

Peregrine

BI Portal 5.1

Administration Guide

For Windows, AIX, and Solaris

Copyright © 2004 Peregrine Systems, Inc. or its subsidiaries. All rights reserved.

© Copyright 2004 Peregrine Systems, Inc.

PLEASE READ THE FOLLOWING MESSAGE CAREFULLY BEFORE INSTALLING AND USING THIS PRODUCT. THIS PRODUCT IS COPYRIGHTED PROPRIETARY MATERIAL OF PEREGRINE SYSTEMS, INC. ("PEREGRINE"). YOU ACKNOWLEDGE AND AGREE THAT YOUR USE OF THIS PRODUCT IS SUBJECT TO THE SOFTWARE LICENSE AGREEMENT BETWEEN YOU AND PEREGRINE. BY INSTALLING OR USING THIS PRODUCT, YOU INDICATE ACCEPTANCE OF AND AGREE TO BE BOUND BY THE TERMS AND CONDITIONS OF THE SOFTWARE LICENSE AGREEMENT BETWEEN YOU AND PEREGRINE. ANY INSTALLATION, USE, REPRODUCTION OR MODIFICATION OF THIS PRODUCT IN VIOLATION OF THE TERMS OF THE SOFTWARE LICENSE AGREEMENT BETWEEN YOU AND PEREGRINE IS EXPRESSLY PROHIBITED.

Information contained in this document is proprietary to Peregrine Systems, Incorporated, and may be used or disclosed only with written permission from Peregrine Systems, Inc. This book, or any part thereof, may not be reproduced without the prior written permission of Peregrine Systems, Inc. This document refers to numerous products by their trade names. In most, if not all, cases these designations are claimed as Trademarks or Registered Trademarks by their respective companies.

Peregrine Systems, AssetCenter, AssetCenter Web, BI Portal, Dashboard, Get-It, Get-Services, Get-Resources, Peregrine Mobile, and ServiceCenter are registered trademarks of Peregrine Systems, Inc. or its subsidiaries.

Microsoft, Windows, Windows 2000, SQL Server, and names of other Microsoft products referenced herein are trademarks or registered trademarks of Microsoft Corporation. Oracle is a registered trademark of Oracle Corporation. DB2 is a registered trademark of International Business Machines Corp. IBM and Tivoli are trademarks of International Business Machines Corporation in the United States, other countries, or both. This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>). This product also contains software developed by: Sun Microsystems, Inc., Netscape Communications Corporation, and InstallShield Software Corporation. This product includes code licensed from RSA Data Security.

This product includes software developed by Business Objects, S.A. Portions, copyright 1995 - 2004, Business Objects, S.A. All rights reserved.

The information in this document is subject to change without notice and does not represent a commitment on the part of Peregrine Systems, Inc. Contact Peregrine Systems, Inc., Customer Support to verify the date of the latest version of this document. The names of companies and individuals used in the sample database and in examples in the manuals are fictitious and are intended to illustrate the use of the software. Any resemblance to actual companies or individuals, whether past or present, is purely coincidental. If you need technical support for this product, or would like to request documentation for a product for which you are licensed, contact Peregrine Systems, Inc. Customer Support by email at support@peregrine.com. If you have comments or suggestions about this documentation, contact Peregrine Systems, Inc. Technical Publications by email at doc_comments@peregrine.com. This edition of the document applies to version 5.1 of the licensed program.

Peregrine Systems, Inc.
Worldwide Corporate Headquarters
3611 Valley Centre Drive San Diego, CA 92130
Tel 800.638.5231 or 858.481.5000
Fax 858.481.1751
www.peregrine.com



Contents

	About this Guide	7
	Using this Guide	8
	Related Documentation	8
	Documentation Conventions	9
	Contacting Peregrine Systems	9
	Customer Support	9
	Documentation web site	10
	Education Services web site	10
Chapter 1	Peregrine OAA Architecture Overview	11
	Peregrine OAA Platform architecture	12
	OAA scalability	14
	Archway internal architecture	15
	Archway requests	16
	BI Portal architecture	19
Chapter 2	Customizing the Peregrine Portal	21
	Deploying the Classic theme variations	22
	Changing the default theme	23
	Changing the header graphic for all themes.	23
	Creating a custom theme	25
	Layers properties	29
	Changing framesets.	30

Chapter 3	Using the Peregrine Portal	33
	Logging in to the Peregrine Portal.	34
	Using the Activity menu.	35
	Personalizing the Peregrine Portal	36
	Adding components	36
	Changing the layout	38
	Changing themes	40
	Displaying form information	42
Chapter 4	Using the OAA Administration Module	43
	Accessing the Peregrine Portal Admin module	44
	Using the Control Panel.	46
	Viewing the Deployed Versions.	47
	Using the Settings page	48
	Setting parameters using the Admin module	48
	Logging.	50
	Logging format	51
	Log file rollover	54
	Viewing the Server Log	55
	Verifying Script Status	56
	Displaying Message Queues	56
	Showing Queue Status	57
	Importing and exporting personalizations	58
	Viewing adapter transactions.	58
	Using the IBM Websphere Portal	59
	Displaying form information.	59
	Displaying form details	61
	User self-registration	62
	Changing passwords	63
	Logging and monitoring user sessions	63
	Understanding the usage.log file	63
	BI Portal administration.	64
	Setting the PortalDB adapter.	65
	Using the BI Portal Administration page.	65
	BI tab	73

Chapter 5	Security	77
	Password encoding methods	78
	User registration	79
	Authenticating users	80
	Default security configuration	80
	Custom JAAS configuration	81
	JAAS LoginModule control flags	83
	JAAS configuration options	86
	Example: Defining an LDAP custom configuration	90
	Standard Sun Microsystems JAAS configuration	90
	Command line options	91
	Integrated Windows Authentication.	91
	Setting up Integrated Windows Authentication.	92
	Testing the settings.	100
	Integrating with single sign-on tools.	100
	Testing access to BI Portal from a single sign-on tool	102
	Authentication models	103
	ServiceCenter authentication components	103
	OAA contact and operator associations	103
	Regular operator authentication	104
	Algorithm for looking up contacts	104
	Contact creation	105
	Contact-based authentication	105
	Creating an alternate login page	114
	Creating a login Web page.	114
	Specifying an alternate authentication method	115
	BI Portal security overview.	116
	Security groups	117
	Out-of-box role-level security groups	117
	Out-of-box group-level security groups for ServiceCenter	117
	Data-level security groups.	118
Chapter 6	BI Portal Administrator Functions	121
	Overview	121
	Uploading	122
	Group management	123

	Capability words	127
	BI Capabilities.	129
	User management	130
	Document management.	131
	Synchronizing users	132
	Publishing sample documents	133
	Scheduling automatic data synchronization	135
	Restricting report data access.	138
Chapter 7	Troubleshooting	147
	Browser issues	147
	Navigation Issue	148
	Tomcat issues	148
	WebSphere Portal Server issues.	149
	BI Portal fails to start	149
	BO Administration settings on BI Portal Administration page fail verification	150
	“BI Initialization Failed” after server reset	154
	Reports do not return any data	154
	“BI Server Not Available” message	154
	Duplicate groups appear in BI Portal or the Business Objects Supervisor tool	155
Appendix A	BI Portal and ServiceCenter Synchronization	157
	Manually synchronize new BI Portal users with ServiceCenter database.	157
	Index.	159



About this Guide

This *BI Portal Administration Guide* provides information about administration of BI Portal. The guide includes extensive information about Peregrine OAA, the software platform on which BI Portal is based, and specific information about BI Portal.

Using this Guide

This guide includes the following chapters:

This chapter	Describes
Chapter 1	Describes the Peregrine Open Application Architecture.
Chapter 2	How to customize the Peregrine Portal.
Chapter 3	How to use the Peregrine Portal.
Chapter 4	How to use the OAA Administration module.
Chapter 5	Describes security options for the portal.
Chapter 6	How to use the BI Portal Administration function.
Chapter 7	Troubleshooting suggestions.

Prior to using this guide, you should read the following sections:

- *Related Documentation* on page 8
- *Documentation Conventions* on page 9
- *Contacting Peregrine Systems* on page 9

Related Documentation

In addition to this guide, the following documentation is available for the BI Portal product:

This manual...	Provides information on...
<i>BI Portal User Guide</i>	standard reports and describes how to create and work with both standard and custom reports.
<i>BI Portal Installation Guide</i>	Installing and configuring the application and database servers for BI Portal.

This manual...	Provides information on...
<i>BI Portal Release Notes</i>	Last-minute enhancements, known issues, and closed issues.
<i>WebIntelligence User's Guide</i>	Describes how to use WebIntelligence (a component of Business Objects) for building and running queries, reporting, and analysis.

Documentation Conventions

The following typographical conventions are used in this guide.

Text Formatting	Meaning
<i>italics</i>	Text that acts as a placeholder for information you will provide. Italics are also used for book titles and for emphasis.
sans serif font	Text that you type. Examples are filenames and URLs. This font is also used for samples of code and commands.
bold	Names of user interface elements. Examples are menu items and names (select Open from the File menu), button names (click Accept), and names of screens or dialogs (the Server Manager window).

Contacting Peregrine Systems

For help with this release, you can contact customer support, download documentation or schedule training.

Customer Support

For further information and assistance with Product Name Short in general, contact Peregrine Systems' Customer Support at the Peregrine CenterPoint web site.

To contact customer support:

- 1 In a browser, navigate to <http://support.peregrine.com>
- 2 Log in with your user name and password.
- 3 Follow the directions on the site to find the information you need.

The KnowledgeBase contains informational articles about all categories of Peregrine products. If the KnowledgeBase does not contain an article that addresses your concerns, you can search for information by product; search discussion forums; and search for product downloads.

Documentation web site

For a complete listing of current BI Portal documentation, see the Documentation pages of the Peregrine Customer Support web site.

To view the document listing:

- 1 In a browser, navigate to <http://support.peregrine.com>.
- 2 Log in with your login user name and password.
- 3 Click either **Documentation** or **Release Notes** at the top of the page.
- 4 Click the BI Portal link.
- 5 Click a product version link to display a list of documents that are available for that version of BI Portal.
- 6 Documents may be available in multiple languages. Click the Download button to download the PDF file in the language you prefer.

You can view PDF files using Acrobat Reader, which is available on the Customer Support Web site and through Adobe at <http://www.adobe.com>.

Important: Release Notes for this product are continually updated after each release of the product. Ensure that you have the most current version of the Release Notes.

Education Services web site

Peregrine Systems offers classroom training anywhere in the world, as well as “at your desk” training via the Internet. For a complete listing of Peregrine’s training courses, refer to the following web site:

<http://www.peregrine.com/education>

You can also call Peregrine Education Services at +1 858.794.5009.

1 Peregrine OAA Architecture Overview

CHAPTER

Because BI Portal is based on the Peregrine Open Application Architecture (OAA), this guide includes extensive information about the platform.

Peregrine Open Application Architecture (OAA) platform is a software platform that enables the hosting of a variety of Web applications over a corporate intranet. The platform is Java based, encompassing the latest in Java technology including Java servlets, JAAS login authentication, and JSP pages that enable Web pages to display data dynamically.

Peregrine OAA Platform is the underlying architecture for many Peregrine products., Peregrine OAA Platform provides a Web portal, Peregrine Portal, from which users can access their Web applications. The Peregrine Portal also provides access to the Admin module, from which all aspects of the Peregrine OAA Platform are monitored and maintained.

The base of Peregrine OAA Platform includes:

- Archway—a Java servlet that processes HTTP requests from a browser, sends the requests through an adapter to a back-end system, and returns XML data to be displayed in the browser.
- Core files—the Peregrine OAA Platform contains jsp and XML. The core consist mainly of low level Java utility classes used by the Portal Web applications built on the base OAA framework.
- Peregrine Portal—includes a login page and provides access to your Peregrine Web applications and to the Admin module for configuration of your application.

- Skins and style sheets—provide a choice for the appearance of the Web pages.

The Peregrine OAA Platform includes a number of optional components that are configured for use with Web applications as they are needed. These include:

Adapters—enables connection to the back-end system database. The adapter required by your Web application is deployed during the installation.

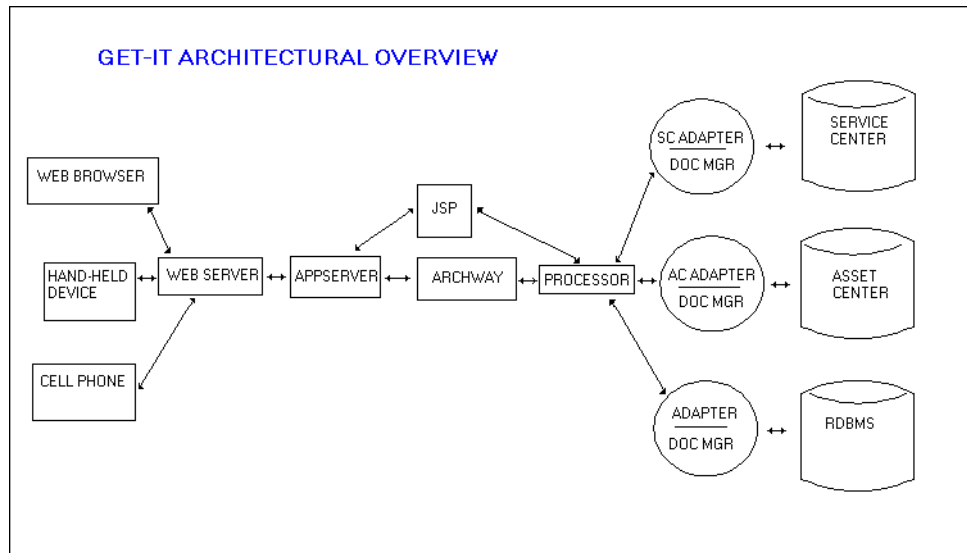
Peregrine OAA Platform architecture

Peregrine OAA Platform applications and interfaces use Web-based building blocks that include:

HTTP	A simple and widely supported protocol for sending client requests to a server. Variations such as HTTPS provide security as well.
XML	Extensible Markup Language. A documentation meta-language that allows you to format data, which can then be displayed through a Web browser. Unlike HTML, you create your own XML tags and define them any way you want.
Commercial web servers	The services provided by the Archway architecture can be served from any commercial Web server, including IIS and Apache.
Application servers	Peregrine OAA Platform supplies Apache Tomcat for an application server with the installation. WebSphere is also supported.
Common clients	Applications can be deployed via Web browsers (IE, Netscape), handheld devices (Palm Pilot), or mobile phones (through HDML).

