Logging Messages portlet, you can set search criteria, view the messages, and clear the search index. See "Viewing Logging Messages" on page 153.

Portal Configuration

Name	Description
Alias Management	Enables you to manage URL aliases to portal objects. You can create, view, edit, or delete custom aliases. "Managing Portal Aliases" on page 166.
Cluster Administration	Enables you to specify the logical server names of servers within a cluster and to select one or more portal roles for which the server is responsible. See "The Cluster Administration Portlet" on page 284.
DataSource Administration	Enables you to connect to external databases and make them available to the portal. From this portlet, you can add a new data source, view non-modifiable information about the portal metadata repository (the default data source), and view a short description of each data source. See "Managing External Data Sources" on page 174.
Email Administration	Enables you to configure the mail server settings used by the system when processing e-mail. You can specify the mail server (the hostname of the SMTP server) used to route e-mail messages, the SMTP port, the sender name and the sender address (the reply-to-address attached to any outgoing notifications). See "Managing E-Mail Settings" on page 181.
HTTP Header Authentication Administration	Enables you to configure webMethods Portal to accept External HTTP authentication credentials from third party security and access control products, such as Computer Associates or Oblix. These credentials are case-sensitive. Common examples are sm_user or SM_USER, depending on your platform and Web server. See "Configuring External Configuration Credentials" on page 181.
Install Administration	Enables you to install and register portal components, such as portlets, or deployable packages, with the Portal server. See "Deploying Portal Components" on page 184.
Manage Components	Enables portal administrators to globally configure and manage how portlets and portal objects called Extended Types or Dynamic Business Objects (DBOs) are made available to end users. A *DBO* is a portal object that is created from existing base level portal objects such as content, folders, forms, links, and portlets.
SAML Authentication Administration	Enables you to configure a Portal server as a target for single sign-on using SAML (Security Assertion Markup Language). See "Setting up Single Sign-On" on page 190.

Name	Description
Security Realms Administration	Enables you to manage Security Realms used on the Portal server. Security Realms allow you to manage permissions for resources based on users, groups, or roles, making it easier to manage large portals. See "Using Security Realms" on page 139.
System Information	Provides a wealth of information about the current state of the Portal server. The portlet gathers the information dynamically at the time you open each tab.

Portal Content

Name	Description
Content Migration Wizard	Allows portal administrators to migrate portal content from one Portal server instance to another; that is. migrating from development to staging to production. This portlet can be used to migrate the following types of portal content - documents, folders, external links, internal links (using aliases), portal pages (including layouts), portlets, Dynamic Business Objects (DBOs), permissions, subscriptions, and portlet wiring properties. See "Migrating Portal Content" on page 200.
Content Service	Enables portal administrators to manage the storage locations available for content published to the portal. Content published to the portal is physically stored in the locations configured in the content service. See "Managing Content Storage" on page 203.
Group Subscriptions	Enables portal administrators to create subscriptions for Groups exposed by the underlying portal user directory (for example, LDAP or ADSI). Use this portlet to create new group subscriptions and manage existing subscriptions. See "Managing Group Subscriptions" on page 205.
Manage Subscriptions	Enables portal administrators to view existing subscriptions within the Portal server. It allows an administrator to view subscriptions for a given user, resource, group, or group subscription created by any given user. See "Managing Subscriptions for Individual Users" on page 205.
Publish	Enables portal administrators to publish content (files, folders, forms, links, and portlets) to the portal. The Publish portlet is intended for use by portal administrators and power users. It allows an administrator to publish custom portal objects (Dynamic Business Objects) built using the portal's extensibility framework. See "Publishing Portlets as an Administrator" on page 207.
Search Admin	Enables portal administrators to manage the search service configuration and to manually synchronize the search engine(s) with the current portal content. See "Managing the Search Engine" on page 208.

Portal User Interface

Name	Description
Manage Login Page Rules	Enables portal administrators to define governing the login page to which a given user, group, or role should be directed. See "Creating Login Page Rules" on page 217.
Manage Rendering Rules	Enables portal administrators to define rendering and personalization rules for portal objects, such as folders and portal pages. Rendering rules dictate the visual layout of items, such as portlets, content, links, and so forth, within a given container. webMethods Portal provides a number of renderers that can be used to define rendering rules. See "Creating Rendering Rules" on page 217.
Manage Shell Rules	Enables portal administrators and developers to define rules that determine what shell is displayed for a given user based on LDAP attributes or group membership, or for a given resource. Shell rules dictate the physical structure of your portal pages, similar to a template. See "Managing Shell Rules" on page 224.
Manage Skin Rules	Enables portal administrators and developers to define rules that determine what skin is displayed for a given user based on LDAP attributes or group membership, or for a given portal resource. Skin rules dictate the look and feel (graphics, logos, colors, fonts, and so forth) for your portal pages. See "Managing Skin Rules" on page 222.
Shell Administration	Enables portal administrators to define personalization rules that govern what type of portal shell is applied to a given user, group or role. Additional information on shells can be found in the *webMethods Portal Design Guide*.
Skin Administration	Enables portal administrators to define personalization rules that govern what type of portal skin is applied to a given user, group, or role. Additional information on skins can be found in the *webMethods Portal Design Guide*.
Manage Start Page Rules	Enables portal administrators to define personalization rules that govern what the default Home page is for a given user, group, or role. See "Creating Start Page Rules" on page 219.

User Management

Name	Description
Directory Services Administration	Enables portal administrators to manage directory services on the portal. See Chapter 3, "External Directory Services" for more information.
Locate a User's Home Folder	Enables portal administrators to locate and browse to a user's personal folders. This feature can be especially helpful when items become unavailable to the user because of permission changes or content removal when a user is no longer actively using the portal. See "Locating a User's Home Folder" on page 65.
Principal Profile Administration	The Principal Profile Administration portlet allows you to choose which Principal Attribute Providers to display on a Profile page and the order in which they appear. See Chapter 6, "Attribute Providers" for more information.
Managing Users, Groups, and Roles	You can perform a variety of management activities with regard to users, groups, and roles. See Chapter 4, "User and Group Management" and Chapter 5, "Role Management" for more information.

Delegating Administrative Functions

By default, only portal administrators have access to the Administration Dashboard. However there are several ways that administrative responsibilities can be delegated to other administrators.

To delegate specific administrative tasks, the primary portal administrator can modify the permissions of the portlets contained within the Administration Dashboard to selectively allow other administrators access to them.

For example, the primary portal administrator can delegate the Administration portlet to another portal administrator, grant them access to it, and allow them to only view the three target Administration portlets that the primary administrator wants them to access. As a result, that administrator will see only those three portlets in the Administration Dashboard when they login to webMethods Portal.

Creating Custom Portal Pages for Delegated Administrators

Another way for a portal administrator to share administrative tasks is to create and assign an Administration portal page.

Instead of using the Administration Dashboard, a portal administrator publishes a portlet to a portal page and grants another administrator access to the portlet on that portal page.

Note: To grant access to portlets, a portal administrator must edit the permissions for the individual portlets through the Manage Components in the Administration Dashboard. See "Managing Portal Objects" on page 187 for instructions.

The chapters that follow provide step-by-step instructions for using each of the administrative portlets described in this chapter.

webMethods

CHAPTER 2

Using the Portal Server Configurator

What is the Configurator?

The webMethods Portal Server Configurator is a tool that allows you to initialize or edit the configuration of webMethods Portal, or delete a server you no longer need. When you perform an installation of Portal, you use the Configurator as described in the *webMethods Installation Guide*. After you have initialized Portal, you can use the Configurator as described in this chapter.

Note: Run the Configurator on the same machine where you want to install Portal or modify the configuration.

Guidelines for Multiple Portal Servers

Each Portal server must have its own external resources. The following guidelines apply:

- Each Portal server must have its own portal database; for a given database server, the following Configurator entries must be unique among all Portal servers, regardless of which machine they are on:

Configurator tab	Field name
MSSQL	Portal database User name Portal database name
Oracle	Portal database User name Portal Tablespace name

- Each Portal server that uses JMS messaging must have its own JMS provider; with webMethods Broker running on a given host, this Configurator entry must be unique among all Portal servers, regardless of which machine they are on:

Configurator tab	Field name
Broker	webMethods Broker JMS provider name

- For Portal servers running concurrently on the same machine, the following host/port number combinations, if used, must be unique among all Portal servers:

Configurator tab	Field name
Portal (Jetty Web server)	**Jetty AJP13 Listener Host/Port** **Jetty HTTP Listener Host/Port** **Jetty HTTPS Listener Host/Port** **Portal RMI Listener Host/Port**
IIS	**IIS Web server Host/Port**
Apache	**Apache Web server Host/Port**

These parameters are described in more detail in the *webMethods Installation Guide* and in "Editing an Existing Portal Server Configuration" on page 32.

Starting the Configurator

To start the Configurator, follow these steps:

To start the Configurator

1 Start the Portal Configurator as follows:

System	Action
Windows	On the **Start** menu, point to **Programs**, point to **webMethods**, point to **Tools**, then click **webMethods Portal Server Configurator**.
UNIX	Enter this command: `/webMethods_install_dir/Portal/tools/configurator/run.sh`

The webMethods Portal Server Configurator window appears.

2 Select one of the following options:

This option...	Does this...
Create Portal Server	Creates a new Portal server instance in addition to the default Portal server. See "Creating a New Portal Server" on page 45.
Edit Portal Server	Allows you to modify the configuration of an existing Portal server. See "Editing an Existing Portal Server Configuration" next in this chapter.
Delete Portal Server	Deletes an existing Portal server instance. See "Deleting a Portal Server" on page 46.

3 Click **Start Wizard**. The Configurator changes its display to match the option you have selected.

Editing an Existing Portal Server Configuration

To edit an existing Portal server, follow these steps:

To edit an existing Portal server configuration

1 Start the Configurator as described in "Starting the Configurator" on page 31, select the **Edit Portal Server** option, and click **Start Wizard**, the Configurator displays the **Server Instance** tab. Do the following:

2 In the **Portal Server Instance** list of the **Server Instance** tab, select the name of the Portal server for which you want to edit the configuration.

3 Move to the tab you want to edit, using either of these methods:

To do this...	Do this...
Move consecutively among the tabs	Click **Next** to move forward or click **Back** to move backward.
Move directly from one tab to another	Click the title of the destination tab.

The various tabs in the Configurator are described in the following sections.

The General Tab

Entries in the **General** tab determine the content of remaining tabs in the Configurator.

Edit the **General** tab as follows:

Parameter	Setting	
Database server type	Type of database server the Portal server is to use.	
	For this database server type...	**Select...**
	Microsoft SQL Server 2000 SP3	**myssql**
	Oracle 9.2	**oracle**
Messaging provider type	Type of Java messaging system (JMS) the Portal server is to use to monitor user and system-level events. If the Portal server is not part of a cluster of Portal servers, you do not need a JMS provider. If the Portal server is part of a cluster, you must use webMethods Broker.	
	For this JMS type...	**Select...**
	webMethods Broker	**broker**
	None	**none**
Web server type	Type of Web server for the Portal server to use to give clients access through a network.	
	For this Web server type...	**Click...**
	Jetty internal server	**internal**
	Internet Information Server (IIS)—Windows computers	**iis**
	Apache—UNIX computers	**apache**

The Components Tab

In the **Components** tab, select or clear components of webMethods Portal to be deployed when the Portal server is initialized. It is recommended that for an initial installation of the default server, you use the default set of Portal components.

Important! Only an experienced portal administrator should attempt to configure a Portal server instance with less than the default set of Portal components. The absence of components can lead to loss of necessary functions.

Component Group	Purpose
Portal Services	A set of portlets that provide a variety of services, including subscriptions and notifications, version control, and support for directory services.
Administration Components	A set of portlets needed for administration of the Portal services, including portal analysis, configuration, and content management.
Default Components	A set of portlets that provide basic elements of the Portal user interface and let you manage communication between portals and external resources, such as WebDAV or FTP servers
Default Content	A set of portlets providing default webMethods content for the Portal server.
Portal Development	A set of portlets useful for portal developers. Includes the Portlet Developer plug-in that can be installed on the Eclipse Platform.
Samples	A set of samples and demonstrations of portal technology. Samples include source code.
Extras	A set of portlets that add capabilities to a portal page or enable the proper functioning of other portlets.
Mobile UI Support	A set of portlets that support the delivery of HTML pages to mobile devices.

The MSSQL Tab

Important! Whenever you initialize a server instance for the first time or upgrade an existing server instance to a newer version or service pack, the server may need to create additional schema objects in the database. For this reason, you must ensure that the database user has privileges to create or alter schema objects. These privileges are not otherwise required for normal server operation and can be revoked for security or other reasons.

Note: If one of the other database tabs is displayed instead of the **MSSQL** tab, navigate to the **General** tab and change the **Database server type** parameter to **mssql**.

webMethods Portal uses an external database server to store portal information. Multiple server instances can share a single database server, but each server instance must have its own database, distinguished by a name, user name, and schema that is unique among Portal databases.

Entries in the **MSSQL** tab provide information needed by the Configurator to create or modify the Microsoft SQL Server database that will manage Portal.

Note: Portal does not support case-sensitive collations in Microsoft SQL Server. During a custom installation of SQL Server it is possible to select an option for case-sensitive collations. Do *not* select this option.

Note: If you do not have database administrator access to the database server, have the administrator create a user name and an empty database for you.

Edit the **MSSQL** tab as follows:

Parameter	Setting
MSSQL Server Host/Port	To change from one database server to another, in the left field, type the name or IP address of the machine that hosts the database server Portal is to use. In the right field, type the port Portal uses to communicate with the database server. The default port number is 1433.
Portal database User name	Type a user name that is valid for the database server.
Portal database User password	In the left field, type a valid password for the portal database user. In the right field, retype the password to confirm it.
MSSQL Server administrator name	Option 1 only. Type the administrator user name for the database server.
MSSQL server Administrator password	Option 1 only. In the left field, type the administrator password for the database server. In the right field, retype the password to confirm it.
Portal database name	Type the name of the Portal database.

When using the Configurator in edit mode there are three actions you can take with respect to the Portal database by selecting one of the **Initialize Portal Database** options:

Option	Purpose
1. YES. Create a new Portal database, User, and Schema	Switch to a new database server, change to a new database user, or to reset an existing Portal database to its default state. All existing data is lost. You need database administrator rights. To create a new Portal database, change the parameters in the **MSSQL** tab, as described in the preceding table, and click **Next**. You can click **Validate MSSQL Administrator connectivity** to verify the administrator name and password, and connectivity to the database server.
2. YES. Create a new Schema for an existing Portal database	Create a new schema in an empty Portal database. You need database user rights. To use this option have the database administrator erase the schema in the existing database. To create a new schema in the Portal database, change the parameters in the **MSSQL** tab, as described in the preceding table, and click **Next**. You can click **Validate Portal User connectivity** to verify the database user name and password, and connectivity to the database server.
3. NO. Validate connectivity to an existing Portal database	Check validity of the connection to the Portal database that is currently associated with Portal. Click **Validate Portal user and database connectivity**.

If for some reason you do not want to have the Configurator create the Portal database automatically, you can run the script from a command line. For information on the command syntax, click **How to Run SQL Scripts manually** at the bottom of the **MSSQL** tab.

The Oracle Tab

Important! Whenever you initialize a server instance for the first time or upgrade an existing server instance to a newer version or service pack, the server may need to create additional schema objects in the database. For this reason, you must ensure that the database user has privileges to create or alter schema objects. These privileges are not otherwise required for normal server operation and can be revoked for security or other reasons.

Note: If one of the other database tabs is displayed instead of the **Oracle** tab, navigate to the **General** tab and change the **Database server type** parameter to **oracle**.

webMethods Portal uses an external database server to store portal information. Multiple server instances can share a single database server, but each server instance must have its own database, distinguished by a name, user name, and tablespace that is unique among Portal databases.

Entries in the **Oracle** tab provide information needed by the Configurator to create or modify the Oracle database that will manage Portal.

Note: If you do not have database administrator access to the database server, have the administrator create a user name and an empty database for you.

Important! On the Oracle system, the NLS_LENGTH_SEMANTICS initialization parameter must be set to BYTE (a default value for most Oracle installations). Setting this parameter to CHAR prevents Portal from initializing successfully. Work with the Oracle database administrator to make certain this initialization parameter is set properly.

Edit the **Oracle** tab as follows:

Parameter	Setting
Oracle Server Host/Port	To change from one database server to another, in the left field, type the name or IP address of the machine that hosts the database server Portal is to use. In the right field, type the port Portal uses to communicate with the database server. The default port number is 1521.
Portal database User name	Type a user name that is valid for the database server.
Portal database User password	In the left field, type a valid password for the portal database user. In the right field, retype the password to confirm it.
Oracle Instance System Identifier (SID)	Type the identifier to be used for connection to the database.
Oracle Administrator name	Option 1 only. Type the administrator user name for the database server.
Oracle Administrator password	Option 1 only. In the left field, type the administrator password for the database server. In the right field, retype the password to confirm it.
Portal Tablespace name	Type the name of the Portal tablespace.

When using the Configurator in edit mode there are three actions you can take with respect to the Portal database by selecting one of the **Initialize Portal Database** options:

Option	Purpose
1. Yes. Create a new Portal Tablespace, User, and Schema	Switch to a new database server, change to a new database user, or to reset an existing Portal database to its default state. All existing data is lost. You need database administrator rights. To create a new Portal database, change the parameters in the **Oracle** tab, as described in the preceding table, and click **Next**. You can click **Test Connection (Admin Credentials)** to verify the administrator name and password, and connectivity to the database server.
2. Yes. Create Portal Schema only	Create a new schema in an empty Portal tablespace. You need database user rights. To use this option, have the database administrator erase the schema in the existing tablespace. To create a new schema in the Portal database, change the parameters in the **Oracle** tab, as described in the preceding table, and click **Next**. You can click **Test Connection to Portal tablespaces (User Credentials)** to verify the database user name and password, and connectivity to the database server.
3. No. Validate connectivity ONLY	Check validity of the connection to the Portal database that is currently associated with Portal. Click **Test Connection to Portal Database (User Credentials)**.

If for some reason you do not want to have the Configurator create the Portal database automatically, you can run the script from a command line. For information on the command syntax, click **How to Run SQL Scripts manually** at the bottom of the **Oracle** tab.

The DB2 Tab

Important! Whenever you initialize a server instance for the first time or upgrade an existing server instance to a newer version or service pack, the server may need to create additional schema objects in the database. For this reason, you must ensure that the database user has privileges to create or alter schema objects. These privileges are not otherwise required for normal server operation and can be revoked for security or other reasons.

Note: If one of the other database tabs is displayed instead of the **DB2** tab, navigate to the **General** tab and change the **Database server type** parameter to **db2**.

webMethods Portal uses an external database server to store portal information. Multiple Portal instances can share a single database server, but each server instance must have its own database, distinguished by a name, user name, and tablespace that is unique among Portal databases.

Entries in the **DB2** tab provide information needed by the Configurator to create or modify the DB2 used by Portal.

Note: Before you can configure a Portal database on DB2, the database administrator must create a user name within a new or existing database. The administrator must grant the user access to a default user temporary tablespace that is required for temporary tables used by Portal.

Edit the **DB2** tab as follows:

Parameter	Setting
DB2 Server Host/Port	To change from one database server to another, in the left field, type the name or IP address of the machine that hosts the database server Portal is to use. In the right field, type the port Portal uses to communicate with the database server. The default port number is 50000.
Portal database User name	Type a user name that is valid for the database server.
Portal database User password	In the left field, type a valid password for the portal database user. In the right field, retype the password to confirm it.
DB2 Server Administrator name	Not available for DB2.
DB2 Server Administrator password	Not available for DB2.
Portal Database name	Type the name of the Portal database.

When using the Configurator in edit mode there are two actions you can take with respect to the webMethods Portal database by selecting one of the **Initialize Portal Database** options:

Option	Purpose
2. Yes. Create Portal Schema for an existing database user.	Create a new schema for the specified user. If the schema already exists, you are prompted to recreate it. You can click **Validate Portal User Connectivity** to verify the database user name and password, and connectivity to the database server.
3. No. Validate connectivity to an existing Portal database.	Check validity of the connection to the webMethods Portal database that is currently associated with this server instance. Click **Validate Portal database and User Connectivity**.

If for some reason you do not want to have the Configurator create the Portal database automatically, you can run the script from a command line. For information on the command syntax, click **How to Run SQL Scripts manually** at the bottom of the **DB2** tab.

The Broker Tab

webMethods Portal can use a Java messaging system (JMS) to monitor user and system-level events. If you are not using Portal in a cluster environment, you do not need a JMS provider to monitor user and system-level events. If Portal is clustered, you must use webMethods Broker as your JMS provider; the cluster requires its own dedicated Broker.

Note: Although the Broker can be installed on a separate computer, you must have the following items installed on the same machine as Portal:

Broker Client Java API
Command Line Tools
JMS Client API

You can install these items at the same time you install Portal.

Note: The Broker must be running at the time you run the Configurator.

To edit the Broker tab

1 In the **Broker JMS provider Host/Port** field on the left, type the name or IP address of the machine that hosts the Broker JMS provider for Portal to use.

Note: Do not use `localhost` to identify the host. Doing so causes the JMS provider to be available only to the instance of Portal residing on the same computer. Servers residing on other computers are locked out.

2 In the field on the right, type the port for webMethods Portal to use to communicate with the JMS. The default port number is 6849.

3 In the **webMethods Broker JMS provider name** field, type the name of the Broker to use. The default is Broker #1.

4 Click **Next** and then do one of the following:

If this happens...	Do this...
The Broker is initialized in a separate window and the Configurator displays the next tab.	The JMS provider is configured. Perform other editing tasks as needed.
The Configurator displays the message **Configurator cannot connect to the server**.	Make sure the Broker is running and that the host and port number you provided in the **Broker** tab are correct. Click **Next**.
The Configurator displays the message **The server requires manual configuration/initialization**.	The Broker is running but the JMS provider is not loaded or is not installed. Click **Yes** to learn how to load the JMS provider manually. For information on the webMethods JMS Administrator, see the *webMethods Broker Administrator's Guide*. With the JMS provider installed and loaded, click **Next**.

The IIS Tab

The internal Jetty Web server is required for the creation of a new Portal server, but you may want to use an external Web server in your particular environment. In Edit Mode on the **General** tab, you can select a **Web server type** of **iis**, which allows you to configure Internet Information Server (IIS) as the Portal Web server.

Note: The IIS Web server requires an AJP13 plug-in to communicate with the Portal server. The plug-in is included in the Portal software, but IIS needs to be configured to use it. See Appendix A, "Integrating webMethods Portal with External Web Servers" for more information.

On the **IIS** tab, do the following:

To edit the IIS tab

1. In the **IIS Web server Host/Port** field on the left, type the name or IP address of the machine that hosts the IIS Web server for this Portal server to use.
2. In the field on the right, type the port for the Portal server to use to communicate with the IIS Web server. The default port number is 80.
3. To determine if the connection to the IIS Web server is correct, click **Attempts to connect to the Web server using the current configuration settings**.
4. Click **Next** and then do one of the following:

If this happens...	Do this...
The next Configurator tab appears without error messages.	The IIS Web server is configured for use with the Portal server. Perform other editing tasks as needed.
The Configurator displays the message **IIS is not available. Either it is not running or the Website is disabled**.	Make sure the connection information in this tab is correct and that the IIS Web server is running.

The Apache Tab

The internal Jetty Web server is required for the creation of a new Portal server, but you may want to use an external Web server in your particular environment. In Edit Mode on the **General** tab, you can select a **Web server type** of **apache**, which allows you to configure Apache as the Portal Web server.

Note: The Apache Web server requires an AJP13 plug-in to communicate with the Portal server. The plug-in is included in the Portal software, but Apache needs to be configured to use it. See Appendix A, "Integrating webMethods Portal with External Web Servers" for more information.

On the **Apache** tab, do the following:

To edit the Apache tab

1 In the **Apache Web server Host/Port** field on the left, type the name or IP address of the machine that hosts the Apache Web server for this Portal server to use.

2 In the field on the right, type the port for the Portal server to use to communicate with the Apache Web server. The default port number is 80.

3 To determine if the connection to the Apache Web server is correct, click **Attempts to connect to the Web server using the current configuration settings**.

4 Click **Next** and then do one of the following:

If this happens...	Do this...
The next Configurator tab appears without error messages.	The Apache Web server is configured for use with the Portal server. Perform other editing tasks as needed.
The Configurator displays the message **Apache is not available. Either it is not running or the Website is disabled**.	Make sure the connection information in this tab is correct and that the Apache Web server is running.

The Portal Tab

Use the **Portal** tab to specify the hosts and port numbers through which the Portal server communicates. The Portal server uses Jetty as an internal Web server, but you can also use an external Web server such as ISS or Apache, in which case you have to identify the AJP13 port through which Jetty listens to the external server.

To edit the Portal tab

1 Enter values for the following parameters and perform the following tasks:

Parameter	Description
Jetty AJP13 Listener Host/Port	If you are using an external Web server, this parameter identifies the host and port number through which Jetty listens to the external server. To use this parameter, select **Enabled**. In the left field, type the host name or IP address. The default is the local host. In the right field, type the port number on which Jetty listens for AJP13 connections. The default is 8009.

Parameter	Description
Jetty HTTP Listener Host/Port	The port on the local host through which Jetty listens for requests. Enabled by default. The port number is 8080 by default.
Jetty HTTPS Listener Host/Port	The port on the local host through which Jetty listens for secure requests. As needed, select **Enabled** to specify an HTTPS listener and port. To use this parameter, select **Enabled**. In the left field, type the host name or IP address. The default is the local host. In the right field, type the port number on which Jetty listens for secure requests. The default is 8443.
Portal RMI Listener Host/Port	The port on which the Portal server listens for commands and communication from other Portal servers in a cluster. In the left field, type the host name or IP address. The default is the local host. In the right field, type the port number on which the Portal server listens. The default is 1097.
Default Log Level	The level of detail you want the Portal server to include in log messages: From the list, select **DEBUG**, **INFO**, **WARN**, or **FATAL**).
Check Portal Server readiness	Select this option to verify that the Portal server and registry ports are not being used by other processes.
Start webMethods Portal Server	Select this option to start or stop the webMethods Portal server application.Typically, you will run the Portal server as an application during portal development.
(Windows only) Install webMethods Portal Server as a Windows Service	Select this option to install or uninstall the Portal server as a Windows service. When installed as a service, the default Portal server starts and shuts down automatically when you start and shut down your system. Typically, you would install a production portal as a service.
(Windows only) Start webMethods Portal Windows Service	If you installed the Portal server as a Windows service, use this option to start this service.

2 Do one of the following:

To do this...	Do this...
Start the Portal server as a console application.	Click **Start webMethods Portal Server as a Console Application**.
Change the Portal server to a Windows service.	Click **Install Start webMethods Portal Server as a Windows Service**. In a separate window, the Configurator changes the Portal server to a Windows service. Click **Start webMethods Portal Windows Service**.

3 In the Information window, if you want to automatically open the default portal page in a browser window, click **Yes**. The Configurator starts the Portal server.

Note: Appendix B, "Running a Portal Server from the Command Line" contains information on starting and stopping Portal servers.

4 To exit the Configurator, on the **File** menu, click **Exit**.

Creating a New Portal Server

Before you create a new Portal server, you should be prepared to make adjustments to some parameters to account for the existence of multiple Portal servers on the same machine, or which may use the same external resources. See "Guidelines for Multiple Portal Servers" on page 30.

To create a new Portal server, start the Configurator as described in "Starting the Configurator" on page 31 and do the following:

To create a new Portal server

1 With the Configurator running, select the **Create Portal Server** option and click **Start Wizard**.

2 In the **New Portal Server Instance Name** field, type the name to be used for this Portal server.

Names must be unique among Portal servers on that computer.

Note: If you type the name of an existing Portal server instance, you will overwrite the existing configuration for that server. If that is your intention, in the Information box, click **Yes**.

3 Click **Next**. The Configurator displays the **General** tab.

4 Follow the configuration procedure, as described in the *webMethods Installation Guide*.

5 After the new Portal server is created, on the **File** menu, click **Exit**.

Deleting a Portal Server

To delete an existing Portal server, start the Configurator as described in "Starting the Configurator" on page 31 and do the following:

To delete a Portal server

1 With the Configurator running, select the **Delete Portal Server** option and click **Start Wizard**.

The Configurator displays the **Delete Server Instance** tab.

2 In the **Existing Portal Server Instance** list, select the name of the Portal server you want to delete.

3 Click Finish.

The Portal server is deleted and all information about it is removed.

4 On the **File** menu, click **Exit**.

webMethods

CHAPTER 3

External Directory Services

What is a Directory Service?

A directory is similar to a database in that it contains a collection of entries (in this case, individuals), each of which has a set of attributes, such as names, e-mail addresses, and so forth. A directory service provides a mechanism for delivering information about the entries in the directory.

The System Directory Service

webMethods Portal includes an internal system directory service. The system directory service is suitable for getting started in using a Portal server, and for maintaining information about a moderate number of users. With the system directory, you can create and manage users, and organize them into groups. See Chapter 4, "User and Group Management" for information on management of users and groups in the system directory service.

External Directory Services

In addition to the system directory, webMethods Portal can support multiple external directory services, allowing you to manage a much larger and diverse group of users, including both internal and external users. If your company or government entity has one or more directory services, webMethods Portal can connect to those services, allowing you to manage the portal user experience for each individual user. webMethods Portal supports the following directory services: SunOne Directory Server 5.2, Active Directory, and ADAM. In addition, you can use an Oracle database as a directory service.

Configuring LDAP, ADSI, or ADAM Directory Services

You can configure an LDAP, ADSI, or ADAM directory service to which you have network connectivity. webMethods Portal provides a wizard with which to do the configuration.

To configure an LDAP, ADSI, or ADAM directory service

1. As a portal administrator, browse to the **Administration Dashboard** and in the **User Management** folder, click **Directory Services Administration**.
2. Click the **Create New Directory Service** tab.

3 In **Directory Type**, click the option describes the type of directory service:

This option...	Configures this type of directory service...
LDAP	Lightweight Directory Access Protocol. An internet protocol that allows client programs to query LDAP directory servers about entries using their attributes.
ADSI	Active Directory Service Interfaces. A set of interfaces for querying and manipulating objects in Microsoft Active Directory, providing an LDAP view of the objects. Active Directory is tightly coupled with the Windows operating system.
ADAM	Active Directory Application Mode, a standalone directory server offered by Microsoft. ADAM is an LDAP implementation that can be installed and uninstalled without affecting the Active Directory structure of a network.

4 Click **Next**.

5 Fill in the appropriate form fields for the directory service you want to add. You should be prepared to provide the following information:

Property	Description
General	
Name	The display name to be used for the directory service within the portal.
Description	(Optional) Descriptive comments about the directory service.
Cache	
Cache Capacity	The number of database queries to be cached. The default is 1000.
Cache Timeout	The length of time queries should remain in the cache unless the cache capacity is exceeded. From the list, select a value. The default is 1 hour.
Connection Information	
Provider URL	The URL for the directory service using this syntax: ldap://*host_name*:*port_number* For example: `ldap://my_host:389`
Base DN	The base distinguished name for the directory service. For example, `ou=Portal,o=webmethods.com`

Property	Description
Groups DN	(Optional) The distinguished name for a group.
User DN	(Optional) The distinguished name for an individual user.
Security Principal	The distinguished name required to log in to the directory service.
Security Credentials	The password required to log in to the directory service.
Failover URLs	One or more provider URLs to be used in case the primary provider fails. Separate multiple URLs with spaces.
Search Timeout	The length of time in seconds before a query times out. The default value is 0, which means the query will not time out.
Global Attributes	
Object Class	The Object Class attribute for the directory service.
Last Modified	The Last Modified attribute for the directory service.
User Attributes	
User Object Class	The User Object Class attribute for the directory service.
User ID	The User ID attribute for the directory service.
First Name	The First Name attribute for the directory service.
Last Name	The Last Name attribute for the directory service.
Full Name	The Full Name attribute for the directory service.
E-mail Address	The E-mail Address attribute for the directory service.
Password	The Password attribute for the directory service.
Group Attributes	
Group Object Class	The Group Object Class attribute for the directory service.
Group ID	The Group ID attribute for the directory service.
Group Name	The Group Name attribute for the directory service.
Group Members	The Group Members attribute for the directory service.
Group E-mail	The Group E-mail attribute for the directory service.

Property	Description
Connection Pool	
Minimum Connections	The minimum number of connections to the directory service to be open at all times. Choose a value from the list.
Maximum Connections	The maximum number of connections allowed to the directory service. Choose a value from the list.
Maximum Connection Time	The maximum time for any connection to be open before being recycled. Choose a value from the list.

6 At the bottom of the page, click **Finish**.

Configuring a Database Directory Service

You can configure a database directory service to which you have network connectivity. webMethods Portal provides a wizard with which to do the configuration.

To configure a database directory service

1 As a portal administrator, browse to the **Administration Dashboard** and in the **User Management** folder, click **Directory Services Administration**.

2 Click the **Create New Directory Service** tab.

3 In **Directory Type**, click **Database**, and then click **Next**.

4 Fill in the appropriate form fields for the database directory service. You should be prepared to provide the following information:

Property	Description
General	
Name	The display name to be used for the directory service within the portal.
Description	(Optional) Descriptive comments about the directory service.
Attributes	
User ID	The name of the query field containing the user ID value.
User DN	The name of the query field containing the distinguished name value for the user.
User First Name	The name of the query field containing the user first name.

Property	Description
User Last Name	The name of the query field containing the user last name.
User Full Name	(Optional) The name of the query field containing the user full name. If you do not supply an attribute, the full name is derived from the **User First Name** and **User Last Name** attributes.
User E-mail	(Optional) The name of the query field containing the user e-mail address.
Group ID	The name of the query field containing the group ID value.
Group DN	The name of the query field containing the distinguished name value for the user.
Group Name	The name of the query field containing the group name.
Group E-mail	(Optional) The name of the query field containing the group e-mail address.
Configuration	
Authentication Handler	The portlet that handles authentication for the database. By default, webMethods Portal provides a clear-text authentication handler. If you want encrypted authentication, you need to create an authentication portlet, deploy it to the Portal server, and click **Browse** to select it. See "Samples" on page 54.
Database	
Datasource	From the list, select the database to be used as a datastore. For a database to appear in the list, you must first use the DataSource Administration portlet to connect to the external database. See "Managing External Data Sources" on page 174. For a sample database directory, see "Samples" on page 54.
Query List Users	A SQL query that returns a list of all users in the record. The query may either return all user attributes at once, or just a list of user ID attributes. This query has no parameters.
Query Lookup User by ID	A SQL query that returns a user record based on the user ID. **Important!** This query must return all user attributes, as described under **Attributes** in this table.

Property	Description
Query Lookup User by DN	(Optional) A SQL query that returns user records by user distinguished name.
Query Search Users	(Optional) A SQL query that returns a list of user records by search term.
Query Authenticate	A SQL query that returns persisted user credentials for authentication.
Query List Groups	(Optional) A SQL query that lists all groups in the directory. The query may either return all group attributes at once, or just a list of group ID attributes. This query has no parameters
Query Lookup Group by ID	A SQL query that returns a group record based on the group ID.
Query Lookup Group by DN	(Optional) A SQL query that returns group records by group distinguished name.
Query Search Groups	(Optional) A SQL query that returns a list of group records by search term.
Query Group Membership for User	(Optional) A SQL query that returns a list of groups the user is a member of.
Query Group Membership for Group	(Optional) A SQL query that returns a list of groups the child group a is member of.
Query Group Members	(Optional) A SQL query that returns list of groups that are members of a parent group.
Query User Members	(Optional) A SQL query that returns list of users who are members of a parent group.
Cache	
Cache Enabled	Determines if the Portal server will attempt to save the load on the database by using cached data whenever possible:

Select this...	To do this...
Yes, enable caching	Have the Portal server cache queries to the database directory service.
No, disable caching	Disable caching of database directory service queries.

Property	Description
Cache Capacity	The number of database queries to be cached. The default is 1000.
Cache Timeout	The length of time queries should remain in the cache unless the cache capacity is exceeded. From the list, select a value. The default is 1 day.

5 At the bottom of the page, click **Finish**.

Samples

You can find a sample authentication template at this location:

*/webMethods_install_dir/*Portal/components/samples/services/directory/wm_dbdir_auth_template.pdp

You can find a sample database directory to use for testing:

*/webMethods_install_dir/*Portal/components/samples/services/directory/wm_dbdir_sample.pdp

To deploy either of these sample portlets, copy it and then paste it into the deploy directory for the Portal server:

*/webMethods_install_dir/*Portal/server/Portal/server/*portal_instance_name*/deploy

Modifying a Directory Service Configuration

To modify the configuration of an existing directory service configuration, use the following procedure.

To modify an external directory service

1 As a portal administrator, browse to the **Administration Dashboard** and in the **User Management** folder, click **Directory Services Administration**.

2 In the **List Directory Services** tab, do one of the following:

- Click the name of the directory service configuration you want to modify.
- Click (Popup Menu) for the directory service configuration and then click **Properties**.

3 Make changes to the Properties form as needed.

4 At the bottom of the page, click **Apply**.

Modifying the Order for Directory Services

Some portal search actions can query multiple directory services. If you want to control the order in which directory services are searched, do the following:

To modify the order in which external directory services are searched

1 As a portal administrator, browse to the **Administration Dashboard** and in the **User Management** folder, click **Directory Services Administration**.

2 Click the **Modify Directory Search Order** tab to bring it to the front.

3 In the **Order** list, to move a directory service, select it and then click the **Move Up** icon or **Move Down** icon as needed.

The top directory service in the list is searched first, followed by the second, and so on.

4 After you have set the search order, click **Apply**.

Note: Setting the search order does not affect the order in which the directory services appear in the **List Directory Services** tab.

Deleting a Directory Service Configuration

To delete an external directory service from the Portal server, use the following procedure.

To delete an external directory service

1 As a portal administrator, browse to the **Administration Dashboard** and in the **User Management** folder, click **Directory Services Administration**.

2 In the **List Directory Services** tab, locate the external directory service configuration you want to delete.

3 Click (Popup Menu) for the directory service configuration and then click **Delete**.

webMethods

CHAPTER 4

User and Group Management

Overview of User Management

Portal users can be granted or denied access to portlets or portal pages based on who they are, what groups they belong to, or what roles they play. Information about those users can be stored internally in a Portal server or can come from external sources called directory services. webMethods Portal provides administrators with a number of tools that can be used to help manage portal users and access to the sources of information about them. In webMethods Portal, users, groups, and roles are sometimes referred to as Principals.

Groups and Roles

In a simple implementation of a portal, it might be possible to manage access for individual users. As the complexity of the portal increases and the number of users grows, it becomes increasingly necessary to manage access to classes of users based on how they are organized and on what roles they play in using portal resources.

A group is a collection of users or other groups. Groups are static in nature because each member of a group is specifically assigned. In addition, the membership of a group is limited to a particular directory service.

A role is similar to a group in that it is a collection of users, groups, or other roles. Roles are different from groups because role membership can be dynamic. For example, membership in a role can be based on an LDAP (Lightweight Directory Access Protocol) query for a particular attribute.

Another difference between groups and roles is that membership in a role can span directory services. If your enterprise has multiple directory services, you can create roles that take members from all of them. See Chapter 5, “Role Management” for more information on roles.

Directory Services

A directory is similar to a database in that it contains a collection of entries (in this case, individuals), each of which has a set of attributes, such as names, e-mail addresses, and so forth. A directory service provides a mechanism for delivering information about the entries in the directory.

The System Directory Service

webMethods Portal includes an internal system directory service. The system directory service is suitable for getting started in using a Portal server, and for maintaining information about a moderate number of users. With the system directory, you can create

and manage users, and organize them into groups. A set of default Principals (users, groups, and roles) is installed as part of the system directory service:

Principal	Description
Users	
Portal Admin	The portal administrator. Can manage the Portal server, including portal analysis, configuration, and content, and user management. As installed, the user ID for this user is "PortalAdmin" and the password is "admin." **Important!** Change the password for this user. For instructions about how to update information for a user, see "Editing Users in the System Directory Service" on page 64.
Portal Guest	An anonymous user. This user can read pages that allow anonymous access, such as the login page. Otherwise, this user cannot read, modify or delete content unless permission is explicitly granted by an administrator. As installed, the user ID for this user is "Portal Guest."
Portal Developer	Portal Developer. Can customize the look and feel of the portal user interface by modifying shells and skins. Can develop portal pages and add content. As installed, the user ID for this user is "PortalDev" and the password is "password." **Important!** Change the password for this user. For instructions about how to update information for a user, see "Editing Users in the System Directory Service" on page 64.
webMethods System	A user account that is used internally by Portal to invoke Web services. Portal uses this account for Web service authentication from one server to another. As installed, the user account is WEB_SYSUSER and the password is "manage," which you should *not* change. **Important!** Do *not* change any information for this user account (for example, the password). Do *not* delete this user. If you change the password or delete this user, Web service authentication will not function properly.
Groups	
Portal Everyone	General user. Cannot read, modify or delete content unless permission is explicitly granted by a portal administrator.

Principal	Description
Portal Developers	Portal Developer. Can customize the look and feel of the portal user interface by modifying shells and skins. Can developer portal pages and add content.
Roles	
Admin Role	Portal administrator. Can manage the Portal server, including portal analysis, configuration, and content, and user management.

External Directory Services

In addition to the system directory, webMethods Portal can support multiple external directory services, allowing you to manage a much larger and diverse group of users, including both internal and external users. See Chapter 3, "External Directory Services" for more information on external directory services.

Managing Users in the System Directory Service

The system directory is an internal directory service in which you can create and manage users, and organize them into groups (see "The System Directory Service" on page 58). You can perform several tasks related to users in the system directory service:

This task...	Is described here...
Add a new user	"Adding a User to the System Directory Service" on page 61
Search for a user	"Searching for Users" on page 61
Save user search criteria	"Saving Searches for Users" on page 62
Edit a user	"Editing Users in the System Directory Service" on page 64
Delete a user	"Deleting Users from the System Directory Service" on page 65

Adding a User to the System Directory Service

To add a new user to the system directory service, use the following procedure.

To add a user to the system directory service

1 As a portal administrator, browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Users**.

2 In the **Users** area, click **Add User**.

3 In the **Create User** form, fill in the following fields for the user you want to add:

In this field...	Specify...
User ID	The user ID for the new user. This value is used in the distinguished name (DN) for the user.
Password	A default password to be used the first time the user logs into the portal.
Confirm Password	The same password you specified in the **Password** field.
First Name	The first name of the new user. webMethods Portal uses the user's first and last name when displaying the user's name on pages in the user interface.
Last Name	The last name of the new user.
E-mail Address	(Optional) Type the e-mail address of the new user.

4 Click **Create**.

Searching for Users

You can search for users, either in the system directory or in an external directory.

To search for a user

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Users**.
- In the global navigation toolbar, click **Directory**.

2 In the search field of the **Search** tab, do one of the following:

To find this...	Specify...
A specific user	The user ID. A partial ID can match multiple entities.
A list of all users on a directory service	Leave the search field empty.

3 In the **Directory Service** list, choose the directory service that contains the users you want to find, and click **Go**.

The **Users** area contains a list of users who match the search criteria.

For information on exporting the results of a search, see "Exporting Search Results to a CSV File" on page 76.

Saving Searches for Users

If there is a user or a collection of users for whom you search regularly, you can save search criteria that you can reuse. The following sections describe some tasks you can perform with saved searches:

This task...	Is described here...
Create a new saved search	"Creating a Saved Search for a User" on page 62
Use a saved search	"Using a Saved Search to Find a User" on page 63
Modify a saved search	"Modifying a Saved Search for a User" on page 63
Delete a delete a saved search	"Deleting a Saved Search for a User" on page 64

Creating a Saved Search for a User

To create a saved search for a user, follow these steps:

To create a saved search for a user

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Users**.
- In the global navigation toolbar, click **Directory**.

2 In the search field of the **Search** tab, type the complete or partial user ID to be used as search criteria.

3 In the **Directory Service** list, choose the directory service that contains the users you want to find.

4 Click on the right side of the **Search** tab.

5 In the **Search Name** field of the Save Searches dialog box, type a name by which you can identify the search criteria and click **OK**.

Using a Saved Search to Find a User

You can use a saved search to find users who match the criteria.

To perform a saved search for a user

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Users**.
- In the global navigation toolbar, click **Directory**.

2 Click the **Saved** tab to bring it to the front.

3 In the **Saved Search** list, choose the name of the saved search and click **Go**.

Modifying a Saved Search for a User

You can modify an existing saved search.

To modify a saved search for a user

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Users**.
- In the global navigation toolbar, click **Directory**.

2 Click the **Saved** tab to bring it to the front.

3 In the **Saved Search** list, choose the name of the saved search to be modified and click **Details**.

4 Do either or both of the following:

- In the search field of the **Saved** tab, change the search criteria.
- In the **Directory Service** list, change the directory service in which to perform the search.

5 Click on the right side of the **Saved** tab and click **OK** to update the saved search.

Deleting a Saved Search for a User

When you no longer need a saved search, you can delete it.

To delete a saved search for a user

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Users**.
- In the global navigation toolbar, click **Directory**.

2 Click the **Saved** tab to bring it to the front.

3 In the **Saved Search** list, choose the name of the saved search to be deleted, click **Delete**, and click **OK** to delete the saved search.

Editing Users in the System Directory Service

To view and modify information about a user in the system directory service, use the following procedure.

To edit information about a user in the system directory service

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Users**.
- In the global navigation toolbar, click **Directory**.

2 In the search field of the **Search** tab, type a partial or complete user ID for the user you want to edit.

3 In the **Directory Service** list, choose the **system** directory service, and click **Go**.

4 In the **Users** area, click  for the user you want to edit.

5 In the **User Information** form, modify any of the following fields:

In this field...	Specify...
Password	A default password to be used the first time the user logs into the portal.
Confirm Password	The same password you specified in the **Password** field.
First Name	The first name of the user. webMethods Portal uses the user's first and last name when displaying the user's name on pages in the user interface.

In this field...	Specify...
Last Name	The last name of the user.
E-mail Address	(Optional) Type the e-mail address of the user.

The **User ID** and **DN** fields appear in this form, but you cannot modify them.

6 After you have finished editing the form, click **Apply**.

Deleting Users from the System Directory Service

To delete one or more users from the system directory service, use the following procedure.

To delete one or more users from the system directory service

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Users**.
- In the global navigation toolbar, click **Directory**.

2 In the search field of the **Search** tab, type a partial or complete user ID for the users you want to delete.

3 In the **Directory Service** list, choose the **system** directory service, and click **Go**.

4 For each user you want to delete from the system directory service, select the check box to the left of the **First Name** column.

5 Click **Delete** and in the confirmation list, click **Delete** again.

Locating a User's Home Folder

The Locate a User's Home Folder portlet enables a portal administrator to locate and browse to a user's personal folders. This feature can be especially helpful when items become unavailable to the user because of permissions changes, and for removing their content when a user is no longer actively using the portal.

To locate a user's Home folder

1 As a portal administrator, browse to the **Administration Dashboard** and in the **User Management** folder, click **Locate a User's Home Folder**.

2 Under **Selected User**, click **Browse**.

3 On the left side of the portal resource selector, navigate to the user and click the **Select** icon.

The selected user appears in the **Selected Items** panel.

4 Click **Select**.

5 Click **Apply** to open the Home Folder for the user you selected.

Managing Groups in the System Directory Service

The system directory is an internal directory service in which you can create and manage groups (see "The System Directory Service" on page 58). You can perform several tasks on groups in the system directory service:

This task...	Is described here...
Add a new group	"Adding Groups to the System Directory Service" on page 66
Search for a group	"Searching for Groups" on page 67
Save group search criteria	"Saving Searches for Groups" on page 68
Edit a group	"Editing Groups in the System Directory Service" on page 70
Delete a group	"Deleting Groups from the System Directory Service" on page 71

Adding Groups to the System Directory Service

To add a new group to the system directory service, use the following procedure.

To add a group to the system directory service

1 As a portal administrator, browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Groups**.

2 In the **Groups** area, click **Add Group**.

3 In the **Create Group** form, fill in the following fields for the group you want to add:

In this field...	Specify...
Group ID	The group ID for the new group. This value is used in the distinguished name (DN) for the group.

In this field...	Specify...
Group Name	a display name for the new group.
E-mail Address	(Optional) The e-mail address of the new group.

4 Click **Create**.

Searching for Groups

You can search for groups, either in the system directory or in an external directory.

To search for a group

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Groups**.
- In the global navigation toolbar, click **Directory** and click the **Groups** tab to bring it to the front.

2 In the search field of the **Search** tab, do one of the following:

To find this...	Specify...
A specific group	The group ID. A partial ID can match multiple entities.
A list of all groups on a directory service	Leave the search field empty.

3 In the **Directory Service** list, choose the directory service that contains the groups you want to find, and click **Go**.

The **Groups** area contains a list of groups that match the search criteria.

For information on exporting the results of a search, see "Exporting Search Results to a CSV File" on page 76.

Saving Searches for Groups

If there is a group or a collection of groups for which you search regularly, you can save search criteria that you can reuse. The following sections describe some tasks you can perform with saved searches:

This task...	Is described here...
Create a new saved search	"Creating a Saved Search for a Group" on page 68
Use a saved search	"Using a Saved Search to Find a Group" on page 69
Modify a saved search	"Modifying a Saved Search for a Group" on page 69
Delete a delete a saved search	"Deleting a Saved Search for a Group" on page 70

Creating a Saved Search for a Group

To create a saved search for a group, follow these steps:

To create a saved search for a group

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Groups**.
- In the global navigation toolbar, click **Directory** and click the **Groups** tab to bring it to the front.

2 In the search field of the **Search** tab, type the complete or partial group ID to be used as search criteria.

3 In the **Directory Service** list, choose the directory service that contains the groups you want to find.

4 Click  on the right side of the **Search** tab.

5 In the **Search Name** field of the Save Searches dialog box, type a name by which you can identify the search criteria and click **OK**.

Using a Saved Search to Find a Group

You can use a saved search to find groups that match the criteria.

To perform a saved search for a group

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Groups**.
- In the global navigation toolbar, click **Directory** and click the **Groups** tab to bring it to the front.

2 Click the **Saved** tab to bring it to the front.

3 In the **Saved Search** list, choose the name of the saved search and click **Go**.

Modifying a Saved Search for a Group

You can modify an existing saved search.

To modify a saved search for a group

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Groups**.
- In the global navigation toolbar, click **Directory** and click the **Groups** tab to bring it to the front.

2 Click the **Saved** tab to bring it to the front.

3 In the **Saved Search** list, choose the name of the saved search to be modified and click **Details**.

4 Do either or both of the following:

- In the search field of the **Saved** tab, change the search criteria.
- In the **Directory Service** list, change the directory service in which to perform the search.

5 Click  on the right side of the **Saved** tab and click **OK** to update the saved search.

Deleting a Saved Search for a Group

When you no longer need a saved search, you can delete it.

To delete a saved search for a group

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Groups**.
- In the global navigation toolbar, click **Directory** and click the **Groups** tab to bring it to the front.

2 Click the **Saved** tab to bring it to the front.

3 In the **Saved Search** list, choose the name of the saved search to be deleted, click **Delete**, and click **OK** to delete the saved search.

Editing Groups in the System Directory Service

To view and modify information about a group in the system directory service, use the following procedure.

To edit information about a group in the system directory service

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Groups**.
- In the global navigation toolbar, click **Directory** and click the **Groups** tab to bring it to the front.

2 In the search field of the **Search** tab, type a partial or complete group ID for the group you want to edit.

3 In the **Directory Service** list, choose the **system** directory service, and click **Go**.

4 In the **Groups** area, click  for the group you want to edit.

5 In the **Group Information** form, modify either of the following fields:

In this field...	Specify...
Group Name	A display name for the group.
E-mail Address	(Optional) The e-mail address of the group.

The **Group ID** and **DN** fields appear in this form, but you cannot modify them.

6 After you have finished editing the form, click **Apply**.

Deleting Groups from the System Directory Service

To delete one or more groups from the system directory service, use the following procedure.

To delete one or more groups from the system directory service

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Groups**.
- In the global navigation toolbar, click **Directory** and click the **Groups** tab to bring it to the front.

2 In the search field of the **Search** tab, type a partial or complete group ID for the groups you want to delete.

3 In the **Directory Service** list, choose the **system** directory service, and click **Go**.

4 For each group you want to delete from the system directory service, select the check box to the left of the **Group Name** column.

5 Click **Delete** and in the confirmation list, click **Delete** again.

Managing Group Membership

For users and groups in the system directory service, you can manage group membership. You can add users to groups and remove them, and you can add groups to other groups and remove them. You can display membership information about groups in external directory services but you cannot manage them; such groups must be managed in the external directory service.

Managing Group Membership for a User

On the profile page for a user in the system directory service, you can view and manage membership in groups. In the **Groups** tab, there are some tasks you can perform to manage group membership for the user.

This task...	Is described here...
Make the current user a member of a group	"Adding a User to a Group" on page 72
Remove the user as a member of a group	"Removing a User from a Group" on page 73

Note: You cannot use this feature to manage group membership for users in an external directory service.

Adding a User to a Group

From the **Groups** tab, you can add a user in the system directory service to a group.

To add a user to one or more groups

1. As a portal administrator, do one of the following:
   - Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Users**.
   - In the global navigation toolbar, click **Directory**.
2. In the search field of the **Search** tab, type a partial or complete user ID for the user you want to manage.
3. In the **Directory Service** list, choose the **system** directory service, and click **Go**.
4. In the **Users** area, click  for the user you want to manage.
5. On the user's profile page, click the **Groups** tab to bring it to the front.
6. In the left panel, browse to the group to which the user should be added.

   If you cannot find the group, it may belong to an external directory service.
7. To move the group to the **Selected Items** panel, click the  **Select** icon for the group.
8. Repeat the selection process, if needed, for multiple groups.
9. Click **Apply**.

You can also add a user to a group from the profile page for a group, as described in "Adding Users or Other Groups to the Current Group" on page 74.

Removing a User from a Group

You can remove a user in the system directory service from a group.

To remove a user from one or more groups

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Users**.
- In the global navigation toolbar, click **Directory**.

2 In the search field of the **Search** tab, type a partial or complete user ID for the user you want to manage.

3 In the **Directory Service** list, choose the **system** directory service, and click **Go**.

4 In the **Users** area, click  for the user you want to manage.

5 On the user's profile page, click the **Groups** tab to bring it to the front.

6 In the **Selected Items** panel, click the  **Unselect** icon for the group from which the user should be removed.

7 Repeat removal from the **Selected Items** panel, if needed, for multiple groups.

8 Click **Apply**.

You can also remove a user from a group from the profile page for a group, as described in "Removing Users or Groups from the Current Group" on page 76.

Managing Group Membership For a Group

On the profile page for a group in the system directory service, there are some tasks you can perform to manage group membership:

This task...	Is described here...
Make the current group a member of another group	"Adding the Current Group to Another Group" on page 74
Make users or other groups members of the current group	"Adding Users or Other Groups to the Current Group" on page 74

This task...	Is described here...
Remove the current group as member of another group	"Removing the Current Group from Another Group" on page 75
Remove users or other groups as members of the current group	"Removing Users or Groups from the Current Group" on page 76

Note: You cannot use this feature to manage groups in an external directory service.

Adding the Current Group to Another Group

From the **Groups** tab for a group in the system directory service, you can add that group to one or more other groups in the system directory service.

To add a the current group to one or more groups

1. As a portal administrator, do one of the following:
   - Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Groups**.
   - In the global navigation toolbar, click **Directory**.
2. In the search field of the **Search** tab, type a partial or complete group ID for the group you want to manage.
3. In the **Directory Service** list, choose the **system** directory service, and click **Go**.
4. In the **Groups** area, click  for the group you want to manage.
5. On the profile page for the group, click the **Groups** tab to bring it to the front.
6. In the left panel, browse to the group to which the current group should be added.

   If you cannot find the group, it may belong to an external directory service.
7. To move the group to the **Selected Items** panel, click the  **Select** icon for the group.
8. Repeat the selection process, if needed, for multiple groups.
9. Click **Apply**.

   The current group becomes a member of the selected group.

Adding Users or Other Groups to the Current Group

From the **Group Members** tab on a profile page for a group in the system directory service, you can add users or other groups to that group.

To add users or groups to the current group

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Groups**.
- In the global navigation toolbar, click **Directory**.

2 In the search field of the **Search** tab, type a partial or complete group ID for the group you want to manage.

3 In the **Directory Service** list, choose the **system** directory service, and click **Go**.

4 In the **Groups** area, click  for the group you want to manage.

5 On the profile page for the group, click the **Group Members** tab to bring it to the front.

6 In the left panel, browse to the user or group to be added to the current group.

If you cannot find the user or group, it may belong to an external directory service.

7 To move the user or group to the **Selected Items** panel, click the  **Select** icon.

8 Repeat the selection process, if needed, for multiple users or groups.

9 Click **Apply**.

The selected user or group becomes a member of the current group.

Removing the Current Group from Another Group

From the **Groups** tab for a group in the system directory service, you can remove that group from another group.

To remove the current group from one or more groups

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Groups**.
- In the global navigation toolbar, click **Directory**.

2 In the search field of the **Search** tab, type a partial or complete group ID for the group you want to manage.

3 In the **Directory Service** list, choose the **system** directory service, and click **Go**.

4 In the **Groups** area, click for the group you want to manage.

5 On the profile page for the group, click the **Groups** tab to bring it to the front.

6 In the **Selected Items** panel, click the **Unselect** icon for the group from which the current group should be removed.

7 Repeat removal from the **Selected Items** panel, if needed, for multiple groups.

8 Click **Apply**.

Removing Users or Groups from the Current Group

From the **Group Members** tab on a profile page for a group in the system directory service, you can remove users and groups from membership in that group.

To remove users or groups from the current group

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Groups**.
- In the global navigation toolbar, click **Directory**.

2 In the search field of the **Search** tab, type a partial or complete group ID for the group you want to manage.

3 In the **Directory Service** list, choose the **system** directory service, and click **Go**.

4 In the **Groups** area, click for the group you want to manage.

5 On the profile page for the group, click the **Group Members** tab to bring it to the front.

6 In the **Selected Items** panel, click the **Unselect** icon for users or groups to be removed.

7 Repeat removal from the **Selected Items** panel, if needed, for multiple users or groups.

8 Click **Apply**.

Exporting Search Results to a CSV File

You can export search results to a a comma-delimited text file (.csv file) if the search results panel includes the **Export Table** function.

After exporting search results to a .csv file, you can then import the .csv file into Microsoft Excel, Microsoft Access, or any other application that accepts the .csv file format.

To export search results

1 Click **Export Table**, which is located in the top right of the search results.

2 From the **Character Encoding** list, select the character encoding to use

3 Click **Export**.

4 Use the file-download mechanism in your browser to browse to the location where you want to save the .csv file.

webMethods

CHAPTER 5

Role Management

What are Roles?

A role is similar to a group in that it is a collection of users, groups, or other roles. Role membership can be static, as it is with groups, but it can also be dynamic. For example, membership in a role can be based on an LDAP (Lightweight Directory Access Protocol) query for a particular attribute. If the attribute for a directory entry is modified, that entries might automatically become a member of a role, or might be removed. Role membership can also be based on rules. For example, you could assign roles based on HTTP headers. If a user logs in from within the Enterprise LAN, full access to the portal is granted; if the same user logs in from an external (perhaps unsecure) site, access to sensitive information is denied.

Roles differ from groups in two important ways: Role membership can span multiple directory services and can be either static or dynamic. To create a role, you can use a Role Provider, which defines how the role functions. A set of default Roles and Role Providers is installed with the Portal server:

Default Item	Description
Roles	
Admin Role	The portal administrator role. Anyone assigned to this role has full administrative privileges on the Portal server.
Role Providers	
Static	Creates a role that is a simple collection of users, groups, and roles. Similar to a group except that it spans multiple directory services.
LDAP Query	Creates a role that is based on an LDAP query. Any Principal in a directory service that matches the query is a member of the role.
Rule Based	Creates a role that is based on a Portal rule. Any Principal that matches the rule is a member of the role.
Database	Creates a role that is based on a query to a database directory service. Any Principal that matches the rule is a member of the role.

There are several types of tasks you can perform on roles:

This task...	Is described here...
Add a new role	“Adding Roles” on page 81
Search for a role	“Searching for Roles” on page 87
Save role search criteria	“Saving Searches for Roles” on page 88
Edit a role	“Editing Roles” on page 90
Delete a role	“Deleting Roles” on page 96

Adding Roles

There are multiple types of roles you can add to a Portal server, as described in the following sections:

Adding these roles	Is described here
Static roles	"Adding a Static Role" on page 81
LDAP query roles	"Adding an LDAP Query Role" on page 82
Rule-based roles	"Adding a Rule-Based Role" on page 83
Database roles	"Adding a Database Role" on page 86

Adding a Static Role

A static role is a simple collection of users, groups, and other roles.

To create a static role

1 As a portal administrator, browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Roles**.

2 In the **Roles** area, click **Add Role**.

3 In the **Role Name** field, type a descriptive display name for the role.

4 If the Role Providers do not appear in the left panel, in the **Location** list, select **Root**, and then click **Role Providers**.

5 Click the **Select** icon for **Static Role Providers** to move it to the **Selected Items** panel.

6 At the bottom of the page, click **Create Role**.

The Role Membership page is displayed for the newly created role.

7 To add Principals, in **Principals**, click **Add**.

8 In the left panel browse to any of the following:

Within this...	Browse to these...
Roles	Any role. You can collect LDAP query, rule-based, database, or static roles into a static role.
Directory Services	Any user or group that can be located within all available directory services.

9 Click the **Select** icon for the user, group, or role to move it to the **Selected Items** panel.

You can accumulate multiple entries in the **Selected Items** panel.

10 Click **Select**.

In **Principals**, you should see all members of the role.

11 At the bottom of the Properties page, click **Apply**.

Adding an LDAP Query Role

An LDAP query role is based on an LDAP query to an external directory service. Any user or group that meets the requirements of the query is a member of the role.

To create an LDAP query role

1 As a portal administrator, browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Roles**.

2 In the **Roles** area, click **Add Role**.

3 In the **Role Name** field, type a descriptive display name for the role.

4 If the Role Providers do not appear in the left panel, in the **Location** list, select **Root**, and then click **Role Providers**.

5 Click the **Select** icon for **LDAP Query Role Provider** to move it to the **Selected Items** panel.

6 At the bottom of the page, click **Create Role**.

7 In the **LDAP Query** field type a valid LDAP query.

8 Select the **Simple Query** option if the query in the **LDAP Query** field contains simplified LDAP query syntax.

Unless you are creating a complex LDAP query, the query syntax can be cumbersome to use. With the **Simple Query** option, the syntax is filled in for you. For example, to find all persons whose manager has the user ID abrown, the simple query syntax is `manager=abrown`.

9 In **LDAP Directory Service**, click **Browse**.

10 If the available directory services do not appear in the left panel, in the **Location** list, select **Root**, and then click **Available Directory Services**.

There can be only one directory service associated with an LDAP query role.

11 Click the **Select** icon for an LDAP directory service to move it to the **Selected Items** panel, and click **Select**.

12 In the **Principal Type** list, choose whether the query searches for **Users** or **Groups**.

13 At the bottom of the page, click **Apply**.

Adding a Rule-Based Role

A rules-based role is based on a portal rule. Any Principal that matches the rule is a member of the role.

To create a rule-based role

1 As a portal administrator, browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Roles**.

2 In the **Roles** area, click **Add Role**.

3 In the **Role Name** field, type a descriptive display name for the role.

4 If the Role Providers do not appear in the left panel, in the **Location** list, select **Root**, and then click **Role Providers**.

5 Click the **Select** icon for **Rule Based Role Provider** to move it to the **Selected Items** panel.

6 At the bottom of the page, click **Create Role**.

The Role Membership page is displayed for the newly created role.

7 Under the **Match Criteria** heading, select **Match All Criteria Below** or **Match Any Criteria Below** as the criteria for the rule-based role.

8 Fill in the appropriate match criteria for the rule-based role using the following guidelines:

User DN Value(s)—A regular expression that matches any part of the current user's directory distinguished name (DN). In the field, type the portions of the DN to which you want a match.

For example, `ou=Engineering.*ou=US` matches a user with the following DN:

```
uid=joe,ou=Development,ou=Engineering,ou=Midwest,ou=US,o=webMethods
```

Domain Name Expression—A regular expression that matches any part of the name of the current user's directory service as registered in the portal. In the field, type the directory service name to which you want a match.

For example, US (without quotes) matches a user from the US Corporate directory service. This is a very effective way to govern the look and feel for users that may be in different user directories, such as partners.

Group DN and Role DN Expression—A regular expression that matches any part of any group or role of which the current user is a member. In the field, type the portions of the DN to which you want a match.

For example, `ou=Engineering` matches a user belonging to a group with the following DN:

```
cn=portal,ou=Engineering,ou=Midwest,ou=US,o=webMethods.
```

User Attributes—One or more pairs of user attributes and their values from the user's record. If you have more than one user attribute, the value set in **Match Criteria** determines how attributes are matched:

Match Criteria value	How the rule is applied
Match All Criteria Below	Each regular expression must match some part of the corresponding attribute value for the current user.
Match Any Criteria Below	Any regular expression in the list can match some part of the corresponding attribute value for the current user.

For example, if the rule is configured to match all criteria, and the configured user attribute pairs are the following:

Name	Value
`office`	Bellevue
`telephonenumber`	(425) 564-0000

and the current user's attribute values are the following:

Name	Value (current user)
`office`	Bellevue
`telephonenumber`	(206) 123-4567

the rule does not match the current user because it matches the `office` attribute value but not the `telephonenumber` attribute value. If, however, the rule is configured to match any criteria, the preceding example rule does match the current user.

To create an attribute-value pair, click **Add**. At the prompt, type the attribute name and click **OK**. At the prompt, type the value to be matched and click **OK**.

Request Headers—One or more pairs of HTTP header attributes and values. You can match anything that appears within an HTTP header, such as the browser agent string or the kinds of MIME types the user will accept. The rule can be a regular expression, or a simple

text string. If you have more than attribute-value pair, the value set in **Match Criteria** determines how attributes are matched:

Match Criteria value	How the rule is applied
Match All Criteria Below	Each regular expression must match some part of the corresponding attribute value for the request header.
Match Any Criteria Below	Any regular expression in the list must match some part of the corresponding attribute value for the request header.

For example, if the rule is configured to match all criteria, and the configured request header pairs are the following:

Name	Value
Accept-Charset	utf-8
Accept-Language	ja

and the request header values for the current user are the following:

Name	Value (current user)
Accept-Charset	ISO-8859-1,utf-8;q=0.7
Accept-Language	en-us,en;q=0.5

the rule does not match the current user because it matches the Accept-Charset header value but not the Accept-Language header value. If, however, the rule was configured to match any criteria, the rule does match the current user.

To create an attribute-value pair, click **Add**. At the prompt, type the attribute name and click **OK**. At the prompt, type the value to be matched and click **OK**.

Parent Resource—A portal resource that matches the current portal resource or a parent of the current resource. To select a portal resource, click **Browse** to open the portal resource selector and select a portal resource against which to match the rule.If you want match a resource that is referenced by a portal alias, you can optionally click **Use Alias** to select an existing alias on the Portal server.

Resource Type—A resource type that matches the current resource type. To select a resource type, click **Browse** to open the portal resource selector and select a resource type, from the Extended Types folder, against which to match the rule.If you want match a resource type that is referenced by a portal alias, you can optionally click **Use Alias** to select an existing alias on the Portal server.

Resource Property—One or more pairs of portal resource properties and values. If you know the internal name of a property associated with a portal resource, you can match it.

If you have more than one property-value pair, the value set in **Match Criteria** determines how properties are matched:

Match Criteria value	How the rule is applied
Match All Criteria Below	Each regular expression must match some part of the corresponding attribute value for the request header.
Match Any Criteria Below	Any regular expression in the list must match some part of the corresponding attribute value for the request header.

For example, if you want to match files that are PDFs, the property-attribute pair is `mimeType=pdf`.

To create an property-value pair, click **Add**. At the prompt, type the attribute name and click **OK**. At the prompt, type the value to be matched and click **OK**.

9 At the bottom of the page, click **Apply**.

Adding a Database Role

A database role is based on a query to a database directory service. Any Principal that matches the rule is a member of the role.

To create a database role

1 As a portal administrator, browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Roles**.

2 In the **Roles** area, click **Add Role**.

3 In the **Role Name** field, type a descriptive display name for the role.

4 If the Role Providers do not appear in the left panel, in the **Location** list, select **Root**, and then click **Role Providers**.

5 Click the **Select** icon for **Database Role Provider** to move it to the **Selected Items** panel.

6 At the bottom of the page, click **Create Role**.

The Role Membership page is displayed for the newly created role.

7 From the **Datasource** list, select the database to be used as a datastore. For a database to appear in the list, you must first use the DataSource Administration portlet to connect to the external database. See "Managing External Data Sources" on page 174.

8 If the role can include users, in the **Query User** field, type a SQL query that returns a record for a given user in the database who should be a member of the role.

The parameters to the query are:

- {uid}—Principal unique ID
- {dn}—Principal distinguished name

An example of a valid query is:

```
select * from user-roles where roleID='Admin' and userid='{uid}'
```

9 If the role can include groups, in the **Query Group** field, type a SQL query that returns a record for a given group in the database that should be a member of the role.

10 At the bottom of the page, click **Apply**.

Searching for Roles

To search for roles, follow this procedure.

To search for a role

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Roles**.
- In the global navigation toolbar, click **Directory** and click the **Roles** tab to bring it to the front.

2 In the search field of the **Search** tab, do one of the following:

To find this...	Specify...
A specific role	The role name. A partial name can match multiple entities.
A list of all roles on the Portal server	Leave the search field empty.

3 Click **Go**.

The **Roles** area contains a list of roles that match the search criteria.

For information on exporting the results of a search, see "Exporting Search Results to a CSV File" on page 76.

Saving Searches for Roles

If there is a group or a collection of roles for which you search regularly, you can save search criteria that you can reuse. The following sections describe some tasks you can perform with saved searches:

This task...	Is described here...
Create a new saved search	"Creating a Saved Search for a Role" on page 88
Use a saved search	"Using a Saved Search to Find a Role" on page 88
Modify a saved search	"Modifying a Saved Search for a Role" on page 89
Delete a delete a saved search	"Deleting a Saved Search for a Role" on page 89

Creating a Saved Search for a Role

To create a saved search for a role, follow these steps:

To create a saved search for a role

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Roles**.
- In the global navigation toolbar, click **Directory** and click the **Roles** tab to bring it to the front.

2 In the search field of the **Search** tab, type the complete or partial role name to be used as search criteria.

3 Click  on the right side of the **Search** tab.

4 In the **Search Name** field of the Save Searches dialog box, type a name by which you can identify the search criteria and click **OK**.

Using a Saved Search to Find a Role

You can use a saved search to find roles that match the criteria.

To perform a saved search for a role

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Roles**.

- In the global navigation toolbar, click **Directory** and click the **Roles** tab to bring it to the front.

2 Click the **Saved** tab to bring it to the front.

3 In the **Saved Search** list, choose the name of the saved search and click **Go**.

Modifying a Saved Search for a Role

You can modify an existing saved search.

To modify a saved search for a role

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Roles**.
- In the global navigation toolbar, click **Directory** and click the **Roles** tab to bring it to the front.

2 Click the **Saved** tab to bring it to the front.

3 In the **Saved Search** list, choose the name of the saved search to be modified and click **Details**.

4 In the search field of the **Saved** tab, change the search criteria.

5 Click  on the right side of the **Saved** tab and click **OK** to update the saved search.

Deleting a Saved Search for a Role

When you no longer need a saved search, you can delete it.

To delete a saved search for a role

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Roles**.
- In the global navigation toolbar, click **Directory** and click the **Roles** tab to bring it to the front.

2 Click the **Saved** tab to bring it to the front.

3 In the **Saved Search** list, choose the name of the saved search to be deleted, click **Delete**, and click **OK** to delete the saved search.

Editing Roles

For information on editing each type of role, see one of the following sections:

Editing these roles	Is described here
Static roles	"Editing a Static Role" on page 90
LDAP query roles	"Editing an LDAP Query Role" on page 91
Rule-based roles	"Editing a Rule-Based Role" on page 91
Database roles	"Editing a Database Role" on page 95

Editing a Static Role

For a static role, you can edit the users, groups, and other roles that are its members.

To edit a static role

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Roles**.
- In the global navigation toolbar, click **Directory** and click the **Roles** tab to bring it to the front.

2 In the search field of the **Search** tab, type a partial or complete name for the role you want to edit.

3 In the **Roles** area, click  for the role you want to edit.

4 To edit Principals, click **Browse**, and do the following:

To do this...	Do this
Add a Principal	In the left panel, navigate to any Principal to be added to the role. Click the  **Select** icon for the Principal to move it to the **Selected Items** panel.
Remove a Principal	In the **Selected Items** panel, click the **Unselect** icon for the Principal that should be removed.

5 At the bottom of the page, click **Apply**.

Editing an LDAP Query Role

For an LDAP query role, you can edit the query that determines the requirements to be a member of the role.

To edit an LDAP query role

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Roles**.
- In the global navigation toolbar, click **Directory** and click the **Roles** tab to bring it to the front.

2 In the search field of the **Search** tab, type a partial or complete name for the role you want to edit.

3 In the **Roles** area, click  for the role you want to edit.

4 Edit the role as needed:

To edit this...	Do this...
Edit the query	In the **LDAP Query** field type a valid LDAP query
Change to a different LDAP directory service	In **LDAP Directory Service**, click **Browse**. In the left panel, navigate to the new LDAP directory service and click the **Select** icon to move it to the **Selected Items** panel. The old directory service is removed because there can be only one directory service associated with an LDAP query role.
Change between users and groups	In the **Principal Type** list, choose whether the query searches for **Users** or **Groups.**

5 In the **LDAP Query** field type a valid LDAP query.

6 At the bottom of the page, click **Apply**.

Editing a Rule-Based Role

For a rules-based role, you can edit the rules that determine the requirements to be a member of the role.

To edit a rule-based role

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Roles**.
- In the global navigation toolbar, click **Directory** and click the **Roles** tab to bring it to the front.

2 In the search field of the **Search** tab, type a partial or complete name for the role you want to edit.

3 In the **Roles** area, click  for the role you want to edit.

4 Edit the rules as needed:

User DN Value(s)—A regular expression that matches any part of the current user's directory distinguished name (DN). In the field, type the portions of the DN to which you want a match.

For example, `ou=Engineering.*ou=US` matches a user with the following DN:

```
uid=joe,ou=Development,ou=Engineering,ou=Midwest,ou=US,o=webMethods
```

Domain Name Expression—A regular expression that matches any part of the name of the current user's directory service as registered in the portal. In the field, type the directory service name to which you want a match.

For example, US (without quotes) matches a user from the US Corporate directory service. This is a very effective way to govern the look and feel for users that may be in different user directories, such as partners.

Group DN and Role DN Expression—A regular expression that matches any part of any group or role of which the current user is a member. In the field, type the portions of the DN to which you want a match.

For example, `ou=Engineering` matches a user belonging to a group with the following DN:

```
cn=portal,ou=Engineering,ou=Midwest,ou=US,o=webMethods.
```

User Attributes—One or more pairs of user attributes and their values from the user's record. If you have more than one user attribute, the value set in **Match Criteria** determines how attributes are matched:

Match Criteria value	How the rule is applied
Match All Criteria Below	Each regular expression must match some part of the corresponding attribute value for the current user.
Match Any Criteria Below	Any regular expression in the list can match some part of the corresponding attribute value for the current user.

For example, if the rule is configured to match all criteria, and the configured user attribute pairs are the following:

Name	Value
`office`	Bellevue
`telephonenumber`	(425) 564-0000

and the current user's attribute values are the following:

Name	Value (current user)
`office`	Bellevue
`telephonenumber`	(206) 123-4567

the rule does not match the current user because it matches the `office` attribute value but not the `telephonenumber` attribute value. If, however, the rule is configured to match any criteria, the preceding example rule does match the current user.

To create an attribute-value pair, click **Add**. At the prompt, type the attribute name and click **OK**. At the prompt, type the value to be matched and click **OK**.

Request Headers—One or more pairs of HTTP header attributes and values. You can match anything that appears within an HTTP header, such as the browser agent string or the kinds of MIME types the user will accept. The rule can be a regular expression, or a simple text string. If you have more than attribute-value pair, the value set in **Match Criteria** determines how attributes are matched:

Match Criteria value	How the rule is applied
Match All Criteria Below	Each regular expression must match some part of the corresponding attribute value for the request header.
Match Any Criteria Below	Any regular expression in the list must match some part of the corresponding attribute value for the request header.

For example, if the rule is configured to match all criteria, and the configured request header pairs are the following:

Name	Value
Accept-Charset	utf-8
Accept-Language	ja

and the request header values for the current user are the following:

Name	Value (current user)
Accept-Charset	ISO-8859-1,utf-8;q=0.7
Accept-Language	en-us,en;q=0.5

the rule does not match the current user because it matches the Accept-Charset header value but not the Accept-Language header value. If, however, the rule was configured to match any criteria, the rule does match the current user.

To create an attribute-value pair, click **Add**. At the prompt, type the attribute name and click **OK**. At the prompt, type the value to be matched and click **OK**.

Parent Resource—A portal resource that matches the current portal resource or a parent of the current resource. To select a portal resource, click **Browse** to open the portal resource selector and select a portal resource against which to match the rule.If you want match a resource that is referenced by a portal alias, you can optionally click **Use Alias** to select an existing alias on the Portal server.

Resource Type—A resource type that matches the current resource type. To select a resource type, click **Browse** to open the portal resource selector and select a resource type, from the Extended Types folder, against which to match the rule.If you want match a resource type that is referenced by a portal alias, you can optionally click **Use Alias** to select an existing alias on the Portal server.

Resource Property—One or more pairs of portal resource properties and values. If you know the internal name of a property associated with a portal resource, you can match it. If you have more than one property-value pair, the value set in **Match Criteria** determines how properties are matched:

Match Criteria value	How the rule is applied
Match All Criteria Below	Each regular expression must match some part of the corresponding attribute value for the request header.
Match Any Criteria Below	Any regular expression in the list must match some part of the corresponding attribute value for the request header.

For example, if you want to match files that are PDFs, the property-attribute pair is `mimeType=pdf`.

To create an property-value pair, click **Add**. At the prompt, type the attribute name and click **OK**. At the prompt, type the value to be matched and click **OK**.

5 At the bottom of the page, click **Apply**.

Editing a Database Role

For a database role, you can edit the query that determines the requirements to be a member of the role.

To edit a database role

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Roles**.
- In the global navigation toolbar, click **Directory** and click the **Roles** tab to bring it to the front.

2 In the search field of the **Search** tab, type a partial or complete name for the role you want to edit.

3 In the **Roles** area, click  for the role you want to edit.

4 Edit the role as needed:

To edit this...	Do this...
Change to a different database directory service	From the **Datasource** list, select the database to be used as a datastore. For a database to appear in the list, you must first use the DataSource Administration portlet to connect to the external database. See "Managing External Data Sources" on page 174.
Edit the user query	In the **Query User** field, type a SQL query that returns a record for any user in the database that should be a member of the role.
Edit the group query	In the **Query Group** field, type a SQL query that returns a record for any group in the database that should be a member of the role.

5 At the bottom of the page, click **Apply**.

Deleting Roles

To delete a role, use the following procedure.

To delete a role

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Roles**.
- In the global navigation toolbar, click **Directory** and click the **Roles** tab to bring it to the front.

2 In the search field of the **Search** tab, type a partial or complete name for the role you want to delete.

3 For each role you want to delete, select the check box to the left of the **Role Name** column.

4 Click **Delete** and in the confirmation list, click **Delete** again.

webMethods

CHAPTER 6

Attribute Providers

What are Attribute Providers?

There are a variety of ways to provide and use attributes belonging to portal users. Basic to each user are the Portal attributes: portal home page, skin, and number of lines displayed per page. In addition, there are Principal Attribute Providers:

Attribute provider	Description
Core Attributes	A set of core attributes such as user ID and e-mail address. If the user is in the system directory service, some fields are editable. If the user is in an external directory service, all fields are read only. See "The Core Attributes Attribute Provider" on page 100.
User Profile	A rich set of user attributes that you can maintain regardless of which directory service the user is a member of. The attributes are stored in the portal database. Once established for each user, the User Profile Attributes can be used for wiring globally within the portal. See "The User Profile Attribute Provider" on page 103
LDAP	A set of attributes from the external directory service. You can specify which attributes are exposed from a given directory service. See "The LDAP Attribute Provider" on page 105.
Database	A set of attributes from an external database directory service. You can specify which attributes are exposed from a given directory service. See "The Database Attribute Provider" on page 107.
Notification	A set of addresses, such as e-mail, at which the user can receive notifications from the Portal server. See "The Notification Attribute Provider" on page 109.
Dynamic	A set of attributes whose values can change depending on the roles the user is a member of. See "The Dynamic Attribute Provider" on page 110.

Principal Attribute Providers are useful because any attribute they expose can be made available as wiring for a portlet. For example, suppose a portlet uses a postal code to display certain information when a user views a portal page. If the postal code is provided by wiring from a Principal Attribute Provider, when the postal code attribute is modified within a directory service, the portlet uses the modified attribute value.

Principal Attribute Providers are not enabled by default. To enable them, use the Principal Profile Administration portlet, described in "Managing the Display of Principal Attribute Providers" on page 116.

Using Attribute Providers

The profile page for a user, group, or role displays the various sets of attributes as well as memberships in groups or roles. Depending on the directory service to which a user or group belongs, you can edit some attributes, or expose them for use in global wiring.

To see an example of the profile page, as a portal administrator, in the global navigation toolbar, click **My Profile**. The page displayed is the profile page for PortalAdmin.

To see the profile page for any Principal (user, group, or role), follow this search procedure:

To search for a user, group, or role

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Users**, **Manage Groups**, or **Manage Roles**.
- In the global navigation toolbar, click **Directory** and click the **Users**, **Groups**, or **Roles** tab to bring it to the front.

2 In the search field of the **Search** tab, do one of the following:

To find this...	Specify...
A specific user	The user ID. A partial ID can match multiple entities.
A specific group	The group ID. A partial ID can match multiple entities.
A specific role	The role name. A partial name can match multiple entities
A list of all Principals on a directory service	Leave the search field empty.

3 (Users or groups) In the **Directory Service** list, choose the directory service that contains the users you want to find, and click **Go**.

The **Users**, **Groups**, or **Roles** area contains a list of Principals who match the search criteria.

4 In the **Users**, **Groups**, or **Roles** area, click  for the Principal for which you want to see the profile page.

The following sections describe the Attribute Providers available in webMethods Portal.

This Attribute Provider...	Is described here...
Core Attributes	"The Core Attributes Attribute Provider" on page 100
User Preferences	"The User Preferences Attribute Provider" on page 103
User Profile Attributes	"The User Profile Attribute Provider" on page 103
Ldap Attributes	"The LDAP Attribute Provider" on page 105
Database Attributes	"The Database Attribute Provider" on page 107
Notification Attributes	"The Notification Attribute Provider" on page 109
Dynamic Attributes	"The Dynamic Attribute Provider" on page 110

The Core Attributes Attribute Provider

The Core Attributes Attribute Provider contains a set of attributes such as user ID and e-mail address. Some fields are editable, depending on directory service membership.

User Information Tab

For individual users, the contents of the Core Attributes Attribute Provider appears on the profile page as the **User Information** tab. For users in the system directory service, some fields, such as the e-mail address, are editable. For members of external directory services, this information is not editable, but it is available for the global wiring feature described in "Using Global Wiring" on page 115.

To edit the User Information tab for a user

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Users**.
- In the global navigation toolbar, click **Directory**.

2 In the search field of the **Search** tab, type a partial or complete user ID.

3 In the **Directory Service** list, choose the directory service to which the user belongs, and click **Go**.

4 In the **Users** area, click  for the user.

5 Make changes to the following attributes as needed (all attributes shown here, but some are not editable):

Attribute	Description
User Id	The user ID that is part of the Distinguished Name for the user. Not editable.
Password	The user's password. Editable only for users in the system directory.
Confirm Password	A confirmation of the user's password. Editable only for users in the system directory.
First Name	The user's first name. Editable only for users in the system directory.
Last Name	The user's last name. Editable only for users in the system directory.
E-mail Address	The user's e-mail address. Editable only for users in the system directory.
Distinguished Name (DN)	The user's Distinguished Name. Not editable.

6 Click **Apply**.

Group Information Tab

For groups, the contents of the Core Attributes Attribute Provider appears on the profile page as the **Group Information** tab. For groups in the system directory service, some fields, such as the e-mail address, are editable. For groups in external directory services, this information is not editable but it is available for the global wiring feature described in "Using Global Wiring" on page 115.

To edit the Group Information tab for a group

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Groups**.
- In the global navigation toolbar, click **Directory** and click the **Groups** tab to bring it to the front.

2 In the search field of the **Search** tab, type a partial or complete group ID.

3 In the **Directory Service** list, choose the directory service to which the group belongs, and click **Go**.

4 In the **Groups** area, click  for the group.

5 Make changes to the following attributes as needed (all attributes shown here, but some are not editable):

Group Attribute	Description
Group ID	The group ID that is part of the Distinguished Name for the group. Not editable.
Group Name	The group's display name. Editable only for groups in the system directory.
E-mail Address	The group's e-mail address. Editable only for groups in the system directory.
Distinguished Name (DN)	The group's Distinguished Name. Not editable.

6 Click **Apply**.

Role Information Tab

For roles, the contents of the Core Attributes Attribute Provider appears on the profile page as the **Role Information** tab. The fields are not editable, but the information is available for the global wiring feature described in "Using Global Wiring" on page 115.

To view the Role Information tab for a group

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Roles**.
- In the global navigation toolbar, click **Directory** and click the **Roles** tab to bring it to the front.

2 In the search field of the **Search** tab, type a partial or complete role name.

3 Click **Go**.

4 In the **Roles** area, click  for the role.

The **Role Information** tab has the following information.

Group Attribute	Description
Group Name	The display name of the role
Distinguished Name (DN)	The Distinguished Name of the role
Principals	A list that contains all Principals that are members of the role.

The User Preferences Attribute Provider

User preferences are basic to any user of the portal. A portal administrator and the individual user (if given permission) can edit these basic attributes:

To use the User Preferences Attribute Provider

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Users**.
- In the global navigation toolbar, click **Directory**.

2 In the search field of the **Search** tab, type a partial or complete user ID.

3 In the **Directory Service** list, choose the directory service to which the user belongs, and click **Go**.

4 In the **Users** area, click  for the user.

5 On the profile page, click the **User Preferences** tab to bring it to the front.

6 Make modifications to the attributes as needed.

Attribute	Description
Home Page	The home page displayed when the user logs into the Portal. Click **Browse**. In the **Location** panel, browse to the page and click the  **Select** icon. With the page in the **Selected Items** panel, click **Select**.
Skin	The look of portal pages displayed for the user. In the **Skins** list, choose a skin.
Items Per Page	The number of items to display on one page when the Portal displays lists of resources. The user can navigate to succeeding items in the list. In the **Items Per Page** list, choose the number items.

7 Click **Apply**.

The User Profile Attribute Provider

The User Profile Attribute Provider has a rich set of user attributes that you can maintain regardless of which directory service the user is a member of. The attributes are stored in the portal database. Once established for each user, the User Profile Attributes can be used with the global wiring feature described in "Using Global Wiring" on page 115.

A portal administrator and the individual user (if given permission) can edit the User Profile attributes. You need to enter the user profile attributes individually for each user, or allow the user to do so. You can use all of the attributes or a subset that is appropriate to your needs.

To edit attributes in the User Profile Attribute Provider

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Users**.
- In the global navigation toolbar, click **Directory**.

2 In the search field of the **Search** tab, type a partial or complete user ID.

3 In the **Directory Service** list, choose the directory service to which the user belongs, and click **Go**.

4 In the **Users** area,  for the user.

5 On the profile page, click the **User Profile** tab to bring it to the front.

6 Make modifications to the attributes as needed.

Attribute	Description
Middle Name	The user's middle name.
Title	The user's title, for example, Mr., Mrs., or Ms. If the title you want to use does not appear in the list, select Other. You are prompted for the title you want to use.
Name Suffix	The suffix that should appear after the name, if any, for example, Jr., Sr., PhD, III. If the suffix you want to use does not appear in the list, select Other. You are prompted for the suffix you want to use.
Preferred Language/Locale	The language that the Portal server should use when displaying the user interface when the user logs in.
Country/Region ID	The country where the user is located.
Address 1 **Address 2**	The street address where the user is located.
City	The city where the user is located.
State/Province	The state or province where the user is located.
Postal Code	The postal code, for example, a ZIP Code if the user is located in the United States.