The application server processes data (JSP pages, XML, and so forth) that it receives from the database or client that is specifically related to the Peregrine Systems Web applications. The Web server converts the data into a form (HTML) that can be displayed in a Web browser.

The following diagram illustrates the architecture:



The Archway component listens to HTTP requests from clients, routes the requests to an appropriate server, and returns data or documents. The requests supported by Archway can vary, but they fundamentally consist of queries, data updates, or system events.

For example, a client can contact Archway and ask to query a database for a list of problem tickets. Another client could contact Archway and supply it with a new purchase request to be entered into the database.

All requests and responses are formatted using XML. For example, a problem ticket expressed in XML could appear as follows:

```

<problem>
  <number>PM5670</number>
  <contact> Joe Smith </contact>
  <description> My printer is out of paper </description>
</problem>
  
```

Clients that interact with Archway can do anything they need with the XML that is returned as a response. Very frequently, the client initiating the request is a user interface such as a Web browser. Such a client could easily display the XML documents returned by Archway. However, to be of better use, the XML documents are often displayed within a formatted HTML page. This is accomplished by using Java Server Pages (JSP).

JSP provides a syntax for creating HTML pages that is pre-processed by the Web server before being sent to the browser. During this processing, XML data obtained from Archway is merged into the HTML page.

Archway's architecture includes special support for automatically generating the HTML and JSP pages that make up a Web application.

OAA scalability

You can ensure that OAA applications perform well as the number of users in your organizations grows. For complete information, see the *Guide to OAA architecture and optimization*, which is available for download in PDF format in the Employee Self Service section of Product News at <http://support.peregrine.com/support/BI Portal>.

Archway internal architecture

Archway is implemented as a Java servlet. The Java servlet is an application executed by a Web server that processes HTTP requests from client Web browsers and sends the request, by way of an adapter, to a database. It then retrieves the requested information from the database and returns it to the client. Archway requires both a Java environment and a Web server.

Each request is interpreted to determine its destination. Archway is able to communicate with a variety of back-end systems, including the AssetCenter or ServiceCenter products from Peregrine.

Requests can be handled in one of three ways:

- A request can be sent directly to an adapter that talks to a back-end server. For instance, a query request for opened tickets could be forwarded to an adapter capable of communicating with ServiceCenter.
- A request can be sent to a script interpreter hosted by Archway. This enables you to define your own application-specific services. Within a script, calls can be made back to Archway to access the back-end system with database operations and events.
- Finally, a request can be sent to a component known as a Document Manager. This component provides automated services for combining logical documents.

Archway communicates with back-end systems with the help of specialized adapters that support a predefined set of interfaces for performing connections, database operations, events, and authentication. All adapters use DLLs to communicate with each application.

Messages can be routed to a script interpreter hosted by Archway. The interpreter supports ECMAScript, a European standard based on the Core JavaScript language used by Netscape (JavaScript) and Microsoft Internet Explorer (JScript).

Messages can be routed to the Document Manager component. This component reads special schema definitions that describe application documents for logical entities such as a purchase request, problem ticket, or product catalog. The script interpreter uses these schemas to automatically generate database operations that query, insert, or update such documents.

Archway requests

Archway supports a variety of requests, all of which are based on two basic technologies: HTTP and XML. The HTTP protocol defines a simple way for clients to request data from a server. The requests are stateless and a client/server connection is maintained only during the duration of the request. All this brings several advantages to Archway, including the ability to support a large number of requests with the help of any of today's commercial Web servers.

Another important advantage is that any system capable of making HTTP requests can contact Archway. This includes Web browsers, of course. But in addition, all modern programming environments support HTTP. This makes it very simple to write new adapters that communicate with Peregrine servers without the need of specialized APIs.

You can test the output generated by your server-side onload scripts and schemas by using URL queries to the Archway servlet.

Archway will invoke the server script or schema as an administrative user and return the output as an XML document. Your browser will need an XML renderer to display the output of the XML message.

Note: Your browser may prompt you to save the XML output of the URL query to an external file.

URL Script Queries

Archway URL script queries use the following format:

```
http://server name/oaaservlet/archway?script name.function name
```

- For *server name*, enter the name of the Java-enabled Web server. If you are testing the script from the computer running the Web server, you can use the variable `localhost` as the server name.

The `/oaaservlet` mapping assumes that you are using the default URL mapping that BI Portal automatically defines for the Archway servlet. If you have defined another URL mapping, replace the servlet mapping with the appropriate mapping name.

- For *script name*, enter the name of the script you want to run.
- For *function name*, enter the name of the function used by the script.

Note: URL queries functionality can be removed by configuring the `WEB.xml` file. This is a recommended security setting.

URL Schema Queries

Archway URL schema queries use the following format:

```
http://server name/oaaservlet/archway?adapter name.Querydoc
&_document= schema name
```

- For *adapter name*, enter the name for the back-end database adapter the schema uses. The adapter listed here will use the ODBC connection that you have defined in the Admin module Settings page.
- For *schema name*, enter the name defined in the <document name="schema name"> element of the schema file.

The `/oaaservlet` mapping assumes that you are using the default URL mapping that BI Portal automatically defines for the Archway servlet. If you have defined another URL mapping, replace the servlet mapping with the appropriate mapping name.

URL SQL Queries

Archway URL SQL queries use the following format:

```
http://server name/oaaservlet/archway?adapter name.query&_table=
table name&field name=value&_[optional]=value
```

- For *adapter name*, enter the name for the back-end database adapter the schema uses. The adapter listed here will use the ODBC connection that you have defined in the Admin module Settings page.
- For *table name*, enter the SQL name of the table you want to query from the back-end database.
- For *field name*, enter the SQL name of the field you want to query from the back-end database.
- For *value*, enter the value you want to the field or optional parameter to have.
- For *_[optional]*, enter any optional parameters to limit your query. Examples include:

- `_return`. Returns the values only of the fields you list.
- `_count`. Specifies how many records you want returned with the query.

The `/oaaservlet` mapping assumes that you are using the default URL mapping that BI Portal automatically defines for the Archway servlet. If you have defined another URL mapping, replace the servlet mapping with the appropriate mapping name.

The following are sample URL SQL queries:

- `host name/oa/servlet/archway?sc.query&_table=probsummary&priority.code=1`

This sends a query request to ServiceCenter for all records in the probsummary table with a priority code of 1.

- `host name/oa/servlet/archway?ac.query&_table=amAsset&_return=Brand;mPrice;Model&_count=2`

This sends a query request to AssetCenter for the first two records in the amProduct table. Only the Brand, mPrice, and Model fields are returned for each record.

The screen below shows the XML results of a query for products from AssetCenter.

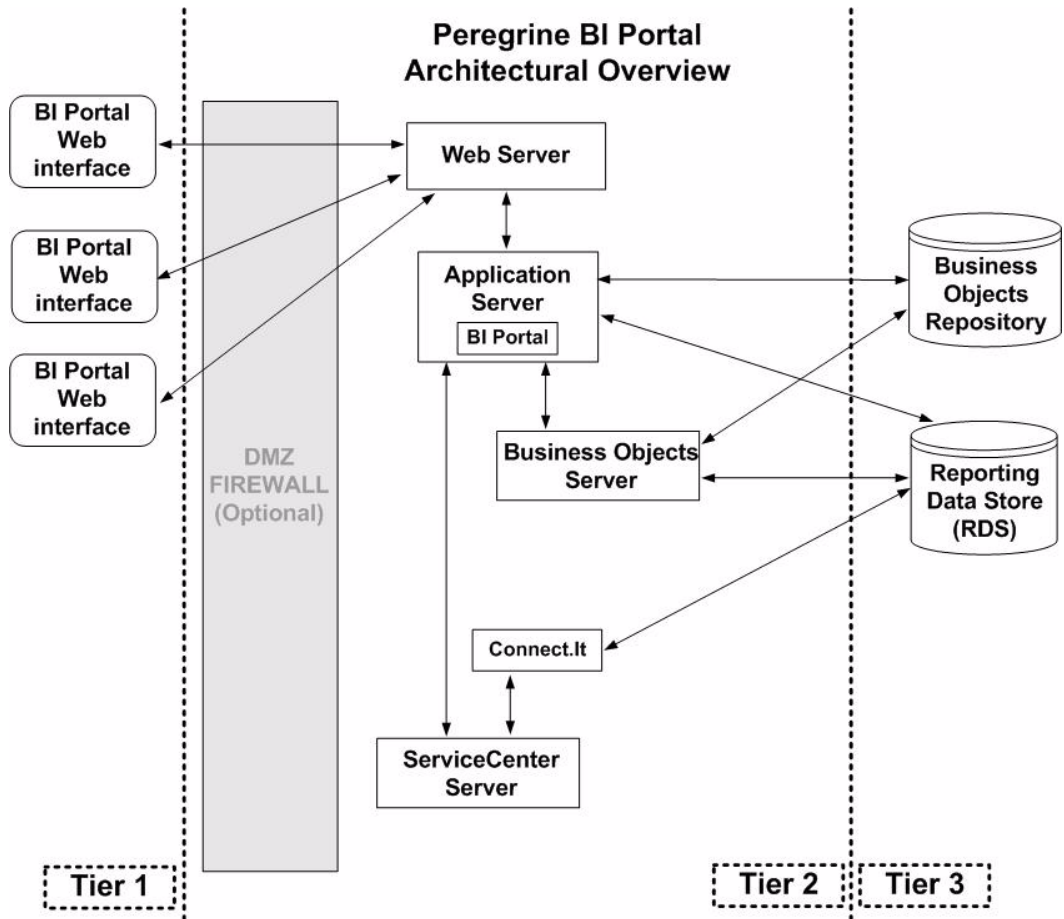
```

<?xml version="1.0"?><recordset _count="2" _countFound="2" _more="1" _start="0">
  <amProduct>
    <Brand>IBM</Brand>
    <mPrice>179.00</mPrice>
    <Model>10/100 ETHERNET CARDBUS ADAPTER F</Model>
  </amProduct>
  <amProduct>
    <Brand>IBM</Brand>
    <mPrice>299.00</mPrice>
    <Model>10/20GB TR5 IDE INTERNAL TAPE DRIVE</Model>
  </amProduct>
</recordset>

```

BI Portal architecture

The following figure illustrates the BI_Portal architecture.



2 Customizing the Peregrine Portal

CHAPTER

Peregrine Open Application Architecture (OAA) provides a number of ways to customize the interface of an application built on the platform. You can make a quick change, such as replacing the logo with your company logo, or a more complex change such as rewriting the code that defines layer placement or frameset size.

This chapter includes advanced procedures for changing the Peregrine Portal interface. To use this information effectively, you should have knowledge of XML and the CSS2 specifications established by the W3C as outlined at www.w3.org.

Topics in this chapter include:

- *Deploying the Classic theme variations*
- *Changing the default theme*
- *Changing the header graphic for all themes*
- *Creating a custom theme*
- *Layers properties*
- *Changing framesets*

Deploying the Classic theme variations

The Classic theme is the default theme that applications built on Peregrine OAA use. It has a gray and teal design and is the theme shown in all the screenshots in the guide. This is the theme you will use to create a customized theme for your enterprise.

There are four variations of the Classic theme:

- *Accessible*, which makes the screen available to users who need high contrast colors or better accessibility support.
- *Baja*, which adds southwestern green and beige hues to the Classic design.
- *Quicksilver*, which adds silver and blue hues to the Classic design.
- *Sierra*, which adds teal hues to the Classic design.

These themes, as well as a number of other optional themes, are deployed with the application installation. Once you create your customized theme, Peregrine Systems recommends that you delete all other themes to prevent users from selecting one of them and overriding your custom theme. If you decide later that you want to manually deploy a theme that has been deleted, or if you did not deploy all themes during the installation, use the following procedure to deploy the themes. The additional themes are zip files located in the `C:\Program Files\Peregrine\oaa\packages` directory. You can identify the theme names from these zip file names.

To deploy an alternate Classic design

- 1 Open a command prompt window, and change directories to your `oaa\packages` directory. The default path is:
`C:\Program Files\Peregrine\oaa\packages`

- 2 Type:

```
java -jar OAADeploy.jar <name of the theme>
```

Note: List each theme you want to deploy, separated by a space; for example,
`java -jar OAADeploy.jar bluestheme hightechtheme bajatheme.`

- 3 Press ENTER.
- 4 Stop and restart your application server.

The themes you deployed appear as options the next time you log in to BI Portal.

Changing the default theme

You can change the default theme that all users see when they log in to BI Portal. Out-of-box, the default theme is classic.