Attribute	Description
Custom Address	Optionally, additional information that is needed when more than a postal code is required for the address, for example, special instructions.
Phone 1 Area Code	The telephone area code.
Phone 1 Number	The telephone number.
Phone 1 Extension	The telephone extension, if any.
Phone 1 Country Code	The country code associated with the telephone number.

7 Click **Apply**.

Note: The First Name and Last Name attributes are taken from the User Information attributes for a user, and are not editable in the **User Profile** tab.

The LDAP Attribute Provider

The LDAP Attribute Provider displays a specified set of attributes from the external directory service to which a user or group belongs. The attributes displayed in the **LDAP Attributes** tab are not editable but they are available for the global wiring feature described in "Using Global Wiring" on page 115.

Note: The LDAP Attribute Provider is not enabled by default. See "Managing the Display of Principal Attribute Providers" on page 116.

This attribute provider is not applicable to users or groups in the system directory service. Similar attributes are included in the User Profile Attribute Provider described in "The User Profile Attribute Provider" on page 103.

Displaying the LDAP Attribute Provider

You cannot modify the contents of the **LDAP Attributes** tab, but you can display it if needed.

To view the LDAP Attribute Provider for a user or group

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Users** or **Manage Groups**.
- In the global navigation toolbar, click **Directory**.

2 In the search field of the **Search** tab, type a partial or complete user ID or group ID.

3 In the **Directory Service** list, choose the directory service to which the user or group belongs, and click **Go**.

4 In the **Users** or **Groups** area, click for the user or group.

5 On the profile page, click the **LDAP Attributes** tab to bring it to the front.

Exposing LDAP Attributes from an External Directory Service

The LDAP Attributes Provider displays user attributes that are exposed from an external directory service. You can expose selected attributes that are then available for the global wiring feature.

To expose LDAP attributes from an external directory service

1 As a portal administrator, in the global navigation toolbar, click **Administration**.

2 On the title bar, click **System**.

3 In the System folder, click **Service**.

4 In the Service folder, click **Directory**.

5 In the Directory folder, click **Principal Attribute Providers**.

6 In the Principal Attribute Provider Folder, do one of the following:

To expose attributes for...	Do this...
Users	Click **User Principal Attribute Providers**.
Groups	Click **Group Principal Attribute Providers**.

7 Click (Popup Menu) for **Ldap Attributes**, and then click **Properties**.

You should now be on the Properties page for Ldap Attributes.

8 Under **LDAP Attribute Names**, click **Add**.

9 Type the attribute name exactly as it is used in the external directory service and click **OK**.

For example, the attribute name for e-mail on a particular directory service might be `mail`.

10 Under **LDAP Attribute Titles**, click **Add**.

11 Type a display name for the attribute for use within the portal and click **OK**.

For example, for the `mail` attribute, you might type a display name of `E-mail`.

12 If you have multiple LDAP attributes, click the **Move Up** icon or **Move Down** icon to make sure the order in the **LDAP Attribute Names** and **LDAP Attribute Titles** lists are the same.

The order in which attributes and titles appear in the lists determine the order in which they are displayed in the **Ldap Attributes** tab on the Profile page.

13 Click **Apply**.

14 To determine if the LDAP attributes are exposed, follow the procedure in "Displaying the LDAP Attribute Provider" on page 105.

The Database Attribute Provider

The Database Attribute Provider displays a specified set of attributes from the external database directory service to which a user or group belongs. The attributes displayed in the **Database Attributes** tab are not editable but they are available for the global wiring feature described in "Using Global Wiring" on page 115.

Note: The Database Attribute Provider is not enabled by default. See "Managing the Display of Principal Attribute Providers" on page 116.

This attribute provider is not applicable to users or groups in the system directory service. Similar attributes are included in the User Profile Attribute Provider described in "The User Profile Attribute Provider" on page 103.

Displaying the Database Attribute Provider

You cannot modify the contents of the **Database Attributes** tab, but you can display it if needed.

To display the Database Attribute Provider for a user or group

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Users** or **Manage Groups**.
- In the global navigation toolbar, click **Directory**.

2 In the search field of the **Search** tab, type a partial or complete user ID or group ID.

3 In the **Directory Service** list, choose the directory service to which the user or group belongs, and click **Go**.

4 In the **Users** or **Groups** area, click for the user or group.

5 On the Profile Page, click the **Database Attributes** tab to bring it to the front.

Exposing Database Attributes from an External Directory Service

The Database Attributes Provider displays user or group attributes that are exposed from an external database directory service. You can expose selected attributes that are then available for the global wiring feature.

To expose database attributes from an external database directory service

1 As a portal administrator, in the global navigation toolbar, click **Administration**.

2 On the title bar, click **System**.

3 In the System folder, click **Service**.

4 In the Service folder, click **Directory**.

5 In the Directory folder, click **Principal Attribute Providers**.

6 In the Principal Attribute Provider Folder, do one of the following:

To expose attributes for...	Do this...
Users	Click **User Principal Attribute Providers**.
Groups	Click **Group Principal Attribute Providers**.

7 Click (Popup Menu) for **Database Attributes**, and then click **Properties**.

You should now be on the Properties page for Database Attributes.

8 Under **Attribute Names**, click **Add**.

9 Type the attribute name exactly as it is used in the external database directory service and click **OK**.

Important! An attribute used here must be returned by the Query Lookup User by ID attribute in the database directory service. See "Configuring a Database Directory Service" on page 51.

For example, the attribute name for postal code on a particular directory service might be `zipcode`.

10 Under **Attribute Titles**, click **Add**.

11 Type a display name for the attribute for use within the portal and click **OK**.

For example, for the `zipcode` attribute, you might type a display name of `Zip Code`.

12 If you have multiple database attributes, click the **Move Up** icon or **Move Down** icon to make sure the order in the **Attribute Names** and **Attribute Titles** lists are the same.

The order in which attributes and titles appear in the lists determine the order in which they are displayed in the **Database Attributes** tab on the profile page.

13 Click **Apply**.

14 To determine if the database attributes are exposed, follow the procedure in "Displaying the Database Attribute Provider" on page 107.

The Notification Attribute Provider

The Notification Attribute Provider allows you to specify the various addresses at which a user can receive notifications. A portal administrator and the individual user (if given permission) can edit these attributes.

Note: The Notification Attribute Provider is not enabled by default. See "Managing the Display of Principal Attribute Providers" on page 116.

To modify settings in the Notification Attribute Provider

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Users**.
- In the global navigation toolbar, click **Directory**.

2 In the search field of the **Search** tab, type a partial or complete user ID.

3 In the **Directory Service** list, choose the directory service to which the user belongs, and click **Go**.

4 In the **Users** area, click for the user.

5 On the Profile Page, click the **Notifications** tab to bring it to the front.

6 As appropriate, provide notification information:

In this field...	Do this...
E-mail Address	Not editable. Information for this field is taken from the User Information tab for the user.
Pager Text Address	Type the pager text address to which a notification should be sent (used, not by webMethods Portal, but by other webMethods components).

In this field...	Do this...
Mobile Phone Text Address	Type the mobile phone address to which a notification should be sent (used, not by webMethods Portal, but by other webMethods components).
Instant Messenger Service	From the list, select the IM service over which a notification is sent. Valid IM services are MSN, Yahoo!, AOL, and ICQ. In the field, type the username to which the notification should be sent. IM notification is available only if you have deployed the Instant Messenger Notification Administration portlet described in "Managing Instant Messenger Accounts" on page 194.
Instant Messenger User Name	Type the username for the Principal in the specified IM service.

7 Click **Apply**.

The Dynamic Attribute Provider

The Dynamic Attribute Provider allows you to provide an attribute for a role. A Principal that is a member of a role has all dynamic attributes of the role. If a user is a member of multiple roles, and multiple roles have attributes with the same key, you can determine which role will have precedence. In addition, you can assign an attribute value to a user, overriding the attribute values provided by roles. Dynamic attributes are available for the global wiring feature described in "Using Global Wiring" on page 115.

Note: The Dynamic Attribute Provider is valid only for roles. Users and groups have dynamic attributes based on roles of which they are members.

You can perform the following tasks with the Dynamic Attribute Provider:

This task...	Is described here...
Add a new dynamic attribute	"Adding Dynamic Attributes to a Role" on page 111
Edit an existing dynamic attribute	"Editing Dynamic Attributes for a Role" on page 112
Change the order in which dynamic attributes are displayed	"Changing the Display Order of Dynamic Attributes for a Role" on page 112

This task...	Is described here...
Change the order of precedence of a dynamic attribute for an individual user	"Changing the Order of Precedence of Dynamic Attributes" on page 113
Delete a dynamic attribute	"Deleting Dynamic Attributes for a Role" on page 115

Adding Dynamic Attributes to a Role

The following procedure describes how to create and edit dynamic attributes in a role.

To create and edit dynamic attributes for use by roles

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Roles**.
- In the global navigation toolbar, click **Directory** and click the **Roles** tab to bring it to the front.

2 In the search field of the **Search** tab, type a partial or complete name for the role you want to edit.

3 In the **Roles** area, click  for the role you want to edit.

4 If the **Dynamic Attributes** tab is not active, click it to bring it to the front.

5 Under **Attributes**, click **Add Attribute**.

6 In the **Add an Attribute** form, make the following entries:

In this field...	Do this...
Attribute Name	Type the internal name for the dynamic attribute. There are no restrictions on what characters you can use for this name.
Display Name	Type a display name for the dynamic attribute. This name can appear on UIs visible to individual users.
Data Type	From the list, select the data type for the attribute. Choices are String, Integer, Boolean, Long, Float, Double, and Date.
Value	Type the value to be assigned to the attribute. The value must be valid for the data type you have selected.

7 Click **Apply**.

Editing Dynamic Attributes for a Role

The following procedure describes edit dynamic attributes for a role.

To edit dynamic attributes for a role

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Roles**.
- In the global navigation toolbar, click **Directory** and click the **Roles** tab to bring it to the front.

2 In the search field of the **Search** tab, type a partial or complete name for the role you want to edit.

3 In the **Roles** area, click  for the role you want to edit.

4 If the **Dynamic Attributes** tab is not active, click it to bring it to the front.

5 Under **Attributes**, locate the dynamic attribute and make any of the following changes:

In this field...	Do this...
Attribute Name	Replace the old internal attribute name with a new one. There are no restrictions on what characters you can use for this name.
Display Name	Replace the old display name with a new one. This name can appear on UIs visible to individual users.
Value	Type the value to be assigned to the attribute. The value must be valid for the data type assigned when you first added the dynamic attribute.

6 Click **Apply**.

Changing the Display Order of Dynamic Attributes for a Role

You can change the order in which dynamic attributes are display for a role. Changing the order affects how the attributes are displayed in the **Role Member Attributes** area for a Principal, but does not otherwise affect how they are used by the Portal server.

To change the order of dynamic attributes for a role

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Roles**.

- In the global navigation toolbar, click **Directory** and click the **Roles** tab to bring it to the front.

2 In the search field of the **Search** tab, type a partial or complete name for the role you want to edit.

3 In the **Roles** area, click for the role you want to edit.

4 If the **Dynamic Attributes** tab is not active, click it to bring it to the front.

5 Click **Change Attribute Order**.

6 In the **Attributes** list, select a dynamic attribute, and click the **Move Up** icon or **Move Down** icon as needed.

7 After you have change the order of the dynamic attributes, click **Apply**.

Changing the Order of Precedence of Dynamic Attributes

You can manage the dynamic attributes for a user from the **Role Member Attributes** tab of the user's profile page. On this tab, you can specify the order of precedence in which dynamic attributes are taken from roles or you can add an attribute value that overrides the values provided by roles. The Dynamic Attribute Provider chooses a value for a specific attribute in this order of precedence:

1 If the **Role Member Attributes** tab has a specifically assigned value for an attribute in the **User Value** field, that value is used.

2 If there is no entry in the **User Value** field for an attribute, the attribute provider searches the **Role Precedence** list for the first occurrence of the attribute.

For example, a user is a member of three roles:

Role Precedence	Attribute	Data Type	Value	User Value
Role1	Dynamic_A	String	one	seven
	Dynamic_B	String	one	
Role2	Dynamic_A	String	two	
	Dynamic_B	String	two	
Role3	Dynamic_A	String	three	
	Dynamic_B	String	three	
	Dynamic_C	String	three	

The values of dynamic attributes for the user are determined as follows:

Attribute	Value	Reason
Dynamic_A	seven	The value in the **User Value** field overrides values from any role.
Dynamic_B	one	The first role containing the Dynamic_B attribute is Role1.
Dynamic_C	three	The first role containing the Dynamic_C attribute is Role3.

To manage precedence for attributes in the Role Member Attributes tab

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Users**.
- In the global navigation toolbar, click **Directory**.

2 In the search field of the **Search** tab, type a partial or complete user ID for the user.

3 In the **Directory Service** list, choose the directory service to which the user belongs, and click **Go**.

4 In the **Users** area, click  for the user.

5 On the Profile Page, click the **Roles** tab to bring it to the front.

The **Role Precedence** list contains roles of which the user is a member. If a role has dynamic attributes, they appear under **Role Member Attributes**.

6 To move a role up or down in the Role Precedence list, select the role and click the  **Move Up** icon or  **Move Down** icon.

The higher a role is in the list, the higher its precedence is. After you apply changes, **Role Member Attributes reflects** the new order.

7 To override an attribute value for this user, find any occurrence of the attribute under **Role Member Attributes** and, in the **User Value** field, type the value.

After you apply changes, the value you have typed appears in the **User Value** field for all occurrences of the attribute.

8 At the bottom of the **Role Member Attributes** tab, type **Apply**.

Deleting Dynamic Attributes for a Role

The following procedure describes hot to delete dynamic attributes for a role.

To delete dynamic attributes for a role

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Roles**.
- In the global navigation toolbar, click **Directory** and click the **Roles** tab to bring it to the front.

2 In the search field of the **Search** tab, type a partial or complete name for the role you want to edit.

3 In the **Roles** area, click  for the role you want to edit.

4 If the **Dynamic Attributes** tab is not active, click it to bring it to the front.

5 For each dynamic attribute you want to delete, select the check box in the **Select** column.

6 Click **Delete Selected Attributes**.

7 Click **Apply**.

Using Global Wiring

Users and groups have a set of Principal Attributes that you can wire to a portlet. For example, suppose a portlet uses a postal code to display certain information when a user views a portal page. If the postal code is provided by wiring from a Principal Attribute Provider, when the postal code attribute is modified within a directory service, the portlet uses the modified attribute value.

To wire a Principal Attribute to a portlet

1 At the right edge of the title bar for the portlet, click (Popup Menu) and then click **Wiring**.

2 In the **Portlet** list, choose **Other**.

A new window opens.

3 In the **Location** list, choose **Root**.

4 Click **Global Wiring Data**.

Depending on what Principal Attributes exist on the Portal server, you can see one or more of the following:

Principal Attribute Provider	Description
Core Attributes Wiring	A set of attributes valid for all users of the portal.
User Profile Wiring	A set of user attributes maintained by the portal administrator.
Ldap Attributes Wiring	A set of attributes exposed from external directory services.

5 Click the **Select** icon for the Principal Attribute set to move it to the **Selected** panel, and click **Select**.

6 Click **Browse**.

A new window opens, containing attributes belonging to the selected Principal Attribute Providers.

7 From the list, select the attribute you want to wire to the portlet and click **Select**.

The portlet is now wired to use the attribute value belonging to the user who views the portal page on which it appears.

Managing the Display of Principal Attribute Providers

If all Principal Attribute Providers were displayed on a Profile page by default, the page would be crowded and potentially difficult to read. The Principal Profile Administration portlet allows you to choose which Principal Attribute Providers to display on a Profile page and the order in which they appear. The portlet has the following areas:

This area...	Configures the display of...
USER Attribute Providers	The profile page for a user. By default, the Core Attributes Provider is displayed as the **User Information** tab. Other default attribute providers are Groups, Roles, and User Preferences. You can add any Principal Attribute Provider applicable to an individual user.

This area...	Configures the display of...
GROUP Attribute Providers	The profile page for a group. By default, the Core Attributes Provider is displayed as the **Group Information** tab.The default attribute providers are Groups and Group Members. You can add any Principal Attribute Provider applicable to a group.
ROLE Attribute Providers	The profile page for a role. By default, the Core Attributes Provider is displayed as the **Role Information** tab.The other default attribute provider is Dynamic Attributes.

You can perform the following tasks in the Principal Profile Administration portlet:

This task...	Is described here...
Add a Principal Attribute Provider to the Profile page	"Adding a Principal Attribute Provider" on page 117
Rearrange the position of Principal Attribute Providers on the Profile page	"Changing the Display Order for Principal Attribute Providers" on page 118
Remove a Principal Attribute Provider from the Profile page	"Removing a Principal Attribute Provider" on page 118

Adding a Principal Attribute Provider

To add a Principal Attribute Provider to a profile page, use the following procedure.

To add a Principal Attribute Provider to a profile page

1. As a portal administrator, browse to the **Administration Dashboard** and in the **User Management** folder, click **Principal Profile Administration**.
2. In the **USER**, **GROUP**, or **ROLE Attribute Providers** area, click **Add**.
3. On the left side of the portal resource selector, navigate to the Principal Attribute Provider and click the **Select** icon.

   The selected Principal Attribute Provider appears in the **Selected Items** panel. You can add multiple attribute providers as needed.
4. Click **Select**.
5. At the bottom of the page, click **Apply**.

Changing the Display Order for Principal Attribute Providers

To change the order in which Principal Attribute Providers appear on a profile page, use the following procedure.

To change the display order for Principal Attribute Providers

1. As a portal administrator, browse to the **Administration Dashboard** and in the **User Management** folder, click **Principal Profile Administration**.
2. In the **USER**, **GROUP**, or **ROLE Attribute Providers** area, select a Principal Attribute Provider from the list and click the **Move Up** icon or **Move Down** icon as needed.

   The first attribute provider in the list has the left-most position on the profile page, followed by the second attribute provider, and so on.
3. At the bottom of the page, click **Apply**.

Removing a Principal Attribute Provider

To remove a Principal Attribute Provider from a profile page, use the following procedure.

To remove a Principal Attribute Provider from a profile page

1. As a portal administrator, browse to the **Administration Dashboard** and in the **User Management** folder, click **Principal Profile Administration**.
2. In the **USER**, **GROUP**, or **ROLE Attribute Providers** area, select a Principal Attribute Provider from the list and then click **Remove**.
3. At the bottom of the page, click **Apply**.

webMethods

CHAPTER 7

Managing Portal Security

Overview of Portal Security

webMethods Portal has many different features and functions that contribute to its overall security infrastructure. When discussing security, it is always necessary to separate the discussion of authentication (Auth) from Authorization (AZ). While they are almost always related, the two concepts are distinct and work together to contribute to an overall security solution.

Authentication is defined as an assurance that a party to some computerized transaction is not an impostor. Authentication typically involves using a password, certificate, PIN, or other information that can be used to validate identity. The goal of authentication is to simply verify that "you are who you say you are."

Authorization is defined as the process of determining, by evaluating applicable access control information, whether a party is allowed to have the specified types of access to a particular resource. Usually, authorization is in the context of authentication. Once a party is authenticated, that party may be authorized to perform different types of activities.

webMethods Portal provides built-in infrastructure for both authentication and authorization. Portal is also is designed in a way that allows it to be extended so that existing security infrastructure can be re-used and leveraged for both authentication and authorization. This chapter discusses both the built in mechanisms and the extensible mechanisms.

In webMethods Portal, you can apply both authentication and authorization to the entire Portal server or to individual portal resources, which include folders, portal pages, portlets, links, documents, files, or custom objects.

Portal Authentication

webMethods Portal supports many different ways for users to identify themselves. These different methods are called Authentication Schemes. These schemes are simply different ways to gather user credentials and validate their authenticity. The different types of authentication schemes that are supported are:

This authentication scheme...	Is described here...
Forms authentication	"Forms Authentication" on page 121
Anonymous authentication	"Anonymous Authentication" on page 121
Basic authentication	"Basic Authentication" on page 121
NTLM authentication	"NTLM Authentication" on page 121
HTTP header authentication	"HTTP Header Authentication" on page 122
User-defined authentication schemes	"Extended and Extensible Authentication Schemes" on page 122

Forms Authentication

Forms authentication is the default authentication scheme for webMethods Portal. This authentication scheme presents a form to a user and gathers the necessary credentials that are passed to the Portal server by means of a form POST (data is passed to the Portal server's standard input). It is simple to customize the form or portal page that is used for authentication. It is also easy to present different forms and pages based on a wide variety of different criteria. For example, it is very likely that you would want to provide different login experiences for users accessing a portal from mobile devices than for users accessing the portal from a browser.

Anonymous Authentication

The anonymous authentication scheme is used when you do not want to challenge users for credentials. The Portal server honors an anonymous request and establishes a session with the portal as a special Portal Guest user, but the user is never prompted for credentials. The anonymous authentication scheme is used for unprotected areas of the portal that might be public facing and do not contain sensitive information. By associating the request with a session and a user ID of Portal Guest, an administrator can extend behaviors of anonymous access by controlling permissions of the Portal Guest user. Portal Guest is one of the default Principals installed as part of the system directory service (see "The System Directory Service" on page 58). It is also possible to track session activity of anonymous users for reporting requirements.

Basic Authentication

Basic authentication is one of the original and most compatible authentication schemes for programs using HTTP as a transport mechanism. Unfortunately, it is also one of the least secure, as it sends the username and password unencrypted to the server. The credentials are typically passed in as HTTP header parameters. The user experience for basic authentication is a popup window that renders in the native windowing system. For example, when you use basic authentication on Windows, a Windows dialog box opens to prompt the user for credentials before the request can be honored.

NTLM Authentication

NTLM (Windows NT LAN Manager) is an authentication protocol used in various Microsoft network protocol implementations and supported by the NTLM Security Support Provider (NTLMSSP). Originally used for authentication and negotiation of secure DCE/RPC, NTLM is also used throughout Microsoft's systems as an integrated single sign-on mechanism. On Windows deployments, when NTLM is set up and configured as an authentication scheme for webMethods Portal, users do not need to re-authenticate for portal resources if they are already logged into a Windows domain. To use NTLM authentication you need to explicitly specify the Primary Domain Controller for the domain, as described in "Specifying a Primary Domain Controller for NTLM" on page 134.

HTTP Header Authentication

webMethods Portal can be configured to accept External HTTP authentication credentials from third-party security and access control products (such as Computer Associates, Oblix, and so forth). These credentials are case sensitive, depending on platform and Web server and are most likely to be headers such as sm_user or SM_USER.

When you configure and set up HTTP header authentication within webMethods Portal, the Portal server uses credentials from a third-party authentication engine. Typically, these third parties use a security agent to intercept the request prior its getting to the Portal server. The basic flow of events in this request is:

1. The user attempts to go to a portal resource.
2. Prior to connecting to the portal, if the third-party security agent does not see the proper credentials, the agent redirects the user to a mechanism that gathers credentials.
3. The user provides the credentials and is then redirected back to the portal resource.
4. The portal reads the appropriate HTTP header and maps the user appropriately.

To configure this interaction between the Portal server and the third-party security agent, you need to take these actions:

1. After Portal installation, configure the third-party product to protect the Portal, which typically involves creating a policy that protects the portal URL.
2. Verify that the Portal server and the third-party security product are configured to look at the same directory store. See Chapter 3, “External Directory Services” for more information on directory services.
3. Configure the Portal server to look for the right HTTP header. See “Configuring External Configuration Credentials” on page 181.

Note: In the case of Siteminder from Computer Associates, it is also necessary to specify the Logout URI in Siteminder.

In the Siteminder Administrator applet, modify the logoutURI attribute to be '/?method=logout' (without the quotes)

Extended and Extensible Authentication Schemes

webMethods Portal provides hooks for developers to provide their own custom authentication schemes. To develop a custom authentication scheme, create a portlet, implement the correct interfaces, and register it with the Portal server. Once created, the new authentication scheme participates in the security infrastructure just like any other authentication scheme that is provided as part of webMethods Portal.

webMethods Portal has a concept of a default authentication scheme that is applied to an entire portal deployment. A newly configured Portal server uses forms as its default

authentication scheme. The portal challenges initial requests for protected resources with a form requiring the user to type a user name and password.

At any time, you can change the default authentication scheme for a Portal server to one of the registered authentication schemes. For more information, see "Specifying a Default Authentication Scheme" on page 131.

Every portal resource can have an authentication scheme that overrides the setting for the entire portal deployment. For example, you might have one set of pages and portlets that are completely anonymous and others that require user credentials to be presented. You would do this by associating the anonymous authentication scheme with the resources that do not require authentication. For information on managing authentication schemes for individual portal resources, see "Assigning an Authentication Scheme to a Portal Resource" on page 132.

Extending Login and Splash Page Behavior

To understand the login process and flow of events, it helps to analyze an example of how a portal administrator would extend a deployment to have custom login page behavior. The following set of steps uses the concepts of anonymous access, forms-based authentication, and login portlets to form a solution. Some of the steps require portal developer knowledge.

1. Design a portal page that has a login portlet on it. For information on creating portal pages, see the *webMethods Portal Design Guide*. Once the page is created, set the authentication scheme of the page to "anonymous" so everyone can get to the page and be presented with the login portlet.

   Optionally, you can set access rights on other parts of the page so that the login page has different appearances, depending on the identities of users. To address even broader requirements of personalizing the login page, it is also easy to set up custom login pages based on rules themselves.

2. After setting the authentication scheme of the page to anonymous, make sure the login portlet itself can be seen by a Portal Guest user (see Portal Guest in "The System Directory Service" on page 58).

   You may also want to modify the look and feel of the page by removing title bars, adding explicit instructions, or implementing other business requirements.

3. You can control where a user is redirected after login. In the Properties page for the login portlet, modify the Login Target property to the page where the user is redirected. Keep in mind that the Login Target be static or it can be an alias. If you use an alias like /user.current.start.page, you can alternatively set up start page rules to govern different start pages based on information about the user logging in.

It is also possible to redirect a request, if not authenticated, to go to the appropriate login page. To do so, modify the Redirect URI property of the authentication scheme assigned to the page. When an unauthenticated user requests the page, the user is redirected to the specified page. As with login targets, a redirect URI can be either static or an alias.

Security Assertion Markup Language

webMethods Portal supports single sign-on through the Security Assertion Markup Language (SAML), an XML-based framework for the exchange of security information. Using SAML, an application on a target computer grants access based on an assertion from the source computer.

webMethods Portal can be the calling program, or Security Provider, or can be configured as an Artifact Receiver, which authenticates the user sign-on for a target Web application. For information, see "Setting up Single Sign-On" on page 190.

Portal Authorization

After a user request has been authenticated by the Portal server, it is usually necessary to do some authorization checks to make sure that the user making the request has the necessary privilege to act on that resource. In webMethods Portal, the most common way to do authorization checks is by evaluating Access Control Lists (ACLs). ACLs can be associated with every kind of portal resource, such as portal pages, portlets, and so forth.

More advanced concepts like portal verbs and mechanics (groupings of business logic) are portal resources as well, and therefore also participate in the Portal ACL evaluation model. This feature allows portal developers to programmatically lock down capabilities of the Portal.

To understand the authorization engine in webMethods Portal, look at the composition of an ACL. An ACL is a list of Access Control Entries (ACEs). An ACE is a simple structure containing an element called a Principal and an element called a Right Set.

A *Principal* is a user, group or role. Some examples of Principals are:

Principal	Example of a Principal
User	Myles Perkins
Group	Members of the Perkins family
Role	A role definition that resolves to Myles, such as, "Users who have the 'Job Title" attribute value set to 'Product Manager.'"

Right Sets are groupings of actions that can be performed on a portal resource. An example of a Right Set is "Grant the ability to read." Right Sets themselves are broken down into two distinct parts, Capabilities and Settings. Different types of portal resources have different Capabilities associated with them. For example, portal pages have Capabilities that include "Add Portlet To Page" while folders have Capabilities that include "Create Sub Folder" and "Can Read Items in this Folder."

The other part of a Right Set, the Setting, can have four possible values: DELEGATE, DENY, GRANT or NONE. Each Capability that makes up a Right Set has a Setting value.

Right Sets are made up of many Capability-Setting pairings. Here is an example of a Right Set:

```
DENY + create sub folder
GRANT + read
```

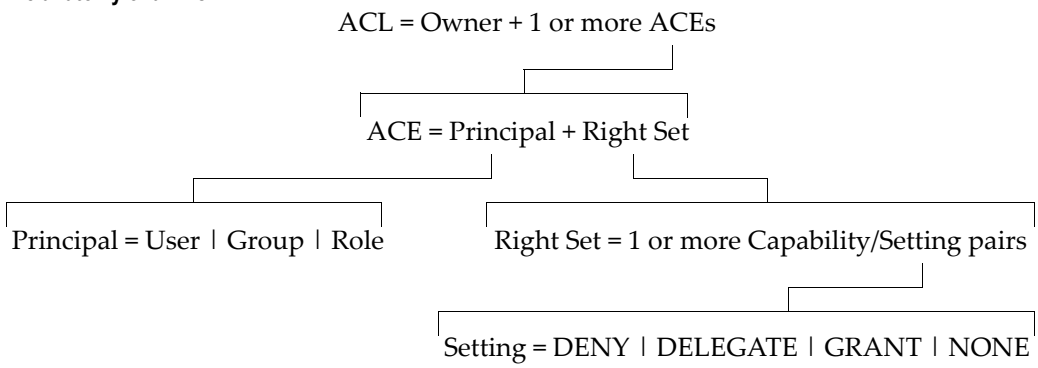
This particular Right Set is made up of two Capability-Setting pairings. If associated with a folder resource, this Right Set is resolved to deny a Principal the ability to create sub folders but grant the ability to actually read the folder.

The values for Settings have the following meanings:

This Setting value...	Has this effect for the Principal...
DENY	Denies the access to perform the capability.
GRANT	Explicitly grants access to perform the capability.
DELEGATE	Explicitly grants access and gives the right to assign the capability to another Principal.
NONE	Provides no explicit Setting. Authorization for this portal resource will be determined from another source. The decision process is shown in "Authorization Decisions in webMethods Portal" on page 129.

"The anatomy of an ACL" shows the relationships described in this section.

The anatomy of an ACL



As an example, to deny read access to Brian and the Marketing Group from the Engineering portal page, we would have the following setup:

- The portal resource is the Engineering portal page.

- The Engineering portal page has an ACL associated with it that contains two ACEs:

Principal	Right Set
Brian	DENY read
Marketing Group	DENY read

Controlling Permissions on Portal Resources

If you have authorization to change access to a portal resource, you use the Permissions portlet of webMethods Portal to assign access control to it. For example, if you are the owner of the Engineering folder in the previous example, a wizard in the Permissions portlet allows you to select one or more Principals and Right Sets, and associate them with that folder. For more information on controlling permissions, see "Managing Permissions" on page 135.

You do not have to explicitly grant and deny access for every newly created object. If you give your taxonomy a little forethought, you can keep the potential maintenance burden to a minimum. webMethods Portal employs a method called *static propagation* of its access rights on portal objects when they are created. This means that at creation time, a portal resource receives its access rights from its parent resource. If subsequent changes are made to the parent's access rights, these rights are not dynamically updated in the child object. However, you can use the Permissions portlet to cause parent objects to apply access rights explicitly to their children.

To illustrate static propagation and parent-child interaction as it relates to access rights, we will return to the previous example of the Engineering folder. In that example, the Engineering folder has BRIAN DENY. As the owner of the Engineering folder, a user creates a sub folder called Secret Project. Because of static propagation, the new Secret Project folder has BRIAN DENY at the time of creation. If the owner goes back and changes the permissions of the Engineering Folder to allow Brian access, Brian still does **not** have access to the Secret Project sub folder.

The user can, however, go back to the Engineering Folder and choose to apply the access rights explicitly down to the Secret Project sub folder (and potentially its children or sub folders as well). For more information, see "Managing Permissions to the Descendents of a Portal Resource" on page 138.

Authorization Determination

Now that you have a background in the concepts of making an authorization decision, you can see how access is actually determined at run time. When a portal resource is requested, the Portal server evaluates the ACL associated with that resource against the context in which the current request is generated. If a user requests access to a portal page, the ACL for that portal page is evaluated to determine whether the user request should be honored.

There are a few simple rules in determining authorization that handle a large percentage of any conflicts that may arise:

1. DENY always takes precedence over Allow (It is good to be paranoid in dealing with security)
2. Users always take precedence over groups and roles

To illustrate these rules and how they are applied to resolve conflict, we return to the example Engineering folder. In the following example, there are three ACE entries in the ACL associated with the Engineering folder:

```
BRIAN + DENY READ
MARKETING GROUP + DENY READ
BRIAN + GRANT READ
```

If Brian is a member of the Marketing group (and even if he wasn't) he is denied access to the Engineering folder. The user-based ACE takes precedence over the group-based ACE so the MARKETING GROUP ACE has no effect. Subsequently, the conflict between BRIAN being granted and denied access is resolved by denying access because DENY always wins.

"Authorization Decisions in webMethods Portal" on page 129 shows a detailed flow chart for authorization decisions. The flow chart highlights some of the conflict resolution activities.

Lists, pages, child objects and Searches

As mentioned earlier, a Principal can be a user, group, or role. Information about a Principal comes from a directory service. webMethods Portal has an embedded system directory service, described in "The System Directory Service" on page 58, as well as the ability to tie to external directory servers. Examples of these external directory servers are Active Directory, LDAP servers, ADAM, and an RDBMS. In addition, group and role information for webMethods Portal authorization decisions is determined when a user logs into the portal. If a user's group membership changes during an active portal session, the change is not reflected in the portal until the user logs out and logs back in. See Chapter 4, "User and Group Management" for more information about users, groups, roles, and directory services.

Security Realms

webMethods Portal provides a feature called Security Realms to augment its security model. *Security Realms* are collections of portal resources that share the same ACL. The use of Security Realms makes it possible to easily manage permissions on large numbers of portal resources. By adding the resources directly to a Security Realm, a portal administrator can add Principal information to that realm to control access.

Security Realms become very useful if you have a large number of portal resources and only a few access levels. For example, you may have a large customer-facing portal that has a large number of portlets, pages and areas of taxonomy. However, this portal may only have three levels of access that need to managed: Gold, Silver and Bronze. With each

level represented by a Security Realm with the appropriate pages, portlets and taxonomy elements in them, a portal administrator needs only to add a new customer to the appropriate Security Realm, granting the customer the correct level of access. Likewise, changing a customer from one level to another is a simple one-step operation.

Used in the appropriate deployments, Security Realms add value, not only by minimizing the administrative burden, but by greatly reducing the number of underlying records required to support the security model. For example, assume a portal has 500,000 portal resources and you are managing permissions for 50 users, all of whom have the same access:

- Managing permissions by ACL requires 25 million records in the Portal database.
- Managing permissions by Security Realm uses one Security Realm and one role with 50 members, requiring a total of three records in the Portal database.

It should be noted that if a portal resource is added to a Security Realm, the Security Realm access control has precedence over an individual ACL and authentication scheme for that resource.

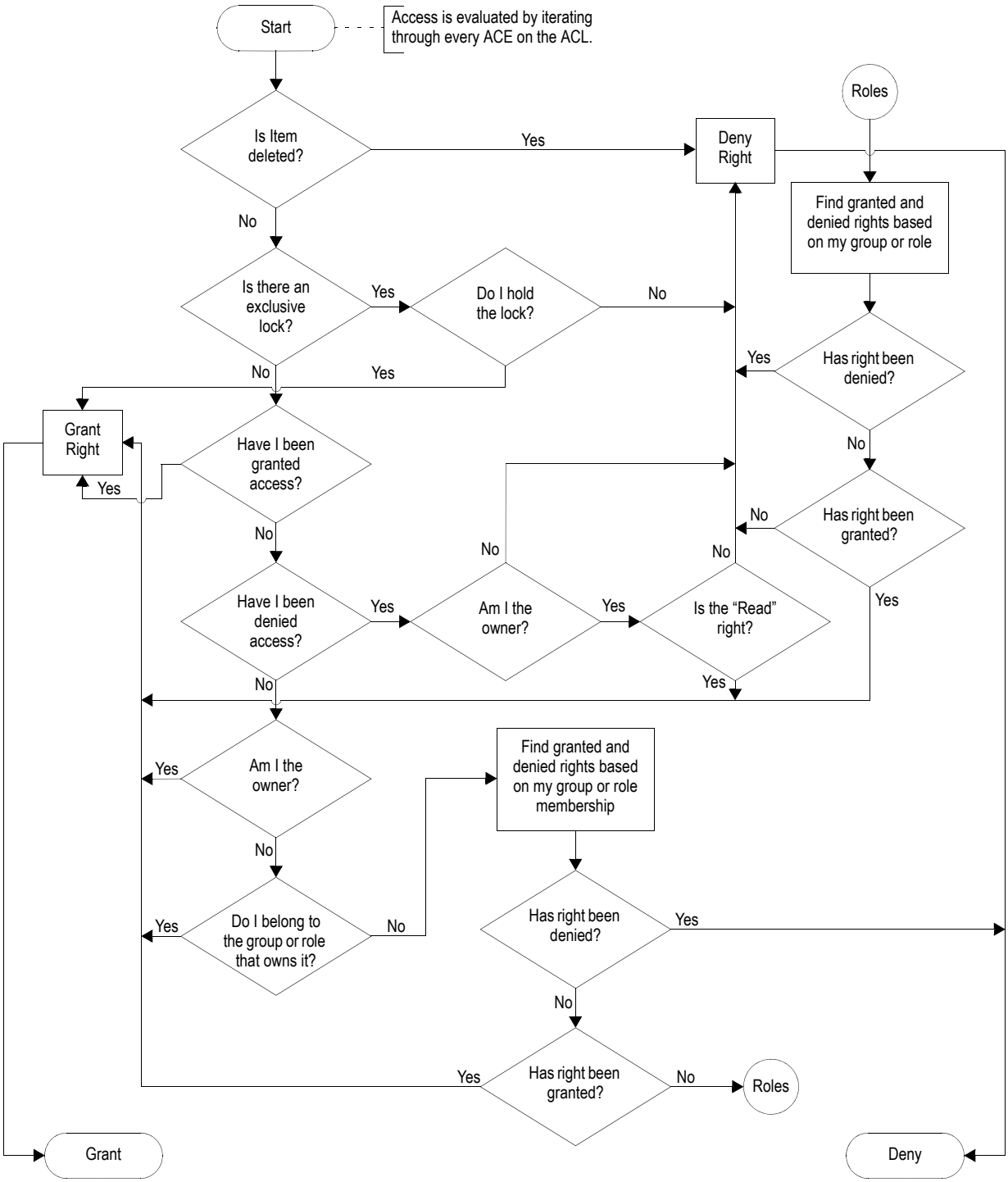
Portal Verbs and Access Control

A *portal verb* is an operation such as publishing, deleting, updating, subscribing, and setting permissions, which is available through the Portal API. As noted earlier, portal verbs are portal resources that can also participate in the security model of the portal. In this way, one can control granular access to portal capabilities programmatically as well as through the Administrative Dashboard. It should be noted that portal verbs typically have two levels of security checks, performed in this order:

1. Does the user have access to the portal verb itself?
2. Does the user have the rights to the resource upon which the portal verb is trying to act.

A portal administrator can control access to portal verbs using the Security Realms Administrative Portlet. webMethods Portal ships with default Security Realms to help administrators manage access to different portal capabilities. The default Security Realms are described in "Using Security Realms" on page 139.

Authorization Decisions in webMethods Portal



Managing Authentication

An authentication scheme is a way to gather user credentials and validate their authenticity. Within webMethods Portal, you can manage authentication for a Portal server as a whole by specifying a default authentication scheme. As delivered, the forms authentication scheme is the default for all portal resources. In addition, every portal resource can have an authentication scheme that overrides the setting for the entire portal deployment.

Note: A Security realm always takes precedence over an authentication scheme.

webMethods Portal uses the following authentication schemes:

Scheme	Description
anonymous	Allows unrestricted access to a portal resource. Used for unprotected areas of the portal that might be public facing and do not contain sensitive information. Because a user is not challenged for credentials, the anonymous authentication scheme is appropriate for login pages.
forms	Presents a form to an unauthenticated user and gathers the necessary credentials that are passed to the Portal server. The forms authentication scheme is the default for all portal resources because it redirects unauthenticated requests to a default portal login page.
basic	Typically passes credentials as HTTP header parameters. The user experience for basic authentication is a popup window that renders in the native windowing system.
httpHeader	Accepts external HTTP authentication credentials from third-party security and access control products (such as Computer Associates, Oblix, and so forth). After this authentication scheme is enabled, the Portal server ignores all other authentication schemes. See "Configuring External Configuration Credentials" on page 181.

Scheme	Description
ntlm	Used for authentication in various Microsoft network protocol implementations. On Windows deployments, when the ntlm authentication scheme is the default for a Portal server, users do not need to re-authenticate for portal resources if they are already logged into a Windows domain.To use NTLM authentication you need to explicitly specify the Primary Domain Controller for the domain, as described in "Specifying a Primary Domain Controller for NTLM" on page 134.
saml	Supports single sign-on through the Security Assertion Markup Language (SAML). Using SAML, an application on a target computer grants access based on an assertion from the source computer. See "Setting up Single Sign-On" on page 190.

You can perform the following types of tasks to manage authentication in webMethods Portal.

This task...	Is described here...
Change the default authentication scheme to be used for the Portal server.	"Specifying a Default Authentication Scheme" on page 131
Specify an authentication scheme for an individual portal resource	"Assigning an Authentication Scheme to a Portal Resource" on page 132
Redirect a user to a page other than the login page after logging in.	"Redirecting a User After Login" on page 133
Redirect an unauthenticated request for a protected portal resource to a specified login page other than the default login page.	"Redirecting an Unauthenticated Request" on page 134
For Portal servers using NTLM authentication, identifies the Primary Domain Controller responsible for authentication on the network.	"Specifying a Primary Domain Controller for NTLM" on page 134

Specifying a Default Authentication Scheme

When a Portal server is initialized, the forms authentication scheme is the default. the forms authentication scheme redirects unauthenticated requests to a default portal login page. You can change the default authentication scheme for a Portal server to one of the registered authentication schemes.

Note: Do not use this procedure if you intend to use the httpHeader authentication scheme to accept credentials from third-party security providers. Instead, use the HTTP Header Authentication Administration portlet, described in "Configuring External Configuration Credentials" on page 181.

To change the default authorization scheme for a Portal server

1. As a portal administrator, in the global navigation toolbar, click **Administration**.
2. On the title bar, click **System**.
3. In the System folder, click **Authentication Schemes**.
4. Click the **forms** authentication scheme (or whichever authentication scheme that is currently the default for the Portal server).
5. Under **Aliases** in the Properties page for the authentication scheme, click the auth.scheme.default alias to select it, and then click **Remove**.
6. At the bottom of the Properties page, click **Apply**.
7. Click the authentication scheme that is to become the default.
8. Under **Aliases** in the Properties page for the authentication scheme, click **Add**.
9. In the prompt window that opens, type `auth.scheme.default` and then click **OK**.
10. At the bottom of the Properties page, click **Apply**.

Assigning an Authentication Scheme to a Portal Resource

Every portal resource can have an authentication scheme that overrides the default authentication scheme for the Portal server.

To assign an authentication scheme for an individual portal resource

1. In the upper right-hand corner of the portal resource, such as a portal page, click the menu icon.
2. On the menu, click **Permissions**.
3. On the sub-tab bar of the Permissions page, click **Authentication Scheme**.
4. From the **Authentication Scheme** list, choose the authentication scheme to apply to the portal resource.

5 If you also want to apply the same authentication scheme to any portal pages or individual portlets contained by this portal page, select the **Apply to all descendants** check box.

6 Click **Done**.

Redirecting a User After Login

By default, when a user logs into a portal, the Portal server redirects the user to the same page. You can alter the Login Target property of the login portlet so a successful login redirects the user to a page of your choosing.

To redirect a user to another page after login

1 At the right edge of the title bar for the login portlet, click (Popup Menu) and then click **Properties**.

2 For the **Login Target** property, do one of the following:

Click this...	And do this...
Browse	On the left side of the portal resource selector, browse to the target page, click the **Select** icon, and then click **Select**.
Use Alias	In the **Alias Name** field of the portal resource selector, type the alias of the portal page to which the user should be redirected. Click **Test** to determine if the alias is valid and the alias target is the correct one. If the alias is correct, click **Select**.
	Note: If you type `/user.current.start.page`, the user is redirected to the start page defined by start-page rules.

3 At the bottom of the Properties page, click **Apply**.

Redirecting an Unauthenticated Request

Using the forms authentication scheme, an unauthenticated request to a protected portal resource results in the user being redirected to a default login page. Alternatively, you can redirect the user to a target of your choosing, whether it is a custom login page or a page that provides unprotected content.

To redirect an unauthenticated request to a different page

1 As a portal administrator, in the global navigation toolbar, click **Administration**.

2 On the title bar, click **System**.

3 In the System folder, click **Authentication Schemes**.

4 Click (Popup Menu) for the default authentication scheme, and then click **Properties**.

By default, the forms authentication scheme redirects unauthorized requests to the default login page. You can verify that an authorization scheme is the default by looking at the Properties page; the **Aliases** list contains the auth.scheme.default alias.

5 In the **Performs Redirect** list of the Properties page for the authentication scheme, make sure **Yes, this performs a redirect** is selected.

6 Under **Redirect URI**, do one of the following:

Click this...	And do this...
Browse	On the left side of the portal resource selector, browse to the resource, click the **Select** icon, and then click **Select**.
Use Alias	In the **Alias Name** field of the portal resource selector, type the name of the alias belonging to the portal resource to which the Principal should be redirected. Click **Test** to determine if the alias is valid and the alias target is the correct one. If the alias is correct, click **Select**.

7 At the bottom of the Properties Page, click **Apply**.

Specifying a Primary Domain Controller for NTLM

Using NTLM authentication, a user who has logged into a Windows domain does not have to re-authenticate to log in to a portal. A Primary Domain Controller is a Microsoft Windows server responsible for handling all accounts in a domain. To use NTLM authentication, you must explicitly specify the Primary Domain Controller in the NTLM Authentication Scheme.

To specify a Primary Domain Controller for NTLM authentication

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Configuration** folder, click **NTLM Authentication Administration**.

2 In the **Domain Controller Name** field of the Properties page, type the hostname of the Primary Domain Controller and click **Submit**.

To disable NTLM Authentication

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Configuration** folder, click **NTLM Authentication Administration**.

2 In the **Domain Controller Name** field of the Properties page, delete all characters including spaces and click **Submit**.

Managing Permissions

You can control the access of any Principal to a portal resource or a hierarchy of portal resources. Denying access to a portal resource also prevents a Principal from seeing the resource in portal navigation, such as in any listing of the resource's siblings or the contents of the resource's parent.

This task...	Is described here...
Determine which Principals have access rights specified for a portal resource and what rights are assigned to each.	"Viewing Permissions for a Portal Resource" on page 136
Add a Principal to the permissions list for a portal resource.	"Adding a Principal to the Permissions for a Portal Resource" on page 136
Modify the permissions for a Principal who currently has access rights assigned for the portal resource.	"Modifying Permissions for a Portal Resource" on page 137
Remove a Principal from the permissions list for a portal resource.	"Removing a Principal from Portal Resource Permissions" on page 138
Change the owner of a portal resource.	"Changing the Owner of a Portal Resource" on page 138
Manage permissions to the descendents of a portal resource, such as portlets that reside on a particular portal page.	"Managing Permissions to the Descendents of a Portal Resource" on page 138

The list of Principals who have specific permissions to a portal resource appears on the Permissions page for the resource. You can add Principals to the list, modify their permissions, or remove them from the list.

Viewing Permissions for a Portal Resource

To view the existing permissions for a portal resource

1. In the upper right-hand corner of the portal resource, click the menu icon.
2. On the menu, click **Permissions**.
3. For an entry (Principal) on the Permissions page, click the menu icon at the right and click **Edit Permissions**.

Note: The first entry in this listing is always the owner, and the owner always has complete control of the portal resource.

The Permissions column lists the various permissions (Capabilities) that are applicable to the portal resource. To the right of each permission, you can see the type of access (Setting) that is granted

4. To return to the Permissions listing, click **Cancel**.
5. When you are finished viewing permissions, click **Done**.

Adding a Principal to the Permissions for a Portal Resource

To add a Principal to the permissions for a portal resource

1. In the upper right-hand corner of the portal resource, click the menu icon.
2. On the menu, click **Permissions**.
3. On the Permissions page, click **Add Users/Groups**.
4. In the Location list, select the directory service to which the Principal you want to add belongs.
5. To add a Principal, click the **Select** icon.

   The selected Principal appears in the **Selected Items** panel.
6. Click **Next**.

7 For each action listed, select one of the following options:

This Option...	Means that you...
Delegate	Explicitly grant the Principal permission to execute the action, and you explicitly grant the Principal permission to edit the permissions of other users and groups for the particular action for this particular portal resource.
Grant	Explicitly grant the Principal permission to execute the action.
Deny	Explicitly deny the Principal permission to execute the action.
None	Neither explicitly grant nor deny the Principal permission to execute the action; the permissions settings for other Principals to which the Principal belongs will determine whether or not the Principal can execute the action.

8 Click **Finish**.

9 In the Permissions listing, click **Done**.

Modifying Permissions for a Portal Resource

To modify the permissions for a portal resource

1 In the upper right-hand corner of the portal resource, click the menu icon.

2 On the menu, click **Permissions**.

3 For the name corresponding to a specific Principal on the Permissions page, click the menu icon at the right and click **Edit Permissions**.

4 For each Capability listed, select one of the following options:

This Option...	Means that you...
Delegate	Explicitly grant the Principal permission to execute the action, and you explicitly grant the Principal permission to edit the permissions of other users and groups for the particular action for this particular portal resource.
Grant	Explicitly grant the Principal permission to execute the action.
Deny	Explicitly deny the Principal permission to execute the action.
None	Neither explicitly grant nor deny the Principal permission to execute the action; the permissions settings for other Principals to which the Principal belongs will determine whether or not the Principal can execute the action.

5 Click **Apply**.

6 In the Permissions listing, click **Done**.

Removing a Principal from Portal Resource Permissions

To remove a Principal from the permissions for a portal resource

1 In the upper right-hand corner of the portal resource, click the menu icon.

2 On the menu, click **Permissions**.

3 For the name corresponding to a specific Principal on the Permissions page, click the menu icon at the right and click **Remove**.

4 Click **Done**.

Changing the Owner of a Portal Resource

To change the owner of a portal resource

1 In the upper right-hand corner of the portal resource, click the menu icon.

2 On the menu, click **Permissions**.

3 On the Permissions page, locate the owner of the portal resource and click **Change**.

4 In the Location list, select the directory service to which the new owner belongs.

5 Click the **Select** icon.

The selected owner appears in the **Selected Items** panel.

6 Click **Set Owner**.

7 In the Permissions listing, click **Done**.

Managing Permissions to the Descendents of a Portal Resource

To apply permissions to the descendents of a portal resource

1 In the upper right-hand corner of the portal resource, click the menu icon.

2 On the menu, click **Permissions**.

3 On the Permissions page, select the **Apply to all descendents** check box and click **Apply**.

To remove all permissions to the descendents of a portal resource

1 In the upper right-hand corner of the portal resource, click the menu icon.

2 On the menu, click **Permissions**.

3 On the Permissions page, clear the **Apply to all descendents** check box and click **Apply**.

To remove permissions to the descendents of a portal resource for an individual Principal

1 In the upper right-hand corner of the portal resource, click the menu icon.

2 On the menu, click **Permissions**.

3 On the Permissions page, locate the Principal for whom you want to remove permissions to descendents of the portal resource and click the menu icon.

4 Click **Remove from all descendents** and then click **Apply**.

Using Security Realms

When you manage permissions, as described in "Managing Permissions" on page 135, you do so one resource at a time. This method is satisfactory for small portals, but can be cumbersome as the number of portal pages and users increases. Security Realms allow you to manage permissions for resources based on users, groups, or roles, making it easier to manage large portals. After a Security Realm is applied to a resource, individually set permissions do not apply unless you specifically choose to set them.

For convince, you can organize Security Realms into folders called *containers*. A Portal server has the following Security Realm containers by default:

This container...	Holds...
Forum Realms	Security Realms that manage permissions for portal forums.
Portal Resources	Security Realms that manage permissions for Portal server resources

The Security Realms Administration portlet allows you to create, rename, and remove containers, as described in these sections:

This task...	Is described here...
Create a container	"Creating a Container" on page 141

This task...	Is described here...
Remove a container	"Removing a Container" on page 142
Rename a container	"Renaming a Container" on page 142

There are several default Security Realms that manage permissions for Portal server resources, all of which reside in the Portal Resources container. Portal administrators have the right to read, modify or delete the portal resources; other users have permissions as described here:

This Security Realm...	Manages permissions for these Portal server portlets...
Administrative Commands	Administrative portlets. Permits only portal administrators to read, modify, or delete the resource.
Directory Management Commands	Portlets that manage users, group, and roles. Permits portal users to view or execute the resource. Anonymous users are denied access.
Directory Service Commands	Portlets that manage directory services. Permits portal users to view or execute the portlets. Anonymous users are denied access.
Portal Developer Commands	Portlets for the development and maintenance of portal pages and content. Members of the Portal Developers group are granted the right to read, modify, or delete the resource. Permits portal users to view or execute the resource. Anonymous users are denied access.
Public Commands	Portlets for interacting with a portal, such as logging in. Permits all users, including anonymous users, to read or execute the resource, but not to modify or delete it.
Restricted Commands	Portlets for interacting with a portal after one has logged in. Permits users who have logged in to read or execute the resource, but not to modify or delete it. Anonymous users are denied access.
User Profile Management Commands	Portlets that control the look and feel of the portal. Permits portal users to view or execute the resource. Anonymous users are denied access.

The Security Realms Administration portlet allows you to create and manage Security Realms you can use for your portal content. There are several tasks you can perform in this portlet:

This task...	Is described here...
Create a Security Realm	"Creating a Security Realm" on page 143
Remove a Security Realm	"Removing a Security Realm" on page 144
Rename a Security Realm	"Renaming a Security Realm" on page 145
Add resources to a Security Realm	"Adding Resources to a Security Realm" on page 145
Remove resources from a Security Realm	"Removing Resources from a Security Realm" on page 146

Creating a Container

You can create a container at the same level as the default containers or you can create a container within a container.

To create a new container

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Configuration** folder, click **Security Realms Administration**.

2 Do one of the following:

To create a container...	Do this...
At this level	Go on to step 3.
Within a container at this level	Click the name of the container to reveal its contents.

3 Click the **Create New Container** tab to bring it to the front.

4 In the **Name** field, type a display name for the container.

5 (Optional) In the **Description** field, type a description.

6 Click **Create Container**.

Removing a Container

Important! If you remove a container, any Security Realms or other containers within it are also removed.

To remove a container, do the following:

To remove a container

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Configuration** folder, click **Security Realms Administration**.

2 Click (Popup Menu) for the container you want to remove, and then click **Remove Container**.

Renaming a Container

To rename a container, do the following:

To rename a container

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Configuration** folder, click **Security Realms Administration**.

2 Click (Popup Menu) for the container you want to rename, and then click **Modify Container**.

3 In the **Name** field, type the new name.

4 Optionally, in the **Description** field, type a new description.

5 Click **Update**.

Creating a Security Realm

To create a Security Realm, do the following:

To create a new Security Realm

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Configuration** folder, click **Security Realms Administration**.

2 Click the name of the container in which to create the Security Realm.

For information on creating containers, see "Creating a Container" on page 141.

Note: After you have created a Security Realm within a container, you cannot move it to another container.

3 Click the **Create New Security Realm** tab to bring it to the front.

4 In the **Name** field, type a display name for the Security Realm.

5 (Optional) In the **Description** field, type a description.

6 (Optional) To add an external policy provider, under **Location**, navigate to the policy provider and click the **Select** icon.

The selected policy provider appears in the **Selected Items** panel.

7 Click **Create Security Realm**.

The new Security Realm appears on the **View Security Realms** tab of the Security Realms Administration page.

8 Click (Popup Menu) for the new Security Realm, and then click **Configure Permissions**.

9 Click the **Access List** tab to bring it to the front.

10 To add new users, groups, or roles to the access list, click **Add Users/Groups**.

11 In the left panel browse to any of the following:

Within this...	Browse to these...
Roles	Any role. You can collect LDAP query, rule-based, or static roles into a Security Realm.
Directory Services	Any user or group that can be located within all available directory services.

12 Click the **Select** icon for a user, group, or role to move it to the **Selected** panel.

You can accumulate multiple entries in the **Selected** panel.

13 Click **Select**.

14 Click (Popup Menu) for the each member of the Security Realm, Click **Edit Permissions** and do the following:

a For each action listed, select one of the following options:

This Option...	Means that you...
Delegate	Explicitly grant the user, group, or role permission to execute the action, and you explicitly grant the user, group, or role permission to edit the permissions of other users and groups for the particular action for this particular page.
Grant	Explicitly grant the user, group, or role permission to execute the action.
Deny	Explicitly deny the user, group, or role permission to execute the action.
None	Neither explicitly grant nor explicitly deny the user, group, or role permission to execute the action; the permissions settings for other groups to which the user, group, or role belongs will determine whether or not the user, group, or role can execute the action.

b Select the **Apply to all descendents** option if the permissions set here are to apply to all descendents of a resource.

If you leave the option clear for a portal page, portlets on the page are not affected by the permission set for the page.

c Click **Apply**.

15 When permissions have been set, at the bottom of the page, click **Done**.

Removing a Security Realm

To remove a Security Realm, do the following:

To remove a Security Realm

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Configuration** folder, click **Security Realms Administration**.

2 Click the name of the container in which the Security Realm resides.

3 Click (Popup Menu) for the Security Realm you want to remove, and then click **Remove Security Realm**.

Renaming a Security Realm

To rename a Security Realm, do the following:

To rename a Security Realm

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Configuration** folder, click **Security Realms Administration**.

2 Click the name of the container in which the Security Realm resides.

3 Click (Popup Menu) for the Security Realm you want to rename, and then click **Modify Security Realm**.

4 In the **Name** field, type the new name.

5 Optionally, in the **Description** field, type a new description.

6 Click **Update Security Realm**.

Adding Resources to a Security Realm

To add resources to a Security Realm, do the following:

To add resources to a Security Realm

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Configuration** folder, click **Security Realms Administration**.

2 Click (Popup Menu) for the Security Realm you want to manage, and then click **Manage Objects**.

3 In the **Manage Security Realm** tab, click **Add Portal Resource**.

4 In the left panel, browse to a Portal resource to be added to the Security Realm.

5 To move the resource to the **Selected** panel, click the **Select** icon for the resource.

Multiple resources can appear in the **Selected** panel at the same time.

6 At the bottom of the page, click **Add Items**.

Removing Resources from a Security Realm

To remove resources from a Security Realm, do the following:

To remove resources from a Security Realm

1. As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Configuration** folder, click **Security Realms Administration**.
2. Click the name of the container in which the Security Realm resides.
3. Click (Popup Menu) for the Security Realm you want to manage, and then click **Manage Objects**.
4. In the for the resource you want to remove, click **Remove**.

Clearing Session Passwords from Memory

By default, when a user logs in, the password is stored until the user logs out or until the session times out. You can, however, cause the Portal server to clear passwords from memory immediately after the login is completed. This setting clears all passwords presented to the Portal server; you cannot clear passwords on a case-by-case basis.

To clear session passwords from memory

1. As a portal administrator, in the global navigation toolbar, click **Administration**.
2. On the title bar, click **System**.
3. In the System folder, click **Managers**.
4. In the Managers folder, click **sessionManager**.
5. In the sessionManager folder, click **default**.
6. In the default folder, click **validate**
7. Under **Configuration XML** in the validate Properties page, click **Edit**.
8. In the Edit Text Area, change this text:

   ```
   clearPassword="false"
   ```

   to this:

   ```
   clearPassword="true"
   ```
9. To save the file and close the editor, click **Update**.
10. In the validate Properties page, click **Apply**.

This setting remains until you change it, even if you stop and restart the Portal server.

To retain session passwords in memory

- Follow the steps in the procedure to clear passwords, except that in the Edit Text Area, change this text:

  ```
  clearPassword=”true”
  ```

  to this:

  ```
  clearPassword=”false”
  ```

webMethods

CHAPTER 8

Portal Analysis, Reporting, and Troubleshooting

Overview

webMethods Portal provides administrators with a number of tools for analyzing, reporting, managing, and maintaining portal deployment. This chapter provides detailed instructions on how to use these tools.

Controlling Portal Logging

The Logging Configuration portlet enables you to control logging for the Portal server. With this portlet, you can set thresholds for individual categories of logging information. In addition, you can set the collector threshold for the View Logging Messages portlet.

By default, Portal log files roll over to a new set of files once a day at midnight. You can modify the frequency of log-file rollover using the logging.properties file.

Setting Logging Thresholds

As it runs, the Portal server collects logging information in a variety of categories. Using the Logging Configuration portlet you can determine the level of information provided for each category individually. This feature makes it possible to limit the growth of log files except in categories where you want more information.

A logging message is assigned one of four log levels of increasing importance. When you set a threshold at a particular log level, messages at that level, and all higher levels, are included. The following table describes the levels, from the lowest level to the highest:

Log level	Description
DEBUG	The server issues messages at multiple points within a Portal event. DEBUG messages are useful for debugging a problem, but log files grow quickly. Messages of all log levels are included in the log.
INFO	The server issues a message to indicate that a Portal event has occurred. Messages of all log levels except DEBUG are included in the log.
WARN	A non-fatal error has occurred. Only WARN and FATAL messages are included in the log.
FATAL	A fatal error has occurred. Only FATAL messages are included in the log.

Logging information is collected in two stages, which you can control independently. When the Portal server collects a log message, it sends the message to a specified category. If the log level of the message meets or exceeds the category threshold, the Portal server forwards the message on to the logging outputs; if the message does not meet the

threshold, it is discarded. The logging categories are displayed on the **Logging Thresholds** tab of the Logging Configuration portlet.

The Portal server forwards messages that meet a category threshold to valid outputs for the category. If the log level of the message meets or exceeds the output threshold, the Portal server writes the message to the output; if the message does not meet the threshold, it is discarded.

You can set both category thresholds and output thresholds on the **Logging Thresholds** tab of the Logging Configuration portlet. A category threshold takes precedence over an output threshold; a logging message discarded for a category cannot be written to output.

To set a category or output threshold

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Analysis** folder, click **Logging Configuration**.

2 Click the **Logging Thresholds** tab to bring it to the front.

3 For each logging category you want to modify, in the **Category Threshold** list, select the log level to the lowest level of message you want to accept.

Tip! To set all logging categories to the same logging level, click (Popup Menu) to the right of the **Category Threshold** label and then click the log level to be used.

4 For each output threshold you want to modify, in the **Output Threshold** list, select the log level to the lowest level of message you want to accept.

Tip! To set all logging categories to the same logging level, click (Popup Menu) to the right of the **Output Threshold** label and then click the log level to be used.

5 At the bottom of the page, click **Apply**.

Setting the Collector Threshold for View Logging Messages

The Logging Collector is an agent that listens for logging activity and log messages that meet the collector threshold available to the View Logging Messages portlet, described in "Viewing Logging Messages" on page 153. You can use the **Logging Collector** tab of the Logging Configuration portlet to enable or disable message collection and control the log level of messages being collected.

Note: Input to the Logging Collector is dependent on the category threshold settings described in "Setting Logging Thresholds" on page 150. The Logging Collector cannot receive a message with a log level that does not meet a category threshold.

To control the collection of messages for the View Logging portlet

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Analysis** folder, click **Logging Configuration**.

2 Click the **Logging Collector** tab to bring it to the front.

3 In the **Collector Threshold** list, select the log level to the lowest level of message you want to collect for the View Logging Messages portlet.

Valid log levels are INFO, WARN (the default), and FATAL.

4 Under **Log Collection Enabled**, do one of the following:

Click this option...	To do this...
Yes	Enable the collection of log messages.
No	Disable the collection of log messages.

5 Click **Apply**.

Modifying the Log-File Rollover Period

Portal log files reside in the `/webMethods_install_dir/P`ortal/server/*portal_server*/logs directory. Periodically, the logging process rolls over to a new set of files, making it easier locate a specific date and time, and to discard old log files as needed. By default, the rollover occurs once a day at midnight, but you can modify the rollover period from once a month to once a minute. The directory structure for log files looks like this:

/logs/*YYYY-MM-DD*/*Host*/*HH-MM*

Where this...	Means...
YYYY	The calendar year in which the rollover occurs.
MM	The month in which the rollover occurs.
DD	The day in which the rollover occurs.
Host	The name of the machine on which the Portal server is running.
HH	The hour at which the rollover occurs.
MM	The minute at which the rollover occurs.

If the default Portal server is running on the machine myhost and the rollover occurs at midnight on April 15th, 2005, log files are created here:

`/webMethods_install_dir/P`ortal/server/default/logs/2005-04-15/myhost/00-00

To change the log-file rollover period, you need to modify a single line in this file:

*/webMethods_install_dir/*Portal/server/*portal_server*/config/logging.properties

To modify the log-file rollover period

1 Open the logging.properties file in a text editor.

2 Locate this portion of the file:

```
#   Sets the rollover pattern.
#It is possible to specify a rollover period from once a month to once a minute.
#log4j.rollover='.'yyyy-MM          (Rollover at the beginning of each month)
#log4j.rollover='.'yyyy-ww         (Rollover at the first day of each week. The
#                                   The first day of the week depends on the
#                                   locale.)
#log4j.rollover='.'yyyy-MM-dd       (Rollover at midnight each day.)
#log4j.rollover='.'yyyy-MM-dd-a     (Rollover at midnight and midday of each
day.)
#log4j.rollover='.'yyyy-MM-dd-HH    (Rollover at the top of every hour.)
#log4j.rollover='.'yyyy-MM-dd-HH-mm (Rollover at the top of every minute.)

#Modify the following line by copying and pasting from the examples in the
#preceding lines.
log4j.rollover='.'yyyy-MM-dd
```

3 Replace the date-and-time portion of the `log4j.rollover` statement with one from the example statements in the preceding lines.

For example, to cause log-file rollover to occur at the top of every hour, change the statement from this:

```
log4j.rollover='.'yyyy-MM-dd
```

to this:

```
log4j.rollover='.'yyyy-MM-dd-HH
```

Do not include the descriptive comments that accompany the example statements.

4 Restart the Portal server.

Changes to the logging.properties file do not take effect until the Portal server is restarted.

Viewing Logging Messages

The View Logging Messages Portlet allows you to search for the occurrence of log messages that have been collected by the Logging Collector. In the View Logging Messages portlet, you can set search criteria, view the messages, and clear the search index.

You can only search for log messages that have already been collected. For the View Logging Messages portlet to be useful, you need to make sure you are collecting the right messages for your needs. Use the Logging Configuration portlet to set message collection criteria:

In this tab...	Do this...
Logging Threshold	Make sure the threshold settings in the **Category Threshold** column are set low enough that your messages are not discarded before they reach the Logging Collector. See "Setting Logging Thresholds" on page 150.
Logging Collector	Make sure the collector is enabled and that the threshold is set low enough that your messages are collected. See "Setting the Collector Threshold for View Logging Messages" on page 151.

You can manage the search engine used for logging searches using the Search Administration portlet that can be found in the Portal Content folder of the Administration Dashboard. See "Managing the Search Engine" on page 208.

Using the Search Logged Messages Tab

Use the **Search Logged Messages** tab of the View Logging Messages portlet to set the criteria and initiate log searches.

To search for log messages

1. As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Analysis** folder, click **View Logging Messages**.
2. Click the **Search Logged Messages** tab to bring it to the front.
3. Use the search fields provided to set criteria for your log-message search:

Search field	Description
Priority Threshold	From the list, select the lowest log-level of messages to be included in the search. Valid levels are INFO, WARN, and FATAL. You can also choose to have no level selected.
Log Category	From the list, select a log category to be included in the search.
Log Message	Type the text of the log message to be included in the search.
Host	Type the name of the host on which the Portal server is running.

Search field	Description
Timestamp Range	The two fields in Timestamp Range allow you to select beginning and ending days from which to search. Click the **Select Date / Time** icon to display a calendar, and then choose a date.
Stack Trace	Type a stack trace to be included in the search.
Thread	Type a thread to be included in the search.

4 In the **Maximum Results** list, choose the maximum number of log messages to be displayed. The default is 100 messages.

5 In the **Match Criteria** list, choose one of these criteria:

This criterion...	Does this...
All Fields	(Default) Causes the search engine to include only those messages that match all search fields in which you have entries.
Any Fields	Causes the search engine to include a log message that matches any of the search criteria you have selected.

6 To start the search, click **Search**.

The search results appear in the **View Logged Messages** tab, which appears only when you conduct a search.

Using the Manage Search Index Tab

Use the **Manage Search Index** tab of the View Logging Messages portlet to remove all log messages that have been collected by the Logging Collector.

To remove log messages from the Logging Collector

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Analysis** folder, click **View Logging Messages**.

2 Click the **Manage Search Index** tab to bring it to the front.

3 Click **Click here to clear the logging search index**.

The Logging Collector removes all collected log messages and displays the **Search Logged Messages** tab.

Monitoring Real-Time User Activity

The Session Monitor portlet can be used to monitor real-time user activity for a portal deployment and send status messages to active portal users by means of e-mail. For active users, a portal administrator can accomplish two important tasks:

- view a user's profile information
- send the user e-mail directly from within this portlet

To view all active portal sessions

1. As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Analysis** folder, click **Session Monitor**.
2. Optionally, on the list of active sessions, click a portal user's name to view that user's profile.
3. Optionally, on the list of active sessions, click the **E-mail this Page** icon.

   If you have an e-mail client installed on the machine you are working on, an e-mail message window is displayed allowing you to compose and send an e-mail to the selected user. If the user does not have a valid e-mail address in User Information, the To field is empty.

Collecting Data for My webMethods

The Portal DCA portlet serves as a DCA (Data Collection Agent) to gather data about the operation of the Portal server. The DCA makes the data available to webMethods Optimize for analysis. For more information on Optimize, see the *webMethods Optimize and webMethods Manager Console Administrator's Guide* and *webMethods Optimize and webMethods Manager Console User's Guide*.

The Portal DCA portlet is part of a standard webMethods Portal installation but is not deployed by default. Before you can use the portlet, you must first deploy it on the Portal server and configure it.

Deploying the Portal DCA Portlet

To deploy the Portal DCA portlet on a Portal server

1 Locate the Portal DCA portlet at this location in the webMethods Portal directory structure:

```
/webMethods_install_dir/Portal/components/admin/analysis/
wm_portaldca.pdp
```

2 Copy the wm_portaldca.pdp file and paste it into the Deploy directory:

```
/webMethods_install_dir/Portal/server/server_name/deploy
```

where *server_name* is the name of the Portal server. After a few seconds, the portlet is automatically deployed on the server.

Configuring the Portal DCA Portlet

To configure the Portal DCA portlet, you need to know the location of the Optimize server to which the collection agent will send data.

To configure the Portal DCA portlet

1 As a portal administrator, in the global navigation toolbar, click **Administration**.

2 On the title bar, click **System**.

3 In the System folder, click **Portlets**.

4 In the Portlets folder, click **Administration**.

5 In the Administration folder, click **Portal DCA**.

6 On the Portal DCA page, click **Edit Settings**.

7 In the **Portal System Name Used by Optimize** field, type the name by which this Portal server is to be identified on the Optimize server.

8 In the **Optimize Server Address and Port** field, type the host name and port number of the Optimize server to receive the data.

The default port number for Optimize servers is 12005.

9 In the **Update Timer Value** field, type the time interval, in seconds, at which data updates occur.

The default is 60 seconds. The more often data updates occur, the greater the impact on Portal server performance.

10 Use the **Enable Optimize webService satellite to monitor Portal** check box to control data collection by doing one of the following:

Do this...	To have this effect...
Select the check box	Enable the collection of data. Even if the collection monitor settings in the following step are selected, the Portal DCA portlet does not collect data unless this setting is enabled.
Clear the check box	Disable all collection of data.

11 Select to enable or clear to disable, the three types of data collection monitors for the Portal server:

Select this...	To collect this kind of data...
Enable Cache Monitor	Caches used by the Portal server. Types of information include cache size, maximum size, and number of valid entries.
Enable Event Monitor	Events that occur on the Portal server. Types of events include creates and deletes, logins, publishes, and updates.
Enable JVM Memory Monitor	JVM memory levels on the Portal server. Memory values include free memory, maximum allowed memory and total memory.

12 Click **Apply**.

Note: If you have trouble getting the Optimize server to recognize the DCA, check the Properties page for the Portal DCA portlet and make sure the complete **Endpoint Address** value is http://*host_name*:*port_number*/glue/WSOperationalDataCollector.

Portal Collection Data

The data collection agent collects the following information about the Portal server:

Collection type	Description
Cache (Alias, Container, Portlet Transient, Presentation, Thing, Thing Relation)	
Cache Size	Current number of entries in the cache.
Expirable Entries	Current number of cache entries that can expire.
Expired Entries	Number of entries that have expired (the expiration date has been met) during the collection interval.

Collection type	Description
Invalid Entries	Number of entries that are no longer considered to be valid. A large number may indicate that a failure has occurred.
Maximum Size	The maximum number of entries that can appear in the cache. This value is set manually.
Total Dependencies	The total number of dependencies for all entries.
Unique Keys	The number of entries with unique keys.
Valid Entries	The number of entries in the cache that are considered to be valid.
Events	
Create	The number of Create events that have occurred during the collection interval.
Delete	The number of Delete events that have occurred during the collection interval.
Get	The number of Get events that have occurred during the collection interval.
First Login	The number of times that users have logged in for the first time in a day.
Login	The number of logins during the day.
Login Failed	The number of failed logins during the day.
Logout	The number of logouts during the day.
Publish	The number of publish events during the collection interval
Subscribe	The number of notifications of subscription events during the collection interval
Unknown	The number of unknown or undefined login events.
Update	The number of portal resource updates during the collection interval.
Memory	
Free memory	The amount of free memory (memory available for future allocated objects) in the Java Virtual Machine, measured in bytes.

Collection type	Description
Max Allowed Memory	The maximum amount of memory the Java Virtual Machine will attempt to use, measured in bytes.
Total Memory	The total amount of memory (memory available for current and future objects) in the Java Virtual Machine, measured in bytes.

Collecting Data about Portal Events

The Events Collector portlet collects data about events on the Portal server so they can be used by other portlets.

When deployed on a Portal server, the Events Collector portlet captures information about certain types of portal events and places them in the portal database.

- Login and logout.
- Get events, such as when a user browses a portal page.
- Operation events, such as when an object is created, updated, moved, or deleted.

For each event captured, the portlet collects information on the user associated with the event, the date and time of the event, the host name of the machine, and where possible, information about the operation being performed.

To take advantage of data collected by this portlet, another portlet performs a query against the portal database and then displays the results on a portal page. Assuming that samples have been included in the installation of webMethods Portal, you can find examples of portlets that perform these queries in the *webMethods_install_dir*/Portal/samples/analysis directory. To try one or more of these portlets, you need to take the following actions:

This task...	Described here...
Deploy the Events Collector portlet and the sample portlets on the Portal server.	"Deploying the Events Collector Portlet" on page 161.
Configure the Events Collector portlet	"Configuring the Events Collector Configuration Portlet" on page 161
Populate a portal page with the sample portlets that display portal events	The *webMethods Portal Design Guide*.

Sample portlets include portlet source code so you can import the portlet into the Portlet Developer and see how they function. An example of the database schema used by the Events Collector portlet for placing data into the portal database appears in "Events Collector Database Schema" on page 162.

Deploying the Events Collector Portlet

The Events Collector portlet is part of a standard webMethods Portal installation but is not deployed by default. Before you can use the portlet, you must first deploy it on the Portal server.

To deploy the Events Collector Configuration portlet on a Portal server

1 Locate the Events Collector Configuration portlet at this location in the webMethods Portal directory structure:

`/webMethods_install_dir/Portal/components/extras/analysis/wm_eventscollector.pdp`

2 Copy the wm_eventscollector.pdp file and paste it into the Deploy directory:

`/webMethods_install_dir/Portal/server/server_name/deploy`

where *server_name* is the name of the Portal server. After a few seconds, the portlet is automatically deployed on the server.

Configuring the Events Collector Configuration Portlet

By default, the Events Collector Configuration portlet is ready to begin collecting data on events as soon as you deploy it, but you may want to change how long data is kept, or to disable the portlet.

To configure the Events Collector Configuration portlet

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Analysis** folder, click **Events Collector Configuration**.

Note: If you cannot find the Events Collector Configuration portlet in the Portal Analysis folder, it may not be deployed. See "Deploying the Events Collector Portlet" on page 161.

2 Use the **Collection Enabled** check box to control data collection by doing one of the following:

Do this...	To have this effect...
Select the check box	Enable the collection of portal event data. Data collection is enabled by default.
Clear the check box	Disable the collection of portal event data.

3 In the **Keep Data for** list, select how long to keep portal event data.

Choices range from **One Day** to **One Year**. The default is **One Month**.

4 Click **Apply**.

Events Collector Database Schema

The Events Collector portlet uses the following database schema. Examples of queries used against these tables appear in *webMethods_install_dir*/Portal/samples/analysis.

```
tblwEvents (main table where events data is being collected)
   idEvent      - Primary key
   idType       - Foreign key to tblwEventTypes. Stores the type of an event.
   idHost       - Foreign key to tblwEventHosts. Stores the host where the event occurs.
   timestamp    - Time stamp of an event, defined as the number of milliseconds since epoch
                  (java.lang.System.currentDateMillis()).
   userID       - Database ID of the user who performed an operation.

   thingID_1    - object_1. For example, for Get type events this is the database ID of the object
                  being viewed.
   thingID_2    - object_2. Used in rare cases where two objects are involved, for example when an
                  object is created. Then object_1 is the database ID of the container, and object_2
                  is the database ID of an object that was created.
   action       - Used for Login events: 1 - user logged in, 2 - user logged out.

tblwEventHosts (stores mapping between hostID and hostname)
   idHost       - Host id.
   hostname     - Actual host name where the event occurs.
tblwEventTypes (stores mapping between eventID and eventTypeName)
   idType       - Event type ID.
   eventType    - Event type name.

Possible eventType name values:
   com.webmethods.portal.event.add.impl.CreateEvent    - New object is created.
   com.webmethods.portal.event.impl.GetEvent           - Object is being browsed.
   com.webmethods.portal.event.system.impl.LoginEvent  - User logs in/out.
   com.webmethods.portal.event.modify.impl.UpdateEvent - Object is updated.
   com.webmethods.portal.event.remove.impl.DeleteEvent - Object is deleted.
```

Capturing Portal Environment Diagnostic Information

If you need help from webMethods Customer Care in troubleshooting problems with webMethods Portal, you will likely be asked to supply information about the server environment. webMethods provides a tool that captures information about the Portal configuration along with a set of log files, and writes it to a .zip file you can attach to e-mail. If you collect this information before you contact Customer Care, it can speed up the resolution of your problem.

You run the Portal environment capture tool from the command line. The tool captures information regardless of whether the server instance is running or not.

To capture Portal environment diagnostic information

1. At a command line prompt, type the following command to move to the Portal env_capture directory:

   ```
   cd webMethods_install_dir/Portal/tools/env_capture
   ```

2. Run the run.bat or run.sh script, appending it with the server name, as shown in the example below:

   ```
   > run -s server_name
   ```

   where *server_name* corresponds to the name of the Portal instance. For example:

   ```
   > run -s default
   ```

The environment capture tool creates this file:

webMethods_install_dir/Portal/tools/env_capture/portal-env.zip

webMethods

CHAPTER 9

Portal Configuration

Overview

webMethods Portal provides administrators with a number of tools that can be used to help configure your Portal server. You perform these tasks after installing and configuring a default Portal server instance. This chapter provides detailed instructions on how to use the Portal Configuration tools and portlets to configure your webMethods Portal deployment.

Managing Portal Aliases

The Alias Management portlet lets you manage URL aliases as portal objects. With this portlet, you can create, view, modify, or delete custom URL aliases and create more friendly URLs for various parts of your portal.

For example, if you want to create an area of the portal for the Sales Department, and you have already created a folder for the Sales team in your portal's Public Folders, it might be referenced by a non-intuitive URL such as:

http://*portalserver*/meta/default/folder/0000002216

To make it easier for the Sales team to remember the location of the Sales portal, you can use the Alias Management portlet to create a more user friendly URL such as:

http://*portalserver*/Sales

You can perform the following tasks within the Alias Management portlet:

This task...	Is described here...
Create a new alias	"Creating an Alias to a Portal Resource" on page 167
Search for aliases	"Searching for Portal Aliases" on page 168
Save alias searches	"Using Saved Alias Searches" on page 170
Modify the target portal resource for an alias	"Modifying an Alias to Point to a Different Portal Resource" on page 173
Delete an alias	"Deleting an Alias" on page 174

Creating an Alias to a Portal Resource

To create an alias for a portal resource, use the following procedure.

To create an alias to a portal resource

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Configuration** folder, click **Alias Management**.

2 In the **Portal Aliases** area, click **Create**.

3 In the **Alias Name** field, type the name for the new alias you want to create (such as Sales).

Note: Do not include spaces in your alias name, or the alias will not function properly.

4 In the **Target** area, select a target for the new alias by doing one of the following:

If you want to...	Do this...
Target a portal resource	Select the **Resource** option and then click **Browse**. On the left side of the portal resource selector, browse to the resource (folder, item, or portlet), click the **Select** icon for the resource, and then click **Select**. **Note:** To pass parameters or invoke a portal command on the resource the alias references, click the **Append this string** option, and then append the string portion of the alias.
Target an external resource	Select the **Path** option. In the Path box, type the path to the resource. For example, `http://www.webmethods.com`

5 After you have selected the target for your alias, click **Add Alias**.

Tip! Confirm that your alias behaves as expected by browsing to the user-friendly URL for your new alias.

By default, when you create an alias, it is appended to the root URL for your Portal server. For example, if you create an alias called Sales, you can access the new alias by typing the URL `http://portalserver:port/Sales`.

Searching for Portal Aliases

You can use the Alias Management portlet to search for existing portal aliases. The portlet places search results in a list from which you can modify or delete aliases, or view target resources.

Tip! In the alias search field, you can use a single wildcard character (*) to substitute for text anywhere within the name.

Performing a Simple Alias Search

To search for portal aliases, use the following procedure.

To perform a simple search for portal aliases

1. As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Configuration** folder, click **Alias Management**.
2. In the **Portal Alias Search** area, click the **Search** tab to bring it to the front.
3. In the search field, type the name of the alias you want to find.

   To specifically include or exclude system aliases from search criteria, see "Specifically Including or Excluding System Aliases" on page 168.
4. Click **Go**.

   All aliases that match the search appear in a table in the **Portal Aliases** area.

Specifically Including or Excluding System Aliases

To include or exclude system aliases during a search, use the following procedure.

To include or exclude system aliases during a search

1. As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Configuration** folder, click **Alias Management**.
2. In the **Portal Alias Search** area, click the **Search** tab to bring it to the front.
3. In the search field, type the name of the alias you want to find.
4. In the **Search** tab, click **Refine**.

5 In the **Include System Aliases** list, choose one of the following:

Choose this...	To do this...
Yes	Include system aliases in the search
No	Exclude system aliases from the search

6 Click **Go**.

7 To close the refined search area, click **Close**.

Searching Within a Folder

To limit an alias search to within a folder, use the following procedure.

To limit an aliases to within a folder

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Configuration** folder, click **Alias Management**.

2 In the **Portal Alias Search** area, click the **Advanced** tab to bring it to the front.

3 In the search field, type the name of the alias you want to find.

4 In the **Include System Aliases** list, choose one of the following:

Choose this...	To do this...
Yes	Include system aliases in the search
No	Exclude system aliases from the search

5 For the **Alias Target** area, do one of the following:

Click this...	And do this...
Browse	On the left side of the portal resource selector, browse to the target resource, click the **Select** icon for the resource, and then click **Select**.
Use Alias	In the **Alias Name** field of the portal resource selector, type the alias of the target resource. Click **Test** to determine if the alias is valid and the alias target is the correct one. If the alias is correct, click **Select**.

6 Click **Go**.

Performing an Advanced Alias Search

To perform an advanced search for portal aliases, use the following procedure.

To perform an advanced search for portal aliases

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Configuration** folder, click **Alias Management**.

2 In the **Portal Alias Search** area, click the **Advanced** tab to bring it to the front.

3 In the search field, type the name of the alias you want to find.

4 Modify any or all of the following search criteria:

Search criteria	Actions
System aliases	In the **Include System Aliases** list, choose one of the following:

Choice	Action
Yes	Includes system aliases in the search
No	Excludes system aliases from the search

Search criteria	Actions
Search within a resource	For the **Alias Target** area, do one of the following:

Choice	Action
Browse	On the left side of the portal resource selector, browse to the target resource, click the **Select** icon for the resource, and then click **Select**.
Use Alias	In the **Alias Name** field of the portal resource selector, type the alias of the target resource. Click **Test** to determine if the alias is valid and the alias target is the correct one. If the alias is correct, click **Select**.

5 To perform the alias search, click **Go**.

6 If you want to save the advanced alias search, click to the right of the **Go** button.

Using Saved Alias Searches

You can save an alias search for regular use. The following sections describe how to save, use, modify, and delete alias searches.

Saving an Alias Search

To save an alias search, use the following procedure.

To save an alias search

1. As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Configuration** folder, click **Alias Management**.
2. In the **Portal Alias Search** area, click the **Search** tab to bring it to the front.
3. In the search field, type the alias search you want to perform.
4. Click  to the right of the **Go** button.
5. In the Save Search dialog box, type a name for the search and click **OK**.

The use of saved searches is described in "Performing Saved Searches for Aliases" next in this section.

Performing Saved Searches for Aliases

To use a previously saved alias search, use the following procedure.

To use a previously saved alias search

1. As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Configuration** folder, click **Alias Management**.
2. In the **Portal Alias Search** area, click the **Saved** tab to bring it to the front.
3. In the **Saved Search** list, choose the saved search you want to perform.
4. Click **Go**.

Modifying Saved Alias Searches

To modify a previously saved alias search, use the following procedure.

To modify a previously saved alias search

1. As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Configuration** folder, click **Alias Management**.
2. In the **Portal Alias Search** area, click the **Saved** tab to bring it to the front.
3. In the **Saved Search** list, choose the saved search you want to modify.
4. Click **Details**.

5 Modify any or all of the following search criteria:

Search criteria	Actions
Search field	In the search field, type the alias search you want to perform.
System aliases	In the **Include System Aliases** list, choose one of the following:

Choice	Action
Yes	Includes system aliases in the search
No	Excludes system aliases from the search

Search criteria	Actions
Search within a resource	For the **Alias Target** area, do one of the following:

Choice	Action
Browse	On the left side of the portal resource selector, browse to the target resource, click the **Select** icon for the resource, and then click **Select**.
Use Alias	In the **Alias Name** field of the portal resource selector, type the alias of the target resource. Click **Test** to determine if the alias is valid and the alias target is the correct one. If the alias is correct, click **Select**.

6 To save the modified alias search, click to the right of the **Go** button.

7 If you want to perform the modified search, click **Go**.

8 To close the expanded area, click **Close**.

Deleting Saved Alias Searches

To delete a previously saved alias search, use the following procedure.

To delete a previously saved alias search

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Configuration** folder, click **Alias Management**.

2 In the **Portal Alias Search** area, click the **Saved** tab to bring it to the front.

3 In the **Saved Search** list, choose the saved search you want to delete.

4 Click **Delete**.

Modifying an Alias to Point to a Different Portal Resource

To modify an alias to point to a different portal resource, follow these steps:

To modify an existing alias to point to a different portal resource

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Configuration** folder, click **Alias Management**.

2 Use the **Portal Alias Search** area to find the alias you want to modify, as described in "Searching for Portal Aliases" on page 168.

3 Click  in the row of the alias to be modified.

4 In the **New Target** area, select a new target for the alias by doing one of the following:

If you want to...	Do this...
Target a portal resource	Select the **Resource** option and then click **Browse**. On the left side of the portal resource selector, browse to the resource (folder, item, or portlet), click the **Select** icon for the resource, and then click **Select**. The new resource replaces the one previously selected. **Note:** To pass parameters or invoke a portal command on the resource the alias references, click the **Append this string** option, and then append the string portion of the alias.
Target an external resource	Select the **Path** option. In the Path box, type the path to the resource. For example, `http://www.webmethods.com`

5 In the **Update Alias** area, click **Update**.

Deleting an Alias

To delete an alias, use the following procedure.