To change the default theme

- 1 Open your Web browser and log in to the Admin module (`localhost/oa/admin.jsp`).
- 2 Click **Settings** > **Themes**. Change the following parameters:
 - a In the **Default skin/Theme** field, change the parameter to the name of the theme you want to use (for example, *Baja*).
 - b In the **Default stylesheet** field, change the parameter to the appropriate name for the CSS file (for example, *baja.css*).
 - c In the **Default XSL stylesheets** field, change the parameter to the name of the theme you want to use (for example, *Baja*).
- 3 Scroll to the bottom of the page, and then click **Save**.
- 4 When the Control Panel opens, click **Reset Server**.
- 5 Refresh your browser to see the new default theme.

Changing the header graphic for all themes

You can add your corporate logo to all themes in the Peregrine Portal from the Administration Settings page.

Warning: The administration setting discussed below overrides the image used by all themes. If you change this setting then you will see the same logo in all themes. If you want to use a different corporate logo for each theme, see [Creating a custom theme](#).

To change the header graphic for all themes

- 1 Create a custom header graphic.

Note: To fit within the default header frame, your customized header logo must be 514 pixels wide and 59 pixels high. If you want to change the header frame size, see *Changing framesets*.



- 2 Save your custom header graphic to the following location:

C:\Program Files\Peregrine\Common\Tomcat4\webapps\oaa\images\skins\classic

Note: The Classic theme is the default theme.

- 3 Log in to the BI Portal administration page (admin.jsp).
- 4 Click **Settings > Themes**.
- 5 In the **Default Peregrine Portal logo** field, enter the name of your custom header logo.

Portal	Common	Service Desk	Portal DE	Themes	Web Application	Logins	ServiceCenter	XSL	E-mail
Internet Explorer stylesheet path:					Directory path for CSS stylesheets for Internet Explorer browser.				
css/									
Images path:					Set the images directory location. The directory name must be specified relative to the "presentation" directory. Setting this allows you to move the default location of the images directory to another location. The default is "images/". You must add the slash at the end of this path.				
images/									
Skins/Themes:					Set the Skins directory location. The directory name must be specified relative to the "presentation" directory. Setting this allows you to move the default location of the skins directory to another location. The default is "skins/". You must add the slash at the end of this path.				
skins/									
Default skin/Theme:					Set the Default Skin name for user sessions. Enter only the name of the skin. The default is "classic".				
classic									
Default stylesheet:					Set the CSS Stylesheet name for user sessions. To see all the styles used in The Peregrine Portal, click to see the Peregrine Portal Stylesheet Key . This file can be useful for customizing stylesheets. The default is "classic.css".				
classic.css									
Default XSL templates:					The default XSL template set to use when the user has not set a theme. This should be the same as the default skin when specifying a theme provided by Peregrine Portal.				
classic									
Default Peregrine Portal logo:					Set the global logo to be used in the application. The logo is skinned and is located at the root level of each skin directory in Themes. To add a new custom logo, add it to the skin template. Type in the name for the new logo image. Instructions for adding new images are included in the Peregrine Portal Tailoring Guide. The default logo is "getit_header_logo.gif".				
getit_header_logo.gif									
Application Tab Order:					List one module from each of the tab groups in the order that the tabs should appear. Tabs that are omitted will appear at the end of the list in no particular order.				
portal									

Type your new image name.

- 6 Scroll to the bottom of the page, and then click **Save**.
- 7 When the Control Panel opens, click **Reset Server**.
- 8 Refresh the browser to view your changes.

Creating a custom theme

You can create custom themes by copying and modifying the classic theme provided with BI Portal.

To create a custom theme

- 1 Copy classic theme images, stylesheets, and XSL templates. These files are located at:
 - Images. `<application server>\oaa\images\skins\classic`
 - Stylesheets. `<application server>\oaa\css\classic`
 - XSL templates. `<application server>\oaa\WEB-INF\templates\classic`
- 2 Paste and then rename the folders for the classic theme to a new name. For example:
 - Images. `<application server>\oaa\images\skins\myTheme`
 - Stylesheets. `<application server>\oaa\css\myTheme`
 - XSL templates. `<application server>\oaa\WEB-INF\templates\myTheme`
- 3 Open and edit each image that you want to change in your new theme. Use the following image conventions.
 - Image file names must remain the same. BI Portal uses these image names to display theme elements.
 - Image height and width should remain the same unless you are also changing the size of the framesets to accommodate new image sizes.
- 4 Open and edit the `classic.css` file in your new theme.

The following table lists some of the more commonly modified styles.

Style Name	Style Description
<code>.ActionButton</code>	The style used on buttons throughout the Portal.
<code>.ActiveMenuLink</code>	Used when the mouse hovers over a menu link.
<code>.ActiveModuleMenu</code>	Designates the currently-selected page within the navigational subset.
<code>.CurrentModuleMenu</code>	Designates the currently-selected navigational subset.
<code>.FormTitle</code>	Used for the title of forms. Normally used to title DocExplorer window content.

Style Name	Style Description
.ListBoxEvenRow	A bolded version of TableEvenRow.
.ListBoxHeading	A bolded version of Table Heading.
.ListBoxOddRow	A bolded version of TableOddRow.
.MenuLink	Used within all module menus.
.ModuleMenu	Used for the left-hand navigational menu.
.ModuleMenuTitle	Designates the navigational subsets title.
.PageTitle	Used on the page title located directly below the logo and tabs.
.TableEvenRow	Used within the table heading with alternating background colors for ease of reading. Has a background color of white.
.TableHeading	Used for application headings for both search and results functions.
.TableOddRow	Used within the table heading with alternating background colors for ease of reading. Has a background color of light gray.
a.ListBoxEvenRow	Designates the style with a link attribute.
a.ListBoxOddRow	Designates the style with a link attribute.
a.TableEvenRow	Designates the style with a link attribute.
a.TableOddRow	Designates the style with a link attribute.

Tip: Modify the style sheets after you complete your overall theme design. Use your image editor's color picker to ensure that the your stylesheet colors match your image colors.

Note: You can see a detailed stylesheet key in the themes Administration section of the Portal. To access the stylesheet key, locate the Default stylesheet field on the Themes tab of the Admin Settings page and click the [Peregrine Portal Stylesheet Key](#) link.

Portal	Common	Service Desk	Portal DB	Themes	Web Application	Logging	ServiceCenter	XSL	Email
Internet Explorer stylesheet path:					Directory path for CSS stylesheets for Internet Explorer browser.				
css/									
Images path:					Set the images directory location. The directory name must be specified relative to the 'presentation' directory. Setting this allows you to move the default location of the images directory to another location. The default is "images/". You must add the slash at the end of this path.				
images/									
Skins/Themes:					Set the Skins directory location. The directory name must be specified relative to the 'presentation' directory. Setting this allows you to move the default location of the skins directory to another location. The default is "skins/". You must add the slash at the end of this path.				
skins/									
Default skin/Theme:					Set the Default Skin name for user sessions. Enter only the name of the skin. The default is "classic".				
classic									
Default stylesheet:					Set the CSS Stylesheet name for user sessions. To see all the styles used in The Peregrine Portal, click to see the Peregrine Portal Stylesheet Key . This file can be useful for customizing stylesheets. The default is "classic.css".				
classic.css									
Default XSL templates:					The default XSL template set to use when the user has not set a theme. This should be the same as the default skin when specifying a theme provided by Peregrine Portal.				
classic									
Default Peregrine Portal logo:					Set the global logo to be used in the application. The logo is skinned and is located at the root level of each skin directory in Themes. To add a new custom logo, add it to the skin template. Type in the name for the new logo image. Instructions for adding new images are included in the Peregrine Portal Tailoring Guide. The default logo is "getit_header_logo.gif".				
getit_header_logo.gif									
Application Tab Order:					List one module from each of the tab groups in the order that the tabs should appear. Tabs that are omitted will appear at the end of the list in no particular order.				
portal									

- 5 Save your theme stylesheet with the same name as your new theme. For example, `<application server>\oaa\css\myTheme\myTheme.css`.
- 6 Open and edit the `layers_<xx>.jsp` file to change any layer descriptions. To change layers for Internet Explorer, open `layers_ie.jsp`. To change layers for Netscape open `layers_gecko.jsp` extension. For more information about editing layers see [Layers properties](#).
- 7 Open and edit any XSL stylesheets you want to change.

Warning: Do not change these files unless you have knowledge of XSL and HTML transformation.

The XSL stylesheets determine how BI Portal displays form components in the main portal frame.

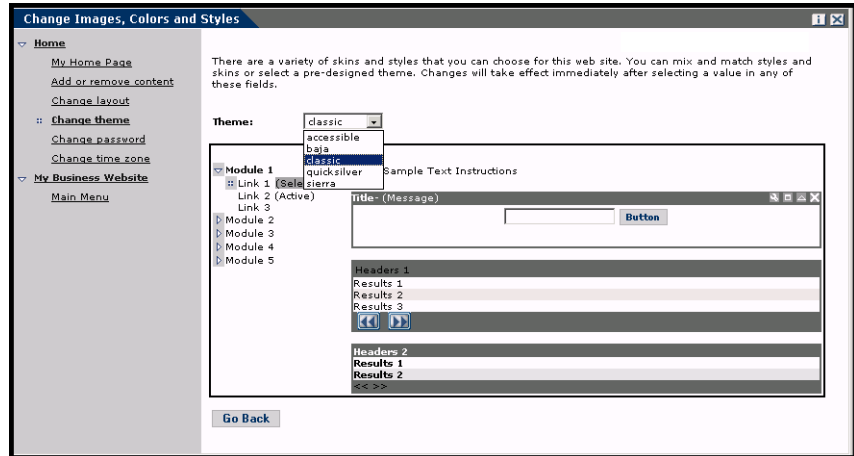
The following table lists the XSL stylesheets you can change.

To change	edit this XSL stylesheet
Attachment picker	attachments.xml
HTML form generation	basic-form.xml

To change	edit this XSL stylesheet
Action (button) properties	button.xsl
Template components	components.xsl
Debugging message properties	copy_nodes.xsl
Date-time picker properties	datetime.xsl
Text edit field properties	edit_fields.xsl
Entry table form component (see administration page for examples)	entrytable.xsl
Field section properties	fieldsection.xsl
Field table properties	fieldtable.xsl
HTML page generation	form.xsl
Frameset properties	frames.xsl
Images properties	image_fields.xsl
Label properties	labels.xsl
Link properties	link.xsl
Building of DocExplorer lists	list-builder.xsl
Lookup field properties	lookup_fields.xsl
Money text field properties	money_fields.xsl
Portal properties	portal.xsl
Radio check box properties	radio_checkbox_fields.xsl
Read-only text field properties	readonly_fields.xsl
Select text field properties	select_fields.xsl
Spinner properties	spinner_fields.xsl
SVG image properties	svg_cad.xsl
Table properties	table.xsl
Navigation tab properties	tabs.xsl

- 8 Stop and restart your application server.

You can view your new theme by selecting it from the *Change theme* page, available from the Peregrine Portal Home page.



Layers properties

The following sections describe the `layers_ie.jsp` and `layers_gecko.jsp` files. Each layer is defined by a separate `<div>` tag entry and includes an `id` attribute that names the layer. You can change layer properties as needed, but the following layers are required and should not be removed:

- **logo**

```
<div id="logo" style="position:absolute; left: 0px; top: 0px; width:
100%; height: 40px; z-index: 3;">

</div>
```

- **time**

```
<div id="time" style="position:absolute; right: 4px; top: 84px;
width: 100%; z-index: 13;" onmouseover="_pauseAlert()"
onmouseout="_startAlert()" class="userBarText">
</div>
```

- **toolbar**

```
<div id="toolbar" style="position:absolute; width: 50px; top: 59px;
right: 0px; z-index: 12;"></div>
```

- **user**

```

<div id="user" style="position:absolute; top: -4px; right: 0px;
z-index: 14;">
<table width="100%" border="0" cellpadding="0" cellspacing="0"
align="right">
<tr>
<td width="50%">&nbsp;</td>
<td nowrap width="3" align="right" valign="top">
">
</td>
<td nowrap align="right" valign="top" width="100%" background="<%=
Archway.getSkinImagePath("backgrounds/rt_tile.gif", user ) %>">
">
</td>
<td nowrap><font class="userBarText" size="1" face="Arial, Helvetica,
sans-serif"><%=userTitle%></font>&nbsp;&nbsp;&nbsp;</td>
</tr>
</table>
</div>

```

■ tabs

```

<div id="tabs" style="position:absolute; left: 0px; top: 60px; width:
100%; z-index: 11;" >
</div>

```

■ form titles

```

<div id="formTitles" style="position:absolute; left: 10px; top: 81px;
width: 200px; z-index: 16;">&nbsp;&nbsp;&nbsp;
</div>

```

Changing framesets

Important: You must have advanced knowledge of HTML, JSP, and framesets to modify these files. Keep all of the frames and do not change the names of any of the frames. Doing so will result in JavaScript errors.

There are two framesets to be modified for each browser. These files are in C:\Program Files\Peregrine\Common\Tomcat4\webapps\oaa\images\skins*<your theme>*.

The `frames_xx.jsp` files are for the pages that you access when logging in as an end-user (`login.jsp`). The `admin_frames_xx.jsp` files contain the configuration for the Admin module (accessed when you log in using `admin.jsp`).

To change framesets

- 1 Stop your application server.
- 2 Open the browser-specific frameset file `frames_<xx>.jsp` in a text editor (where `<xx>` is `ie` for Internet Explorer and `gecko` for Netscape).
- 3 Modify the frameset properties.
- 4 Save the file.
- 5 Restart your application server.

You can now test your changes in your Web browser.

The following sections show the complete `_ie.jsp` files as examples of the frameset files.