To delete an existing alias

1. As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Configuration** folder, click **Alias Management**.
2. Use the **Portal Alias Search** area to find the alias you want to delete, as described in "Searching for Portal Aliases" on page 168.
3. In the Portal Aliases field, select the check box to the left of the alias to be deleted.

Note: To select all aliases in the list for deletion, click the check icon at the top of the column of check boxes.

4. In the **Portal Aliases** area, click **Delete**.

Managing External Data Sources

The DataSource Administration portlet allows you to connect to external data sources (such as databases) and make them available to the portal. From the DataSource Administration portlet, you can add a new data source.

After you configure a data source through the Administration Dashboard, you can use the data source to create data-driven portlets that interact with the underlying database(s). The DataSource Administration portlet supports connections to the following database products: Microsoft SQL Server, Oracle, DB2 Universal, Sybase Adaptive Server, or Informix databases. There are also options for configuring an ODBC and custom connection.

Note: Before you configure a data source for connecting to DB2 Universal, Sybase Adaptive Server, or Informix databases, you *must* have a corresponding database driver for each respective database application. webMethods Portal distribution does *not* include database drivers for DB2 Universal, Sybase Adaptive Server, or Informix databases.

You can perform the following tasks within the Datasource Administration portlet:

This task...	Is described here...
Add a data source for a Microsoft SQL Server database	"Adding a Microsoft SQL Server Data Source" on page 175
Add a data source for a Oracle database	"Adding a Oracle Data Source" on page 176

This task...	Is described here...
Add a data source for a DB2 Universal database	"Adding a DB2 Universal Data Source" on page 176
Add a data source for a Sybase Adaptive Server database	"Adding a Sybase Adaptive Server Data Source" on page 177
Add a data source for an Informix database	"Adding an Informix Data Source" on page 178
Add a data source for a generic ODBC database	"Adding a Generic ODBC Data Source" on page 179
Add a data source for a custom database	"Adding a Custom Data Source" on page 179
Modify an existing data source	"Modifying an Existing Data Source" on page 180
Delete an existing data source	"Deleting an Existing Data Source" on page 181

Adding a Microsoft SQL Server Data Source

To add a new data source for a Microsoft SQL Server database, do the following.

To add a new data source for Microsoft SQL Server databases

1. As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Configuration** folder, click **DataSource Administration**.
2. Click **Add DataSource**.
3. Type a unique **DataSource Name** to be used by webMethods Portal on the **View DataSources** tab.
4. Type a **Display Name** to be used when you identify a data source to use for a database directory service.
5. Select **MS SQL Server** from the **Server Type** list and click **Next**.
6. Type the SQL Server host name.
7. Type the port number used by the SQL Server. The default port is `1433`.
8. Type the database name.
9. Type a valid SQL Server username and password that, at a minimum, has READ access to the database to which you will connect.
10. Click **Submit**.

Adding a Oracle Data Source

To add a new data source for an Oracle database, do the following.

To add a new data source for Oracle databases

1. As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Configuration** folder, click **DataSource Administration**.
2. Click **Add DataSource**.
3. Type a unique **DataSource Name** to be used by webMethods Portal on the **View DataSources** tab.
4. Type a **Display Name** to be used when you identify a data source to use for a database directory service.
5. Select **Oracle** from the **Server Type** list and click **Next**.
6. Type the Oracle host name.
7. Type the port number on which the Oracle host is running. The default port is `1521`.
8. Type the instance name (SID) for the database.
9. Type a valid Oracle database username and password that, at a minimum, has READ access to the database to which you will connect.
10. Click **Submit**.

Adding a DB2 Universal Data Source

To add a new data source for a DB2 Universal database, do the following.

To add a new data source for DB2 Universal databases

1. Before creating a data source connection to a DB2 Universal database, you need to make sure you have the appropriate DB2 JDBC drivers available to the portal. Depending on your DB2 server type, the required DB2 Driver files are:
   - common.jar
   - db2jcc.jar
   - db2jcc_license_cu.jar (you may have a different db2jcc_license_XX.jar file depending on your DB2 Server type).

   You can get the driver files from your existing DB2 product installation. To make these drivers available to the portal, copy the driver `*.jar` files into the *`webMethods_install_dir`*`/Portal/server/`*`portal_instance_name`*`/lib` directory.

2 With the drivers in place, restart your webMethods Portal instance.

3 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Configuration** folder, click **DataSource Administration**.

4 Click **Add DataSource**.

5 Type a unique **DataSource Name** to be used by webMethods Portal on the **View DataSources** tab.

6 Type a **Display Name** to be used when you identify a data source to use for a database directory service.

7 Select **DB2 Universal** from the **Server Type** list and click **Next**.

8 Type the DB2 host name.

9 Type the port number that DB2 is running on.

10 Type the instance name for the database.

11 Type a valid DB2 username and password that, at a minimum, has READ access to the database to which you are connecting.

12 Click **Submit**.

Adding a Sybase Adaptive Server Data Source

To add a new data source for a Sybase Adaptive Server database, do the following.

To add a new data source for Sybase Adaptive Server databases

1 Before creating a data source connection to a Sybase Adaptive Server database, you need to make sure you have the appropriate Sybase, jConnect JDBC drivers available to the portal. The required Sybase driver files are:

- 3Pclasses.jar
- jconn2.jar
- jTDS2.jar

You can get the driver files from your existing Sybase Adaptive Server installation. To make these drivers available to the portal, copy the driver `*.jar` files into the *`webMethods_install_dir`*`/Portal/server/`*`portal_instance_name`*`/lib` directory.

2 With the drivers in place, restart your webMethods Portal instance.

3 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Configuration** folder, click **DataSource Administration**.

4 Click **Add DataSource**.

5 Type a unique **DataSource Name** to be used by webMethods Portal on the **View DataSources** tab.

6 Type a **Display Name** to be used when you identify a data source to use for a database directory service.

7 Select **Sybase Adaptive Server** from the **Server Type** list and click **Next**.

8 Type the Sybase Server host name.

9 Type the port number that Sybase Server is running on.

10 Type the instance name for the database.

11 Type a valid Sybase Server username and password that, at a minimum, has READ access to the database to which you are connecting.

12 Click **Submit**.

Adding an Informix Data Source

To add a new data source for an Informix database, do the following.

To add a new data source for Informix databases

1 Before creating a data source connection to an Informix database, you need to make sure you have the appropriate Informix JDBC driver available to the portal. The required driver is jfxjdbc.jar

The driver file can be obtained from your existing Informix production installation or from the IBM support site (http://www.ibm.com/support).

To make these drivers available to the portal, copy the driver `*.jar` files into the *`webMethods_install_dir`*`/Portal/server/`*`portal_instance_name`*`/lib` directory.

2 With the drivers in place, restart your webMethods Portal instance.

3 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Configuration** folder, click **DataSource Administration**.

4 Click **Add DataSource**.

5 Type a unique **DataSource Name** to be used by webMethods Portal on the **View DataSources** tab.

6 Type a **Display Name** to be used when you identify a data source to use for a database directory service.

7 Select **Informix** from the **Server Type** list and click **Next**.

8 Type the Informix host name.

9 Type the port number on which the Informix host is running.

10 Type the Informix server name.

11 Type a valid Informix username and password that, at a minimum, has READ access to the database to which you are connecting.

12 Click **Submit**.

Adding a Generic ODBC Data Source

Note: webMethods Portal can use any ODBC connection that is manually configured at the operating system level (such as Windows Server). webMethods Portal uses a standard Java JDBC-ODBC bridge driver to connect to the ODBC data sources on the underlying operating system. Consult your Microsoft vendor documentation for details on how to configure an ODBC data source at the operating system level.

To add a new data source for a generic ODBC database, do the following.

To add a new data source for generic ODBC databases

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Configuration** folder, click **DataSource Administration**.

2 Click **Add DataSource**.

3 Type a unique **DataSource Name** to be used by webMethods Portal on the **View DataSources** tab.

4 Type a **Display Name** to be used when you identify a data source to use for a database directory service.

5 Select **Generic ODBC** from the **Server Type** list and click **Next**.

6 Type the ODBC data source name that matches the ODBC data source configured at the operating system level.

7 Type a valid username and password that, at a minimum, has READ access to the database to which you are connecting.

8 Click **Submit**.

Adding a Custom Data Source

Note: This option is an advanced data source configuration and requires you to specify a valid JDBC driver class name, connection URL, username, and password. Consult your vendor documentation to get specific instructions on where to locate the proper database drivers for the database application that you wish to connect to from the portal.

To add a new data source for a custom database, do the following.

To add a new data source for a custom database

1. Before creating a customized data source, you must ensure that you have appropriate drivers available to the portal. To make these drivers available to the portal, copy the driver `*.jar` files into your *`webMethods_install_dir`*`/Portal/server/`*`portal_instance_name`*`/lib` directory.
2. With the drivers in place, restart your webMethods Portal instance.
3. As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Configuration** folder, click **DataSource Administration**.
4. Click **Add DataSource**.
5. Type a unique **DataSource Name** to be used by webMethods Portal on the **View DataSources** tab.
6. Type a **Display Name** to be used when you identify a data source to use for a database directory service.
7. Select **Custom JDBC** from the **Server Type** list and click **Next**.
8. Type the JDBC Connection class for the custom drivers you want to use for the data source connection.
9. Type a valid connection URL.
10. Type a valid username and password that, at a minimum, has READ access to the database to which you are connecting.
11. Click **Submit**.

Modifying an Existing Data Source

To modify an existing data source, do the following.

To modify an existing data source

Note: You cannot modify the default data source, which is the webMethods Portal database

1. As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Configuration** folder, click **DataSource Administration**.
2. Click (Popup Menu) for the data source you want to modify, and then click **Modify**.
3. Make the desired property modifications.

4 Click **Submit**.

Deleting an Existing Data Source

To delete an existing data source, do the following.

To delete a data source

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Configuration** folder, click **DataSource Administration**.

2 Click (Popup Menu) for the data source you want to delete, and then click **Remove**.

Managing E-Mail Settings

The Email Administration portlet is used to configure the mail server settings used by the system when processing e-mail.

To configure an e-mail server to send portal notifications

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Configuration** folder, click **Email Administration**.

2 Type the SMTP Host Address for the e-mail server you want to use as the mail server to send portal notifications. For example: `smtp.server.com`

3 Type the SMTP Server Port. For example: `25`

4 Configure the default sender e-mail address by entering the e-mail address in the **From** field.

Note: The Sender Address is the reply-to e-mail address that is attached to outgoing e-mail portal notifications.

5 Select the skin that will be used to format the portal notifications to be delivered by e-mail.

6 Click **Save Settings**.

Configuring External Configuration Credentials

The HTTP Header Authentication Administration portlet allows portal administrators to configure webMethods Portal to accept external HTTP authentication credentials from third party security and access control products such as SiteMinder (Computer

Associates) or Oblix. These credentials are case-sensitive and, depending on the platform and Web server, will most likely be sm_user or SM_USER.

Enabling Authentication

Important! The HTTP Header Authentication Administration portlet should only be enabled if you are using a third-party security provider. After the portlet is enabled, the Portal server acts as though all users have been authenticated.

To accept authentication from a third party security and access control product

1. As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Configuration** folder, click **HTTP Header Authentication Administration**.
2. For **User Header Name**, type `sm_user` or `SM_user`.
3. Select the **Enable HTTP Header Authentication** check box.
4. If appropriate, in the **Logout URL** field, type the URL to which the user is redirected after logging out of the portal.
5. Click **Submit**.
6. Configure the third party security and access control software as directed in your vendor's product documentation.

Note: To properly configure an external security and access control product with webMethods Portal, both webMethods Portal and the third party product *must* point to the same directory server instance (SunOne, Active Directory, or ADAM).

Checking Logs for HTTP Header Authentication Problems

If you are having a problem in getting HTTP Header authentication on to work properly, you can check log files to assist in diagnosing the problem. Log messages for HTTP Header authentication are assigned to the portalLogin category. Before you can display HTTP Header authentication logging messages, you need to change the logging threshold values. The default thresholds for writing to the console, the _full.log file, and the portalLogin.log file are set to the INFO log level but HTTP Header authentication logging messages use the DEBUG log level, which is lower.

Portal log files reside in the `/webMethods_install_dir/P`portal/server/*portal_server*/logs directory. For information on controlling the collection of logs, see "Controlling Portal Logging" on page 150. For information on searching for log messages, see "Viewing Logging Messages" on page 153.

Setting Login Logging Thresholds

You need to set both the category and output settings to DEBUG if you want the logging messages to be written to the output. For information on setting logging thresholds, see "Controlling Portal Logging" on page 150.

To set category and output thresholds for HTTP Header authentication

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Analysis** folder, click **Logging Configuration**.

2 Click the **Logging Thresholds** tab to bring it to the front.

3 In the **Category Threshold** list, select the DEBUG log level for any or all of the following logging categories:

Logging category	Controls output for...
root	The console and the _full.log file
portalLogin	The portalLogin.log file

4 In the **Output Threshold** list, select the DEBUG log level for any or all of the following logging output types:

Logging output	Controls output for...
Console	Logging messages sent to the console
_full.log	Logging messages sent to the _full.log file
portalLogin	Logging messages sent to the portalLogin.log file

5 At the bottom of the page, click **Apply**.

Checking HTTP Header Authentication Logs for Problems

With HTTP Header authentication enabled, the Portal server acts as though all users have been authenticated. With this in mind, the log messages will reveal one of three likely outcomes, as described in the following sections.

The Login is Successful

Messages for a successful login using HTTP Header authentication look similar to the following example:

```
Date_and Time (portalLogin : DEBUG) - HttpHeaderHandler Auth Handler
      looking for: user_name
Date_and Time (portalLogin : DEBUG) - Found userID: user_name
```

where *user_name* is the name of the user who logged in under HTTP Header authentication.

HTTP Header Authentication is Disabled

If you have not enabled HTTP Header authentication, the log message looks similar to the following example:

```
Date_and Time (portalLogin : DEBUG) - HttpHeaderHandler Auth Handler is
      not enabled
```

To enable HTTP Header authentication, see "Enabling Authentication" on page 182.

The Problem Rests with the Third-Party Site

If the third-party site is not configured correctly, HTTP Header authentication will fail. The resulting log message looks similar to the following example:

```
Date_and Time (portalLogin : DEBUG) - HttpHeaderHandler Auth Handler
      looking for:
Date_and Time (portalLogin : DEBUG) - No value found!
```

Deploying Portal Components

Portal administrators have the following options available to them when installing portal components, such as portlets or DBOs, on a Portal server.

- Through the Install Administration portlet on the Administration Dashboard.
- Through the Deploy folder on the Portal server's File System. This folder allows portal administrators and developers to copy or paste a newly developed portlet package (such as a portlet, DBO, or deployable package) into a specific directory that is periodically polled by the Portal server. If the Portal server detects new deployable components in this folder, these components are automatically retrieved and installed on the Portal server. You have the option to configure the polling interval that specifies how often the Portal server will poll the Deploy directory to detect any new components.

You can perform the following tasks within the Datasource Administration portlet:

This task...	Is described here...
Modify the polling interval used in deploying portlets to a Portal server	"Modifying the Polling Interval" on page 185
Install a portlet using the Deploy folder for a Portal server	"Installing a Portlet Using the Deploy Folder" on page 186

This task...	Is described here...
Install a portlet or other deployable component using the Install Administration portlet	"Installing Portlets or Other Deployable Portal Components" on page 186
Uninstall a portal component	"Uninstalling Portal Components" on page 187

Modifying the Polling Interval

If your organization is developing multiple portlets, this installation method may be more convenient than manually installing portlets one at a time. The default file system location for the Deploy folder is
*/webMethods_install_dir/*Portal/server/*portal_instance_name*/deploy

Note: Polling can be turned on or off by modifying the PhaseProvider.xml configuration file on the Portal server's file system. Use the following instructions to modify the polling interval.

To modify the polling interval

1. From the portal root install directory, navigate to the following location:

   */webMethods_install_dir/*Portal/server/*portal_instance_name*/config

2. Open the phaseProvider.xml configuration file in a text editor or equivalent XML editing facility. Locate the following XML fragment:

```
<Phase name="deploySync" enabled="true"
class="com.webmethods.portal.system.init.impl.MasterServerPhase">
<PhaseInfo name="startTimedSyncDeploy" enabled="true"
class="com.webmethods.portal.bizPolicy.biz.install.impl.
SyncDeployService" interval="5" />
</Phase>
```

3. To turn polling off, change the enabled attribute from `true` to `false`.

4. To change the polling interval, modify the interval attribute to the desired value. The default setting is 5 seconds.

   Note: This setting will *not* have an impact on overall performance

5. Save the file.

6. Restart your Portal server instance.

Installing a Portlet Using the Deploy Folder

To use the Deploy folder to install a portlet on a Portal server, do the following.

To install a portlet using the Deploy folder

- Copy and paste the portal component(s) that you want to deploy into the deploy directory.

  The Portal server will fire an event every five seconds that polls this folder, so no further action is needed.

Note: If any portal component fails to deploy, the Portal server will automatically create a Failed directory on the Portal server's file system in the Deploy folder. All components that do not install properly will be copied into the Failed directory.

Installing Portlets or Other Deployable Portal Components

To use the Install Administration portlet to install portlets or other deployable portal components, do the following

To install a portlet or other deployable portal component

1. As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Configuration** folder, click **Install Administration**.
2. Choose **Install** and click **Next**.
3. Choose **Local or Network Location** or **Remote Location**.
4. Type the complete path to the component you want to install if you are installing from a remote location (such as FTP, HTTP), or click **Browse** and navigate to the deployable component you want to install if it resides on your local file system.
5. Click **Next**.
6. Review the Component Info Summary and then click **Install**.

   If the component is installed successfully, you will get a confirmation message verifying that the install succeeded.

Note: If a component install fails, that component is automatically uninstalled. Be sure to check your log files to troubleshoot the installation failure.

Uninstalling Portal Components

Before you uninstall a component, determine how its removal will affect all of its instances on a portal user's portal page. Uninstalling will break any portal page that contains specific portlet instances of the portlet that was uninstalled, and disrupt any portlets that may be wired to that portlet using the portlet wiring feature.

For example, you are not warned about wiring relationships when removing a portlet that is wired to another portlet.

You may want to change the portlet's status property to Hidden or Disabled to phase out the portlet before you uninstall it. After users are informed of the impending uninstall and have removed it from their portal page, it will then be safe to uninstall it.

Important! When an uninstalled portlet's instances are broken, it causes errors on each page on which that portlet is being used. It also may remove the data for a portlet and its instances, the configuration files, the portlet database tables, and the portlet packaging files. Reinstalling will *not* restore the broken references caused by uninstalling a portlet.

To uninstall a component using the Install Administration portlet

1. As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Configuration** folder, click **Install Administration**.
2. Select the **Uninstall** option and click **Next**.
3. Navigate to the component you want to uninstall, click (Popup Menu) and click **Uninstall**.
4. Confirm the summary information for the component you are going to uninstall and then click **Uninstall**.
5. Click **Return** to go back to the first step in the Install Administration portlet.

Managing Portal Objects

The Manage Components portlet allows portal administrators to globally configure and manage how portal objects, called Extended Types or Dynamic Business Objects (DBOs), are made available to end users. *Extended Types* (DBOs) are portal objects that are created from existing base level portal objects such as content, folders, portal pages, forms, links, and portlets.

The Manage Components portlet allows portal administrators to configure the default properties and permissions for all Extended Types, regardless of whether they are installed as part of the regular portal installation process, or are created by a portlet developer using the Portlet Developer and installed at a later date.

You can perform the following tasks within the Manage Components portlet:

This task...	Is described here...
Configure the properties of managed components	"Configuring Properties for Managed Components" on page 188
Configure permissions for managed components	"Configuring Permissions for Managed Components" on page 189

Configuring Properties for Managed Components

To configure properties of managed components, do the following.

To configure properties using the Manage Components portlet

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Configuration** folder, click **Manage Components**.

2 To modify the default Properties on a given DBO (content, folder, form, link, or portlet) click on the link for the specific Extended Type you want to modify. This will display a list of all descendents of that particular Extended Type.

For example, if you want to configure the default Properties on the Basic Folder object, which is a descendent of the folder object, click on the folder link. This will display a list of all Extended Types that are based on the folder object.

3 Click (Popup Menu) for the Extended Types (such as a Basic Folder) for which you want to you want to modify properties.

4 Select **Properties**. This will display a list of properties for the Extended Type you selected earlier. At this point, depending upon the type of Extended Type, you will have the option to configure the default properties for that Extended Type instance.

For example, if you want to modify the default properties for the Basic Folder Extended Type, which is based on the Folder Extended Type, you have the option to modify the following properties:

Status Property

This property allows you to define the default Status for *all* instances of this portlet that are published to the portal.

To set the default status for a given Extended Type (such as Basic Folder), select one of the three options from the drop down menu.

Enabled	Can run. Can publish. Selecting this option means that end users can execute this portlet and publish instances of this portlet. The portlet will appear in Portal Page Designer tool.
Hidden	Can run. Cannot publish. Selecting this options means that end users can execute this portlet, but *not* publish instances of it. The portlet will *not* appear in Portal Page Designer tool.
Disabled	Cannot run, cannot publish. Selecting this option means that end users cannot run or publish instances of this portlet. The portlet will *not* appear in Portal Page Designer tool.

Note: Portal developers that build portlets using the Portlet Developer can configure additional Extended Properties on portlets as they develop them. These properties are then made available for further configuration using the Managed Components portlet.

Configuring Permissions for Managed Components

To configure permissions for managed components, do the following.

To configure permissions for Managed Components portlets

1 Browse the Administration Dashboard and click the **Manage Components** link in the **Portal Configuration** folder.

2 To modify the permissions on a given Extended Type (content, folder, form, link, and portlet) click on the link for the specific Extended Type you want to modify. This will display a list of all instances of that particular Extended Type.

   For example, if you want to configure the default Permissions on the RSS portlet, which is based on the folder object, click on the folder link. This will display a list of all Extended Type instances that are based on the folder object.

3 Click (Popup Menu) for the Extended Type instance (such as RSS Folder) that you want to modify and select **Permissions**.

4 Make the appropriate changes to the default Permissions using the Permissions Wizard and then click **Apply**.

5 Click **Done** to return to the **Manage Components** page.

Setting up Single Sign-On

Single sign-on is the ability for a user to log into one application and then use other applications without having to log into each one separately. webMethods Portal supports single sign-on through the Security Assertion Markup Language (SAML), an XML-based framework for the exchange of security information. Using SAML, an entity on a target computer grants access based on an assertion from the source computer that the user is logged into the source computer. webMethods Portal can provide a single sign-on capability in the following ways:

- Between a source Portal server and one or more target Portal servers
- Between a Portal server and other webMethods components that have single sign-on capability
- Between a Portal server and a third-party application that supports SAML
- Between a Portal server, an Artifact Receiver that authenticates the user sign-on, and a target Web application

Using this model, one Portal server is the source, providing a central login for users. Links on portal pages on the source Portal server point to any number of SAML-capable entities. The target entities all point back to one source Portal server. If the target is another Portal server, that server can accept SAML assertions from only one source.

To take advantage of single sign-on, a user must be known on both the source Portal server and the target entity. In most cases, common knowledge of a user is provided by use of the same directory service.

Configuring a Portal Server as a Target for Single Sign-On

A Portal server can be a target for only one single sign-on source at a time.

To configure a Portal server to be a target for single sign-on

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Configuration** folder, click **SAML Authentication Administration**.

2 Modify **Properties** as follows:

For this property...	Do this...
Artifact Parameter Name	If this is a SAML connection with another webMethods Portal server, do not change the default value SAMLart. If this is a SAML connection to a third-party source, type the artifact parameter name used by the third-party application.
Security Provider URI	Type the URI of the SAML security provider (source). If this is a connection with another webMethods Portal server, use this syntax: `server_name:port/services/SAML` where *server_name* is the host where the source Portal server is running and *port* is the Portal server port number. The default port number is 8080.

3 Click **Submit**.

Once submitted, the Portal server will accept SAML assertions from the specified source entity.

Setting SAML Links on a Source Portal Server

On any portal page, you can add a link to a SAML target entity, such as a Portal server. If the target accepts SAML assertions from the source Portal server, when a known user clicks the link, no login credentials are required. If the target entity does not accept SAML assertions from the source Portal server, or if the user is not known on the target entity, login credentials may be required.

Under the SAML specification, an intermediary called an artifact receiver can perform authentication on behalf of the target Web application. In such a case, the SAML source requires two URLs: one for the Artifact Receiver and one for the target Web application.

You can place one or more SAML links on any portal page you have permission to edit.

To create a SAML link on a source portal page

1 In the upper right-hand corner of the portal page, click the menu icon.

2 On the menu, click **Edit Portal Page**.

3 In the **Root** list of the **Available Portlets** panel, click **Links**.

4 In the **Links** list of the **Available Portlets** panel, drag the **Single Sign-on Link** portlet and drop it onto the portal page at the location where you want to add the link.

A red box appears beneath the cursor location whenever the cursor is over a valid portal page location, indicating where the portlet would be positioned if you released the mouse button.

5 On the left side of the page control area, click **Save**.

6 At the right edge of the title bar for the single sign-on portlet, click (Popup Menu) and then click **Properties**.

7 In the Properties page make modifications as appropriate:

Make changes here...	If you want to...
Name	Replace `Single Sign-on Link` with the text that is to go with the link.
SAML Authentication URL	Type the URL for a resource on the target computer. The target can be any portal page on a Portal server. If you are connecting to a Web application through a SAML Artifact Receiver, use this field for the Artifact Receiver URL.
Use POST or GET	Determines the method used to pass data to the target computer. POST — Passes data to a gateway program's STDIN. POST, the default, is the preferred method for single sign-on data. GET — Passes data as a string appended to the URL after a question mark.
artifactParameterName	If this is a SAML connection with another Portal server or other webMethods component, do not change the default value SAMLart. If this is a SAML connection to a third-party source, type the artifact parameter name used by the third-party application.

Make changes here...	If you want to...
Application Target URL	If you have typed the URL for a SAML Artifact Receiver in the **SAML Authentication URL** field, type the URL for a Web application. Otherwise, leave this field empty.

8 At the bottom of the page, click **Apply**.

Checking Logs for SAML Problems

If you are having a problem in getting single-sign on to work properly, you can check log files to assist in diagnosing the problem. Log messages for SAML are assigned to the portalLogin category. Assuming logging thresholds are set to the default values, SAML logging messages are written to the console, the _full.log file, and the portalLogin.log file.

Portal log files reside in the */webMethods_install_dir/*Portal/server/*portal_server*/logs directory. For information on controlling the collection of logs, see "Controlling Portal Logging" on page 150. For information on searching for log messages, see "Viewing Logging Messages" on page 153

If the SAML Login is Successful

A message for a successful SAML login has an INFO log level and looks similar to the following example:

```
Date_and Time (portalLogin : INFO) - SAML authenticated user: user_name
```

where *user_name* is the name of the user for whom the SAML authentication was performed.

If the SAML Login Fails

A failed SAML notification has a WARN log level, contains an exception message, and looks similar to the following example:

```
Date_and Time (portalLogin : WARN) - Failed SAML > authentication
com.webmethods.portal.PortalException:[POP.012.0002.wm_xt_samlsecurityservice]
     The SAML artifact is invalid or has expired.
         <Stack dump>
```

The stack dump that accompanies the exception message can help determine where the authentication has failed.

Managing Instant Messenger Accounts

Note: The Instant Messenger Notification Administration portlet is not deployed by default. To use this portlet, you need to deploy it from this location:

webMethods_install_dir/Portal/components/extras/subscriptions/wm_imagent.pdp

using one of the methods described in "Deploying Portal Components" on page 184.

One of the methods by which the Portal server provides notification to portal subscribers is through an Instant Messenger (IM) account. To use IM for notification you need to set up one or more IM accounts to be used by the Portal server. webMethods Portal supports the four major IM services, MSN, Yahoo!, AOL, and ICQ.

Using IM for notification does not provide guaranteed delivery. After Portal server sends the notification, there is no way to verify that the message is received. If the subscriber is not logged into IM, the IM server is down, or if the Portal server fails before it can send the message, the notification is lost.

There are two things you must do to configure a Portal server to use IM for notification:

To do this...	Look here...
Configure the Portal server to send notifications through IM	"Setting Up IM Accounts for the Portal Server" on page 194
Configure IM account information for users	"Setting Notification Attributes for a User" on page 195

In addition, you can check status of IM notifications, described in "Checking Status of IM Accounts on the Portal Server" on page 196.

Setting Up IM Accounts for the Portal Server

Before setting up IM account information on the Portal server you need have an IM account for the server on each of the IM services you want to support. Valid IM services are MSN, Yahoo!, AOL, and ICQ.

To set up Instant Messenger accounts for the Portal server

1. As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Configuration** folder, click **Instant Messenger Notification Administration**.
2. Click the **IM Sender Accounts** tab to bring it to the front.

3 For each IM account you want the Portal server to support do the following:

In this field...	Type this...
Username	The username of the IM account you have created for the Portal server.
Password	The password associated with the IM account you have created for the Portal server.

If you leave the fields for an IM service empty, the Portal server cannot support notification over that service.

4 Click **Submit**.

Setting Notification Attributes for a User

To send an IM notification to a user, you need to specify the IM service and the username to which the message should be sent.

To specify the IM account at which a user is to receive an IM notification

1 As a portal administrator, do one of the following:

- Browse to the **Administration Dashboard** and in the **User Management** folder, click **Manage Users**.
- In the global navigation toolbar, click **Directory**.

2 In the search field of the **Search** tab, type a partial or complete user ID for the user.

3 In the **Directory Service** list, choose the directory service to which the user belongs, and click **Go**.

4 In the **Users** area, click the icon in the **Edit** column for the user.

5 On the Profile Page, click the **Notifications** tab to bring it to the front.

6 From the **Instant Messenger Service** list, select the IM service to which the notification should be sent.

7 In the **Instant Messenger Service** field, type the username belonging to the user.

8 Click **Apply**.

Checking Status of IM Accounts on the Portal Server

To check the status of Instant Messenger accounts on the Portal server

1. As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Configuration** folder, click **Instant Messenger Notification Administration**.
2. Click the **Instant Messenger Status** tab to bring it to the front.
3. Find the status for each IM account:

This status value...	Means this...
Disconnected	The Portal server is not connected to the IM service, or does not have an IM account configured. This value appears if the Portal server has sent no IM notifications since the server was started or since you have clicked the **Submit** button on the **IM Sender Accounts** tab.
Connecting	The Portal server is connecting to the IM service. This status value occurs when the server needs to send a notification after having been in a Disconnected state.
Connected	The Portal server is connected to the IM service.
Failed	The Portal server has attempted to connect to the IM service but has failed to do so.

Displaying Portal System Information

The System Information portlet provides a wealth of information about the current state of the Portal server. The portlet gathers the information dynamically at the time you open each tab.

Displaying the System Information Portlet

To display system information about the current state of the Portal server

1. As a portal administrator, in the global navigation toolbar, click **Administration**.
2. On the title bar, click **System**.
3. In the System folder, click **Portlets**.
4. In the Portlets folder, click **Administration**.

5 In the Administration folder, click **System Information**.

System Information Data

The System Information portlet contains five tabs. When you click a tab to bring it to the front, the portlet dynamically collects the data for display.

Tab / Information	Description
Request/Response tab	Information that is gleaned from the user's Web request.
Request Information	Typical cgi-bin parameters describing the requested path.
Request Headers	Incoming HTTP headers.
Request Parameters	Incoming HTTP parameters on the URL.
Request Attributes	Attributes (objects) stored on the current request.
Response Information	Miscellaneous information, such as encoding and locale, gleaned from the request.
Session Misc tab	User session information.
Session Attributes	Attributes (objects) stored on the user's session.
Locale Information	The current locale of the user.
Presentation Data	Various information used to render requests for this user.
Session Attributes tab	Portlet Controller Session objects associated with this user.
Request Attributes tab	Portlet Controller Request objects associated with this user's request.
Application Attributes tab	Information shared throughout the portal (across all users).
System Information	Environment variables, such as Classpath, path, and so forth).
Server Information	Information about the current front-end server.
Context Information	Servlet object information.

webMethods

CHAPTER 10

Managing Portal Content

Overview

webMethods Portal provides administrators with a number of tools that can be used to help manage portal content. This chapter provides detailed instructions on how to use webMethods Portal tools and portlets to manage portal content.

Migrating Portal Content

The Content Migration Wizard Portlet enables portal administrators to migrate portal content from one Portal server instance to another, such as from development to staging to production.

This portlet can be used to migrate the following types of portal content: documents, folders, external links, internal links (using aliases), portal pages (including layouts), portlets, Dynamic Business Objects (DBOs), permissions, subscriptions, and portlet wiring properties.

Content Migration Considerations

Content migration involves two distinct activities: exporting the content from the source Portal server instance, followed by importing the content on the target Portal server instance. Before performing these actions, consider the following:

- **Migrating portlets and DBOs**: If you are developing or installing any portlets on a development server and want to migrate portal pages that contain instances of these portlets, you *must* deploy them on the target Portal server *before* migrating any portal pages or published instances of the portlets that were developed or installed on the development server instance.
- **Migrating published content**: Content published to the Portal's Content Management system can be migrated from one Portal server instance to another. If you are using your development environment to configure portal permissions on items published to the content management system, you have the option to migrate the permissions as well. To properly migrate permissions and subscriptions associated with published content, see **Migrating permissions and subscriptions** below.
- **Migrating portal links**: To properly migrate internal portal links with references to other portal objects, such as a link from one portal page to another, create aliases for these links instead of using the base portal URL.

  For example, if you want to publish a link to an existing portal page, such as a Sales portal page that has the following as its initial URL:

  `http://portalserver/meta/default/folder/0000002132`

Create an alias that points to this URL, but has a more "friendly" URL such as the following:

`http://portalserver/Sales`

- **Migrating permissions and subscriptions**: To properly migrate permissions and subscriptions from a source to target Portal server instance, be sure that both portals are pointing to the same directory services.

Migrating Portal Content using Export/Import Processes

The following procedures describe the basic export/ import process for migrating portal content from one Portal server instance to another.

The examples that follow describe only one scenario for migrating from a development server to a production server.

To export portal content from a source development server to another target Portal server instance

1. As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Content** folder, click **Content Migration Wizard**.
2. Select **Export** and click **Next**.
3. Under the **Exporting Properties** heading enter an export name for the components you want to export. For example, `Sales Portal`.
4. Click **Browse** to open the portal resource selector to select the item to export. For example, if the Sales Portal is located under Public Folders, you would use the resource selector to browse to the Sales Portal folder and click the **Select** icon. After you select the folder you want to export, click **Select**.
5. If the item you want to export contains child folders, portal pages, content items, and so forth, you can explicitly set the export depth. The default value for this setting is -1, which means that all child items under the item you selected in the preceding step will be exported. If you only want to export content down to a specific child level, enter a value that corresponds to the number of child levels that you want to export.
6. Optionally, select the **Create Auto Deployable Component** option if the portal resource is intended to be an auto-deployable component.

   This option is intended for auto-deployable components, which are automatically retrieved and installed on the Portal server when you place them in the Deploy directory for the server. When imported, auto-deployable components install only in the parent container from which they were exported.
7. Optionally, select the **Export Content (Documents)** option to include content items that may have been published within the folder you want to export.

8 Optionally, select the **Export Access Control Lists** option if you want to export all permissions that may have been set on the folder, or items published within the folder you are exporting.

9 Optionally, select the **Export Subscriptions** option if you want to export all subscriptions that may have been set on the folder or items published within the folder you are exporting.

10 Click **Next**. You will see a message confirming that the export was successful.

11 You are prompted to save the export archive to your local file system or network location. Click **Save** to complete the export process.

To import portal content on a target Portal server instance

Note: If you are importing content with portal pages that have portlets and/or DBOs that were created and deployed to your development Portal server (source), you *must* deploy the portlets and/or DBOs *before* you use the following import procedures.

Note: The export archive you created in the previous instructions contains a .zip file extension. You *must* remove the .zip file extension before using the following Import procedure. For example, if the Export process generates the file SalesPortalExport.cdp.zip, you would rename the file to `SalesPortalExport.cdp`.

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Content** folder, click **Content Migration Wizard**.

2 Select the **Import** option and click **Next**.

3 For **Install Destination,** click **Browse** to open the portal resource selector and select a destination folder for content import. To import the content to a location on your target server that is referenced by a portal alias, you can optionally click **Use Alias** to select an existing alias on your target server.

Note: If the export archive was created with the **Create Auto Deployable Component** option selected, the Content Migration wizard ignores the selected install destination and installs the component in the parent container from which it was exported.

4 For the **Install Component,** click **Browse** to locate the export archive you want to import, such as on your file system.

5 Click **Next**.

6 After the import process is complete, you will see a message that confirms the import was successful.

Tip! If you run into problems, don't forget to check the webMethods Advantage Web site. See "Troubleshooting Information" on page 15.

Managing Content Storage

The Content Service portlet allows Portal Administrators to manage the storage locations available for content published to the portal, which is physically stored in the locations configured in the content service. It typically resides on a separate file server for backup and redundancy purposes.

To configure a new Content Service for the Portal Repository

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Content** folder, click **Content Service**.

2 Click **Create New Content Service**.

3 In the **Service Name** field, type a name for your new content service.

The user ID can be 1 through 255 characters and can contain only alphanumeric ASCII characters with no spaces.

4 From the **Type** list, select one of content service types and click **Next**.

5 Depending on your choice of content service type do the following:

If you choose **File System**, type a physical storage location for your content service. Valid locations include the following types of network paths:

- `file:\\y:\` (where `y:\` is a mapped network drive to an external file server)
- `f:\repository` (where `f:\` repository is a separate hard drive on the Portal server machine)

Note: There are many ways to configure an external content repository for webMethods Portal. The two examples here assume that your network administrator has provided the proper security settings to allow the Portal server to access a network shared on a separate file server.

—OR—

If you choose **Ftp**, do the following:

a In the **Location** field, type a valid FTP server name.

b In the **User name** field, type a user name valid on the FTP server.

c In the **Password** field, type the password associated with the user name.

6 Click **Apply**.

7 To make the new content service the default content service, click (Popup Menu) and then click **Set As Default**.

The new Content Service becomes the default location for storing new content that is published to the portal.

To import content from an existing content service

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Content** folder, click **Content Service**.

2 Locate the content service into which you want to migrate the contents of an existing content service, click (Popup Menu) and then click **Import Content**.

3 For the **Target Folder** property, do one of the following:

Click this...	And do this...
Browse	On the left side of the portal resource selector, browse to the target page, click the **Select** icon, and then click **Select**.
Use Alias	In the **Alias Name** field of the portal resource selector, type the alias of the portal page to which the user should be redirected. Click **Test** to determine if the alias is valid and the alias target is the correct one. If the alias is correct, click **Select**.

4 At the bottom of the page, click **Import**.

To set the maximum file size for content published to the Portal Repository

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Content** folder, click **Content Service**.

2 Click **Set Max File Size**.

3 In the **Size (MB)** field, type a maximum publish size (in Megabytes).

4 Click **Apply**.

Managing Subscriptions for Individual Users

The Manage Subscriptions portlet allows Portal Administrators to view existing subscriptions within the Portal server. It allows an administrator to view subscriptions for a given user, resource, group, or group subscription created by any given user.

To view or modify subscriptions for a specific user

1. As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Content** folder, click **Manage Subscriptions**.
2. Click the **View Subscriptions for a Specific User** link.
3. On the User Subscriptions screen, select the user from the portal user directory list, and then click the **Select** icon to enter the user in the **Selected Items** list.
4. Click **Select**.
5. Optionally, if you want to modify the subscription rules for a subscription, click on the subscription, select or clear checkboxes as desired, and then click **Apply**.
6. Optionally, if you want to delete one or more subscriptions for a given user, select the user subscription from the list by selecting the corresponding check box and click **Delete Selected**.
7. Optionally, if you want to view subscriptions for a specific group, return to the Manage Subscriptions portlet, and follow the same procedures outlined in steps 1-6 of these instructions.

Managing Group Subscriptions

The Group Subscriptions portlet allows portal administrators to create subscriptions for groups exposed by the underlying portal user directory (such as LDAP or ADSI). Use this portlet to create new group subscriptions and manage existing subscriptions.

To configure a new group subscription

1. As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Content** folder, click **Group Subscriptions**.
2. Click **Create New Group Subscription.**
3. Navigate through the Portal Folder and select the portal resource (file, folder, portlet, or portal page) for which you want to configure a subscription. Click the **Select** icon to make your selection from the resource in the **Selected Items** list.

4 Click **Select**.

5 On the Select Group screen, select the group that you want to subscribe to the resource you selected in the previous step. Click the **Select** icon to enter the selected group into the **Selected Items** list.

6 Click **Select**.

7 On the Create Subscription screen, define your subscription rules by selecting or clearing checkboxes as desired. Click **Create**.

Note: The subscription rules that are available depend on the type of resource to which you are subscribing. For example, subscriptions on folders have slightly different subscription rules than a Content item has.

To view or modify group subscriptions that you have created

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Content** folder, click **Group Subscriptions**.

2 Click on the **View Group Subscriptions I've Created** link.

3 Click on the subscriber group that you want to change.

4 On the Subscription Rules screen, change rules by selecting or clearing checkboxes as desired, and then click **Apply**.

5 Optionally, if you want to delete a group subscription, select the group subscription from the list by selecting the corresponding check box and click **Delete Selected**.

To view all subscriptions for a given group

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Content** folder, click **Group Subscriptions**.

2 Click on the **View Subscriptions for a Given Group** link.

3 On the Group Subscriptions screen, select the group whose subscriptions you want to view, and click the **Select** icon to move the group into the **Selected Items** list.

4 Click **Select**.

5 Optionally, if you want to modify the subscription rules for a given subscription, click on the subscription, change the rules by selecting and clearing checkboxes as needed. Click **Apply**.

6 Optionally, if you want to delete one or more subscriptions for a given group, select the group subscription from the list by selecting the corresponding check box and click **Delete Selected**.

Publishing Portlets as an Administrator

The Publish portlet provides portal administrators with expanded publishing capabilities that are generally not exposed to most end users. The Publish portlet allows administrators to publish many different types of content such as files, folders, forms, links, and specific portlet instances. Any custom portal content types such as Dynamic Business Objects or Custom Forms can also be published from this portlet.

To publish content using the Publish portlet

1. As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Content** folder, click **Publish**.
2. Select the corresponding option for the content type you wish to publish. The default options are: File, Folder, Form (for DBOs only), Link, and Portlet.
3. For a given content type, select one of the options from the drop down menu.

Note: If you previously created any custom portal objects that are based on any given content type, they will now show up as options in the drop down menu for the respective content type. As an example, the RSS Feed option under the Folder content type is a Dynamic Business Object. It was created to extend the Folder object type with custom attributes and business logic for publishing RSS syndicated news feeds to a portal folder object type.

4. Click **Next**.
5. From the Location heading, click **Browse** to select a parent folder location for the content item you are publishing.

Note: You can optionally click **Use Alias** if you want to publish the content item to a location that is referenced by an existing portal alias.

6. Click **Next**.
7. Enter a name for the content item you are publishing.
8. Optionally, enter a description for the content item you are publishing.
9. Depending on the type of content you are publishing, fill in any Extended Properties for the given content type (such as. RSS Feed URL for an RSS Feed content item).
10. Click **Next**.
11. A summary screen will appear with all of the values you entered in the previous step for your review. Click **Finish**.

Managing the Search Engine

The Search Administration portlet allows Portal Administrators to manage the Lucene search engine that is offered with webMethods Portal (the link is http://jakarta.apache.org/lucene/docs/index.html) and the logging search engine in the View Logging Messages in the Portal Analysis folder of the Administration Dashboard (see "Viewing Logging Messages" on page 153).

There are two primary search engine management functions that Portal Administrators can execute from this portlet:

- Resynch Search Index
- Optimize Search Indexes.

If the search engine becomes corrupted, you may need to reload it, described in "Reloading the Default Search Engine" on page 209.

Resynchronyzing the Search Indexes

Executing the **Resynch Indexes** command will re-index all portal content that was previously published to the portal and update the default portal search indexes again. A portal administrator might need to do this if the search index somehow becomes corrupted and search stops working.

In the case where the default search index is corrupted, a portal administrator has the option of running the **Resync Indexes** command, which will rebuild the indexes from scratch.

Tip! If your portal has a lot of content published to the content management system, this operation may take a long time to run. You should run this operation at off-peak hours.

To resync the search indexes

1. As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Content** folder, click **Search Admin**.
2. Click (Popup Menu) and the click **Resync Indexes**.

Optimizing the Search Indexes

With the Lucene search engine, the number of files that are stored in the libraries data folder on the file system that are used for the index can grow over time as more content is added to the search index. This file is opened every time a search request comes into the system, and each file in the data folder requires an additional open file handle. If the

number of files grows too large, you may receive an error message related to having too many files open.

To avoid this error, portal administrators can execute the **Optimize Indexes** command, which will attempt to take all of the segments in the index and merge them together. This will reduce the number of files back to a manageable level, thus optimizing the performance of the embedded search engine.

To optimize the search indexes

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Content** folder, click **Search Admin**.

2 Click (Popup Menu) and then click **Optimize Indexes**.

Reloading the Default Search Engine

If the portal search engine configuration somehow becomes corrupted, you have the option of reloading the default search engine configuration in an attempt to fix any corrupt configuration settings. During the initial portal startup, the search service reads the configuration information from the wm_portalsearch portlet and copies that information to the corresponding information fields on the search service. On subsequent portal startups, the configuration is loaded directly from the portal's underlying database.

To reload the search configuration

1 Locate the wm_portalsearch portlet at this location:

*/webMethods_install_dir/*Portal/components/services/search/wm_portalsearch.pdp

2 To deploy the wm_portalsearch.pdp file, copy it and then paste it into the deploy directory for the Portal server:

*/webMethods_install_dir/*Portal/server/Portal/server/*portal_instance_name*/deploy

In addition to fixing a corrupted search configuration, you might also need to reload the configuration because you have manually edited the luceneSearch.xml file.

One reason to edit the file if you are deploying a Portal cluster. When deployed in a cluster, the search index files for the search agent node should be on the local hard drive, rather than on a network file system or on a mapped drive. Read/write operations over a network are slow and can lead to index corruption. When you would edit the LuceneSearch.xml file, change the <INDEX_PATH>home:/data/lucene</INDEX_PATH> value to a local path (for example: c:/Portal/searchdata).

If you have written a custom document converter for a file type the Portal server cannot index by default, need to add an extra node to the <DOCUMENT_CONVERTERS> section.

To make manual changes to the luceneSearch.xml file

1 Extract (unzip) the luceneSearch.xml file from the wm_portalsearch portlet:

*/webMethods_install_dir/*Portal/components/services/search/wm_portalsearch.pdp

2 In a text editor, manually edit the luceneSearch.xml file as needed.

3 Zip the luceneSearch.xml file back into the wm_portalsearch.pdp portlet file.

4 Redeploy the portlet, as described in the preceding procedure.

webMethods

CHAPTER 11

Managing Portal Rules

What are Portal Rules?

webMethods Portal uses rules to determine which users have access to various resources on a portal. Portal allow you to control a variety of user activities, from which page they use to log into the portal, to the appearance of the pages they see. Using rules, you can define default behaviors for the entire portal application or you can dynamically control the experience of a given user, group, or role.You can create rules of the following types:

Rule type	Description
Login page rules	Rules that determine what login page should be used. You can, for example, redirect users to different login pages, depending on whether they are inside or outside the firewall.
Start page rules	Rules that determine what start page should be used. The start page is the page to which the Portal server redirects users after log in.
Rendering rules	Rules that determine what renderer should be used.*Renderers* are user interface formatting capabilities that can be assigned to specific portal objects by defining rendering rules. You can define rendering rules for virtually any portal object type. Rendering rules are useful in providing a consistent look and feel for common object types that can be invoked through explicit rule definitions.
Shell rules	Rules that determine what shell should be used.A *shell* is an installable component that generates the webMethods Portal header, footer, and portlet title bars. Shell rules define what shell elements should be displayed for a given user, group, or role. For example, if a portal serves both employees and customers, you can use shell rules to assign the corresponding shell to a given user group.
Skin rules	Rules that determine what skin should be used. A *skin* is an installable webMethods Portal component that defines the look and feel of the portal user interface. Skin rules define what skin should be displayed for a given user, group, or portal resource. For example, if a portal serves both employees and customers, and there are requirements for a different set of graphics, colors, and fonts for each distinct user population, you can use skin rules to assign the corresponding skin to a given user group.

In addition to the rule types described here, you can use rules for the creation of roles, which are collections of users, groups, and other roles. You can create a rule-based role that defines members based on the same types of criteria as are used for the rule types. For information, see "Adding a Rule-Based Role" on page 83.

These aspects of rule management are described as follows:

This aspect...	Is described here...
The evaluation criteria used to evaluate rules	"The Evaluation Criteria Used in Rules" on page 213
Creating rules	"Creating Login Page Rules" on page 217
	"Creating Rendering Rules" on page 217
	"Creating Start Page Rules" on page 219
	"Creating Skin Rules" on page 223
	"Creating Shell Rules" on page 224
Changing the evaluation order of rules	"Managing the Evaluation Order for Rules" on page 216
Modifying rules	"Modifying a Rule" on page 219
Cloning rules	"Cloning a Rule" on page 220
Removing rules	"Removing a Rule" on page 220

The Evaluation Criteria Used in Rules

All rule types and the role-based role use the same set of evaluation criteria in determining a rule. Use the following guidelines in forming a rule:

- The **Match Criteria** list determines how strictly the evaluation criteria are used:

Match Criteria value	How the rule is applied
Match All Criteria Below	Each regular expression must match some part of the corresponding attribute value for the current user.
Match Any Criteria Below	Any regular expression in the list can match some part of the corresponding attribute value for the current user.

- If you leave any evaluation criterion empty, that criterion is not evaluated.

The rule evaluation criteria are as follows:

User DN Value(s)—A regular expression that matches any part of the current user's directory distinguished name (DN). In the field, type the portions of the DN to which you want a match.

For example, `ou=Engineering.*ou=US` matches a user with the following DN:

```
uid=joe,ou=Development,ou=Engineering,ou=Midwest,ou=US,o=webMethods
```

Domain Name Expression—A regular expression that matches any part of the name of the current user's directory service as registered in the portal. In the field, type the directory service name to which you want a match.

For example, US (without quotes) matches a user from the US Corporate directory service. This is a very effective way to govern the look and feel for users that may be in different user directories, such as partners.

Group DN and Role DN Expression—A regular expression that matches any part of any group or role of which the current user is a member. In the field, type the portions of the DN to which you want a match.

For example, `ou=Engineering` matches a user belonging to a group with the following DN:

```
cn=portal,ou=Engineering,ou=Midwest,ou=US,o=webMethods.
```

User Attributes—One or more pairs of user attributes and their values from the user's record. If you have more than one user attribute, the value set in **Match Criteria** determines how attributes are matched:

Match Criteria value	How the rule is applied
Match All Criteria Below	Each regular expression must match some part of the corresponding attribute value for the current user.
Match Any Criteria Below	Any regular expression in the list can match some part of the corresponding attribute value for the current user.

For example, if the rule is configured to match all criteria, and the configured user attribute pairs are the following:

Name	Value
`office`	Bellevue
`telephonenumber`	(425) 564-0000

and the current user's attribute values are the following:

Name	Value (current user)
`office`	Bellevue
`telephonenumber`	(206) 123-4567

the rule does not match the current user because it matches the `office` attribute value but not the `telephonenumber` attribute value. If, however, the rule is configured to match any criteria, the preceding example rule does match the current user.

To create an attribute-value pair, click **Add**. At the prompt, type the attribute name and click **OK**. At the prompt, type the value to be matched and click **OK**.

Request Headers—One or more pairs of HTTP header attributes and values. You can match anything that appears within an HTTP header, such as the browser agent string or the kinds of MIME types the user will accept. The rule can be a regular expression, or a simple text string. If you have more than attribute-value pair, the value set in **Match Criteria** determines how attributes are matched:

Match Criteria value	How the rule is applied
Match All Criteria Below	Each regular expression must match some part of the corresponding attribute value for the request header.
Match Any Criteria Below	Any regular expression in the list must match some part of the corresponding attribute value for the request header.

For example, if the rule is configured to match all criteria, and the configured request header pairs are the following:

Name	Value
Accept-Charset	utf-8
Accept-Language	ja

and the request header values for the current user are the following:

Name	Value (current user)
Accept-Charset	ISO-8859-1,utf-8;q=0.7
Accept-Language	en-us,en;q=0.5

the rule does not match the current user because it matches the Accept-Charset header value but not the Accept-Language header value. If, however, the rule was configured to match any criteria, the rule does match the current user.

To create an attribute-value pair, click **Add**. At the prompt, type the attribute name and click **OK**. At the prompt, type the value to be matched and click **OK**.

Parent Resource—A portal resource that matches the current portal resource or a parent of the current resource. To select a portal resource, click **Browse** to open the portal resource selector and select a portal resource against which to match the rule.If you want match a resource that is referenced by a portal alias, you can optionally click **Use Alias** to select an existing alias on the Portal server.

Resource Type—A resource type that matches the current resource type. To select a resource type, click **Browse** to open the portal resource selector and select a resource type, from the Extended Types folder, against which to match the rule.If you want match a resource type that is referenced by a portal alias, you can optionally click **Use Alias** to select an existing alias on the Portal server.

Resource Property—One or more pairs of portal resource properties and values. If you know the internal name of a property associated with a portal resource, you can match it. If you have more than one property-value pair, the value set in **Match Criteria** determines how properties are matched:

Match Criteria value	How the rule is applied
Match All Criteria Below	Each regular expression must match some part of the corresponding attribute value for the request header.
Match Any Criteria Below	Any regular expression in the list must match some part of the corresponding attribute value for the request header.

For example, if you want to match files that are PDFs, the property-attribute pair is `mimeType=pdf`.

To create an property-value pair, click **Add**. At the prompt, type the attribute name and click **OK**. At the prompt, type the value to be matched and click **OK**.

Managing the Evaluation Order for Rules

When a user requests a portal resource, the Portal server uses rules to determine how to fill the request. For example, perhaps the look and feel of the portal page is dependent on whether the user is a company employee or a customer. The server evaluates the skin rules to determine which skin to apply, in this order:

1. If there are multiple skin rules, the skin associated with the first rule that matches the user applies.
2. If none of the rules match the user, or if there are no skin rules, the default skin assigned in the **User Preferences** tab of the user's Profile page applies.
3. If no skin is assigned on the Profile page, the default skin for the portal applies.

If there are multiple skin rules, you can determine the order in which they are evaluated.

To change the order in rules are evaluated

1. As a portal administrator, browse to the **Administration Dashboard** and in the **Portal User Interface** folder, click the name of the set of rules you want to manage.

   If there are one or more existing rules, they appear in the **View Rules** tab.

2 Click the **Change Rule Evaluation Order** tab to bring it to the front.

3 In the **Evaluation Order** list, to move a rule, select it and then click the **Move Up** icon or **Move Down** icon as needed.

The rule in the list is searched first, followed by the second, and so on.

4 Click **Update**.

Creating Login Page Rules

The Manage Login Page Rules portlet allows you to define rules that dictate what login page should be used. Login page rules can be defined to dynamically set the default login page for a given for a given user, group, or role.

To create a new login page rule

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal User Interface** folder, click **Manage Login Page Rules**.

2 Click the **Create New Rule** tab to bring it to the front.

3 Type a name for the rule.

4 Optionally, type a description for the new rule.

5 Under the **Target** heading, click **Browse** and navigate to the portal page to be used as a login page.

6 Under the **Role Membership** heading, develop the criteria for the new login page rule using the guidelines in "The Evaluation Criteria Used in Rules" on page 213.

7 When you are finished entering the evaluation criteria for the new rule, click **Create Rule**.

Creating Rendering Rules

The Manage Rendering Rules portlet allows portal administrators to configure rendering rules for specific portal objects, such as a folder, portal page, portlet, and so forth. For example, an administrator who wants all portal folders to display a detailed view of portal content can create a rendering rule that applies a "details" renderer to all portal folder objects.

To create a new Rendering rule

1. As a portal administrator, browse to the **Administration Dashboard** and in the **Portal User Interface** folder, click **Manage Rendering Rules**.
2. Click the **Create New Rule** tab to bring it to the front.
3. Type a name for the rule.

   Example: `folder-thumbnails view (`for image files).
4. Optionally, type a description for your new rule.
5. Select the target renderer from the menu. The renderer you select will be applied to all portal objects that meet the evaluation criteria you define in the following steps.

   For example, the thumbnails renderer is useful for displaying thumbnail views for images that are published to the portal.
6. Under the **Role Membership** heading, select **Match All Criteria Below** or **Match Any Criteria Below** as the criteria for your rule.

Note: Rendering rules are typically applied to portal objects (folders, portlets, content items, and so forth) instead of users. As such, it is *not* recommended that you create rendering rules that are defined based on User DN, Group DN, or other user-oriented attributes. Rendering rules are most commonly applied to specific parent resources or for specific resource types.

7. If you want to configure a rendering rule for an existing portal resource for the **Parent Resource** option, click **Browse** and use the portal resource selector to select a resource to apply the rendering rule. For example, Public Folders.

   If you would like to define a rendering rule for a portal resource that is referenced by an existing portal alias, click **Use Alias** and select an alias.
8. If you want to configure a rendering rule for a specific portal object type (such as content, portlet, folder, or link) for the **Resource Type** option, click **Browse** and select an object.
9. If you want to configure a rendering rule for any resource that matches a specific property name/value pair, enter the name of the property that you want to match and the value for that property and click **Add**.

   This rule configuration is especially useful if you want to apply a custom rendering rule for a set of resources that share a common property name/value pair. For example, if you have several folders for storing image content for all who share a common description property value (such as *picture*), you could define the following Resource property as:

   Name: description Value: picture

With this setting, all portal resources that contain the word *picture* in their description property will dynamically use the renderer.

10 When you finish defining the evaluation criteria for your rendering rule, click **Create Rule**.

Creating Start Page Rules

The Manage Start Page Rules portlet allows portal administrators to define rules that dictate what portal start page should be used. The start page is the page to which the Portal server redirects users after log in. Start page rules can be defined to dynamically set the default start page for a given for a given user, group, or role.

To create a new start page rule

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal User Interface** folder, click **Manage Start Page Rules**.

2 Click the **Create New Rule** tab to bring it to the front.

3 Type a name for the rule.

4 Optionally, type a description for the new rule.

5 Under the **Target** heading, click **Browse** and navigate to the portal page to be used as a start page.

6 Under the **Role Membership** heading, develop the criteria for the new start page rule using the guidelines in "The Evaluation Criteria Used in Rules" on page 213.

7 When you are finished entering the evaluation criteria for the new rule, click **Create Rule**.

Modifying a Rule

After a rule exists, you can modify any portion of it that is editable.

To modify a rule

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal User Interface** folder, click the **Manage *rule-type* Rules** object that contains the rule you want to modify.

2 Click the **View Rules** tab to bring it to the front.

3 At the right edge of the row for the rule you want to modify, click (Popup Menu) and then click **Modify Rule**.

4 Make any needed changes to the evaluation criteria for the rule using the guidelines in "The Evaluation Criteria Used in Rules" on page 213.

5 At the bottom of the **Modify Rule** tab, click **Update Rule**.

Cloning a Rule

If you want to create a rule that is similar to an existing one, you can do so by cloning the existing rule.

To clone a rule

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal User Interface** folder, click the **Manage *rule-type* Rules** object that contains the rule you want to clone.

2 Click the **View Rules** tab to bring it to the front.

3 At the right edge of the row for the rule you want to clone, click (Popup Menu) and then click **Clone Rule**.

4 Type a name for the new rule.

5 Optionally, type a description for the new rule.

6 At the bottom of the **Clone Rule** tab, click **Clone The Rule**.

You can then modify the new rule, as described in "Modifying a Rule" on page 219.

Removing a Rule

To remove a rule, use the following procedure.

To remove a rule

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal User Interface** folder, click the **Manage *rule-type* Rules** object that contains the rule you want to remove.

2 Click the **View Rules** tab to bring it to the front.

3 At the right edge of the row for the rule you want to remove, click (Popup Menu) and then click **Remove Rule**.

4 To confirm that you want the remove the rule, click **OK**.

webMethods

CHAPTER 12

Managing Skins and Shells

Working with Skins

A *skin* is an installable webMethods Portal component that defines the look and feel of the portal user interface. A skin modifies the images, fonts, colors, and other subtle stylable aspects of HTML content, but it does not modify the HTML content in any functional way.

A portal developer creates new custom skins to accomplish many different tasks. Some of these include:

- Branding the portal with corporate, partner, or departmental logos.
- Aligning the portal color scheme with corporate, partner, or departmental colors.

Portal developers create skins with the Skin Administration portlet. See the *webMethods Portal Design Guide* for information about creating your own custom skins.

You can set up many different criteria to determine which skin is used for a particular user request. webMethods Portal offers a variety of ways to configure personalization rules that dictate what skin is displayed for a given user, group, or resource.

You can explicitly assign a particular skin to a specific user or set up rules that dynamically assign a skin based on a variety of criteria.

Explicitly Assigning a Skin

To assign a particular skin to a specific user, you can use the **User Preferences** tab of the profile page for a user. by default, users are granted the right to assign their own skins. See "The User Preferences Attribute Provider" on page 103.

Managing Skin Rules

The Manage Skin Rules portlet allows you to define rules that dictate what skins can be used by users, groups, or roles. This portlet allows a portal administrator to create, modify, or remove rules, and change the evaluation order of a list of rules that are evaluated for each user every time the user logs in. The following list provides information about managing rules:

This information about managing rules...	Is described here...
The evaluation criteria used to evaluate rules	"The Evaluation Criteria Used in Rules" on page 213
Changing the evaluation order of rules	"Managing the Evaluation Order for Rules" on page 216
Creating rules	"Creating Skin Rules" on page 223
Modifying rules	"Modifying a Rule" on page 219

This information about managing rules...	Is described here...
Cloning rules	"Cloning a Rule" on page 220
Removing rules	"Removing a Rule" on page 220

Creating Skin Rules

To create a new skin rule, use the following procedure.

To create a new skin rule

1. As a portal administrator, browse to the **Administration Dashboard** and in the **Portal User Interface** folder, click **Manage Skin Rules**.
2. Click the **Create New Rule** tab to bring it to the front.
3. Type a name for the rule.
4. Optionally, type a description for the new rule.
5. In the **Target** list, select the skin to be used if the rule is applied.
6. Under the **Evaluation Criteria** heading, develop the criteria for the new skin rule using the guidelines in "The Evaluation Criteria Used in Rules" on page 213.
7. When you are finished entering the evaluation criteria for the new rule, click **Create Rule**.

Working with Shells

A *shell* is an installable component of webMethods Portal. A shell is segment is a special kind of portal page that generates the webMethods Portal header, footer, and portlet title bars.

Where regular portlets produce the primary content of a portal page, a shell provides the structure that frames that primary content. Common Web page idioms such as banners, global navigation links, and search boxes appear in a shell.

A portal developer creates new custom shells to accomplish many different tasks, such as:

- Adding a row of links to other corporate Web sites below the page banner
- Changing the default portal search box to one that searches the corporate catalogue
- Adding a left-hand navigation bar to every portal page.

Portal developers create shells with the Skin Administration portlet. See the *webMethods Portal Design Guide* for information about creating your own custom shells.

You can set up many different criteria to determine which shell is used for a particular user request. webMethods Portal offers a variety of ways to configure personalization rules that dictate what shell is displayed for a given user, group, or resource.

Note: Unlike skins, you cannot explicitly assign a particular shell to a specific user. You need to use rules that dynamically assign a shell based on a variety of criteria.

Managing Shell Rules

The Manage Shell Rules portlet allows you to define rules that dictate what shells can be used by users, groups, or roles. This portlet allows a portal administrator to create, modify, or remove rules, and change the evaluation order of a list of rules that are evaluated for each user every time the user logs in. The following list provides information about managing rules:

This information about managing rules...	Is described here...
The evaluation criteria used to evaluate rules	"The Evaluation Criteria Used in Rules" on page 213
Changing the evaluation order of rules	"Managing the Evaluation Order for Rules" on page 216
Creating rules	"Creating Shell Rules" on page 224
Modifying rules	"Modifying a Rule" on page 219
Cloning rules	"Cloning a Rule" on page 220
Removing rules	"Removing a Rule" on page 220

Creating Shell Rules

To create a new shell rule, use the following procedure.

To create a new shell rule

1. As a portal administrator, browse to the **Administration Dashboard** and in the **Portal User Interface** folder, click **Manage Shell Rules**.
2. Click the **Create New Rule** tab to bring it to the front.
3. Type a name for the rule.
4. Optionally, type a description for the new rule.
5. In the **Target** list, select the shell to be used if the rule is applied.

6 Under the **Evaluation Criteria** heading, develop the criteria for the new skin rule using the guidelines in "The Evaluation Criteria Used in Rules" on page 213.

7 When you are finished entering the evaluation criteria for the new rule, click **Create Rule**.

Setting Shells for Requests

To set a specific shell for a request, a portal developer creates a link to a portal resource and adds a shell parameter to the link. The shell parameter value should be an alias to the target shell.

For example, the URL for a link to the public folder with the extranet shell is /folder.public?shell=shell.extranet. When users follow the link, they view the public folder framed with the specified extranet shell. When users click another portal link from the public folder page, they return to whatever shell they were using before, provided the link does not also have a shell parameter.

Setting Shells for Sessions

To set a specific shell for a session, sometimes referred to as a *sticky* shell because the setting is retained for the duration of the session, a portal developer creates a link to the forceShell portal command. This command takes a returnUrl parameter, which redirects a user to the specified URL once the shell has been set.

For example, the URL for a link to the public folder with a sticky extranet shell is /?command=forceShell&shellURI=shell.extranet&returnUrl=folder.public. When users follow the link, they view the public folder now framed with the extranet shell. When users click another portal link from the public folder page, provided the link does not have a shell parameter, they see that page still framed with the extranet shell.

webMethods

CHAPTER 13

Managing and Using a Wiki

What is a Wiki

A *wiki* is a Web interface for a storage organization. A wiki makes it possible to write documents collectively, giving multiple individuals the ability create, edit, and reorganize content. A wiki is a body of individual pages, called wiki pages, interconnected by hyperlinks. A wiki uses a simple markup language with which you can format text, create structure, and add hypertext links within the wiki or to external sites.

The wiki maintains versions of wiki pages. With this feature, you can see who has made various changes to a wiki page or restore an earlier version of a page as the current version.

Managing Participation in a Wiki

Because of the collaborative nature of a wiki, it becomes important to manage access to it. For some wikis, it may be acceptable to allow anyone to make changes to content while others may require limited access. As a portal administrator, you have control over the kinds of actions an individual can perform against a wiki page:

To allow a user to do this...	Grant the user this permission
View a wiki page	View
Modify text and rename the page	Modify properties
Create a subpage or attach a file	Modify properties and Create child
Create a new page	Create child permission for the folder or page where the wiki page is to be created

In addition, everyone who can view a wiki page has permission to browse or search for wiki pages on the Portal server. For more on managing permissions, see "Managing Permissions" on page 135.

Creating a Wiki Page

As portal administrator or a user with portal administrator privileges, you can create a wiki.

To create a wiki

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Content** folder, click **Wiki Administration**.

2 Click **Create New Wiki**.

3 In the **Wiki Name** field, type a display name to identify the wiki page.

There are no restrictions on what characters you can use for this name. The maximum length for a name is 255 characters.

4 In the **Place wiki on the portal page** area, do one of the following:

Click this...	And do this...
Browse	On the left side of the portal resource selector, browse to the target portal page or folder, click the **Select** icon, and then click **Select**.
Use Alias	In the **Alias Name** field of the portal resource selector, type the alias of the target portal page or folder. Click **Test** to determine if the alias is valid and the alias target is the correct one. If the alias is correct, click **Select**.

5 In the editor, type a heading for the wiki page, and any other text you want to start with.

6 At the bottom of the page, click **Next**.

7 Click **Finish**.

Modifying a Wiki Page

Anyone with modify permission for a wiki page can edit the page and perform a variety of actions on the page.

Do do this...	Look here...
Edit a wiki page	"Editing a Wiki Page" on page 229
See wiki syntax	"Wiki Syntax" on page 230

Editing a Wiki Page

To edit a wiki page

1 Locate the wiki page and click or the name of the wiki page to open it.

By default, a wiki page opens on the **View** tab.

2 Click **Edit**.

3 Modify, add, or remove text as appropriate.

4 If you need assistance with the syntax for marking up wiki content, click **Syntax Help** at the bottom of the page.

5 To save your work, do one of the following:

This command...	Does this...
Save	Saves the wiki page, updates wiki history, and sends a notification event to anyone who is subscribed to the wiki page.
Quiet Save	Saves the wiki page but does not update wiki history or send a notification event. Use this command to save changes before you have finished editing.

Both commands close the editor and return the wiki page to the **View** tab.

Wiki Syntax

The following table shows the syntax used in formatting wiki pages:

Formatting Commands		Syntax	Example
Headings	Heading text wrapped with single quotation marks renders a heading style. The number of marks sets the level of heading.	`''Heading_2''`	**Heading_2**
	At least three dashes at the beginning of a line, followed by plus signs and the heading text. The number of plus signs sets the level of heading.	`---+++Heading_3`	**Heading_3**
Paragraph	Two carriage returns or line feeds create a new paragraph.	`First paragraph` `Second paragraph`	1st Paragraph 2nd Paragraph
Force Next Line	Two backslashes (\ \) force a new line.	First line\ \Next line	First Line Second Line
Bold Text	Text enclosed with asterisks (*) is displayed in bold text.	*Bold text*	**Bold text**
Italic Text	Text enclosed with underscores (_) is displayed in italic text.	_Italic text_	*Italic text*
Bold Italic Text	Text enclosed with double underscores (__) is displayed in bold italic text.	__Bold italic text__	***Bold italic text***

Formatting Commands		Syntax	Example
Text Coloring	Text enclosed between %COLOR% and %ENDCOLOR% is displayed in the specified color, where COLOR is one of the sixteen HTML color names.	%BLUE%Blue text%endcolor%	Blue text
Fixed Font	Text enclosed with equal signs(=) is displayed in fixed font.	=Fixed font=	`Fixed font`
Bold Fixed Font	Text enclosed with double equal signs(==) is displayed in bold fixed font.	==Bold fixed font==	**`Bold fixed font`**
Text Style	Text enclosed within style tags ([color,style]) is displayed according to the elements within the tag. Valid style elements are Bold and Italic.	[blue]Blue text[/blue] [red,bold,italic]Red bold italic [/red,bold,italic]	Blue text ***Red bold italic***
Line Separator	At least three dashes at the beginning of a line creates a horizontal rule. You cannot place any other text on the same line.	+++	
HTML Encoding	To show HTML encoding, enclose it with (((and))) (triple parentheses). Otherwise, raw HTML is transformed.	(((tag)))	tag
Bullet List	Three, six, nine (and so forth) spaces followed by a single asterisk (*) define a bullet list. You can also use one, two, three, or more asterisks.	* Level_1 * Level_2 * Level_1 ** Level_2	• Level_1 ◦ Level_2
Numbered List	Three spaces and a 1 start a numbered list. To nest another numbered list inside the first, use three spaces and two 1s. You can also use pound signs (#). Precede each line of the numbered list with #. To nest another numbered list inside the first, use ##, and so on.	1 Item_1 11 Item_a 11 Item_b 1 Item_2 # Item_1 ## Item_a ## Item_b # Item_2	1. Item_1 1. Item_a 2. Item_b 2. Item_2
Tables	Table cells are enclosed in vertical bars (|).	| *L* | *C* | *R* | | A2 | 2 | 2 | | A3 | 3 | 3 | | multi span ||| | A4 | next | next |	

Formatting Commands		Syntax Example
Links to External Sites	To create a link, specify the link reference and the link display text separately using nested square brackets: [[*reference*][*text*]] where [*reference*] is a wiki name or an external link.	[[http://www.yahoo.com][Yahoo]] Displays as: Yahoo
	Optionally, add a link target to the reference to open the link in a new window: [[reference;target=new][text]]	[[http://www.yahoo.com;target=new][Yahoo in a New Browser]] Displays as: Yahoo in a New Browser
Links to Other Wiki Pages	A valid wiki name takes the form: [*WikiPagePath*].*WikiName* where *WikiName* is the valid wiki name without spaces. The name My Wiki becomes MyWiki.	[[MyWiki][My Wiki]] Displays as: My Wiki
	If the wiki page is a subpage, *WikiPagePath* is the parent wiki page where the subpage resides, where *WikiPagePath* is the valid wiki name without spaces. You can omit *WikiPagePath* if the referenced wiki page is a sibling or direct subpage of the current wiki page.	[[MyWiki.MySubpage][My Subpage]] Displays as: My Subpage
URLs	Any valid URL draws itself as a link.	http://www.yahoo.com Displays as: http://www.yahoo.com
URLs to Attachments	To embed an image or a file attached to the wiki page, use the %ATTACHURLPATH% macro followed by the name of the attached file. Use this URL as an <img> tag source to display attached images in place.	

Formatting Commands		Syntax	Example
Table of Contents	The %TOC% macro creates a table of contents of the current page, made up of headings used on the page.	%TOC%	• Heading 1 ◦ Subhead 1 ◦ Subhead 2 • Heading 2
Includes	The %INCLUDE% macro includes content of another wiki page into the current page.	%INCLUDE{"WikiPath.WikiName"}%	

Finding a Wiki Page

As a portal administrator, there are multiple tasks you can take to find and open a wiki.

This task...	Is described here...
Find all wiki pages on the Portal server	"Finding a Wiki Page by Browsing" on page 233
Search for a specific wiki page	"Searching for a Wiki Page" on page 234

Finding a Wiki Page by Browsing

If you know the name of a particular wiki page, you can quickly locate it from a list of wiki pages on the Portal server.

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Content** folder, click **Wiki Administration**.

2 Click **Browse Wiki**.

The Wiki Browse page contains a list of wiki pages stored on the Portal server, including the following information about each wiki page:

Column	Description
Name	The name of the wiki page. Click the **Name** column to open the wiki page.
Location	The location of the wiki page. Click the **Location** column to open the portal page or folder on which the wiki page resides. The location provides this additional information about the wiki:

Column	Description	
	If the location is...	It means this...
	A portal page or folder	The wiki page can be made available to anyone who has access rights to the page or folder.
	Wiki Pages	The wiki page is only available for someone with portal administrator rights.
	Another wiki page	The wiki page is a subpage of another wiki page.
Author	The user name of the creator of the wiki page.	
Date Modified	The date and time the wiki page was last modified or renamed.	

3 Locate the wiki and do one of the following:

Take this action...	To do this...
Click  or the name	To open the wiki page in a **View** tab.
Click the location	To open the portal page or folder on which the wiki page resides.

Searching for a Wiki Page

As a portal administrator, you can search for a wiki page by name or based on criteria such as author name.

To search for a wiki page

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Content** folder, click **Wiki Administration**.

2 Click **Search Wiki**.

3 In the **Query** field, type keywords on which to search, using these guidelines:

- Keywords can be in the wiki name or in the text on the wiki page
- The search is not case sensitive
- Use whole words only

- A space between keywords is an implicit OR (for example, `one two` finds either `one` or `two`)
- A plus sign (+) is an implicit AND (for example, `+one +two` must find both words to match)
- Use an asterisk (*) as a multiple-character wildcard or a question mark (?) as a single-character wildcard to complete a keyword (for example, `thr*`, `th*e`, and `th?ee` all find `three`)
- Use double quotation marks (") to enclose a string (for example `"one two three"`)

4 (Optional) Refine the search using any or all of the following fields:

Field	Description
Start Date	Searches for wiki pages last modified on or after the specified date. Click and click the start date for the search.
End Date	Searches for wiki pages last modified on or before the specified date. Click and click the end date for the search.
Author	Searches for wiki pages created by a specified user. Click **Browse**. On the left side of the portal resource selector, navigate to the user and click the **Select** icon. With the selected user appearing in the **Selected Items** panel, click **Select**. You can select only one user at a time.
Location Folder	Searches for wiki pages located in a specified folder. In the **Location Folder** area, do one of the following: **Browse** — On the left side of the portal resource selector, browse to the target resource, click the **Select** icon, and then click **Select**. **Use Alias** — In the **Alias Name** field of the portal resource selector, type the alias of the target resource. Click **Test** to determine if the alias is valid and the alias target is the correct one. If the alias is correct, click **Select**.

5 Click **Search**.

The Search Results page provides a list of wiki pages that match the search criteria, including the following information about each wiki page:

Column	Description
Rank	An approximate ranking of how closely the item matches the search criteria.
Name	The name of the wiki page. Click the **Name** column to open the wiki page.
Description	The description of the wiki page provided at the time the page was created.
Modified	The date and time the wiki page was last modified or renamed.
Location	The location of the wiki page. Click the **Location** column to open the portal page or folder on which the wiki page resides. The location provides this additional information about the wiki:

If the location is...	It means this...
A portal page or folder	The wiki page can be made available to anyone who has access rights to the page or folder.
Wiki Pages	The wiki page is only available for someone with portal administrator rights.
Another wiki page	The wiki page is a subpage of another wiki page.

6 Locate the wiki and do one of the following:

Take this action...	To do this...
Click  or the name	To open the wiki page in a **View** tab.
Click the location	To open the portal page or folder on which the wiki page resides.

Wiki Saved Searches

After you perform a search for wiki content, as described in "Searching for a Wiki Page" on page 234, you have the opportunity to save the search criteria in the Search Results page. By saving search criteria, you can reuse the same criteria to perform the same search on a regular basis.

To save a wiki search

1 After performing a wiki search, on the Search Results page, click **Add to my Saved Searches**.

2 At the prompt, type a descriptive name for the saved search and click **OK**.

There are no restrictions on what characters you can use for this name. The maximum length for a name is 255 characters. The saved search is stored in your Saved Searches folder.

To use a saved wiki search

1 In the global navigation toolbar, click **My Folders**.

2 In the Saved Searches folder, locate the saved search and click the link.

Moving a Wiki Page

As a portal administrator, you can move a wiki page from one folder to another. When you move the wiki page, any subpages and attached files are moved along with the wiki page.

To move a wiki page

1 As a portal administrator, locate the wiki page you want to move and open it.

2 On the title bar, click (Popup Menu) for the wiki page, then click **Clipboard** and **Cut**.

3 Locate the page or folder where you want the wiki page to reside.

4 On the title bar, click (Popup Menu) for the page or folder, then click **Clipboard** and **Paste**.

Renaming a Wiki Page

A portal administrator or a user with modify permission can rename a wiki page. Renaming a wiki page causes all links to the page to be renamed.

To rename a wiki

1 Open the wiki page you want to rename.

2 Click **Rename**.

3 In the **New Wiki Name** field, type the new name for the wiki.

There are no restrictions on what characters you can use for this name. The maximum length for a name is 255 characters

4 Click **Rename**.

Adding a Subpage to a Wiki Page

A portal administrator or a user with modify permission can add a new subpage to an existing wiki page. A subpage is a separate wiki page that is child to the wiki page in which it is created. After you add a new subpage to a wiki page, it is listed in the **Subpages and Files** tab.

To add a new subpage to a wiki

1 Open the wiki page to which you want to add a subpage.

2 Click **New Subpage**.

3 In the **Wiki Name** field, type the name for the wiki subpage.

There are no restrictions on what characters you can use for this name. The maximum length for a name is 255 characters

4 By default, the new subpage is created on the wiki page from which it is created. If you want to add the subpage to a different wiki page, do one of the following:

Click this...	And do this...
Browse	On the left side of the portal resource selector, browse to the target wiki page, click the **Select** icon, and then click **Select**.
Use Alias	In the **Alias Name** field of the portal resource selector, type the alias of the target wiki page. Click **Test** to determine if the alias is valid and the alias target is the correct one. If the alias is correct, click **Select**.

5 In the editor pane, type a heading for the wiki subpage, and any other text you want to add.

6 At the bottom of the page, click **Next**.

7 Click **Finish**.

Attaching a File to a Wiki Page

A portal administrator or a user with modify permission can attach a file to a wiki page as a means of sharing that file with other users. There are no restrictions on the type of file you can attach. You can control the maximum size of attached files by clicking **Content Service** in the **Portal Content** folder of the **Administration Dashboard**.

To attach a file to a wiki page, do the following:

To attach a file to a wiki page

1. Open the wiki page to which you want to attach a file.
2. Click **Attach File**.
3. In the **Name** field of the Publish page, type a display name for the file.

   There are no restrictions on what characters you can use for this name. The maximum length for a name is 100 characters
4. (Optional) In the **Description** field, type descriptive comments about the file.

   The description appears when you display a list of files attached to the wiki page.
5. In the **File** field, browse to the location of the file to be attached and click **Open**.

   The file must be on a network file system or on a mapped drive for the computer you are using.
6. In the **Encoding** list, do one of the following:
   - Choose the type of encoding suitable for the type of file you are attaching. The default encoding value is **Non text (binary)**.
   - If you do not find the suitable encoding type in the list, choose **Other** from the list, type the correct encoding, and click **OK**.
7. In the **Link Target** field, choose one of the following:
   - **Open content in the current window** (the default)
   - **Open content in a new window**
8. Click **Finish**.

Files that are attached to a wiki page appear in the **Subpages and Files** tab for that page.

Opening a File Attached to a Wiki Page

A portal administrator or a user who has view permission for an attached file can open it.

To open a file attached to a wiki page

1 Open the wiki page to which the file is attached.

2 Click **Subpages and Files**.

3 Click the name of the attached file to open it.

If the file...	The expected behavior is...
Can open in a browser	The file opens in the same window or in a new window according to the setting in the **Link Target** field when the file was attached.
Cannot open in a browser window	The browser offers you the choice of opening the file with an application on your computer or saving the file to disk.

To attach a file to a wiki page, see "Attaching a File to a Wiki Page" on page 239.

Managing Versions of a Wiki Page

One of the features of a wiki is that a version is stored each time someone updates a page. You can go back to view and edit earlier versions, and restore a particular version to be the current version. The wiki displays a list of versions on the **History** tab for a wiki page. You can take the following tasks to manage versions of a wiki page.

This task...	Is described here...
View the list of versions for a wiki page	"Viewing the History of a Wiki Page" on page 240
View a version of the wiki page	"Viewing an Older Version of a Wiki Page" on page 242
Change an older version of the wiki page to be the current version	"Make a Wiki Page the Current Version" on page 242
Compare textual changes between one version and the previous version in the history list.	"Comparing With the Previous Version of a Wiki Page" on page 243

Viewing the History of a Wiki Page

When you view a wiki page, it is the current version of that page. The wiki retains earlier versions of the page and maintains a history of those versions. To view the history of a wiki page, do the following:

To view the history of a wiki page

1 Find and open the wiki page for which you want to view the history, as described in "Finding a Wiki Page" on page 233.

2 Click the **History** tab.

The **History** tab contains a record of versions of the wiki page:

Column	Description
Date	The date and time the version was saved.
Action	The action performed before the version was saved:

Action	Description
Reverted Version	An older version was made to be the current version.
Renamed	The wiki page was renamed.
Updated Text	A change was made to the content of the wiki page.

User	The name of the user who performed the action.
Tools	A popup menu containing further actions you can take on the version.

Action	Description
View	Open this version in the **View** tab.
Compare to Previous	Compare the content of this version to the previous version. See "Comparing With the Previous Version of a Wiki Page" on page 243.
Make This Current	Make this version the current version of the wiki page. "Make a Wiki Page the Current Version" on page 242.

Viewing an Older Version of a Wiki Page

To view an older version of a wiki page, do the following:

To view an older version of a wiki page

1 Find and open the wiki page for which you want to view the history, as described in "Finding a Wiki Page" on page 233.

2 Click the **History** tab.

The version at the top of the **History** tab is the current version.

3 For the version of the wiki page you want to view, do one of the following:

- Click the link in the **Action** column.
- Click (Popup Menu) in the **Tools** column.

4 Take other actions as needed:

To do this...	Do this...
Edit the page	Click the **Edit** tab. For more information, see "Modifying a Wiki Page" on page 229.
View a different version	Click the **History** tab and repeat the steps in this procedure.
Make this page the current version	See "Make a Wiki Page the Current Version" on page 242.

Make a Wiki Page the Current Version

The version at the top of the **History** tab is the current version. To make an older version of a wiki page the current page, do the following:

To make an older version of a wiki page the current page

1 Find and open the wiki page, as described in "Finding a Wiki Page" on page 233.

2 Click the **History** tab.

3 Locate the version of the wiki page that should be the current version.

4 Click (Popup Menu) in the **Tools** column and click **Make This Current**.

This version of the wiki page is displayed in the **View** tab. If you click **History**, you will see an addition at the top of the history list with the **Action** value of **Reverted Version**.

Comparing With the Previous Version of a Wiki Page

For any version of a wiki page on the **History** tab except the first, you can compare text changes between that version and the previous version in the list.

To a compare version of a wiki page with the previous version in the list

1 Find and open the wiki page, as described in "Finding a Wiki Page" on page 233.

2 Click the **History** tab.

3 Locate the version of the wiki page that should be compared.

4 Click (Popup Menu) in the **Tools** column and click **Compare to Previous**.

A comparison view is displayed:

These lines...	Are displayed like this...
Added lines	Blue in color and preceded by >>>
Deleted lines	Red in color, preceded by <<<, and struck through

Editing an Older Version of a Wiki Page

You can locate an earlier version of a wiki page and make changes. When you save the changes, the changed version becomes the current version of the wiki page.

To edit an older version of a wiki page

1 Find and open the wiki page, as described in "Finding a Wiki Page" on page 233.

2 Click the **History** tab.

3 Locate the version of the wiki page that should be edited.

4 Click (Popup Menu) in the **Tools** column and click **View**.

5 With the selected version of the wiki page in the **View** tab, click **Edit**.

6 Make textual changes as needed and click **Save**.

The saved version of the wiki page displays in the **View** tab and becomes the current version of the page.

webMethods

CHAPTER 14

Managing and Using a Forum

What is a Forum?

A *forum* is a Web interface for a discussion board. A forum makes it possible for users to post messages, sharing information and opinions about one or more topics. A forum can be moderated, allowing the Moderator to control access to the forum and accept or reject messages posted to it.

How Forums are Organized

Discussion boards are made up of the following objects:

Object	Description
Category	A container for one or more forums. You can choose to have the forums within a category inherit the options and permissions chosen for the category. A category resides within a folder on the portal.
Forum	A container for one or more topics. A forum can reside within a category or within a folder.
Topic	A container for messages. When you create a topic, you also create the first message it contains. By default, a topic resides within a forum.
Message	The content of a forum topic. Users can post, edit, and reply to messages. Messages reside within topics and can contain attachments.

Roles Associated with Forums

There are a variety of roles associated with a forum. By assigning roles, you can control who is allowed to post, who is allowed only to read, and who is denied access to participate. You can assign roles for a specific forum or forum category ("Modifying Permissions for a Forum or Forum Category" on page 267) or create a forum Security Realm for use throughout the portal ("Managing Forum Security Realms" on page 271).

Standard Roles

The following roles are listed in order of increasing capability:

Forum role	Capability	Description
Denied Access	Does not have permission to view the forum.	
Spectator	Can view forum postings but cannot create topics or messages. Spectators have the following capabilities:	
	View	Can view forum topics and messages. See "Getting Started with Forums as Portal Administrator" on page 249.
	Subscribe	Can receive notifications to changes in the forum. See "Subscribing to a Forum or Forum Category" on page 251.
	Rate	Give a rating from Poor to Excellent to a topic or message. See "Rating a Topic" on page 254.
Contributor	In addition to the capabilities above, can do the following:	
	Create a topic	Open a new topic and create the first message in it. See "Creating a Topic" on page 255.
	Create a message	Reply to an existing topic. See "Creating a Message in an Existing Topic" on page 256
	Request a retraction	Request that message be deleted from the forum. See "Requesting a Retraction" on page 257.
Moderator	In addition to the capabilities above, can perform the following actions:	
	Approve or reject a topic or message	In a moderated forum, allow a new topic or message to be posted or deny permission to do so. See "Moderating a Forum" on page 258.
	Edit a message	Modify the content of an existing message. See "Editing a Message" on page 259
	Delete a topic or message	Delete an existing message, or a topic and all messages within it. See "Deleting a Topic or Message" on page 260

Forum role	Capability	Description
(Forum) Administrator	In addition to the capabilities above, can perform the following actions:	
	Create a forum or forum category	Create a new forum or forum category, placing it in a specified folder. See "Creating a Forum or Forum Category" on page 261.
	Move a forum	Move a forum from one folder to another. "Moving a Forum or Forum Category" on page 265.
	Rename a forum or forum category	Rename a forum or forum category. See "Renaming a Forum or Forum Category" on page 265.
	Edit options	Determine what options will apply, such as whether the forum is moderated or whether attachments are allowed. "Modifying Options of a Forum or Forum Category" on page 266.
	Edit permissions	Assign roles, such as Moderators, Contributors, and Spectators. "Modifying Permissions for a Forum or Forum Category" on page 267.
	Delete a forum or forum category.	Delete a forum or forum category and all topics within it. "Deleting a Forum or Forum Category" on page 269.