`frames_ie.jsp`

```
<%@ include file="../../jshpheader_2.jsp" %>
<%@ include file="../../message_special.jsp" %>

<frameset onload="setTopFrames()" onunload="closeChildWindows()"
border="0" framespacing="0" frameborder="NO" cols="*" rows="102,*">
  <frame scrolling="NO" marginwidth="0" marginheight="0"
src="oaa_header.jsp" name="getit_main_head">
    <frameset cols="185,10,*" rows="*" frameborder="no" border="0"
framespacing="0">
      <frame scrolling="AUTO" marginwidth="0" marginheight="0"
src="apphead.jsp" name="getit_header">
        <frame name="framesep" scrolling="no" marginheight="0"
marginwidth="0" src="framesep.jsp">
          <frameset rows="*,0">
            <frame scrolling="AUTO" marginwidth="6" marginheight="6"
src="e_login_main_start.jsp?<%= user.getADW(msg,"Params" ) %>"
name="getit_main">
              <frame noresize scrolling="NO" marginwidth="0"
marginheight="0" src="backchannel.htm" name="backchannel">
            </frameset>
          </frameset>
        </frameset>
      </frameset>
    </frameset>
```

`admin_frames_ie.jsp`

```
<%@ include file="../../jshpheader_2.jsp" %>
<%@ include file="../../message_special.jsp" %>
```

```
<frameset onload="setTopFrames()" onunload="closeChildWindows()"
border="0" framespacing="0" frameborder="NO" cols="*" rows="102,*">
  <frame scrolling="NO" marginwidth="0" marginheight="0"
src="aaa_header.jsp" name="getit_main_head">
    <frameset cols="185,10,*" rows="*" frameborder="no" border="0"
framespacing="0">
      <frame scrolling="AUTO" marginwidth="0" marginheight="0"
src="apphead.jsp" name="getit_header">
        <frame name="framesep" scrolling="no" marginheight="0"
marginwidth="0" src="framesep.jsp">
          <frameset rows="*,0">
            <frame scrolling="AUTO" marginwidth="6" marginheight="6"
src="e_adminlogin_login_start.jsp?<%= user.getADW(msg, "Params") %>"
name="getit_main">
              <frame noresize scrolling="NO" marginwidth="0"
marginheight="0" src="backchannel.htm" name="backchannel">
            </frameset>
          </frameset>
        </frameset>
      </frameset>
```


3 Using the Peregrine Portal

CHAPTER

The Peregrine Portal includes a Navigation menu, an Activity menu, and buttons that enable you to customize your Portal and to end your session.

Your installed Web applications determine the contents of the Navigation menu. However, if you log in as an administrator, all Navigation menus include an Administration tab that provides access to the Admin module.

The graphics in this chapter use the Classic stylesheet and are examples of a generic interface. Also, the Admin module displays only those features that BI Portal uses. For more advanced changes to the portal, see the chapter on *Customizing the Peregrine Systems Portal*.

Topics in this chapter include:

- *Logging in to the Peregrine Portal* on page 34
- *Using the Activity menu* on page 35
- *Personalizing the Peregrine Portal* on page 36

Logging in to the Peregrine Portal

There are two login screens that provide access to the Peregrine Portal:

- A user login screen—`http://<server>/oaa/login.jsp`
- An administrator login screen—`http://<server>/oaa/admin.jsp`

Note: An alternative to this login method is the Integrated Windows Authentication. See the *Security* chapter of this guide.

This chapter discusses the features available with a user login. For more information about the administrator login, see the chapter on *BI Portal Administration* in this guide.

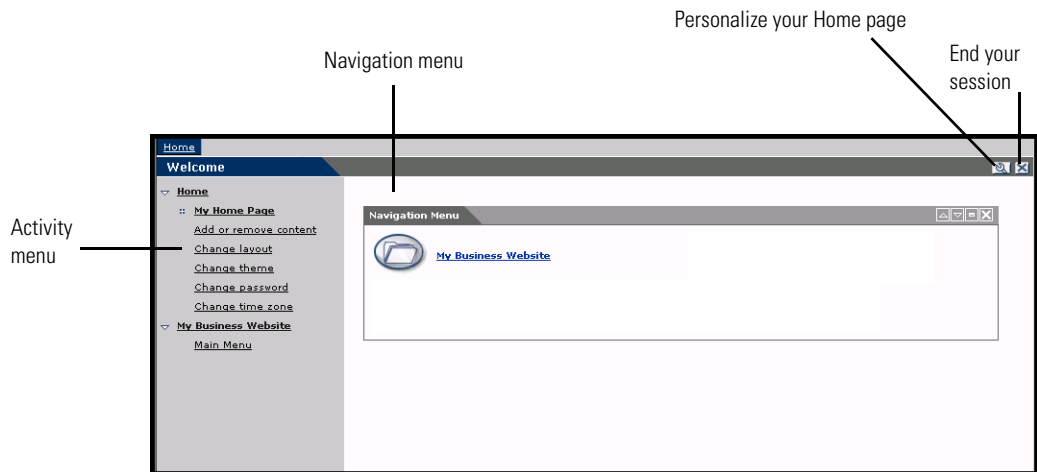
The following is an example of the user login interface.



The screenshot shows the user login interface for the Peregrine Portal. The page has a header with the "Peregrine Portal" logo on the left and "Powered by Peregrine" on the right. Below the header is a "Login" tab and a "Welcome" message. The main content area contains a login form with the following elements:

- A heading: "Please enter your user name and password to enter the Peregrine Portal."
- A "User Name:" label followed by a text input field and a small icon.
- A "Password:" label followed by a text input field.
- A "Language:" label followed by a dropdown menu currently set to "English".
- A "Login" button at the bottom of the form.

The following graphic shows a Portal without any applications installed. The Navigation menu includes modules for your particular application. All applications have the Admin module.



Using the Activity menu

The Activity menu provides access to a number of tasks as you navigate through your Web application. The menu remains visible as you change screens.

The default Activity menu includes the following choices:

Use this option	When you want to
My Home Page	Return to the Peregrine Portal Home page.
Add or remove content	Access the same page as the Personalization button, allowing you to customize your Home page.
Change layout	Change the location of a component or remove it from the Peregrine Portal.
Change theme	Select from several options. Changes take effect immediately after selecting a value in any of these fields. Note: Select the accessible theme to access the alternate text-based interface.
Change time zone	Select the time zone.

Personalizing the Peregrine Portal

By default, the Navigation menu is displayed on the Peregrine Portal. You can personalize the Peregrine Portal to add BI Portal utilities as well as personal tools such as a calendar, calculator, or the date and time. You can also change the layout of these components or minimize a component to hide the component details.

See the chapter on *Using the Personalization Interface* in this guide for more information on personalization.

Adding components

The following components are available:

Personal Utilities

This component	Provides
Calculator	A tool using standard arithmetic functions.
Calendar	A monthly calendar.
Theme Selector	A drop-down list to change themes.
Date and Time	A date and time display for the local time zone.

Peregrine Portal Web application components

This component	Provides
Navigation Menu	Quick links to the various modules that make up this application.
Document List	A display of a document search, list, or detail screen. Configure the component by choosing the document type you want to expose and the type of screen desired.
My Menu	A menu of links that can be configured dynamically. Links can point to arbitrary web sites, other menus, or document explorer screens.

Note: The Calendar and Calculator require Microsoft Internet Explorer 5.0+ or Netscape 6.1+.

Administration components

Only users with Admin capability have access to the Admin components.

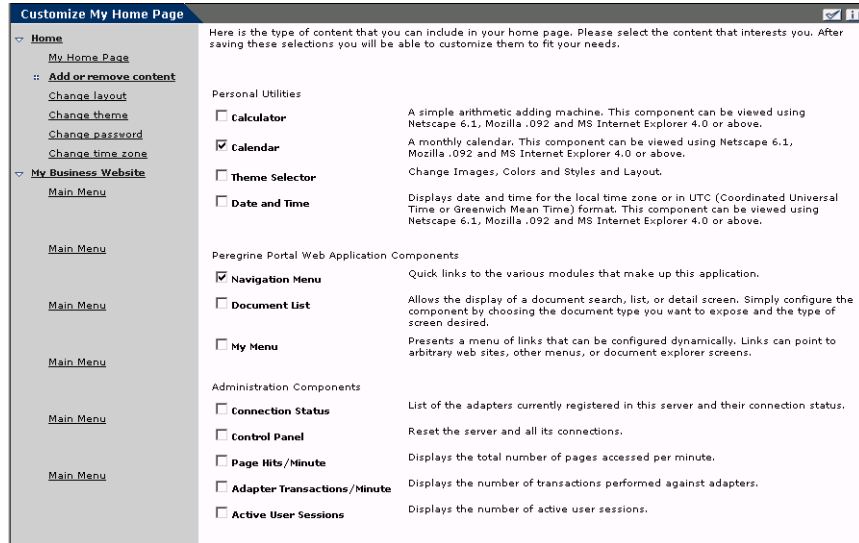
This component	Provides
Connection Status	A list of the adapters currently registered in this server and their connection status.
Control Panel	A button to reset the server and all its connections.
Page Hits / Minute	A list of the total number of pages accessed per minute.
Adapter Transactions / Minute	A list of the number of transactions performed against adapters.
Active User Sessions	A list containing the number of active user sessions.

To add Peregrine Portal components

- 1 Click the **Personalize** (wrench) icon.

Note: You can also select the **Add or remove content** link from the Activity menu.

The **Customize My Home Page** opens containing a list of the available components.



- 2 Select the components you want to add to your Peregrine Portal.
- 3 When you complete your selections, scroll to the bottom of the page, and then click **Save**. To return to the Peregrine Portal without making any changes, click **Go Back**.

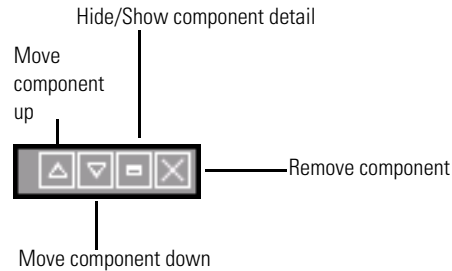
When you return to the Peregrine Portal, the new components appear.

Changing the layout

The following sections contain procedures for changing the location of the components or removing them from the Peregrine Portal. The procedure you use is determined by the Web browser you are using.

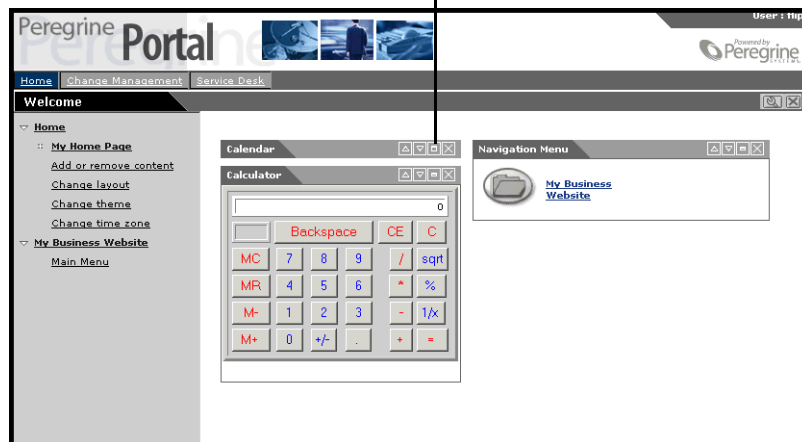
Microsoft Internet Explorer

If you are using Microsoft Internet Explorer as your Web browser, use the buttons in the upper right corner of each component to move the component up or down, remove the component, or hide/show the component detail.



In the following screen, the Calendar is minimized.

Click the Show/Hide detail button to redisplay hidden components.

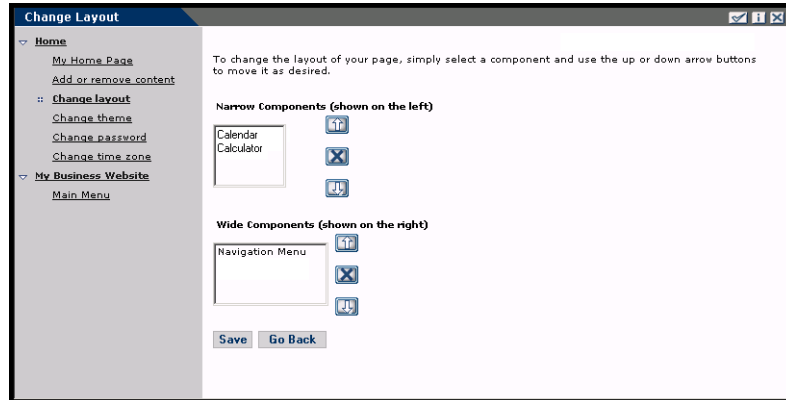


Netscape Navigator

If you are using Netscape Navigator as your Web browser, use the following procedure to change the status of the components on the Peregrine Portal. You can move a component up or down, or remove the component.

- 1 From the Activity menu, select **Change layout**.

A **Change Layout** page opens where you select the components you want to change.



Components can be Narrow (for example, Calendar or Calculator) and are on the left side of the Peregrine Portal. Other components (for example, Navigation Menu) are Wide and are on the right side of the Peregrine Portal.

- 2 Select the component you want to modify, and then click the appropriate button to activate the change.
 - Up arrow moves the component up.
 - Down arrow moves the component down.
 - X removes the component from the Peregrine Portal.
- 3 Click Save.