The Other Role

In addition to the standard roles, you can assign a role named Other. The Other role is neither granted nor denied any permissions. This option is for use when a portal administrator has set some permissions manually that do not translate to a known forum permission setting. See "Managing Permissions" on page 135.

How this Chapter is Organized

The following section ("Getting Started with Forums as Portal Administrator") provides general information on the initial setup of forums and forum categories, along with cross-references to specific procedures later in the chapter. The sections that follow are organized to match the increasing capabilities associated with the various forum roles:

- "Activities You can Perform as a Spectator" on page 249
- "Activities You Can Perform as a Contributor" on page 255
- "Activities You Can Perform as a Moderator" on page 258

Getting Started with Forums as Portal Administrator

Before anyone can use forums in the portal, the portal administrator must create the first forum or forum category, establish initial rules for usage, and establish permissions for various types of forum user. The following steps represent some suggested activities you can perform, depending on the your needs.

1. Create at least one forum or forum category, as described in "Creating a Forum or Forum Category" on page 261.
2. If, necessary, modify usage options for forums and categories, as described in "Modifying Options of a Forum or Forum Category" on page 266.
3. If you want to create the ability for users other than portal administrators to moderate or administrate forums or forum categories, do the following:
   a. Create one or more forum Security Realms in which you identify forum privileges for users and groups, as described in "Managing Forum Security Realms" on page 271.
   b. In individual forums and forum categories, assign forum Security Realms or create custom sets of privileges, as described in "Modifying Permissions for a Forum or Forum Category" on page 267.

After you have established forums and forum categories, the forum Moderators and Administrators can manage daily activities.

Activities You can Perform as a Spectator

If you have Spectator privileges, you are limited to activities needed to find and read forum topics:

This activity...	Is described here...
Reading topics and messages	"Viewing Forum Objects" on page 250
Receiving notifications of changes to topics	"Getting Started with Forums as Portal Administrator" on page 249
Finding topics based on text or keywords	"Searching in a Forum" on page 252
Giving your opinion on the relatively usefulness of a message	"Rating a Topic" on page 254

Viewing Forum Objects

Anyone with at least Spectator privileges can view forum categories, forums, or topics. A table containing forums and forum categories has the same columns:

Column	Purpose
Name	The name of the forum category, forum, or topic: **If the descendent is a...** — **Click the name to display...** Forum category — A table of forums or forum categories that are descendents. Forum — A table of topics within the forum. Topic — A view of postings related to the topic.
Rating	(Optional) For a forum, displays the average rating given to each topic and the number of reviews. To rate a topic, see "Rating a Topic" on page 254. A forum Administrator can enable or disable this option. See "Modifying Options of a Forum or Forum Category" on page 266.
Posts	The number of topics in descendent forums or forum categories.
Last Post	The date, time, and Contributor of the most recent posting to any descendent forum or forum category.
Created	The date, time, and creator of the forum or forum category.

To view a forum, topic, or message

1 To locate the forum, topic, or message, do one of the following:

- Browse to the forum category that contains the forum you want to view.
- Browse to the forum that contains the topic and message you want to view.
- Search for the topic or message, as described in "Searching in a Forum" on page 252.

2 Click the name of the forum to display it.

3 Within a forum, click the name of the topic to display it.

By default, a topic is displayed in the **Details View** tab.

4 As needed click one of the following tabs to change the topic view:

This tab...	Presents this view of a topic...
Details View	Each posting to the topic appears in a separate table row. If you are at least a Contributor, the row includes a list of actions that are available to you, such as **Reply** or **Request Retraction**.
Outline View	A table contains summary information about each posting to the topic. The row has the following columns: **Name** The name of the posting. Click the name of the posting to display it individually (same as Individual View). **Author** The Contributor who made the posting **Date** The date and time the posting was made.
Individual View	Each posting is displayed on a separate page. If you are at least a Contributor, the row includes a list of actions that are available to you, such as **Reply** or **Request Retraction**. Standard navigation features allow you to browse forward and backward among the postings.

Subscribing to a Forum or Forum Category

If you have at least Spectator privileges, you can subscribe to changes in a forum object:

If you subscribe to...	You are notified when...
A forum	A topic or a message is added or deleted.
A forum category	A topic or a message is added or deleted, assuming you have permission to view the parent forum.

To subscribe to a forum or a forum category

1 Browse to the forum or forum category to which you want to subscribe.

2 In the forum or forum category, click **Subscribe**.

3 On the Subscribe page, select subscription options for the forum or forum category:

This option...	Determines whether or not...
Subscribe to this Forum	Select **Yes** to enable subscription or **No** to disable subscription.
Subscription Type	Select how often to receive notifications of subscription events. You can receive individual notifications (the default), a daily digest, or a weekly digest.
Delivery Mechanism	Notifications are delivered by e-mail (the default) or posted to your portal inbox.

4 Click **Apply**.

Tip! To find your inbox, go to the global navigation toolbar at the top of each portal page and click **Inbox**.

Searching in a Forum

If you have at least Spectator privileges, you can search for a forum topic by name, text within the topic, or based on criteria such as author name.

To search for a forum topic or message

1 Browse to any forum or forum category you have permission to view.

2 In the Search list, choose one of the following:

Choose this item...	If...
Search All Forums	You don't know in which forum the topic belongs.
Search This Forum	If you are certain the topic is a descendent of the current forum or forum category.

3 In the query field, type text on which to search, using these guidelines:

- Text can be in the topic name or in the message text.
- The search is not case sensitive.
- Use whole words only.
- A space between keywords is an implicit OR (for example, one two finds either one or two).

- A plus sign (+) is an implicit AND (for example, +one +two must find both words to match)
- Use an asterisk (*) as a multiple-character wildcard or a question mark (?) as a single-character wildcard to complete a keyword (for example, thr*, th*e, and th?ee all find three)
- Use double quotation marks (") to enclose a string (for example "one two three")

4 Click **Go**.

The Search Results page provides a list of topics that match the search criteria, including the following information about each topic:

Column	Description
Forum	The name of the forum to which the topic belongs. Click the forum name to open the forum.
Topic	The name of the topic. Click the topic name to open the topic in the Details View.
Message	The name of the message. Click the message name to open the message in the Individual View (without navigation aids).
Rating	The average rating given to the topic and the number of reviews.
Author	The name of the user who created the topic. Click the author name to display the user information page.
Created	The date and time the message was created.

5 (Optional) To refine the search, click **Advanced Search** and use any or all of the following fields:

Field	Description
Query	Type text on which to search, using the guidelines in step 3, or a forum alias (see the **Search Type** field). By default, the field is filled with the text of the previous search.
Forum	Searches for messages that are descendents of a specified forum or forum category. In the **Forum** area, do one of the following: **Browse** — On the left side of the portal resource selector, browse to the target resource, click the **Select** icon, and then click **Select**.

Field	Description
	Use Alias In the **Alias Name** field of the portal resource selector, type the alias of the target resource. Click **Test** to determine if the alias is valid and the alias target is the correct one. If the alias is correct, click **Select**.
Author	Searches for topics created by a specified user. Click **Browse**. On the left side of the portal resource selector, navigate to the user and click the **Select** icon. With the selected user appearing in the **Selected Items** panel, click **Select**. You can select only one user at a time.
Start Date	Searches for topics last modified on or after the specified date. Click the **Start Date** icon and click the start date for the search.
End Date	Searches for topics last modified on or before the specified date. Click the **End Date** icon and click the end date for the search.
Search Type	Searches based on text or keywords. In the **Search Type** area, choose either of the following options: **Full Text** Searches for text within a topic using the guidelines in step 3. The default. **Keyword** Searches for a keyword assigned to a forum or forum category.

6 Click **Search**.

Rating a Topic

A forum Administrator has the capability to enable or disable the rating of topics within a forum. If rating is enabled and if you have at least Spectator privileges, you can rate a forum topic or message. A rating for a topic or a message is an average of values.

To rate a forum topic or message

1 Browse to a forum topic you have permission to view.

2 In either the Details View for the topic, or the Individual View for the topic or message, click **Rate** at the right side of the title area.

If rating is disabled, the **Rate** link is not visible.

3 On the Rate page, select one of the rating options.

The options and their values are:

Option	Value
Excellent	10
Good	7
Poor	3
Unacceptable	0

4 Click **Rate**.

Activities You Can Perform as a Contributor

If you have Contributor privileges, you can perform all of the activities of a Spectator ("Activities You can Perform as a Spectator" on page 249) and also post topics and messages:

This activity...	Is described here...
Create a new topic	"Creating a Topic" on page 255
Post a message in an existing topic	"Creating a Message in an Existing Topic" on page 256
Request that a message you have posted be retracted	"Requesting a Retraction" on page 257

Creating a Topic

If you have at least Contributor privileges in a forum, you can create a topic and add the first message to it.

To create a topic

1 Browse to the forum or forum category in which you want to create the topic.

If you have at least Contributor privileges, the **New Topic** tab appears on the forum page.

2 In the forum, click **New Topic**.

3 In the **Subject** field, type the title for the new topic.

This value appears in the **Name** column on the forum page.

4 In the editor, type the text of the first message for the topic.

If the **Allow HTML in Posts** option is enabled for the forum, the editor allows you to apply formatting to the text. Otherwise, only a text editor is available.

5 If the **Allow Attachments** option is enabled for the forum, you can add one or more attachments by doing the following:

a In the **Attachments** area, click **Add**.

b In the Attachment field, click **Browse**, browse to the file you want to attach, and click **Open**.

c In the File Encoding list, select the type of file encoding appropriate for the attachment.

The default encoding is Non Text (binary).

d Click **Add**.

The attachment is added to the message.

6 Click **Post**.

If the forum is unmoderated, the topic is added to the forum page. If the forum is moderated, the Moderator must approve the topic.

Creating a Message in an Existing Topic

A topic is a container that holds messages. If you have at least Contributor privileges, you can create a message in an existing topic.

To create a message in an existing topic

1 To find the topic, do one of the following:

- Browse to the forum or that contains the topic and click the topic name.
- Search for the topic, as described in "Searching in a Forum" on page 252 and click the topic name.

By default, the topic opens in the Details View, which displays as many messages as will fit on the screen.

2 Locate a message to which you want to reply and click **Reply**.

When you click a message, the text of that message is placed in the editor. You can delete some or all of the text, depending on the nature of your reply.

3 In the editor, type the text of the message.

If the **Allow HTML in Posts** option is enabled for the forum, the editor allows you to apply formatting to the text. Otherwise, only a text editor is available.

4 If the **Allow Attachments** option is enabled for the forum, you can add one or more attachments by doing the following:

a In the **Attachments** area, click **Add**.

b In the Attachment field, click **Browse**, browse to the file you want to attach, and click **Open**.

c In the File Encoding list, select the type of file encoding appropriate for the attachment.

The default encoding is Non Text (binary).

d Click **Add**.

The attachment is added to the message.

5 Click **Post**.

If the forum is unmoderated, the message is added to the topic. If the forum is moderated, the Moderator must approve the message.

Requesting a Retraction

If you are the author of a topic or a message, you can request that it be deleted from the forum. A topic or message can be deleted only by someone with at least Moderator privileges.

To request that a topic or message be retracted

1 To find the topic, do one of the following:

- Browse to the forum or that contains the topic and click the topic name.
- Search for the topic, as described in "Searching in a Forum" on page 252 and click the topic name.

By default, the topic opens in the Details View, which displays as many messages as will fit on the screen.

2 If you are the author, you can request retraction of a topic or message as follows:

To request retraction of...	If you are the author, do this...
A topic	In the first message, click **Request Retraction**. The entire topic is labeled Requested for Retraction.
A message	Click **Request Retraction**. The message is labeled Requested for Retraction.

The topic or message continues to appear until actually deleted by a Moderator or Administrator. The topic or message waiting to be retracted is labeled **(Requested for Retraction)**.

Activities You Can Perform as a Moderator

If you have Moderator privileges, you can perform all of the activities of these roles:

This role	Is described here
Spectator	"Activities You can Perform as a Spectator" on page 249
Contributor	"Activities You Can Perform as a Contributor" on page 255

You can also moderate forums, and edit or delete postings:

This activity...	Is described here...
In a moderated forum, approve or reject topics and messages	"Moderating a Forum" on page 258
Edit the text of an existing message	"Editing a Message" on page 259
Delete a topic or message from a forum	"Deleting a Topic or Message" on page 260

Moderating a Forum

In a moderated forum, if you have at least Moderator privileges, you can approve or reject topics and messages.

Note: To ensure that you are aware of postings pending approval, you need to subscribe to the forums for which you are responsible. See "Subscribing to a Forum or Forum Category" on page 251.

To moderate a forum

1 When you receive notification of a change in a forum, do one of the following:

If your notification is...	Do this...
Your portal inbox	In the Inbox, click the Subject of the notification and then click **View Topic**.
E-mail	In the e-mail notification you receive, click **View Topic**.

The topic or message waiting to be approved is labeled **(Pending Approval)**. Contributors and Spectators cannot see the topic or message until it is approved.

2 In the new topic or message, do one of the following:

To do this...	Take this action...
Approve the posting	In the message, click **Approve**.
Reject the posting	In the message, click **Reject**.
Edit the posting	In the message, click **Edit**. In the editor, make changes as needed and then click **Update**. You can also edit postings in unmoderated forums.

Editing a Message

If you have at least Moderator privileges, you can edit the text of a message and add or remove attachments. The forum can be either moderated or unmoderated.

To edit a message

1 To find the topic, do one of the following:

- Browse to the topic that contains the message.
- Search for the message, as described in "Searching in a Forum" on page 252 and click the message name.

2 In the message, click **Edit**.

3 In the editor, edit the text as needed.

If the **Allow HTML in Posts** option is enabled for the forum, the editor allows you to apply formatting to the text. Otherwise, only a text editor is available.

4 If the **Allow Attachments** option is enabled for the forum, you can add or remove attachments by doing one of the following:

To this...	Take this action...
Add an attachment	Click **Add**. Browse to the file you want to attach and click **Open**. Select the appropriate file encoding and click **Add**.
Remove an attachment	In the Attachment list, select the file to be removed and click **Remove**.

5 Click **Update**.

Deleting a Topic or Message

If you have at least Moderator privileges, you can a topic or message. The forum can be either moderated or unmoderated.

One reason to delete a topic or message is if the author has requested a retraction, as described in "Requesting a Retraction" on page 257. A topic or message waiting to be retracted is labeled **(Requested for Retraction)**.

Note: To ensure that you are aware of postings for which a retraction has been requested, you need to subscribe to the forums for which you are responsible. See "Subscribing to a Forum or Forum Category" on page 251.

To delete a topic or message

1 To find the topic, do one of the following:

- Browse to the forum or that contains the topic and click the topic name.
- Search for the topic, as described in "Searching in a Forum" on page 252 and click the topic name.

By default, the topic opens in the Details View, which displays as many messages as will fit on the screen.

2 In message to be deleted, click **Delete**.

If this if the first message in the topic, the entire topic is deleted.

3 To confirm that you want to delete the topic or message, click **OK**.

Activities You Can Perform as an Administrator

If you have forum Administrator privileges, you can perform all of the activities of these roles:

This role	Is described here
Spectator	"Activities You can Perform as a Spectator" on page 249
Contributor	"Activities You Can Perform as a Contributor" on page 255
Moderator	"Activities You Can Perform as a Moderator" on page 258

You can also create, manage, and delete forums and forum categories:

This activity...	Is described here...
Create a new forum or forum category within an existing category	"Creating a Forum or Forum Category" on page 261
Move a forum or forum category within existing categories	"Moving a Forum or Forum Category" on page 265
Rename an existing forum or forum category	"Renaming a Forum or Forum Category" on page 265
Determine what options will apply, such as whether the forum is moderated or whether attachments are allowed	"Modifying Options of a Forum or Forum Category" on page 266
Assign roles, such as Moderators, Contributors, and Spectators	"Modifying Permissions for a Forum or Forum Category" on page 267
Delete a forum or forum category and all topics within it	"Deleting a Forum or Forum Category" on page 269

Creating a Forum or Forum Category

A forum category is a container for one or more forums, or forum categories. Categories are useful for organizing forums into groups having similar content. Another feature of a category is that you can you can specify options that are inherited by the forums within it.

As portal administrator or a user with portal administrator privileges, you can create a forum category. If you are not a portal administrator, but have been given forum Administrator privileges for a forum category, you can create a descendent forum or category.

To create a forum or forum category

1 If you are a portal administrator, do the following:

   a Browse to the **Administration Dashboard** and in the **Portal Content** folder, click **Forum Administration**.

   b Do one of the following:

To create a...	Do this...
Forum category	Click **Create New Forum Category**.
Forum	Click **Create New Forum**.

2 If you are a forum Administrator, do the following:

   a Browse to a forum category for which you have Administrator privileges.

   b Do one of the following:

To create a...	Do this...
Forum category	Click **New Category**.
Forum	Click **New Forum**.

3 In the **Name** field, type a name to identify the forum or forum category.

   There are no restrictions on what characters you can use for this name. The maximum length for a name is 255 characters.

4 Optionally, in the **Description** field, type a description for the forum or forum category, which appears in the **Description** field of the folder that contains the category.

5 Optionally, add one or more keywords to be used in searching for the forum or forum category by doing the following:

   a In the **Keywords** area, click **Add**.

   b In the prompt window that opens, type a keyword and then click **OK**.

6 In the **Parent Container** area, do one of the following:

Click this...	And do this...
Browse	On the left side of the portal resource selector, browse to the target portal folder, click the **Select** icon for the resource, and then click **Select**.
Use Alias	In the **Alias Name** field of the portal resource selector, type the alias of the target portal folder. Click **Test** to determine if the alias is valid and the alias target is the correct one. If the alias is correct, click **Select**.

Tip! If you create a forum or forum category from within a forum category, that category is the default container.

7 Click **Next**.

8 On the Options page, select options for the forum or forum category:

This option...	Determines whether or not...
Allow Un-moderated Posts	Messages must be approved by a Moderator or Administrator before they are posted. Select **Yes** to allow unmoderated posts or **No** to require moderated posting.
Allow Attachments	Contributors can post attachments to messages. Select **Yes** to allow attachments or **No** to disable the posting of attachments.
Allow HTML in Posts	Messages can contain HTML formatting. Select **Yes** to allow HTML formatting or **No** to limit postings to plain text.
Allow Ratings	Contributors and Spectators can rate individual messages. Select **Yes** to allow the rating of messages or **No** to disable the rating feature.

9 Click **Next**.

10 On the Permissions page, determine what forum Security Realm is to be applied to the forum category, by doing one of the following:

Click this...	And do this...
Browse	On the left side of the portal resource selector, and click **Forum Realms**. **Tip!** If Forum Realms is not visible, select **Root** from the **Location** list; then click **Security Realms** in the left panel. Locate a forum realm and click the **Select** icon. The default choices are: **Anonymous Users are Contributors** — Anyone, including users without login accounts, can view the forum and post messages to it. **Authenticated Users are Contributors** — Only authenticated users can post messages to a forum. With Forum Realms in the **Selected Items** panel, click **Select**.
Use Alias	In the **Alias Name** field of the portal resource selector, type the alias of the target forum realm. Click **Test** to determine if the alias is valid and the alias target is the correct one. If the alias is correct, click **Select**.

Note: If you do not choose any forum Security Realm, the forum or forum category inherits the permissions set for the parent container in which it was created. You can later change permissions to assign members to the various forum roles and to cause descendents to inherit permissions. See "Modifying Permissions for a Forum or Forum Category" on page 267.

11 Click **Create**.

Moving a Forum or Forum Category

As portal administrator or a user with portal administrator privileges, you can move an existing forum category to a new location. If you are a forum Administrator, you can also move a forum or forum category, but only to a location where you have Administrator privileges.

To move a forum or forum category

1 As a portal administrator or a forum Administrator, browse to the folder that contains the forum or forum category and click the name to open it.

2 In the forum or forum category, click **Move**.

3 On the Move page, do one of the following to find the target folder where the forum or forum category is to reside:

Click this...	And do this...
Browse	On the left side of the portal resource selector, browse to the target portal folder, click the **Select** icon for the resource, and then click **Select**.
Use Alias	In the **Alias Name** field of the portal resource selector, type the alias of the target portal folder. Click **Test** to determine if the alias is valid and the alias target is the correct one. If the alias is correct, click **Select**.

4 With the new location selected, click **Move**.

Renaming a Forum or Forum Category

As portal administrator, user with portal administrator privileges, or a forum Administrator, you can rename a forum or forum category and edit keywords associated with it.

To rename a forum or forum category

1 As a portal administrator or a forum administrator, browse to the folder that contains the forum or forum category and click the name to open it.

2 In the forum category, click **Rename**.

3 In the **Name** field, type a new name to identify the forum or forum category.

There are no restrictions on what characters you can use for this name. The maximum length for a name is 255 characters.

4 Optionally, in the **Description** field, type a description of the forum or forum category, which appears in the **Description** field of the folder that contains the forum or forum category.

5 Optionally, add, edit, or remove keywords to be used in searching for the forum or forum category by doing one of the following in the **Keywords** area:

To do this...	Do this...
Add a keyword	Click **Add**, type a new keyword in the prompt window, and click **OK**.
Edit a keyword	Select the keyword, click **Edit**, type a revised keyword in the prompt window, and click **OK**.
Remove a keyword	Select the keyword, click **Remove**, and click **OK**.

6 Click **Apply**.

Modifying Options of a Forum or Forum Category

As portal administrator, a user with portal administrator privileges, or a forum Administrator, you can modify the options of a forum or forum category. You can specify whether or not the options apply to any descendant forum or forum category.

To modify options of a forum or forum category

1 As a portal administrator or a forum Administrator, browse to the folder that contains the forum or forum category and click the name to open it.

2 In the forum category, click **Options**.

3 On the Options page, change one or more of the following options:

This option...	Determines whether or not...
Allow Un-moderated Posts	Messages must be approved by a Moderator or Administrator before they are posted. Select **Yes** to allow unmoderated posts or **No** to require moderated posting.
Allow Attachments	Contributors can post attachments to messages. Select **Yes** to allow attachments or **No** to disable the posting of attachments.

This option...	Determines whether or not...
Allow HTML in Posts	Messages can contain HTML formatting. Select **Yes** to allow HTML formatting or **No** to limit postings to plain text.
Allow Ratings	Contributors and Spectators can rate individual messages. Select **Yes** to allow the rating of messages or **No** to disable the rating feature.

4 Use the **Apply to Descendents** option to specify whether or not the options apply to any descendant forum or forum category:

Do this...	To do this...
Select the check box	To cause all descendant forums and forum categories to inherit the options.
Clear the check box	To specify that descendant forums and forum categories do not automatically inherit the options.

You can override options within individual descendent forums and forum categories.

Modifying Permissions for a Forum or Forum Category

As portal administrator, a user with portal administrator privileges, or a forum Administrator, you can modify the permissions of a forum or forum category. You can specify whether or not the permissions apply to any descendant forum or forum category.

To modify permissions of a forum or forum category

1 As a portal administrator or a forum Administrator, browse to the folder that contains the forum or forum category and click the name to open it.

2 In the forum category, click **Permissions**.

3 On the Permissions page, do one of the following:

- Select the **Realm** option (the default) and determine what forum Security Realm is to be applied to the forum category, by doing one of the following:

Click this...	And do this...
Browse	On the left side of the portal resource selector, and click **Forum Realms**. **Tip!** If Forum Realms is not visible, select **Root** from the **Location** list; then click **Security Realms** in the left panel. Locate a forum realm and click the **Select** icon. The default choices are: **Anonymous Users are Contributors** — Anyone, including users without login accounts, can view the forum and post messages to it. **Authenticated Users are Contributors** — Only authenticated users can post messages to a forum. With Forum Realms in the **Selected Items** panel, click **Select**.
Use Alias	In the **Alias Name** field of the portal resource selector, type the alias of the target forum realm. Click **Test** to determine if the alias is valid and the alias target is the correct one. If the alias is correct, click **Select**.

—OR—

- Provide a set of custom permissions by doing the following:

a Select the **Custom** option and click **Edit**.

b From the **Scheme** list, select the authentication scheme to be used for this forum category.

The default authentication scheme is inherited from the parent of the forum or forum category or, lacking any custom authentication scheme, from the system default. For information on authentication schemes, see "Managing Authentication" on page 130.

c In the **Authorization** table, do one of the following:

To do this...	Do this...
Add a new user or group	Click **Add Users or Groups**. On the left side of the portal resource selector, browse to a user or group, click the **Select** icon for the resource. Repeat this action to add multiple users and groups to the **Selected** panel and then click **Next**. From the **Capacity** list, select the role to be used by these users and groups and click **Apply**. Standard roles are described in "Standard Roles" on page 247.
Edit a user or group	Locate the user or group in the **Authorization** table and click the **Properties** icon for the resource. From the **Capacity** list, select the role to be used the resource and click **Apply**. Standard roles are described in "Standard Roles" on page 247.
Delete a user or group	Locate the user or group in the **Authorization** table and click the **Delete** icon for the resource. To confirm that the resource should be deleted, click **OK**.

d After you have finished activities in the **Authorization** table, click **Apply**.

4 On the Permissions page, use the **Apply to Descendents** option to specify whether or not the permissions apply to any descendant forum or forum category:

Do this...	To do this...
Select the check box	To cause all descendant forums and forum categories to inherit the permissions.
Clear the check box	To specify that descendant forums and forum categories do not automatically inherit the permissions.

You can override options within individual descendent forums and forum categories.

5 Click **Apply**.

Deleting a Forum or Forum Category

As portal administrator, a user with portal administrator privileges, or a forum Administrator, you can delete a forum or forum category.

Note: Deleting a forum category also deletes any forums or forum categories that are its descendents.

To delete a forum or forum category

1. As a portal administrator or a forum Administrator, browse to the folder that contains the forum or forum category and click the name to open it.
2. In the forum or forum category, click **Delete**.
3. To confirm that the forum or forum category should be deleted, click **OK**.

Managing Forums as Portal Administrator

As a portal administrator or a user with portal administrator privileges, you can perform all of the activities of these forum roles:

This role	Is described here
Spectator	"Activities You can Perform as a Spectator" on page 249
Contributor	"Activities You Can Perform as a Contributor" on page 255
Moderator	"Activities You Can Perform as a Moderator" on page 258
Administrator	"Activities You Can Perform as an Administrator" on page 261

As portal administrator, you can perform the following activities from the Administrative Dashboard:

This activity...	Is described here...
Create forums and forum categories	"Creating a Forum or Forum Category" on page 261
Create, edit, and delete forum Security Realms	"Managing Forum Security Realms" on page 271
Perform advanced searches for forum topics	"Searching Forums as Portal Administrator" on page 274
Create a list of topics and messages pending approval	"Listing Topics and Messages Pending Approval" on page 276
Create a list of messages requested for retraction	"Listing Messages Requested for Retraction" on page 277
Create a variety of forum reports	"Running Forum Reports" on page 278

Managing Forum Security Realms

By default, there are two forum Security Realms:

This Security Realm...	Allows this type of access...
Anonymous users are Contributors	Anyone, including users without login accounts, can view the forum and post messages to it.
Authenticated users are Contributors	Only authenticated users can post a message.

As a portal administrator, you can create additional forum Security Realms that specify the forum privileges of users and groups. Once you have established a forum Security Realm, you can apply it to forums and forum categories, as described in "Modifying Permissions for a Forum or Forum Category" on page 267.

Creating a Forum Security Realm

As a portal administrator or a user with portal administrator privileges, you can create a new forum Security Realm.

To create a forum Security Realm

1. As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Content** folder, click **Forum Administration**.
2. In the Forum Administration page, click **Manage Forum Security Realms**.
3. On the Manage Forum Security Realms page, click **Create New Realm**.
4. In the **Name** field, type a name to identify the forum Security Realm.

   There are no restrictions on what characters you can use for this name. The maximum length for a name is 255 characters.
5. Optionally, in the **Description** field, type a description for the forum Security Realm, which appears in the **Description** field on the Manage Forum Security Realms page.
6. Click **Create**.
7. On the Manage Forum Security Realms page, click the **Properties** icon for the forum Security Realm you have just created.
8. From the **Scheme** list, select the authentication scheme to be used for this forum category.

   The default authentication scheme is inherited from the parent of the Security Realm, or, lacking any custom authentication scheme, from the system default. For information on authentication schemes, see "Managing Authentication" on page 130.

9 Click **Add Users or Groups**.

10 Select the users and groups to be given a set of forum privileges, such as Moderator, as described in "Standard Roles" on page 247, by doing the following:

a On the left side of the portal resource selector, browse to a user or group, click the **Select** icon for the resource. Repeat this action to add multiple users and groups to the **Selected** panel and then click **Next**.

b From the **Capacity** list, select the role to be used by these users and groups and click **Apply**.

11 Repeat step 10 for each set of privileges you want to include in the forum Security Realm.

12 After you have created privileges list created, click **Apply**.

13 On the Manage Forum Security Realms page, click **Done**.

You can now apply the forum Security Realm to any forum or forum category.

Editing a Forum Security Realm

As a portal administrator or a user with portal administrator privileges, you can edit an existing forum Security Realm.

To edit a forum Security Realm

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Content** folder, click **Forum Administration**.

2 In the Forum Administration page, click **Manage Forum Security Realms**.

3 On the Manage Forum Security Realms page, click the **Properties** icon for the forum Security Realm you want to edit.

4 If you want to change the authentication scheme to be used for this forum Security Realm, from the **Scheme** list, select the new authentication scheme.

5 If you want to edit forum privileges in the **Authorization** table, do one or more of the following:

To do this...	Do this...
Add a new user or group	Click **Add Users or Groups**. On the left side of the portal resource selector, browse to a user or group, click the **Select** icon for the resource. Repeat this action to add multiple users and groups to the **Selected** panel and then click **Next**. From the **Capacity** list, select the role to be used by these users and groups and click **Apply**. Standard roles are described in "Standard Roles" on page 247.
Edit a user or group	Locate the user or group in the **Authorization** table and click the **Properties** icon for the resource. From the **Capacity** list, select the role to be used the resource and click **Apply**. Standard roles are described in "Standard Roles" on page 247.
Delete a user or group	Locate the user or group in the **Authorization** table and click the **Delete** icon for the resource. To confirm that the resource should be deleted, click **OK**.

6 After you have finished editing, click **Apply**.

The changes are applied to any forum or forum category that uses this forum Security Realm.

Deleting a Forum Security Realm

As a portal administrator or a user with portal administrator privileges, you can delete an existing forum Security Realm.

To delete a forum Security Realm

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Content** folder, click **Forum Administration**.

2 In the Forum Administration page, click **Manage Forum Security Realms**.

3 On the Manage Forum Security Realms page, click the **Delete** icon for the forum Security Realm you want to delete.

4 To confirm that you want to delete the forum Security Realm, click **OK**.

5 On the Manage Forum Security Realms page, click **Done**.

Any forum or forum category that used the deleted forum Security Realm reverts to the set of permissions it inherited from the parent container in which it was created.

Searching Forums as Portal Administrator

As a portal administrator or a user with portal administrator privileges, you can perform a search of forum topics from within the Forum Administration page. The capabilities are similar to performing an advanced search from within a forum or forum category.

To search for a forum topic or message as a portal administrator

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Content** folder, click **Forum Administration**.

2 In the Forum Administration page, click **Search Forums**.

3 In the query field, type text on which to search, using these guidelines:

- Text can be in the topic name or in the message text.
- The search is not case sensitive.
- Use whole words only.
- A space between keywords is an implicit OR (for example, one two finds either one or two).
- A plus sign (+) is an implicit AND (for example, +one +two must find both words to match)
- Use an asterisk (*) as a multiple-character wildcard or a question mark (?) as a single-character wildcard to complete a keyword (for example, thr*, th*e, and th?ee all find three)
- Use double quotation marks (") to enclose a string (for example "one two three")

4 (Optional) To refine the search, click **Advanced Search** and use any or all of the following fields:

Field	Description
Query	Type text on which to search, using the guidelines in step 3, or a forum alias (see the **Search Type** field). By default, the field is filled with the text of the previous search.

Field	Description
Forum	Searches for messages that are descendents of a specified forum or forum category. In the **Forum** area, do one of the following: **Browse** — On the left side of the portal resource selector, browse to the target resource, click the **Select** icon, and then click **Select**. **Use Alias** — In the **Alias Name** field of the portal resource selector, type the alias of the target resource. Click **Test** to determine if the alias is valid and the alias target is the correct one. If the alias is correct, click **Select**.
Author	Searches for topics created by a specified user. Click **Browse**. On the left side of the portal resource selector, navigate to the user and click the **Select** icon. With the selected user appearing in the **Selected Items** panel, click **Select**. You can select only one user at a time.
Start Date	Searches for topics last modified on or after the specified date. Click the **Start Date** icon and click the start date for the search.
End Date	Searches for topics last modified on or before the specified date. Click the **End Date** icon and click the end date for the search.
Search Type	Searches based on text within a topic or by alias. In the **Search Type** area, choose either of the following options: **Full Text** — Searches for text using the guidelines in step 3. The default. **Keyword** — Searches for a keyword assigned to a forum or forum category.

5 Click **Search**.

The Search Results page provides a list of topics that match the search criteria, including the following information about each topic:

Column	Description
Forum	The name of the forum to which the topic belongs. Click the forum name to open the forum.
Topic	The name of the topic. Click the topic name to open the topic in the Details View.
Message	The name of the message. Click the message name to open the message in the Individual View (without navigation aids).
Rating	The average rating given to the topic and the number of reviews.
Author	The name of the user who created the topic. Click the author name to display the user information page.
Created	The date and time the message was created.

Listing Topics and Messages Pending Approval

As a portal administrator or a user with portal administrator privileges, you can create a list of forum topics and messages pending approval. Messages posted to moderated forums do not appear until they have been approved by someone with at lease Moderator privileges. While forum Moderators and Administrators can be notified of changes to forums by subscribing ("Subscribing to a Forum or Forum Category" on page 251), only a portal administrator can create a list of all forum messages pending approval.

To search for a forum topic or message pending approval as a portal administrator

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Content** folder, click **Forum Administration**.

2 In the Forum Administration page, click **List Topics and Messages Pending Approval**.

The Forums Reports page provides a list of topics that are pending approval, including the following information about each topic:

Column	Description
Forum	The name of the forum to which the topic belongs. Click the forum name to open the forum.
Topic	The name of the topic. Click the topic name to open the topic in the Details View.
Message	The name of the message. Click the message name to open the message in the Individual View (without navigation aids).

Column	Description
Author	The name of the user who created the topic. Click the author name to display the user information page.
Created Date	The date and time the message was created.

Listing Messages Requested for Retraction

As a portal administrator or a user with portal administrator privileges, you can create a list of forum messages that have been requested for retraction. Messages requested for retraction can be deleted only by someone with at lease Moderator privileges. While forum Moderators and Administrators can be notified of changes to forums by subscribing ("Subscribing to a Forum or Forum Category" on page 251), only a portal administrator can create a list of all forum messages requested for retraction.

To search for a forum message requested for retraction as a portal administrator

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Content** folder, click **Forum Administration**.

2 In the Forum Administration page, click **List Messages Requested for Retraction**.

The Forums Reports page provides a list of topics that are requested for retraction, including the following information about each topic:

Column	Description
Forum	The name of the forum to which the topic belongs. Click the forum name to open the forum.
Topic	The name of the topic. Click the topic name to open the topic in the Details View.
Message	The name of the message. Click the message name to open the message in the Individual View (without navigation aids).
Author	The name of the user who created the topic. Click the author name to display the user information page.
Created Date	The date and time the message was created.

Running Forum Reports

As a portal administrator or a user with portal administrator privileges, you can create reports based on a variety of criteria.

To run a forum report

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Content** folder, click **Forum Administration**.

2 In the Forum Administration page, click **Run Report**.

3 In the **Report Type** area choose from among several options:

This option...	Provides the following report...
Messages Pending Approval	A list of messages in moderated forums that are pending approval. Same as the report created in "Listing Topics and Messages Pending Approval" on page 276.
Messages Requested for Retraction	A list of messages that are requested for retraction. Same as the report created in "Listing Messages Requested for Retraction" on page 277.
Messages by Forums	A list of forums and the number of topics (T) and messages (M) in each. Click a forum name to open the forum.
Messages by Forums by Authors	A list of forums, the names of authors posting to each, and the number of topics (T) and messages (M) by each author. Click a forum name to open the forum. Click the author name to display the user information page.
Messages by Authors	A list of authors and the number of topics (T) and messages (M) by each author. Click the author name to display the user information page.
Messages by Authors by Forums	A list of authors and the forums they post to, along with the number of topics (T) and messages (M) posted to each forum. Click the author name to display the user information page. Click a forum name to open the forum.

4 (Optional) To refine the scope of the report, use any or all of the following fields:

Field	Description
Forum Root	Limits the report to messages that are descendents of a specified forum or forum category. In the **Forum Root** area, do one of the following: **Browse** — On the left side of the portal resource selector, browse to the target resource, click the **Select** icon, and then click **Select**. **Use Alias** — In the **Alias Name** field of the portal resource selector, type the alias of the target resource. Click **Test** to determine if the alias is valid and the alias target is the correct one. If the alias is correct, click **Select**.
Author	Limits the report to messages created by a specified user. Click **Browse**. On the left side of the portal resource selector, navigate to the user and click the **Select** icon. With the selected user appearing in the **Selected Items** panel, click **Select**. You can select only one user at a time.
Start Date	Limits the report to messages last modified on or after the specified date. Click the **Start Date** icon and click the start date for the report.
End Date	Limits the report to messages last modified on or before the specified date. Click the **End Date** icon and click the end date for the report.
Interval	Adds columns to report the number of topics (T) and messages (M) in each interval. For example, if you choose the **Daily** option, the report includes a set of **T** and **M** columns for each day in the range reported on. Chose one of these options: **None** — No interval is specified. The default. **Daily** — Number of topics and messages each day. **Weekly** — Number of topics and messages each week. **Monthly** — Number of topics and messages each month. **Yearly** — Number of topics and messages each year.

5 Click **Run Report**.

webMethods

CHAPTER 15

Portal Clustering

Overview of Portal Clustering

This chapter describes how to set up webMethods Portal in a clustered environment. The chapter illustrates only one of many different scenarios for configuring your portal in a clustered configuration. The chapter includes descriptions of the various roles played by portals in a portal cluster, how to plan a cluster, and how to use the Cluster Administration portlet to configure a clustered environment.

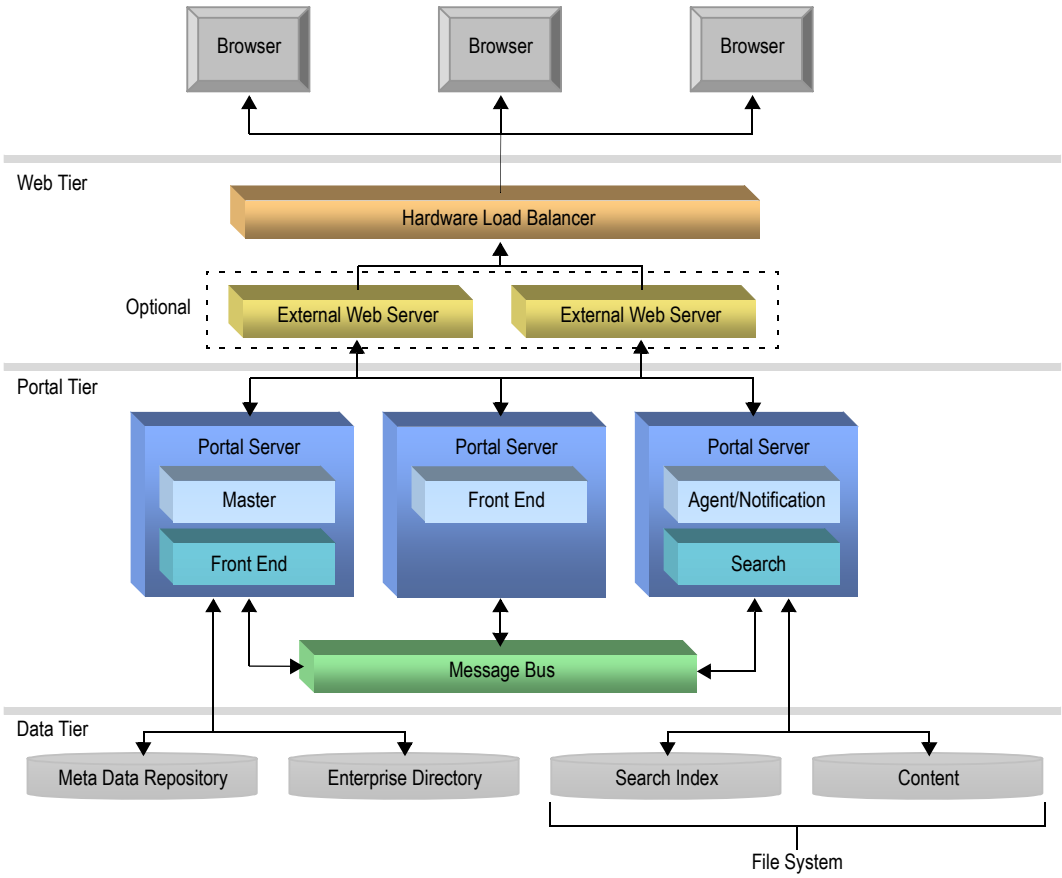
Portal Server Roles

There are several types of Portal server roles that can be assigned to a Portal server instance. These include:

- The **Front End** Portal server role is responsible for processing all requests coming from the portal Web server and responses that are sent back to the client. It also performs most of the portal business logic and JSP processing tasks.
- The **Agent Routing** Portal server role is responsible for managing all agent-based subscriptions within the portal system. For example, the agent routing role handles all processing that is required when a portlet subscribes to one or more events in an asynchronous manner, executes its business logic, and updates data in the portal database.
- The **Notification** Portal server role is responsible for formatting and sending e-mail notifications, and notifications that are sent to a portal user's Notification Inbox.
- The **Search** role is responsible for indexing all content that is exposed to the embedded portal search engine, maintaining the search index, and performing the searches.

Planning your Portal Cluster

The following section describes the process of configuring a portal cluster based on the following network diagram.



The preceding diagram assumes that there will be three Portal server machines operating in a cluster, each with its own Portal server roles, which are organized into segments. The machines defined in the Web tier include a hardware-based Load Balancer and two Web server machines. The following sections illustrate the process that an administrator would work through to start with one Portal server instance and sequentially add additional Portal servers, each with their own roles in the distributed deployment.

Note: This is one of many types of distributed deployments that can be configured with webMethods Portal.

Note: The procedures for configuring IIS or Apache in an external load-balanced Web server cluster configuration with your portal deployment are explained in Appendix A, "Integrating webMethods Portal with External Web Servers" on page 291.

The Cluster Administration Portlet

The Cluster Administration portlet allows portal administrators to configure webMethods Portal in a clustered environment. This portlet provides a GUI-based configuration environment for setting up a portal cluster. You can also set up a webMethods Portal cluster by editing a special configuration file called cluster.xml.

Configuring the Default Segment in the Portal Server Cluster

Setting up a portal cluster requires that you start with a portal installation on a single Portal server. The steps that follow assume that you have already run the webMethods Portal Configurator tool after installing the baseline webMethods Portal software.

For detailed instructions on how to use the Configurator to install a default Portal server, see the *webMethods Installation Guide*.

Note: After running the Configurator, a cluster.xml file is generated and written to the file system on which the initial portal is installed. By default, this file is located in the `/webMethods_install_dir/P`ortal/server/*portal_instance_name*/config directory.

The initial default values stored in the cluster.xml file are based on the configuration choices made when you ran the Configurator.

To verify the default cluster setting

1. Identify the machines that you want to use in your cluster.
2. As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Configuration** folder, click **Cluster Administration**.
3. In the **View Segments** tab, click the **Popup Menu** icon for the **default** segment and then click **Modify Segment**.

4 Using the **Segment Properties** display, verify the default cluster settings as follows:

Property	Value should be set to...
Name	The default name of the first portal front end machine you have in the default segment.
Front End URL	`http://server name:port number` The URL listed is for the front end machine you have in the default segment.

Do not change these values at this time. After you set up the portal front end machines which have their own specific roles for the default segment in your cluster, you have the option of configuring a separate Web server cluster. You do this by pointing to the IP address or server name for your load-balanced Web server farm. See Appendix A, "Integration with Web Servers" on page 292 for procedures.

5 Click **Save**.

Adding Portal Server Machines to the Default Segment in your Cluster

To add Portal server machines to the default Portal server cluster

1 As a portal administrator, browse to the **Administration Dashboard** and in the **Portal Configuration** folder, click **Cluster Administration**.

2 Click the default server cluster and, in the **Modify Segment** tab, click **Add Server**.

3 Under the **Server Properties** heading, type a **Server Name**.

Tip! It is best to specify the role of the Portal server in the **Server Name** field. For example, if you are adding a new Portal server machine to the default segment that will be configured with the Front End role, you could use FE_portalServer1.

4 Under the **Server Roles** heading, select the appropriate role for the Portal server you are configuring. Examples are **Portal Front End**, **Agent Routing**, **Notification**, and **Search**:

   a For each role you want to remove from the list of current server roles, locate and select the server role in the **Current Roles** panel and then click the **Unselect** icon to move the user name into the **Available Roles** panel.

   b For each role you want to add to the list of current server roles, locate and select the server role in the **Available Roles** panel and then click the **Select** icon to move the role into the **Current Roles** panel.

Note: The **Host Name** field for the listeners you will configure in the following typically the host name of the machine where the Portal server is to run. In most cases, the host name is the same name for all four listeners. See your network administrator for information about host names and network setup at your site.

5 Under the **HTTP Listener** heading, type the **Host Name** for the HTTP listener.

6 In the **Port** field, type the port number to be used by the HTTP listener.

   A value of 0 (zero) in this field disables the listener.

7 Under the **HTTPS Listener** heading, type the **Host Name** for the HTTPS listener.

8 In the **Port** field, type the port number to be used by the HTTPS listener.

   A value of 0 (zero) in this field disables the listener.

Note: webMethods Portal includes a sample demo HTTP certificate which you can use to set up and test your HTTPS listener. It is located in the *webMethods_install_dir*/Portal/server/*portal_instance_name*/config/demo.keystore. For production environments, be sure to obtain an actual Certificate from a qualified authority (for example, Verisign).

9 Under the **AJP13 Listener** heading, type the **Host Name** for the AJP13 Listener.

   You use this setting when you are configuring an external Web server with your front end segment.

10 In the **Port** field, type the port number to be used by the AJP13 listener.

   A value of 0 (zero) in this field disables the listener.

11 Under the **RMI Listener** heading, type the **Host Name** for the RMI Listener.

   You use this setting for Inter-cluster communication.

12 In the **Port** field, type the port number to be used by the RMI listener.

   A value of 0 (zero) in this field disables the listener.

13 Click **Save** to save your settings.

14 Repeat this procedure for each Portal server machine that you want to configure as part of the default portal segment.

Note: You must restart the cluster before these changes will take effect.

Reconfiguring the Master Portal Server

After adding the remaining Portal server machines with their own role configurations to the default segment, you must reconfigure the Master Portal Server, which is the first server you installed and configured in your portal cluster.

To reconfigure the Master Portal server front end in the default segment

1 On the Master Portal server, browse to the **Administration Dashboard** and in the **Portal Configuration** folder, click **Cluster Administration**.

Important! The Master Portal server machine in the default segment *must* have the Front End role to function properly.

2 For the default segment click the **default** segment link or click (Popup Menu) and then click **Modify Segment**.

3 Under the **Registered Servers** heading, click the Master server link or click (Popup Menu) and then click **Modify Server**.

4 On the **Roles** list, remove all server roles that are now being handled by other Portal server roles in the default nodes segment, except for the Front End role.

   c For each role you want to remove from the list of current server roles, locate and select the server role in the **Current Roles** panel and then click the **Unselect** icon to move the user name into the **Available Roles** panel.

   d For each role you want to add to the list of current server roles, locate and select the server role in the **Available Roles** panel and then click the **Select** icon to move the role into the **Current Roles** panel.

5 Click **Save**.

Guidelines for Assigning Specific Portal Server Roles in the Default Segment

- You can assign the Front End role to as many Portal server machines in the default segment as you need, but you must have one Master Portal server machine in the default segment that is configured with the Front End role.
- As a point of reference, the remaining Portal server machines in the default segment that are running one or more portal roles can be further broken down and separately clustered. This may be necessary if your scalability requirements warrant setting up additional Portal server roles in the default segment to handle increased portal traffic.

Starting a Cluster of Portal Server Machines in the Default Segment

After configuring all of the Portal server machines in the default segment for your cluster, you can start all of the Portal server machines from one location. Be sure to review "Considerations When Starting a Portal Server in a Clustered Environment" on page 288 below before you start up a Portal server.

To start a Portal server cluster

1. On the file system of your Master Portal server machine, browse to the following directory:

   `/webMethods_install_dir/Portal/bin`

2. Run the portal.bat or portal.sh script, appending it with the server name, as shown in the example below:

   ```
   > portal -n server_name run
   ```

   where *server_name* corresponds to the server name for each Portal server machine in the default cluster. This should be done sequentially for each Portal server machine in the default segment starting with the Master Portal server.

Considerations When Starting a Portal Server in a Clustered Environment

Review the following considerations when you start a Portal server:

- You need to start the Master Portal server first for the cluster to function properly.
- Currently there is a requirement that you mount a network drive and make webMethods Portal software files accessible to all nodes in the cluster by sharing out the files to all Portal server machines in the default segment in the cluster. The entire cluster must be running from a set of shared files that are accessible by all machines in the cluster.

For example, on a Windows system:

a Share /webMethods6/Portal as portal on the portal master machine.

b Give users full rights to access portal share.

c Map `P:` drive to `\\`*portalmachine*`\portal` on the portal master machine.

d Open the Browser, and login into webMethods Portal. Configure the cluster using the Cluster Administration Portlet by adding all Portal server machines in the default segment.

e Map `P:` drive to `\\`*portalmachine*`\portal` on each configured Portal server machine in the default segment.

f From the portal bin directory (*`/webMethods_install_dir/`*`P`ortal/bin) run the following command on each Portal server machine in the default segment:

```
> portal -n server_name run
```

Be sure that you restart each Portal server machine in the default segment after you make changes to the cluster.

- All of the configuration data for each Portal server node and role is stored in the cluster.xml file. It is possible to edit the data for your cluster directly in the cluster.xml file, provided you know the proper data structures and values for the properties of your cluster.
- Any changes to the cluster configuration will require each node to be restarted.

webMethods

APPENDIX A

Integrating webMethods Portal with External Web Servers

Integration with Web Servers

webMethods Portal can integrate with the leading Web servers, such as Microsoft Internet Information Server or Apache HTTP Server. The primary mechanism for integrating webMethods Portal with a third party Web server in a distributed deployment scenario requires the use of a small plug-in that is installed and configured on the Web server. This plug-in forwards HTTP requests from the Web server to the Portal server using the specialized open protocol AJP13.

webMethods Portal provides an integrated servlet engine with Jetty, which is a built-in Web server that supports both HTTP and HTTPS. As such, having a separate Web server tier is *not* a hard requirement.

There are several reasons for configuring webMethods Portal with an external Web server (or cluster of Web servers). The most notable reason is to adhere to corporate IT policies and procedures. webMethods Portal supports a flexible deployment model that allows an external Web server (or cluster of Web servers) to handle all portal-specific HTTP requests that can be separately load balanced.

Integrating an external Web server to handle portal-based HTTP requests requires configuring a Web server plug-in on the external Web server machine(s). The Web server plug-in leverages code from the Jakarta Web server project which is used extensively across many production-quality Web server products.

Configuring webMethods Portal with IIS 5.0

Windows 2000 supports Internet Information Server 5.0.

Configuring webMethods Portal with IIS 5.0

Note: The following configuration is one of many distributed deployment scenarios. To address your specific requirements, please contact webMethods Customer Care for detailed distributed deployment information and guidelines.

To configure webMethods Portal with Internet Information Server (IIS) 5.0

1 After installing webMethods Portal, the components required to configure webMethods Portal to leverage an external Web server connection are located in the following directory on your Portal server machine:

```
/webMethods_install_dir/Portal/bin/ajp-connectors/iis
```

2 If you are configuring webMethods Portal with an IIS Web server running on a separate machine, do the following:

   a On the computer where the Web server resides, create a directory for the plug-in files. For example: `c:/ajp`.

   b Copy all of the files from the Portal server ajp-connectors directory for IIS to the new directory you just created.

      The following files should be copied:

      - isapi_redirect.dll - this file contains the connector code for the plug-in
      - isapi_redirect.properties - configuration file
      - uriworkermap.properties - configuration file
      - workers.properties - configuration file
      - readme.txt - basic setup instructions

3 Modify the configuration files as follows:

   a Isapi_redirect.properties—open this file in a text editor and change the log_level setting from “debug” to “error”.

Note: The debug option should only be used for troubleshooting due to its significant performance impact.

      Make sure the following entries in the isapi_redirect.properties file use fully-qualified paths to the referenced files:

```
log_file=fullpath\iis_redirect.log
worker_file=fullpath\workers.properties
worker_mount_file=fullpath\uriworkermap.properties
```

      Save the file when you are finished editing it.

Note: Do *not* use paths with spaces, such as `c:/program files`. Instead, use `c:\PROGRA~1`.

   b workers.properties—if the Web server is running on a different computer than webMethods Portal, open this file in a text editor and set the worker.portal.host setting to be the hostname or IP address of the actual server the portal is running on.

Note: The default value `localhost` will only work if the Portal server and Web server are on same machine.

c Register the ISAPI Filter - From the Control Panel as follows:

1 Select **Administrative Tools** and **Internet Services Manager**.

2 Right-click **Default Web Site** for your computer and click **Properties**.

3 In the ISAPI Filters tab add an executable pointed at the isapi_redirect.dll you copied from the Portal server to the Web server machine you are configuring:

```
C:\ajp\isapi_redirect.dll
```

4 Enter a Name for the ISAPI filter. Example: portal filter

d Register the extension mapping as follows:

1 Go to the Properties of the Default Web Site (same location as previous step). In the **Home Directory** Tab, click **Configuration**.

2 Add an extension mapping that points to the same executable as above with the extension: '.portal'.

3 Leave all the other default settings and click **OK**.

e Restart IIS.

Using IIS with NTLM

Windows NT LAN Manager (NTLM) was the default network authentication protocol in the Windows NT 4.0 operating system and was included in Windows 2000 for backward compatibility. Using NTLM with IIS requires that the integrated windows authentication be checked and that the client browser must use this setting: Automatic Login with current username and password

In the Windows environment, do the following:

1 In the Windows Control Panel, open Internet Options (or, in Internet Explorer, click **Tools ▸ Internet Options**).

2 Click the **Security** tab to bring it to the front.

3 Choose the **Local Intranet** or **Trusted Sites** Web content zone, and click **Custom Level**.

4 Scroll to **User Authentication** at the bottom and, under **Logon**, click the **Automatic Login with current username and password** option.

5 Click OK.

To change IIS 5.0, edit properties of the default Web server or corresponding portal Web server on the Windows 2000 server.

1 Select **Administrative Tools** and **Internet Services Manager**.

2 Click **Directory Security**.

3 Click **Edit**.

4 Select **Integrated Windows Authentication**.

5 Restart IIS.

6 Set a resource to use NTLM.

Note: If you are developing against a portal installation that uses IIS and integrated windows authentication, it may be wise to go directly to the Jetty HTTP listener port and bypass the IIS Web server port. Otherwise you may run into problems in deploying portlets because IIS will try to use the username and password of the machine you are developing and deploying from.

Configuring webMethods Portal with IIS 6.0

Windows 2003 supports Internet Information Server 6.0.

Note: The following configuration is one of many distributed deployment scenarios. To address your specific requirements, please contact webMethods Customer Care for detailed distributed deployment information and guidelines.

To configure webMethods Portal with Internet Information Server (IIS) 6.0

1 After installing webMethods Portal, the components required to configure webMethods Portal to leverage an external Web server connection are located in the following directory on your Portal server machine:

`/webMethods_install_dir/Portal/bin/ajp-connectors/iis6`

2 If you are configuring webMethods Portal with an IIS Web server running on a separate machine, do the following:

a On the computer where the Web server resides, create a directory for the plug-in files. For example: `c:/jk2`.

b Copy all of the files from the Portal server ajp-connector directory for IIS6 to the new directory you just created.

The following files should be copied:

- isapi_redirector2.dll - this file contains the connector code for the plug-in
- isapi_redirector2.properties - configuration file
- workers2.properties - configuration file

3 Modify the isapi_redirector2.properties configuration file as follows:

```
authComplete=0
extensionUri=/jakarta/isapi_redirector2.dll
log_Level=error
serverRoot=C:\JK2
threadPool=20
workersFile=C:\JK2\workers2.properties
```

4 Modify the workers2.properties configuration file to reflect the machine on which IIS 6.0 is running. In the sample below, modifications for the computer named sauron are indicated in bold:

```
[shm]
# info=Scoreboard. Required for reconfiguration and status with
# multiprocess servers.
file=c:\JK2\jk2.shm
size=1048576



# Example socket channel, override port and host.
 [channel.socket:sauron:8009]
port=8009
host=15.0.0.4


# define the worker
[ajp13:sauron:8009]
channel=channel.socket:sauron:8009


[status:]
info=Status worker, displays runtime information

#----
[uri:/jkstatus/*]
info=The Tomcat /jkstatus handler
# group=status:


[uri:/*]
worker=ajp13:sauron:8009
debug=10

[uri:/]
worker=ajp13:sauron:8009
debug=10
```

```
[logger]
level=ERROR


[logger.file:0]
level=DEBUG
file=c:\JK2\jk.log
debug=10
```

5 Configure IIS 6.0 to run in IIS 5.0 isolation mode by doing the following:

   a Select **Administrative Tools** and **Internet Services Manager**.

   b Right-click **Web Sites** for your computer and click **Properties**.

   c In the **Isolation mode** panel of the **Service** tab, select **Run WWW service in IIS 5.0 isolation mode** and click **OK**.

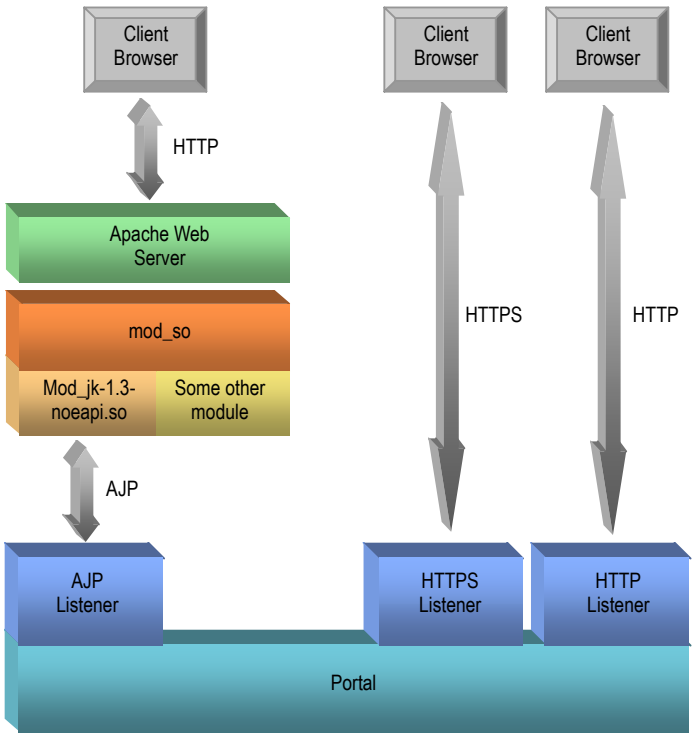
   d Restart IIS.

Configuring webMethods Portal with Apache

webMethods Portal supports the Apache Web Server, from the Apache Software Foundation, on UNIX platforms.

webMethods Portal leverages the Apache JServ Protocol (AJP) for integration and communication with separate Web servers such as Apache. To facilitate this communication an AJP connector is installed into the Apache Web server. The connector intercepts and forwards requests based on its configuration to the Portal server. Portal is configured to have an AJP listener either instead of or in addition to the default HTTP listener. The AJP listener allows Portal to receive and respond to browser requests forwarded from the Apache Web server by means of the AJP tunnel. You can have all or none of the Portal listeners configured; AJP is just one of several Portal options.

To use either of the AJP modules for Apache, you need to configure Apache with mod_so support to allow for the AJP connectors to load. The mod_so utility module loads executable code and modules into the server at start-up time. See your Apache documentation for information on how to do this configuration. If you have SSL configured for your site, use the mod_jk.so module; if you do not have SSL configured, use the mod_jk-1.3-noepi.so module. The following procedure assumes that you do not have SSL configured.



Prerequisites to Configuring Apache

Before you can configure Portal to use the Apache Web server, you need to meet the following requirements:

1 Install Portal and configure it to use the internal Jetty Web server, as described in the *webMethods Installation Guide*.

A simple way to validate this is to log in to the Portal server as PortalAdmin and browse around.

2 Install the Apache Web server and verify that it is responding correctly to its default Web pages.

A simple way to validate this is to browse to the Apache Web server and view the default Apache page.

Locating the Apache Files

After you have installed Portal on a UNIX platform, you will find the Apache components in the following directory on your Portal server machine:

/*webMethods_install_dir*/Portal/bin/ajp-connectors/apache

The following files appear in this directory:

File	Description
http.conf	Example Apache configuration parameters
workers.properties	Example AJP configuration file
mod_jk-1.3-noeapi.so	Binary library file without SSL
mod_jk.so	Binary library file requiring SSL
readme	Information on configuring Portal to communicate with an Apache Web server on UNIX

Configuring the Apache Web Server

If you have met the prerequisites in "Prerequisites to Configuring Apache" on page 298 and found the Apache files as described in "Locating the Apache Files" on page 298, you can configure Portal to use the Apache Web server on a UNIX system. The following procedure provides general guidelines and assumes the implementation of a standard Apache configuration; the requirements of your specific situation may vary.

To configure webMethods Portal with Apache Web server on a UNIX system

1 Copy the mod_jk-1.3-noeapi.so binary file from the location described in "Locating the Apache Files" on page 298 to the Apache /libexec directory.

2 Copy the example workers.properties to the Apache /conf directory.

Note: In the following step, do not copy the http.conf file, as you do not want to overwrite the file that already exists in the Apache /conf file. Rather, use the http.conf file in the Portal directory structure as an example of the correct location for each entry.

3 Edit the http.conf file in the Apache / conf directory to add the following entries.

Add these lines to http.conf

```
LoadModule jk_module libexec/mod_jk-1.3-noeapi.so
JkWorkersFile $APACHE_HOME/conf/workers.properties
JkLogFile $APACHE_HOME/logs/mod_jk.log
JkLogLevel info
JkMount /portal
JkMount /* portal
```

If you have a more complex Apache distribution than just the defaults with shared modules enabled, as shown here, you may need to adjust this configuration in more detail as per your site needs. This example assumes that only the basic components for an Apache Web server are installed. Both Portal and Apache are VERY flexible, this is indented to be only the basics to get this integration to function.

4 Edit the settings in the workers.properties file to ensure that the host entry is correct and has the same port number you intend to use when configuring the Portal AJP13 listener configuration in "Configuring the Portal Server" on page 300.

The following example shows an entry for the host my_host:

```
# Define 1 real worker using ajp13
worker.list=portal

# Set properties for portal (ajp13)
worker.portal.type=ajp13
worker.portal.host=my_host
worker.portal.port=8009
worker.portal.lbfactor=50
worker.portal.cachesize=10
worker.portal.cache_timeout=600
worker.portal.socket_keepalive=1
worker.portal.socket_timeout=300
```

5 Restart the Apache Web server.

Configuring the Portal Server

To configure the Portal server to use the Apache Web server, use the following procedure. The steps refer to sections in Chapter 2, "Using the Portal Server Configurator" which contains more complete information.

To configure the Portal server to use the Apache Web server

1 If you have not already done so, make sure the Apache Web server is running.

2 Start the webMethods Portal Server Configurator as described in "Starting the Configurator" on page 31.

3 In the Configurator window, choose the **Edit Portal Server** option and click **Start Wizard**.

4 In the **Web server type** list on the General tab, choose **apache**.

The **Apache** tab is added to the Configurator.

5 Click the **Apache** tab to bring it to the front.

6 On the **Apache** tab, make sure the host and port number for the Apache Web server are correct, as described in "The Apache Tab" on page 42.

7 Click the **Portal** tab to bring it to the front.

8 In the **Portal** tab, make sure the Jetty AJP13 Listener is enabled and uses the same port number as assigned in the workers.properties file, as described in "Configuring the Apache Web Server" on page 299.

9 Clear the Jetty HTTP Listener or make sure the port number does not conflict with the one used by the Apache Web server.

The HTTP Listener and the Apache Web server cannot, for example, both use port number 8080.

10 Click **Finish**.

11 Restart the Portal server.

Configuring Apache with a Portal Server in a Cluster

If a Portal server is part of a cluster, you need to take some additional steps to configure it for Apache Web server support.

To configure Apache for a Portal server that is part of a cluster

1 If you have not already done so, configure the Portal server for Apache, as described in "Configuring the Portal Server" on page 300.

2 Locate the cluster.xml file for the cluster.

See Chapter 15, "Portal Clustering" for information about using Portal servers in a cluster.

3 In a text editor, edit the cluster.xml file to add a port number to the AJP13 properties for the Portal server and ensure that the remoteservers name is an exact match for the host name in the workers.properties file.

The following code fragment shows a portion of the cluster.xml file. The AJP13 listener port number should be the same as the one assigned in the workers.properties file described in "Configuring the Apache Web Server" on page 299:

```
<Properties
      host="my_host" maxthreads="20" minthreads="5"
      name="ajp13" port="8009"
      remoteservers="my_host,111.1.1.1"/>
```

The relationship between the two files is shown in "Relationship between workers.properties and cluster.xml files" below:

Relationship between workers.properties and cluster.xml files

workers.properties file

```
# Define 1 real worker using ajp13
worker.list=portal

# Set properties for portal (ajp13)
worker.portal.type=ajp13
worker.portal.host=my_host
worker.portal.port=8009
worker.portal.lbfactor=50
worker.portal.cachesize=10
worker.portal.cache_timeout=600
worker.portal.socket_keepalive=1
worker.portal.socket_timeout=300
```

cluster.xml file

```
<Component
  class="com.webmethods.portal.system.cluster.impl.Server"
  enabled="true" name="master">
  <Properties
    host="my_host" maxthreads="20" minthreads="5"
    name="http" port="8080"/>
  <Properties
    host="my_host" maxthreads="20" minthreads="5"
    name="https" port="0"/>
  <Properties
    host="my_host" maxthreads="20" minthreads="5"
    name="ajp13" port="8009"
    remoteservers="my_host,111.1.1.1"/>
  <Properties
    host="my_host" name="rmi"
  port="1097"/>
</Component>
```

4 Restart the Portal server.

webMethods

APPENDIX B

Running a Portal Server from the Command Line

Command Syntax for the Portal Server

There are times when it is useful to start and stop the Portal server from the command line. Starting the server this way, for example, allows you to use debug mode so you can record or display server activity. There are several commands you can use to control operation of the Portal server, as described in the following procedure.

To control the Portal server from the command line

1 At a command line prompt, type the following command to move to the Portal server's bin directory:

```
cd webMethods_install_dir/Portal/bin
```

2 Type the following command:

For Windows: `portal.bat -switch -switch ... command`

For UNIX: `portal.sh -switch -switch ... command`

where *switch* is any of the following:

Switch	Description
-s *servername*	The name of the Portal server instance. Not required if you are controlling the default Portal server. You can find the Portal server instances on a machine by looking here: *webMethods_install_dir*/Portal/server
-n *nodename*	In a clustered environment, the nodename assigned to the Portal server instance. Not required if the server is running standalone, or if it is the master node of a cluster. For information on clusters, see Chapter 15, "Portal Clustering".
-d[ebug]	Starts the Portal server in debug mode. DEBUG statements appear in the console window and a Java debug listener is open on port 5000.

and *command* is any of the following:

Command	Description
run	Starts the Portal server in the same console window.
start	Starts the Portal server in a new console window.
stop	Stops a running Portal server, sending a shutdown command by means of RMI.
restart	Stops a running Portal server and then starts it again.

Command	Description
ping	If the Portal server is stopped, indicates this fact. If the server is running, returns information, including what ports the server is using.
help	Prints command syntax in the console window.
The following commands are for Windows only:	
installservice	Registers the Portal server as a Windows service.
uninstallservice	Unregisters the Portal server as a Windows service.
startservice	Starts a Portal server that is registered as a Windows service.
stopservice	Stops a Portal server that is registered as a Windows service.
restartservice	Stops a Portal server that is registered as a Windows service and then starts it again.

Simple Start and Stop Commands

If you want to start or stop a Portal server, without having to use the servername or nodename as part of the command syntax, there are commands associated with each Portal server instance on a machine. This feature is not necessary for a standalone Portal server, but may be useful if you have multiple servers on a machine.

To start or stop a specific Portal server

1 At a command line prompt, type the following command to move to the Portal server's home directory:

```
cd webMethods_install_dir/Portal/server/server_name/bin
```

where *server_name* is the name of the Portal server.

2 Type one the following commands:

Purpose	Operating system	Command
Start the Portal server in the same console window	Windows	`run.bat`
	UNIX	`run.sh`
Start the Portal server in a new console window	Windows	`startup.bat`
	UNIX	`startup.sh`

Purpose	Operating system	Command
Stop the Portal server	Windows	`shutdown.bat`
	UNIX	`shutdown.sh`

Working with Portal Server Databases

The Portal server uses an external database server to store portal information. You can use the following commands to manage a Microsoft SQL Server, Oracle, or DB2 database used as a portal database.

Important! Whenever you initialize a server instance for the first time or upgrade an existing server instance to a newer version or service pack, the server may need to create additional schema objects in the database. For this reason, you must ensure that the database user has privileges to create or alter schema objects. These privileges are not otherwise required for normal server operation and can be revoked for security or other reasons.

Creating a Database Using the Portal JDBC

You can use the dbcreate command to create a portal database.This command works only on the machine where webMethods Portal is installed; for commands you can use on a different machine, see "Creating a Database using Database Client Tools" on page 309. The actions you can perform with this command are the same as can be done using the webMethods Portal Server Configurator. For specific information about database configuration, see "The MSSQL Tab" on page 34, "The Oracle Tab" on page 36, or "DB2 Universal Database (Portal JDBC)" on page 309.

Microsoft SQL Server (Portal JDBC)

To create a Microsoft SQL Server database using Portal JDBC

1. At a command line prompt, type the following command to move to the Portal server's home directory:

   `cd` *`webMethods_install_dir`*`\Portal\bin\db\scripts\mssql`

2. Type the following command:

   `dbcreate.bat` *`parameters`*

where *parameters* are:

Parameter	Description
server:port	The Microsoft SQL Server host and port number.
database	The name of the portal database to be created or used.
dbauser	The name of the database administrator.
dbapwd	The password of the database administrator.
username	The name of the portal database user.
pwd	The password of the portal database user.
createdb	`y` Creates a new database and user. Gives the new user administrative rights to the database. Use of this parameter requires a database administrator account. `n` Creates a new portal schema. The database must be created before running this script and the portal database user must already exist.

Note for Database Administrators

When you create a portal database user not using the dbcreate command, grant the user the Public and DBowner roles for the database.

Example

The following command creates the `portaldb` database on the `sqlserver` server, creates the `portaluser` login with a password of `portalpassword`, and gives the user ownership rights for the `portaldb` database:

```
dbcreate sqlserver:1433 portaldb sa password portaluser portalpassword y
```

To create a new schema for an existing database (option 2 in the Configurator user interface) use the portal database user and password in place of the database administrator password and set the createdb parameter to `n`.

```
dbcreate sqlserver:1433 portaldb portaluser portalpassword portaluser
portalpassword n
```

Oracle (Portal JDBC)

To create an Oracle database using Portal JDBC

1 At a command line prompt, type the following command to move to the appropriate directory:

```
cd webMethods_install_dir/Portal/bin/db/scripts/oracle
```

2 Type the following command:

For Windows: `dbcreate.bat parameters`

For UNIX: `dbcreate.sh parameters`

where *parameters* are:

Parameter	Description
host:port	The Oracle Server host and port number
instance_name	The name of the Oracle instance to be created or used.
dbauser	The name of the database administrator.
dbapwd	The password of the database administrator.
username	The name of the portal database user.
pwd	The password of the portal database user.
tablespace	The tablespace to be used for portal schema objects.
createts	`y` Creates a new tablespace and new portal database user. Use this option for the purpose of creating tablespaces only. `n` Adds new portal schema objects to the *tablespace* tablespace, which already exists. The *username* user must also already exist.

Note for Database Administrators

When you create a portal database user not using the dbcreate command, grant the user GLOBAL QUERY REWRITE permission, which is required to create a portal schema.

Example

The following command creates the `portal` tablespace in the `portal_db` Oracle instance on the `oraserver` server, creates the `portaluser` login with a password of `portalpassword`:

```
dbcreate oraserver:1521 portal_db sa password portaluser portalpassword
portal y
```

To create a new schema for an existing database (option 2 in the Configurator user interface) use the portal database user and password in place of the database administrator password and set the createts parameter to `n`.

```
dbcreate oraserver:1521 portal_db portaluser portalpassword portaluser
portalpassword portal n
```

DB2 Universal Database (Portal JDBC)

To create a DB2 database using Portal JDBC

1 At a command line prompt, type the following command to move to the Portal server's home directory:

```
cd webMethods_install_dir\Portal\bin\db\scripts\db2
```

2 Type the following command:

```
dbcreate.bat parameters
```

where *parameters* are:

Parameter	Description
server:port	The DB2 host and port number. If you omit the port number, the default is 50000.
database	The name of the portal database to be created or used.
username	The name of the portal database user.
pwd	The password of the portal database user.

Note for Database Administrators

Before a user can configure a Portal database on DB2, you must create a user name within a new or existing database and, if needed, create a user temporary tablespace that is required for temporary tables used by Portal.

Example

The following command creates the `portaldb` database on the `db2server` server, creates the `portaluser` login with a password of `portalpassword`, and gives the user ownership rights for the `portaldb` database:

```
dbcreate db2server:50000 portaldb portaluser portalpassword
```

Creating a Database using Database Client Tools

If you need to create a database from a machine on which webMethods Portal is not installed, you can use the dbcreate_osql or dbcreate_sqlplus command. Each command requires that the appropriate utility be installed on the machine where you use the command:

Database	Command	This utility needs to exist on the target machine
Microsoft SQL Server	dbcreate_osql	OSQL
Oracle	dbcreate_sqlplus	SQL*Plus

Microsoft SQL Server (Database Client Tools)

To create a Microsoft SQL Server database using database client tools

1 On the machine where webMethods Portal is installed, locate the \mssql folder:

`*webMethods_install_dir*\Portal\bin\db\scripts\mssql`

2 Copy the \mssql folder to the machine from which you intend to run the command.

The machine must use a Windows operating system and must have OSSQL utility installed.

3 Run the command using the same parameters described in "Microsoft SQL Server (Portal JDBC)" on page 306:

`dbcreate_osql.bat *parameters*`

Note: Using the OSQL utility, it can take several minutes to create the portal schema.

Oracle (Database Client Tools)

To create an Oracle database using database client tools

1 On the machine where webMethods Portal is installed, locate the /oracle folder:

`*webMethods_install_dir*/Portal/bin/db/scripts/oracle`

2 Copy the /oracle folder to the machine from which you intend to run the command.

The machine must have an operating system compatible with the type of file you are copying (.bat or .sh) and must have the SQL*Plus utility installed.

3 Type the following command:

For Windows: `dbcreate_sqlplus.bat *parameters*`

For UNIX: `dbcreate_sqlplus.sh *parameters*`

where *parameters* are:

Parameter	Description
tns_name	The Oracle TNS (Transparent Network Substrate) name used to connect to the Oracle database.
dbauser	The name of the database administrator.
dbapwd	The password of the database administrator.
username	The name of the portal database user.
pwd	The password of the portal database user.
tablespace	The tablespace to be used for portal schema objects.
createts	`y` Creates a new tablespace and new portal database user. Use this option for the purpose of creating tablespaces only. `n` Adds new portal schema objects to the *tablespace* tablespace, which already exists. The *username* user must also already exist.

Example

The following command uses the `portal` TNS name to create the `portal` tablespace, creates the `portaluser` login with a password of `portalpassword`:

```
dbcreate portal sa password portaluser portalpassword portal y
```

To create a new schema for an existing database (option 2 in the Configurator user interface) use the portal database user and password in place of the database administrator password and set the createts parameter to `n`.

```
dbcreate portal portaluser portalpassword portaluser portalpassword portal
n
```

Dropping a Database Using the Portal JDBC

You can use the dbdrop command to drop a portal database, in which a database user is deleted along with all user objects, such as tables, procedures, packages, and so forth. This command works only on the machine where webMethods Portal is installed; for commands you can use on a different machine, see "Dropping a Database using Database Client Tools" on page 314.

Microsoft SQL Server (Portal JDBC)

To drop a Microsoft SQL Server database using Portal JDBC

1 At a command line prompt, type the following command to move to the appropriate directory:

```
cd webMethods_install_dir\Portal\bin\db\scripts\mssql\
```

2 Type the following command

```
dbdrop.bat parameters
```

where *parameters* are:

Parameter	Description
host:port	The Microsoft SQL Server host and port number.
database	The name of the portal database to be dropped.
dbauser	The name of the database administrator.
dbapwd	The password of the database administrator.
username	The name of the portal database user to be dropped.

Example

The following command drops the `portaldb` database and the `portaluser` user on the `sqlserver` server:

```
dbdrop sqlserver:1433 portaldb sa password portaluser
```

Oracle (Portal JDBC)

To drop an Oracle database using Portal JDBC

1 At a command line prompt, type the following command to move to the appropriate directory:

```
cd webMethods_install_dir/Portal/bin/db/scripts/oracle
```

2 Type the following command:

For Windows: `dbdrop.bat parameters`

For UNIX: `dbdrop.sh parameters`

where *parameters* are:

Parameter	Description
host:port	The Oracle Server host and port number
instance_name	The name of the Oracle instance to be dropped.
dbauser	The name of the database administrator.
dbapwd	The password of the database administrator.
username	The name of the portal database user.

Example

The following command drops the `portal_db` database and the `portaluser` user on the `oraserver` server:

```
dbcreate oraserver:1521 portal_db sa password portaluser
```

DB2 Universal Database (Portal JDBC)

To drop a DB2 database using Portal JDBC

1 At a command line prompt, type the following command to move to the appropriate directory:

```
cd webMethods_install_dir/Portal/bin/db/scripts/db2
```

2 Type the following command:

For Windows: `dbdrop.bat parameters`

For UNIX: `dbdrop.sh parameters`

where *parameters* are:

Parameter	Description
server:port	The DB2 host and port number. If you omit the port number, the default is 50000.
database	The name of the portal database to be dropped.
username	The name of the portal database user.
pwd	The password of the portal database user.

Dropping a Database using Database Client Tools

If you need to drop a database from a machine on which webMethods Portal is not installed, you can use the dbdrop_osql or dbdrop_sqlplus command. Each command requires that the appropriate utility be installed on the machine where you use the command:

Database	Command	This utility needs to exist on the target machine
Microsoft SQL Server	dbdrop_osql	OSQL
Oracle	dbdrop_sqlplus	SQL*Plus

Microsoft SQL Server (Database Client Tools)

To drop a Microsoft SQL Server database using database client tools

1. If you have already copied the /mssql folder to the target machine, go directly to step 4.
2. On the machine where webMethods Portal is installed, locate the \mssql folder:

   webMethods_install_dir\Portal\bin\db\scripts\mssql
3. Copy the \mssql folder to the machine from which you intend to run the command.

   The machine must use a Windows operating system and must have OSSQL utility installed.
4. Run the command using the same parameters described in "Microsoft SQL Server (Portal JDBC)" on page 312:

   dbdrop_osql.bat *parameters*

Oracle (Database Client Tools)

To drop an Oracle database using database client tools

1. If you have already copied the /oracle directory to the target machine, go directly to step 4.
2. On the machine where webMethods Portal is installed, locate the /oracle folder:

   webMethods_install_dir/Portal/bin/db/scripts/oracle
3. Copy the /oracle directory to the machine from which you intend to run the command.

   The machine must have an operating system compatible with the type of file you are copying (.bat or .sh) and must have database client tools installed.

4 Run the command using the same parameters described in "Oracle (Portal JDBC)" on page 312:

For Windows: `dbdrop_sqlplus.bat` *`parameters`*

For UNIX: `dbdrop_sqlplus.sh` *`parameters`*

Glossary

ACE
Access Control Entry. A simple structure containing an element called a Principal (user, group, or role) and an element called a Right Set (a set of rights). ACEs are used in Access Control Lists (see ACL next on this page).

ACL
Access Control List. A list of ACEs. An ACL provides the Portal server with a list of access rights a Principal has to portal resources.

ADAM
Active Directory Application Mode. A standalone directory server offered by Microsoft. ADAM is an LDAP implementation that can be installed and uninstalled without affecting the Active Directory structure of a network.

ADSI
Active Directory Service Interfaces. A set of interfaces for querying and manipulating objects in Microsoft Active Directory, providing an LDAP view of the objects. Active Directory is tightly coupled with the Windows operating system.

alias
See portal alias.

authentication
An assurance that a party to some computerized transaction is not an impostor. Authentication typically involves using a password, certificate, PIN, or other information that can be used to validate identity. See SAML and NTLM.

authorization
The process of determining, by evaluating applicable access control information, whether a party is allowed to have the specified types of access to a particular resource. Usually, authorization is in the context of authentication.

bizpolicy
Business policy. Protocol-independent business logic that leverages mechanics (method classes) and metadata services to perform its function. Business policies use commands to invoke methods, but do not perform actions on objects directly.

DBO
Dynamic Business Object. A portal object (files, links, folders, forms, folders, and portal pages) that has been extended with custom attributes (metadata) and behaviors (business logic).

directory service
A service that provides a mechanism for delivering information, such as names, e-mail addresses, and so forth, about a collection of entries (users) in a directory.

DN
Distinguished name. A fully-qualified unique name, used to identify an object in a directory, that specifies the complete path to the object through the hierarchy of directory containers.

folder
A part of the hierarchical framework for organizing and browsing portal content. While still controlling access based on user permissions, folders help ensure that portal resources are easily accessed and browsed using a familiar, explorer-like interface.

GET
In the HTTP protocol, a method of passing data to a target computer as a string appended to the URL after a question mark. Compare with POST.

group
A static collection of users or other groups. Membership in a group is limited to a single directory service.

JSR 168
Java Specification Request 168. This specification enables interoperability among portlets and portals, defining a set of APIs for portlets and addressing standardization for preferences, user information, portlet requests and responses, deployment packaging, and security.

LDAP
Lightweight Directory Access Protocol. An internet protocol that allows client programs to query LDAP directory servers about entries using their attributes.

LDIF
Lightweight Directory Interchange Format. An ASCII file format used to exchange data and enable the synchronization of that data between Lightweight Directory Access Protocol (LDAP) servers called Directory System Agents (DSAs). LDAP is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network. An LDAP directory can be distributed among many servers. LDIF is used to synchronize each LDAP directory.

login page
The page on which a user logs into a Portal server. You can use rules to direct individual users to different login pages. See also, start page.

mechanics
A helper method class that performs operations on publicly accessible services and the objects returned by services. In addition, mechanics can also provide some logic, such as checking for name violations.

metadata service
A service that controls the lifecycle and storage of data related to the Portal server. The metadata service provides an object model for content, folders, relationships, Portal Pages, Portlet types, Portlet instances, users, groups, and all other data objects that exist in the Portal. The metadata service stores these persistent objects in a central database.

My webMethods Server
The core set of components and services required to host the Web interface for webMethods components, including webMethods Portal.

notification
A message generated when a certain event occurs on a portal resource (such as adding content to a portal page) and sent to a user who has subscribed to the event. Notifications are delivered to the subscriber by e-mail or notification inside the portal in the user's personal Subscription Inbox page. See also, subscription.

NTLM
Windows NT LAN Manager. The default for network authentication in the Windows NT 4.0 operating system. NTLM uses a challenge-response mechanism for authentication, in which clients are able to prove their identities without sending a password to the server.

PCA layout
A portlet layout that is a JSP and the metadata associated with it. The layout conforms to the Portlet Controller Architecture described in portlet controller.

PCA method
A Java method defined in the portlet bean class and the metadata associated with it. The method conforms to the Portlet Controller Architecture described in portlet controller.

portal
A browser-based presentation platform that provides customized access to and interaction with relevant information, applications, and business processes, by select targeted audiences.

portal alias
A URL alias for identifying a portal object, such as a portal page. Internal references to portal objects are non-intuitive, so using an alias makes it easier to create a URL to an object.

portal page

A container for portal resources, providing a convenient access point to portlets, items, and links. Portal pages are Web pages dedicated to organizing and presenting portlets. Each portal page resembles a composite application, and is generally dedicated to accomplishing specific business processes and related tasks.

portal verb
An operation such as publishing, deleting, updating, subscribing, and setting permissions, which is available through the Portal API.

portlet
A server-side, mini-application that resides on the Portal server or a piece of functionality that runs on the back end of the Portal server. A portlet may or may not have a user interface (UI). Architecturally, a portlet is made up of JSP files, XML files, Java classes, and other UI components. All of the UI components within webMethods Portal exist as portlets.

portlet controller
A framework for creating portlets with multiple pages and actions. A portlet controller consists of runtime, base portlet classes, declaration in the portlet descriptor, JSP tag library, and the Portlet Developer plug-in to the Eclipse IDE. The framework conforms to the Portlet Controller Architecture (PCA).

POST
A method of passing data to a target computer in the body of an HTTP request. Compare with GET. Forms passed to the Portal server use this method.

Principal
A user, group, or role. In an Access Control Entry, a Principal has a set of rights associated with it. See ACE.

publish
The act of populating the portal with a variety of resources, including documents, folders, portal pages, portlets, and other structured and unstructured content. The privilege to publish is usually reserved for authorized users, such as portal administrators.

renderer
A mechanism that lays out a view of the portal object as an HTML page and controls a webMethods Portal user's view of portal objects. These objects can be folders, links, content, portal pages, and so forth.

role
A collection of users, groups, or other roles. Membership within a role can be dynamic, and can span multiple directory services.

SAML
Security Assertion Markup Language. An XML-based framework for exchanging security information. Using SAML, an entity on a target computer grants access based on an assertion from the source computer that the user is logged into the source computer.

Security Realm
Collections of portal resources that share the same ACL. The use of Security Realms makes it possible to manage permissions on large numbers of portal resources.

shell
An installable component that generates the webMethods Portal header, footer, and portlet title bars. A shell provides the structure that frames the primary content. Common Web page design elements such as corporate banners, global navigation links, and search boxes, appear in a shell.

skin
An installable webMethods Portal component that defines the look and feel of the portal user interface. A skin modifies the images, fonts, colors, and other subtle stylable aspects of HTML content, but it does not modify the HTML content in any functional way.

start page
The page where a user is directed after logging into the Portal server. You use different start pages based on which login page was used, or you can use rules to direct individual users to different start pages. See also, login page.

system directory service
An internal directory service of webMethods Portal. The system directory service is suitable for getting started in using a Portal server, and for maintaining information about a moderate number of users.

subscription
A standing request to be notified when a certain event occurs on a portal resource. For example, you might want to be notified each time new content is added to a portal page. To subscribe, a user must be authorized to view the resource. See also, notification.

wiki
A *wiki* is a Web interface for a storage organization. A wiki makes it possible to write documents collectively, giving multiple individuals the ability create, edit, and reorganize content.

WSDL
Web Services Description Language. Also, an XML document that describes a Web service, specifying the location of the service and the operations the service exposes.

WSRP
Web Services for Remote Portlets. A definition of how to plug remote Web services into the pages of online portals and other user-facing applications. This standard describes how to embed a Web service from a third party into a section of a portlet, which can then display interactive content and services that are dynamically updated from the provider's own servers.

Index

D

E

F

G

H

I

L

M

N

O

P

R

T

U

V

W