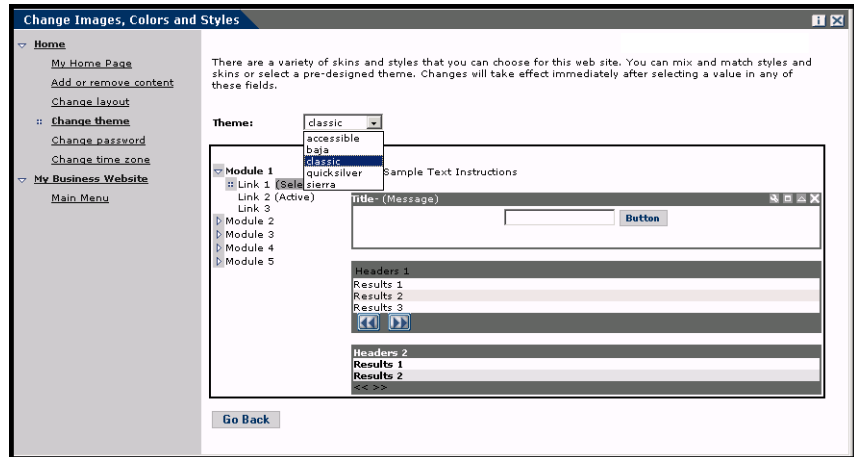
Changing themes

You can choose from a number of themes to change the look of your Web pages. Out of the box, BI Portal provides five themes you can choose between. If you want to deploy additional themes, refer to *Customizing the Peregrine Portal*.

To change the theme

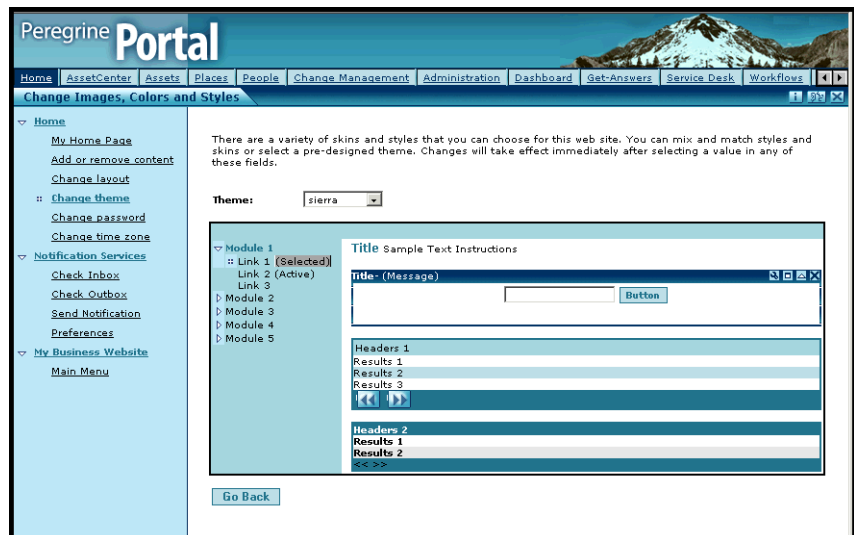
- 1 From the Activity menu on the Portal Home page, select **Change theme**.

The following page opens.



2 Choose from the drop-down list.

As soon as you make your selection, the page updates to reflect your selection. The following example shows the Sierra theme.



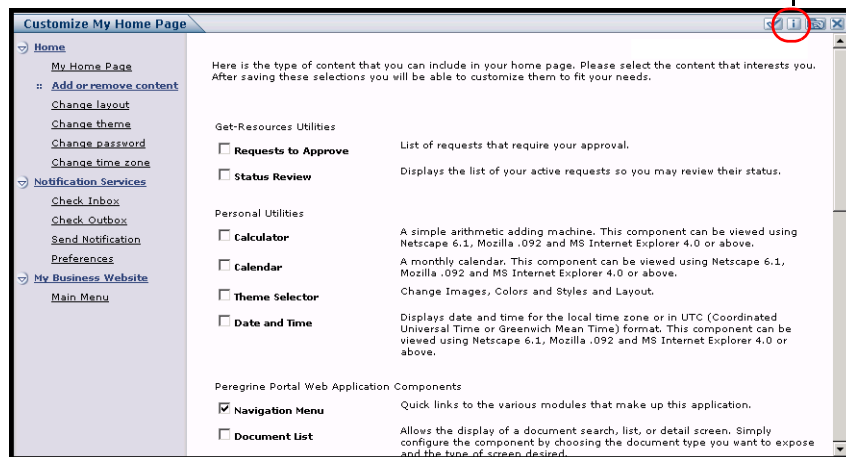
This new configuration remains through subsequent work sessions until changed.

Displaying form information

You can view information about the form you are using. Set this parameter from the Logging tab on the Settings page of the Admin module. See the BI Portal Administration chapter in this guide for more information.

When the **Show form info** parameter is set to Yes, a **Display Form Info** button appears on the upper-right corner of forms.

The Display Form Info button shows information about the form you are using.



4 Using the OAA Administration Module

CHAPTER

This chapter includes instructions for administering your BI Portal system.

Topics in this chapter include:

- *Accessing the Peregrine Portal Admin module* on page 44
- *Using the Control Panel* on page 46
- *Viewing the Deployed Versions* on page 47
- *Using the Settings page* on page 48
- *Logging* on page 50
- *Verifying Script Status* on page 56
- *Displaying Message Queues* on page 56
- *Showing Queue Status* on page 57
- *Importing and exporting personalizations* on page 58
- *Viewing adapter transactions* on page 58
- *Using the IBM Websphere Portal* on page 59
- *Displaying form information* on page 59
- *User self-registration* on page 62
- *Changing passwords* on page 63
- *Logging and monitoring user sessions* on page 63
- *BI Portal administration* on page 64

Accessing the Peregrine Portal Admin module

The Peregrine Portal administrator login page enables access to the Peregrine Portal Admin module. You use the Admin module to define the settings for your Peregrine system.

Note: After installing and building BI Portal, you must log on as a ServiceCenter user with `getit.admin` rights to access the Admin module and administer the BI Portal integration with ServiceCenter. For a list of access capability words and Adapter configuration instructions, see the section on BI Portal security in this guide.

A default administrator, System, gives you access to the Admin module without being connected to a back-end system. After you configure your user name on the Common tab, you can also access the Admin module from the Navigation menu.

Important: When you change parameters using the Admin module, a `local.xml` file is created in the `\<appsrvr>\WEB-INF` directory (where `appsrvr` is the path to your application server) to store these parameters. If you reinstall BI Portal, make a copy of this file and store it outside your BI Portal installation. Failure to do this will result in your parameter values being lost during the new installation.

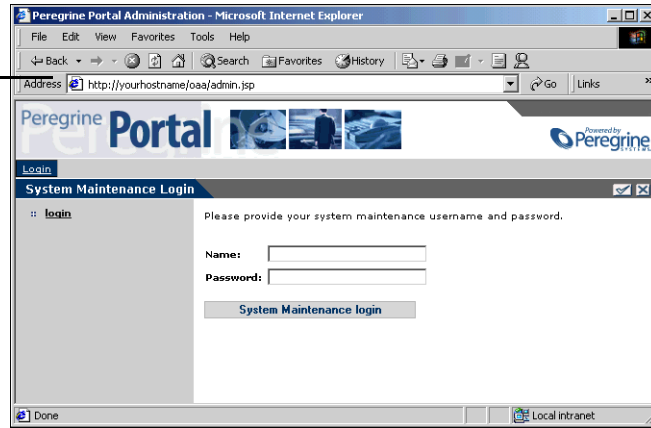
To access the Peregrine Portal administrator login page:

- 1 Verify that your application server (for example, Tomcat) is running.
- 2 In your Web browser Address field, type:
`<hostname>/oaa/admin.jsp`

3 Press Enter to open the Portal administrator login page.

Type your hostname to connect to your local server.

System is the default administrator name.



4 In the Name field, type System.

No password is required on initial login.

5 Click System Maintenance login to open the Control Panel page.

Control Panel

Here is a list of the adapters currently registered in this server. If necessary, you may also reset the server and all its connections.

Connection Status		
Target	Adapter	Status
replication	com.peregrine.ooa.adapter.sc.SCAAdapter	connected
mail	com.peregrine.ooa.adapter.mail.MailAdapter	disconnected
portalDB	com.peregrine.ooa.adapter.sc.SCAAdapter	connected
sc	com.peregrine.ooa.adapter.sc.SCAAdapter	connected

Active User Sessions				
Server Name	Last Min.	5 Min. Avg.	20 Min. Avg.	Peak
localhost	0	0	0	1

Page Hits per Minute				
Server Name	Last Min.	5 Min. Avg.	20 Min. Avg.	Peak
localhost	0	0	0	6

[Reset Server](#)

The activities available in the Admin module include:

Select this option	To do the following
BI Administration	Access the BI settings and configurations for the RDS database, Business Objects repository database, BI Portal, Business Objects administration, and Business Objects and BI Portal application settings.
Control Panel	View the status of connections to the back-end systems.
Deployed Versions	View the list of deployed applications with version numbers on this server.
Server Log	View activity on the BI Portal server.
Settings	View and change settings for the Peregrine Portal.
Show Script Status	View and verify which scripts are running. You can also start and stop scripts from this window.
Show Message Queues	View a list of all message queues.
Show Queue Status	View the current status of the queues: operational and unlocked, or suspended.
Import / Export	Move Personalizations from a development to a production environment.
Adapter Transactions/Minute	View the transactions per minute for the back-end adapter.
IBM Websphere Portal Integration	View the installed OAA portal components in the IBM WPS environment

Using the Control Panel

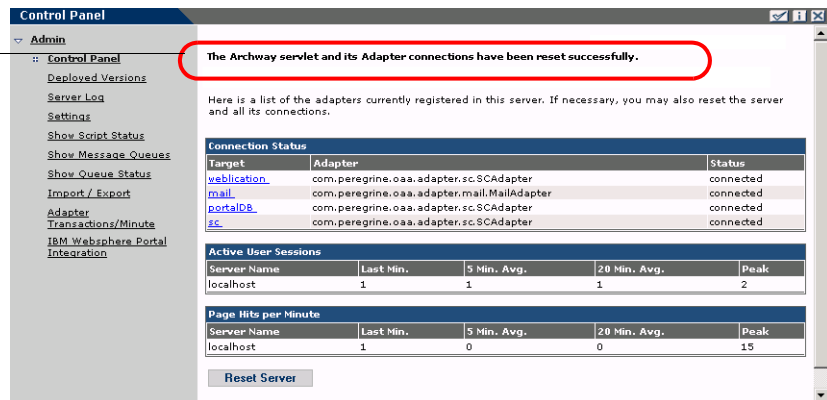
Use the Control Panel page to check the status of the connections to the databases you are accessing with BI Portal and your Web applications. You can also reset the connection between the Archway servlet and the adapters to the back-end systems.

To reset the connection between the Archway servlet and back-end system:

- ▶ Click Reset Server.

A message at the top of the page indicates that the connections are reset.

Informational, warning, and error messages appear at the top of the page.



Viewing the Deployed Versions

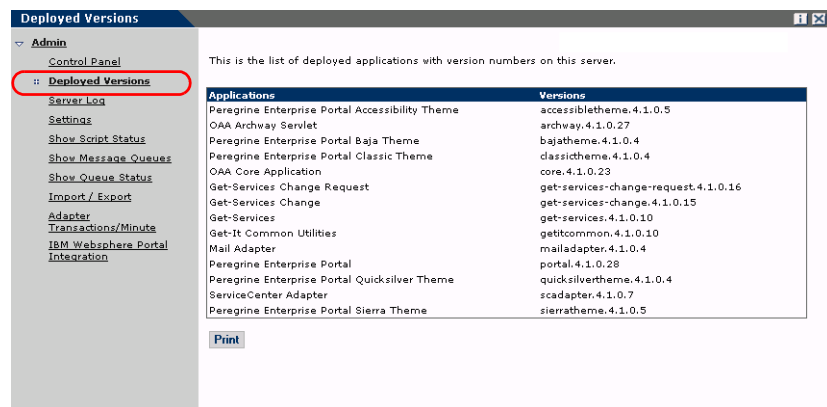
The Deployed Versions screen lists all of the packages that deploy during the installation, including the version number of each package.

To view the Deployed Versions list

- 1 From the Activity menu, select **Deployed Versions**.

A list of the installed packages opens.

Current applications and their versions are available for viewing with the Deployed Versions option.



- 2 Click **Print** for a printout of this list.

Using the Settings page

On the Activity menu, click **Settings** to open the current parameter settings. The Settings page is divided into tabs. The tabs that you see depend on the Web applications that you installed and the adapters that you use. The Common tab is available for all installations.

Settings for the Portal, PortalDB, Web Application tabs are set during the installation (refer to the *BI Portal Installation Guide*). You can access the Settings page at any time to change the installation settings. Set the E-mail tab only when users have access to self-registration (see *User self-registration* on page 62).

To view Settings:

- From the Activity menu, click **Settings**.

Each parameter on the tab has a description that guides you through the settings.

The tabs you see on the Settings page depend on the Web applications you installed.

The screenshot shows the 'Admin Settings' window with the 'Logging' tab selected. The left sidebar contains a navigation menu with options like 'Control Panel', 'Deployed Versions', 'Server Log', 'Settings', 'Show Script Status', 'Show Message Queues', 'Show Queue Status', 'Import / Export', 'Adapter Transactions/Minute', and 'IBM WebSphere Portal Integration'. The main content area is titled 'Logging' and includes the following settings:

- Log domains:** A text input field for entering a semicolon-separated list of execution log traces. A list of choices is provided:
 - dll - Adapter DLL loading and unloading
 - weblication - Web Application and personalization rendering
 - jvm - Java run-time environment management and status
 - locks - Script synchronization locks
 - security - Archway security trace
 - statistics - administration statistics
- Debug script:** Radio buttons for 'Yes' and 'No' (selected).
- Show form info:** Radio buttons for 'Yes' and 'No' (selected).
- Log file:** Text input field containing 'archway.log'.
- Logging Format:** Text input field containing '%d %-5p [%t] %x - %m%n'.
- Log Level:** A dropdown menu set to 'Information'.

Each setting has a corresponding description on the right side of the page.

Setting parameters using the Admin module

When you make changes using the Admin Settings page, a `local.xml` file is created in the `C:\<appsrvr>\WEB-INF` directory. All changes to property settings are stored in this file. Restart Tomcat after making changes that are stored in `local.xml`.

Important: If you change parameters on the Admin Settings page and then need to reinstall BI Portal, it is important that you copy the `local.xml` file to a location other than your BI Portal installation, or all of your settings will be lost when you redeploy BI Portal. After the installation, move the copy back to the `WEB-INF` directory.

To define a parameter

- 1 Locate the setting you want to change and type the new parameter.

Note: If you have previously changed a setting and want to return to the default setting, click the **Click for default** link displayed in the description area for the parameter you want to revert. This link appears only when a setting is different from the default.

- 2 Scroll to the bottom of the page, and then click **Save**.

Note: You must click **Save** on each page before making changes to another setting.

The Control Panel opens.

- 3 Click **Reset Server**.

An information message at the top of the Control Panel indicates that the server has been reset.

Choosing a Login Language

When you log in to the Peregrine Portal, you can choose from the **Language** pull-down list the language that the Portal displays. The default language is English, but you can enable additional languages.

To enable additional login languages:

- 1 Click **Settings** in the Control Panel.
- 2 Scroll down to the **Encoding, Locales, and Sessions** section.
- 3 In the **Locales** field type a comma-delimited list of the languages you want to enable.

The first locale defines the default; in this case “en” for English, which already appears in the field. A locale is specified by the ISO-639 language code, which you can combine with the ISO-3166 Country code, separated with an underline (“_”). For example, “fr” enables French; “en” and “en_US” specify U.S. English, where dates are formatted Month/Day/Year; “en_GB” specifies British English, where dates are formatted Day/Month/Year. The value “en_GB,fr,de,it” specifies that British English, French, German, and Italian are enabled.

- 4 Make sure that **Yes** is specified for **Enable Logout**. This is important because you need to log out of the Peregrine Portal and log back in for your changes to take effect.

Logging

You can use the Logging tab in the Admin Settings page to customize the logging of events in a server log file, whose default name is `archway.log`.

Common	Dashboard	DashboardDB	Email	Logging	Portal	Portal DB	ServiceCenter	Themes	Web Application	XSL
Logging										
Log domains:					Enter a semicolon-separated list of execution log traces you want to enable. Choices include:					
<input type="text"/>					<ul style="list-style-type: none"> • dll - Adapter DLL loading and unloading • weblication - Web Application and personalization rendering • jvm - Java run-time environment management and status • locks - Script synchronization locks • security - Archway security trace • statistics - administration statistics 					
Debug script:					When enabled, information regarding ECMA Script execution is written to the log. Be sure to turn this off in a production system.					
<input type="radio"/> Yes <input checked="" type="radio"/> No										
Show form info:					When selected, form information is displayed in each screen to aid during Web Application development and customization.					
<input type="radio"/> Yes <input checked="" type="radio"/> No										
Log file:					Enter a full directory path to the file used for logging.					
<input type="text" value="archway.log"/>										
Logging Format:					The logging format controls the printing pattern in a log file. The format is composed of literal text and conversion specifiers. The details of the specifiers can be found in the Apache Log4j documentation.					
<input type="text" value="%d %-5p [%t] %x - %m%n"/>										
Log Level:					Controls the level of detail in the log file. Possible values are: all, debug, info, warn, error, fatal and off.					
<input type="text" value="Information"/>										
Log File Rollover Frequency Pattern:					This setting controls the frequency at which the log file is rolled over. The pattern is also used as an extension to name non-active files. By default the log will roll over at midnight on the first day of each week. More information can be found in the Apache Log4j documentation.					
<input type="text" value=".'yyyy-w"/>										
Log Viewer Maximum Size:					This sets the maximum number of lines that the Administration log viewer will display.					
<input type="text" value="70"/>										

You can specify the following log traces in the Log domains field:

- dll - Adapter dll loading and unloading
- weblication - Web application and personalization rendering
- jvm - Java run-time environment management and status
- locks - Script synchronization locks

- security - Archway security trace
- statistics - Administration statistics

Logging format

You can specify in the Logging Format field the printing pattern of a log file. The logging format is composed of literal text and conversion specifiers. The details of the specifiers can be found in the following table, which can be found in its entirety, along with additional information, on the Apache.org web site at

<http://logging.apache.org/log4j/docs/api/org/apache/log4j/PatternLayout.html>.

Logging format table

Conversion character	Effect
c	<p>Used to output the category of the logging event. The category conversion specifier can be optionally followed by <i>precision specifier</i>, which is a decimal constant in brackets.</p> <p>If a precision specifier is given, then only the corresponding number of right-most components of the category name will be printed. By default the category name is printed in full.</p> <p>For example, for the category name “a.b.c” the pattern %c{2} is output as “b.c”.</p>
C	<p>Used to output the fully qualified class name of the caller issuing the logging request. This conversion specifier can be optionally followed by <i>precision specifier</i>, which is a decimal constant in brackets.</p> <p>If a precision specifier is given, then only the corresponding number of right most components of the class name will be printed. By default the class name is output in fully qualified form.</p> <p>For example, for the class name “org.apache.xyz.SomeClass”, the pattern %C{1} is output as “SomeClass”.</p> <p>Note: Generating the caller class information is slow. Avoid it unless execution speed is not an issue.</p>
d	<p>Used to output the date of the logging event. The date conversion specifier may be followed by a <i>date format specifier</i>, which is enclosed in braces, such as</p> <p>%d{HH:mm:ss,SSS}</p> <p>or</p> <p>%d{dd MMM yyyy HH:mm:ss,SSS}</p> <p>If no date format specifier is given then ISO8601 format is assumed.</p>
F	<p>Used to output the file name where the logging request was issued.</p> <p>Note: Generating caller location information is extremely slow. Avoid it unless execution speed is not an issue</p>

Conversion character	Effect
l [lower-case letter]	Used to output location information of the caller that generated the logging event. The location information depends on the JVM implementation, but usually consists of the fully qualified name of the calling method followed by the caller's source, the file name, and the line number enclosed in parentheses. Note: Though location information can be very useful, its generation is <i>extremely</i> slow. Avoid it unless execution speed is not an issue.
L	Used to output the line number from where the logging request was issued. Note: Generating caller location information is extremely slow. Avoid it unless execution speed is not an issue.
m	Used to output the application supplied message associated with the logging event.
M	Used to output the method name where the logging request was issued. Note: Generating caller location information is extremely slow. Avoid it unless execution speed is not an issue.
n	Outputs the platform-dependent line separator character(s), which offer practically the same performance as using non-portable line separator strings such as “\n” or “\r\n”. Thus, it is the preferred way of specifying a line separator.
P	Used to output the priority of the logging event.
r	Used to output the number of milliseconds elapsed between the time when the application started and the time of the logging event.
t	Used to output the name of the thread that generated the logging event.
x	Used to output the NDC (nested diagnostic context) associated with the thread that generated the logging event.

Conversion character	Effect
X	Used to output the MDC (mapped diagnostic context) associated with the thread that generated the logging event. The X conversion character <i>must</i> be followed by the key for the map placed between braces, as in: <code>%X{clientNumber}</code> where <i>clientNumber</i> is the key. The value in the MDC corresponding to the key will be output.
%	The sequence %% outputs a single percent sign.

The format of the log file is determined by the Apache PatternLayout class.

Log file rollover

You can specify in the Log File Rollover Frequency Pattern field the frequency with which the log file is rolled over. The pattern that you enter is also used as an extension to name non-active files. By default the log file rolls over at midnight on the first day of each week, and logs a maximum one week's data. However, you can specify that the log files roll over at the following intervals: monthly, weekly, half-daily, daily, hourly, or every minute. Use the parameters in the following table, which can be found in its entirety, along with additional information, on the Apache.org web site at <http://logging.apache.org/log4j/docs/api/org/apache/log4j/DailyRollingFileAppender.html>

Date pattern	Rollover schedule
'.'yyyy-MM	The beginning of each month
'.'yyyy-ww	The first day of each week, depending on the locale
'.'yyyy-MM-dd	At midnight each day
'.'yyyy-MM-dd-a	At midnight and midday of each day
'.'yyyy-MM-dd-HH	At the top of every hour
'.'yyyy-MM-dd-HH-mm	At the beginning of every minute

Log file rollover frequency is determined by the Apache DailyRollingFileAppender class.

Viewing the Server Log

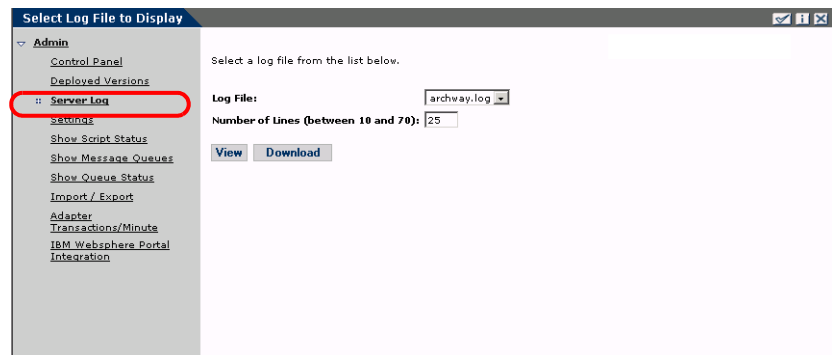
The Server Log provides a history of server events. The default file name is `archway.log`.

To view the Server Log

- 1 From the Activity menu, select **Server Log**.

A form opens with a drop-down list for you to select the log you want to view.

You can view the log file from your Web browser or download it to your preferred location.



- 2 Click the drop-down and select the log file you want to view.
- 3 Set the number of lines to view.
- 4 Do one of the following:
 - Click **View** to see the log file from your Web browser.
 - Click **Download** to initiate the File Download wizard that downloads the `archway.log` file to a location of your choice.

Verifying Script Status

The Script Status page lists the name and status of any script that is currently running.

To verify the script status

- 1 From the Administration Activity menu, click Show Script Status to display the Status of Scripts page that shows the name of each script.



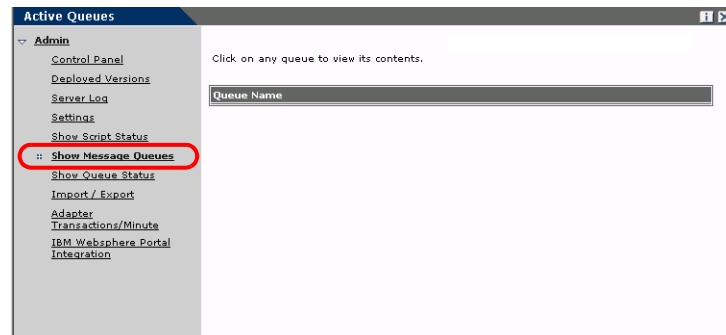
- 2 Click on the script to suspend it.

Displaying Message Queues

The Message Queues are displayed whenever a queue has data waiting to be transferred.

To display message queues:

- 1 From the Administration Activity menu, click Show Message Queues to display the Active Queues page.



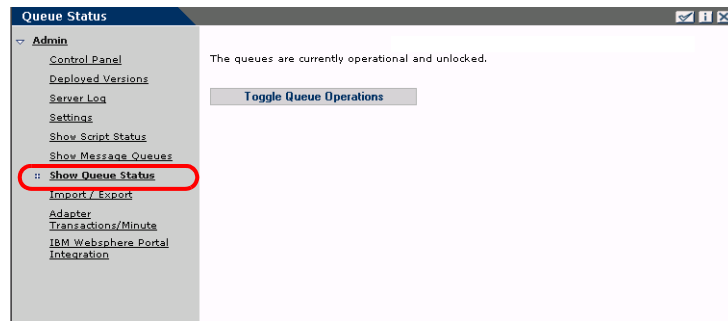
- 2 Click the queue name in the list to view the contents of a queue.

Showing Queue Status

Use the Show Queue Status option to verify or change the status of the message queues.

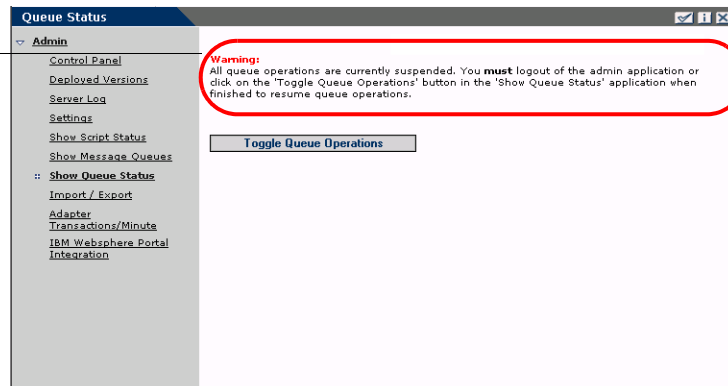
To show queue status

- 1 From the Activity menu, click **Show Queue Status** to open the Queue Status page.



- 2 Click **Toggle Queue Operations** to change the status to suspended.

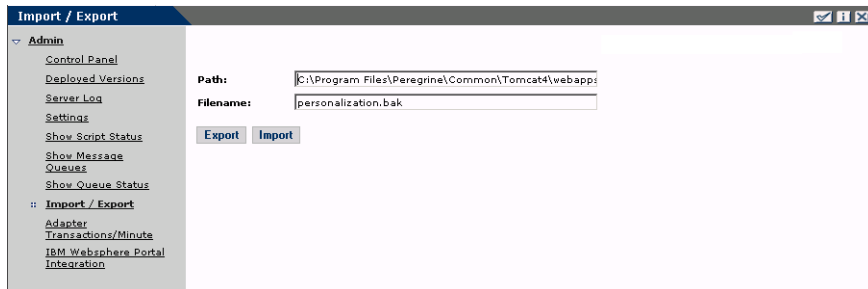
A warning message indicates that the Queue Status is suspended.



- 3 Click **Toggle Queue Operations** to return to the operational status.

Importing and exporting personalizations

You can move personalizations that you created in a development environment to a production environment. See the *Personalization* chapter in this guide for detailed instructions on importing and exporting the personalizations. Select the **Import/Export** option from the Admin activity menu to access the page.

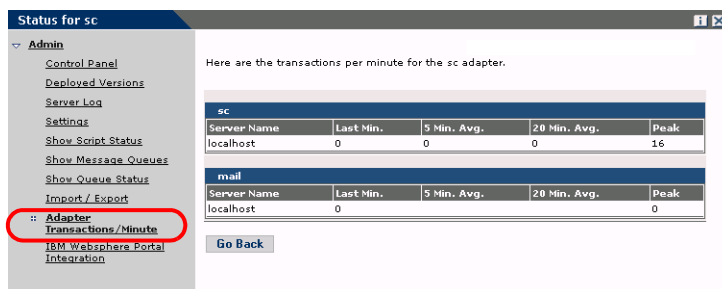


Viewing adapter transactions

You can track your adapter transactions by viewing the adapter Status page.

To view adapter transactions per minute

- ▶ From the Activity menu, click **Adapter Transactions/Minute** to open the adapter Status page.



Using the IBM Websphere Portal

You can generate an IBM Websphere Portal Server web archive (war) file configured with references to installed OAA portal components.

To generate a war file

- 1 From the Activity menu, click **IBM Websphere Portal Integration** to open the **Portal Integration** page.

IBM Websphere Portal Integration

An IBM Websphere Portal Server web archive configured with references to installed OAA portal components can be generated from this page. The websphere.war file found in the installed packages directory is copied and the portlet.xml file within is replaced. Make sure the base URL is the correct URL for accessing pages on this server. Take the generated file and install it using the IBM WPS Portal Administration utility. Anytime new OAA applications are installed, this process should be repeated to expose any new portal components in the IBM WPS environment.

Source Path: Enter the complete source path on the server where the installed websphere.war file can be located.

Destination Path: Enter the destination path on the server where the generated websphere.war file will be created.

Base URL: Enter the base URL of this server.

Generate WAR File

- 2 Enter the following information:
 - source path
 - destination path
 - base URL
- 3 Click **Generate WAR File**.

Displaying form information

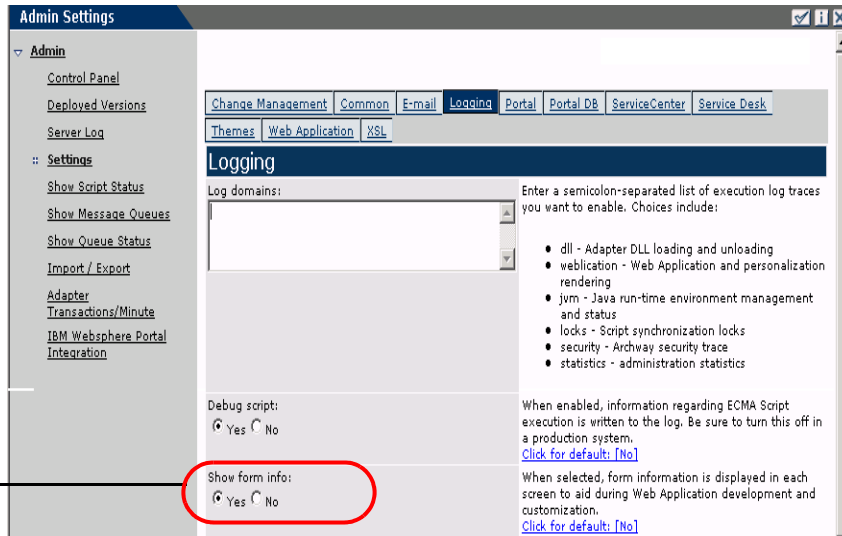
You can use the Admin module to configure Web application forms to display the location and file name of the current form.

To display form information:

- 1 From the Admin module, click **Settings**, then **Logging**.

2 Scroll to the Show form info field, and click Yes if necessary.

Set Show Form Info to Yes.



3 Click Save.

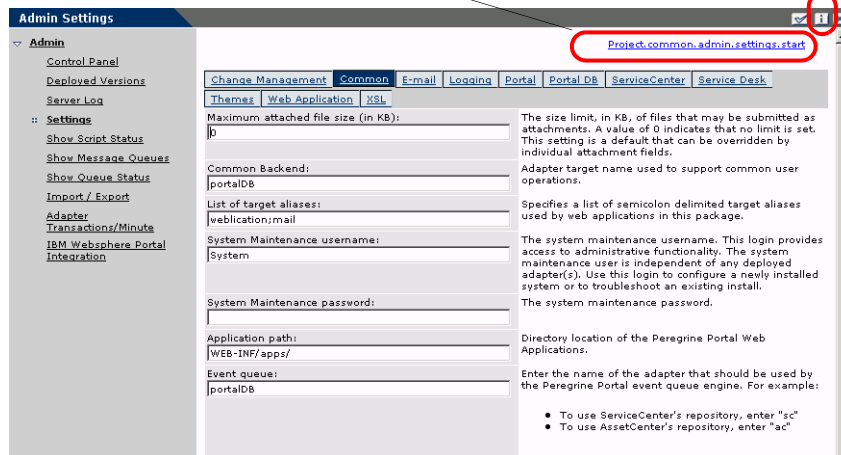
The Control Panel opens.

4 Click Reset Server.

The name of the form is at the top of each form.

The form name is at the top of the page.

Click the Display Form Info button to view the form composition.



Displaying form details

You can also display detailed information about the current form. Click the **Display Form Info** button at the top right of the form. A separate window opens.

View the contents in each tab for more information about the form.

```

Address http://hostname/oaas/display_form_info.htm
Script Input | Script Output | User Session | Log | PreXSL | Browser Source | BackChannel Source | Application Channel Source | Tab Source
Menu Source | Sync/Update Window | Help
<?xml version="1.0" encoding="UTF-8"?>
<_doc>
  <_docExplorerView>
  <_docExplorerModels>
  <_docExplorerContext>AdminSettings</_docExplorerContext>
  <_docExplorerInstance>
  <_docExplorerBackend>webication</_docExplorerBackend>
  <_docExplorerSubType>
  <_docExplorerAction>detail</_docExplorerAction>
  <_form>e_admin_settings_start.do</_form>
  <_module>common</_module>
  <_activity>admin</_activity>
  <_formname>start</_formname>
  <_return/>
  <_count>20</_count>
  <_tabs>
  <tab balloon="$$$IDS(common.configPortalLabel)" caption="$$$IDS(common.configPortalLabel)" url="e_admin_settings_start.do?target=portal/">
  <tab balloon="$$$IDS(common.configCommonLabel)" caption="$$$IDS(common.configCommonLabel)" url="e_admin_settings_start.do?target=common/">
  <tab balloon="$$$IDS(common.configProblemTabLabel)" caption="$$$IDS(common.configProblemTabLabel)" url="e_admin_settings_start.do?target=incidentmtg/>
  <tab balloon="$$$IDS(common.configPortalDBLabel)" caption="$$$IDS(common.configPortalDBLabel)" selected="true" url="e_admin_settings_start.do?target=portalDB/">
  <tab balloon="$$$IDS(common.configThemesLabel)" caption="$$$IDS(common.configThemesLabel)" url="e_admin_settings_start.do?target=themes/">
  <tab balloon="$$$IDS(common.configWebicationLabel)" caption="$$$IDS(common.configWebicationLabel)" url="e_admin_settings_start.do?target=webication/">
  <tab balloon="$$$IDS(common.configLoggingLabel)" caption="$$$IDS(common.configLoggingLabel)" url="e_admin_settings_start.do?target=logging/">
  <tab balloon="$$$IDS(common.configSLabel)" caption="$$$IDS(common.configSLabel)" url="e_admin_settings_start.do?target=sc/">
  <tab balloon="XSL" caption="XSL" url="e_admin_settings_start.do?target=xsl/">
  <tab balloon="$$$IDS(mailadapter.Label)" caption="$$$IDS(mailadapter.Label)" url="e_admin_settings_start.do?target=mail/">
  <tab balloon="$$$IDS(changerequestmtg.configChangeTabLabel)" caption="$$$IDS(changerequestmtg.configChangeTabLabel)" url="e_admin_settings_start.do?target=changemgt/">
  </_tabs>
  <_locale>en</_locale>
</_docExplorerModel>
</_doc>

```

The form has the following tabs.

This tab	Contains
Script Input	the script that sends a request to the back-end system.
Script Output	the information returned by the script request to the back-end system.
User Session	details about the current user session, including browser type, back-end system version, and the access rights established for this user.
Log	a list of actions taken by the script to execute the form.
PreXSL	output from XSL before it gets rendered to the browser.
Browser Source	HTML source code for the current page.
BackChannel Source	HTML source code for frames where the data is stored.
Application Channel Source	HTML source code for the shared applications.

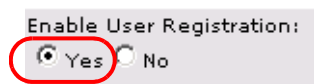
This tab	Contains
Tab Source	HTML source code for tabs.
Menu Source	HTML source code for menus.
Sync/Update Window	HTML source code to synchronize with the page and reload.
Help	Help for debugging the window.

User self-registration

With the Admin module, administrators can choose to have end users self-register for new accounts from the login screen if the user is not already in the ServiceCenter database. When the user registers, ServiceCenter creates an Operator record and a Contact record for the new user with basic user login rights. See the *Security* chapter in this guide for more information about the registration process.

To enable users to self-register from the Login screen

- 1 From the Admin module Settings page, click **Common**.
- 2 Scroll to **Enable User Registration**.



Click Yes to give users the ability to self-register for new accounts.

- 3 Click **Yes**.

Tip: When using an application with ServiceCenter 5.0 as the back-end system, the first name and last name are reversed in the ServiceCenter contact record from the format used in an OAA Platform application.

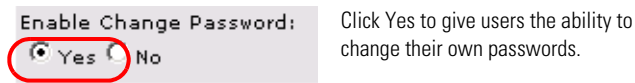
ServiceCenter 5.0 stores names in the format last name/first name. The OAA Platform stores names in the format first name/last name. As a temporary solution, you can change the way operator names are handled in ServiceCenter using the **Use Operator Full Name?** option in the Environment records for Incident and Service Managements. Refer to the *ServiceCenter 5.x Application Administration Guide* for instructions.

Changing passwords

Using the Admin module, administrators can choose to have end users change their own passwords from the Home page.

To enable users to change passwords:

- 1 From the Admin module Settings page, click **Common**.
- 2 Scroll to **Enable Change Password**.



- 3 Click **Yes**.

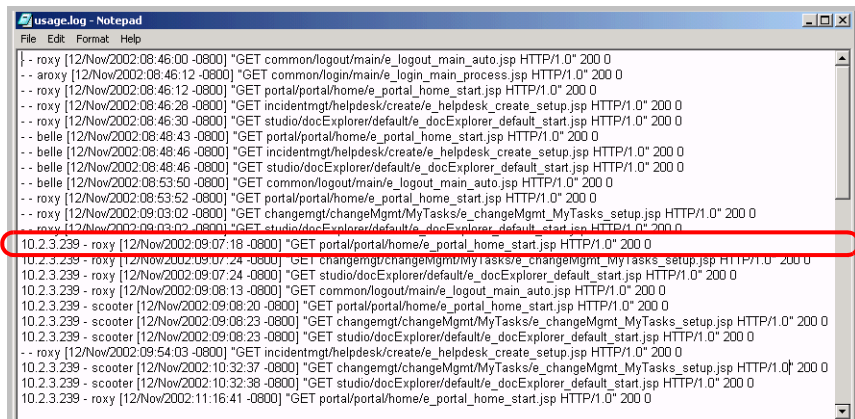
Logging and monitoring user sessions

The `usage.log` file has a record of user logins that is in the `bin` directory of your application server installation. With this file, you can determine which application is in use and how many users access an application during a day.

Understanding the `usage.log` file

The following line shows an excerpt from a `usage.log` file:

```
10.2.3.239 - roxy [12/Nov/2002:09:07:18 -0800] "GET
portal/portal/home/e_portal_home_start.jsp HTTP/1.0" 200 0
```



```
usage.log - Notepad
File Edit Format Help
{ - roxy [12/Nov/2002:08:46:00 -0800] "GET common/logout/main/e_logout_main_auto.jsp HTTP/1.0" 200 0
-- roxy [12/Nov/2002:08:46:12 -0800] "GET common/login/main/e_login_main_process.jsp HTTP/1.0" 200 0
-- roxy [12/Nov/2002:08:46:12 -0800] "GET portal/portal/home/e_portal_home_start.jsp HTTP/1.0" 200 0
-- roxy [12/Nov/2002:08:46:28 -0800] "GET incidentmgmt/helpdesk/create/e_helpdesk_create_setup.jsp HTTP/1.0" 200 0
-- roxy [12/Nov/2002:08:46:30 -0800] "GET studio/docExplorer/default/e_docExplorer_default_start.jsp HTTP/1.0" 200 0
-- belle [12/Nov/2002:08:48:43 -0800] "GET portal/portal/home/e_portal_home_start.jsp HTTP/1.0" 200 0
-- belle [12/Nov/2002:08:48:46 -0800] "GET incidentmgmt/helpdesk/create/e_helpdesk_create_setup.jsp HTTP/1.0" 200 0
-- belle [12/Nov/2002:08:48:46 -0800] "GET studio/docExplorer/default/e_docExplorer_default_start.jsp HTTP/1.0" 200 0
-- belle [12/Nov/2002:08:53:50 -0800] "GET common/logout/main/e_logout_main_auto.jsp HTTP/1.0" 200 0
-- roxy [12/Nov/2002:08:53:52 -0800] "GET portal/portal/home/e_portal_home_start.jsp HTTP/1.0" 200 0
-- roxy [12/Nov/2002:09:03:02 -0800] "GET changemgt/changeMgmt/MyTasks/e_changeMgmt_MyTasks_setup.jsp HTTP/1.0" 200 0
-- roxy [12/Nov/2002:09:03:02 -0800] "GET studio/docExplorer/default/e_docExplorer_default_start.jsp HTTP/1.0" 200 0
10.2.3.239 - roxy [12/Nov/2002:09:07:18 -0800] "GET portal/portal/home/e_portal_home_start.jsp HTTP/1.0" 200 0
10.2.3.239 - roxy [12/Nov/2002:09:07:24 -0800] "GET studio/docExplorer/default/e_docExplorer_default_start.jsp HTTP/1.0" 200 0
10.2.3.239 - roxy [12/Nov/2002:09:08:13 -0800] "GET common/logout/main/e_logout_main_auto.jsp HTTP/1.0" 200 0
10.2.3.239 - scooter [12/Nov/2002:09:08:20 -0800] "GET portal/portal/home/e_portal_home_start.jsp HTTP/1.0" 200 0
10.2.3.239 - scooter [12/Nov/2002:09:08:23 -0800] "GET changemgt/changeMgmt/MyTasks/e_changeMgmt_MyTasks_setup.jsp HTTP/1.0" 200 0
10.2.3.239 - scooter [12/Nov/2002:09:08:23 -0800] "GET studio/docExplorer/default/e_docExplorer_default_start.jsp HTTP/1.0" 200 0
-- roxy [12/Nov/2002:09:54:03 -0800] "GET incidentmgmt/helpdesk/create/e_helpdesk_create_setup.jsp HTTP/1.0" 200 0
10.2.3.239 - scooter [12/Nov/2002:10:32:37 -0800] "GET changemgt/changeMgmt/MyTasks/e_changeMgmt_MyTasks_setup.jsp HTTP/1.0" 200 0
10.2.3.239 - scooter [12/Nov/2002:10:32:38 -0800] "GET studio/docExplorer/default/e_docExplorer_default_start.jsp HTTP/1.0" 200 0
10.2.3.239 - roxy [12/Nov/2002:11:16:41 -0800] "GET portal/portal/home/e_portal_home_start.jsp HTTP/1.0" 200 0
```

Each login is on a line. Within one user session, each module logs only one line.

The following table shows the meaning of each element in the log entry.

Remote Host	Rfc931	User Login	Date	Request	Status	Bytes
10.2.3.239	-	roxy	[12/Nov/2002:09:07:18 -0800]	"GET portal/portal/home/e_portal_home_start.jsp HTTP/1.0"	200	0

This element	Contains
Remote Host	the remote host name or IP address if the DNS host name is not available or was not provided.
Rfc931	the remote login name of the user. This is always a dash because this information is not needed.
User Login	the user name authenticated to log in to the Peregrine Portal.
Date	the date and time of the request.
Request	the module accessed by the user. The name of the module is the first part of the GET parameter. In the previous above, the module accessed is <i>notificationsservices</i> , the location of the login script.
Status	the HTTP response code returned to the client. This value is always 200 to specify that it was a valid request.
Bytes	the number of bytes transferred. The number is always entered as 0, because this information is not needed.

BI Portal administration

For some BI Portal administrative tasks, you need to use the OAA Administration page.

Setting the PortalDB adapter

BI Portal lets you personalize portal application screens without manually changing and compiling code. To enable this feature, BI Portal requires a database adapter connection to store portal settings and customizations in the back-end database. Until a database adapter is defined for the portal page, users cannot see or make personalizations to the Peregrine Portal home page.

To configure BI Portal to save personalization settings in the ServiceCenter back-end database:

- 1 From the Peregrine Portal Admin module, click **Settings**.
- 2 At the top of the Settings page, click the **Portal DB** tab.

This displays the Portal Database settings page.

The screenshot shows the 'Portal DB' configuration page. At the top, there is a navigation bar with tabs: BI, Common, E-mail, Logging, Portal, Portal DB (selected), ServiceCenter, Themes, Web Application, and XSL. Below the tabs, there are two main sections. The first section is 'Default capabilities:' with a text input field containing 'portalDB(getit.portal;getit.home;getit.content;getit.layo'. To the right of this field is a tooltip that reads: 'Semicolon separated list of default access rights that should have regardless of their profile. Access rights assigned to target adapters in the following way: po (getit.portal)'. The second section is 'Alias for:' with a text input field containing 'sc'. To the right of this field is a tooltip that reads: 'Specifies the target configuration for which this target alias.' Below the tooltip is a link: 'Click for default: []'. At the bottom left of the form is a 'Save' button.

- 3 In the **Alias for** field type `sc`. Then click **Save** to return to the Admin Control Panel page.
- 4 Click **Reset Server** at the bottom of the page to apply your changes to the system.
- 5 When the operation completes, verify that the adapter used for the **portalDB** target is `com.peregrine.oaa.adapter.sc.SCAdapter` and displays “Connected” in the Connection Status table.

Important: If you specify one alias and subsequently change that alias, you lose the personalizations of your portal application screens.

Using the BI Portal Administration page

You can setup and configure the connections to Business Objects (BO) and ServiceCenter (SC) using the BI Administration link on the Activity menu or using the BI tab on the OAA Administration page. The BI Administration links leads you through a sequence of configuration and settings pages where

you can test the configuration settings as you proceed through each page. The BI tab provides all of the settings in a single, scrollable page but does not enable you to test the configuration settings and does not support any error messaging in cases where connections fail. Initially at least, you should use the BI Administration function to setup your configuration.

There are four BI Portal administrative functions that need to be setup and verified for connections and configurations required for using BI Portal with Business Objects (BO) and ServiceCenter (SC). These functions are accessed sequentially from the BI Portal Administration tab. They are:

- Reporting Data Store (RDS) Database Settings
- Business Object Repository Database Settings
- BI Portal Portal Settings
- Business Objects Admin and BI Portal Apps Settings

The BI Portal Administration function provides a Test, Restore, and Save button for each of these functions.

- Test button - Test the settings as they are presented on the form. (They may not have saved.) Testing ok does not mean that the settings are saved.
- Restore button - Restore all settings to the values that were last saved.
- Save button - Save the current setting as they are presented on the form. They may not have tested. They are saved in the local.xml.

There are also navigation buttons.

- Back button - Go back to the previous BI Configuration page.
- Next button - Go to the next BI Configuration page in the sequence.
- Finish button - Go to the Control Panel of the Administration module.

To access the BI administration functions

- 1 Login to the Peregrine Portal Admin page.
`http://host/oa/admin.jsp`
- 2 Click **BI Administration** in the Activity menu.

The RDS Database Settings page opens.

You can now begin the sequence of setting up and configuring BI Portal.

To configure RDS database settings

- 1 Set the RDS Database Type. (required)

Note that as you select different database types, the contents of the JDBC drivers and JDBC URL sample field showing examples of JDBC URLs changes. The examples in the this field provide suggestions of how to correctly set the JDBC URL.

- 2 Type the RDS Database User Name. (required)
- 3 Type the RDS Database User Password. (required)
- 4 Type the JDBC Driver. (required)
- 5 Type the JDBC URL. (required)

Note: You can copy the sample URL in the example text box and paste it into the JDBC URL field to create the appropriate syntax and then change only those portions of the JDBC URL necessary for your configuration.

- 6 Click **Test** to test the connection to the RDS database.

The status of the test appears on the top of the form. If you are satisfied with the test you can save these settings or wait until you have completed the entire configuration sequence.

- 7 Click **Save** if you wish to save your settings at this point in the process.
- 8 Click **Next** to continue the configuration process.

The Business Object (BO) Repository (Security) Settings page opens.

- 9 Select the database type for the BO Security Database Type.

Note that as you select different database types, the contents of the JDBC drivers and JDBC URL sample field showing examples of JDBC URLs changes. The examples in the this field provide suggestions of how to correctly set the JDBC URL.

- 10 Type the BO Security Database User Name. (required)
- 11 Type the BO Security Database User Password. (required)
- 12 Type the JDBC Driver. (required)
- 13 Type the JDBC URL. (required)

Note: You can copy the sample URL in the example text box and paste it into the JDBC URL field to create the appropriate syntax and then change only those portions of the JDBC URL necessary for your configuration.

- 14 Click Test to test the connection to the specified database.

The status of the test appears on the top of the form. If you are satisfied with the test you can save these settings or wait until you have completed the entire configuration sequence.

- 15 Click Save if you wish to save your settings at this point in the process.
- 16 Click Next.

The BI Portal Settings page opens.

- 17 Enter numeric values for the following fields. An entry is required for each field.

Setting Label	Default Value	Description
Data Security Refresh Interval	3600	A value in seconds. Business Objects data security definition is extracted and saved into the RDS repository at the specified interval defined by this setting. (For additional information see <i>Chapter 6 - BI Portal Administrator Functions, Viewing and synchronizing data security.</i>)
RDS Log Table Purge Interval	3600	A value in seconds. The log table of the RDS database is purged periodically, at the specified interval defined by this setting

Setting Label	Default Value	Description
User Synchronization Interval	900	<p>A value in seconds. This is the number of seconds before the RDS database is polled for modified users and to update their roles in Business Object security domain. This interval is for synchronizing user's data, automatically.</p> <p>Note: This interval should match the <code>rds_user sync</code> interval set in the Connect-It Service console.</p> <p>(For additional information see <i>Chapter 6 - BI Portal Administrator Functions, Synchronizing users and Scheduling automatic data synchronization.</i>)</p>
BO Admin Server Refresh Interval	1800	<p>A value in seconds. BO administration session is refreshed at the specified interval defined by this setting. This essentially keeps BO administration session alive while BI Portal is in operation.</p>

- 18 Click **Save** if you wish to save your settings at this point in the process.
- 19 Click **Next**.

The Business Objects Administration/ BI Portal Application Settings page opens.

Administration

Business Objects (BO) Administration/BI Portal Application Settings

BI Administration

Admin

- Control Panel
- Deployed Versions
- Server Log
- Settings
- Show Script Status
- Show Message Queues
- Show Queue Status
- Show Script Status
- Show Message Queues
- Show Queue Status
- Show Script Status
- Show Message Queues
- Show Queue Status
- Show Script Status
- Show Message Queues
- Show Queue Status
- Import / Export
- Adapter Transactions/Minute
- IBM Websphere Portal Integration

Please enter changes to your BO Admin settings as well as BI Portal Application settings. If you have an active BI you may update the cluster name, but you will not be able to test the BO settings nor the BIP application setting: Peregrine Portal Application server. Click the Test button to verify the settings. Click the Restore button to reset saved values. Click the Save button to save settings. Click the Finish button to go back to Admin Control Panel to BI configuration will not take effect until Peregrine Portal Application server is reset.

BO Administration Settings

Currently Connected BO ORB Cluster Name: mycluster

New BO ORB Cluster Name: mycluster

Business Entity Name: prgn

BI Portal Group Name: twbip

BO Document Domain Name: tw_document

BO Supervisor Name: tw_supervisor

BO Supervisor Password: *****

BO Designer User Name: tw_designer

BO Designer Password: *****

Broadcast Agent (BCA) Name: tw_bca

Broadcast Agent (BCA) Password: *****

Enable BCA Scheduler:

Yes:

No:

Enable Security Indicator:

Yes:

No:

BI Portal Application Settings

Group Name: sc

Back Test Save Restore Finish

20 Type the associated text for the following fields. An entry is required for each text field.

Note: These entries are based on the names you entered in the Supervisor tool when you created the Business Objects Repository structure. You should verify that the names you enter here match the names you used during installation from the Installation checklist.

- New BO Object Request Broker (ORB) Cluster Name
- Business Entity Name (maximum of 35 characters)
- BI Portal Group Name (maximum of eight characters)
- BO Document Domain Name
- BO Supervisor Name

- f BO Supervisor Password
- g BO Designer User Name
- h BO Designer Password
- i Broadcast Agent (BCA) Name
- j Broadcast Agent (BCA) Password

21 Select **Yes** or **No** for Enable BCA Scheduler.

22 Select **Yes** or **No** for Enable Security Indicators.

If security is enabled, everytime a user logs into the Portal or opens a document, a refresh occurs automatically. If security is disabled, the user has to manually refresh a document; otherwise, the document shows the last refreshed data. If the user has data level security, any document related to the restricted data is not displayed to the user **only after** the user tries to refresh that document.

23 In the BI Portal Applications Setting section type the Group Name for sc (ServiceCenter).

24 Click **Test** to validate your configuration settings.

The following list includes some of the messages that may appear at the top of the page after you test your configuration settings.

- Business Objects cluster configuration was successfully validated.
- Failed to validate Business Objects Admin settings.
- Failed to validate BI Portal application settings for ServiceCenter cannot establish binding.
- Please verify that the Business Objects server is currently running.
- If you changed the cluster name, you need to restart Peregrine Portal before the new cluster can be active.

These messages indicate that something went wrong with the Business Objects server. Various parts of the Business Objects Administration settings failed to validate. The user is advised to check the status of the Business Objects server. Most likely, either the Business Objects server is not running or it is in state that only can be corrected by a restart.

25 Click the **Finish** button.

When you click the Finish button, all of the configuration changes you have made are saved to `local.xml`. Additionally, you are returned to the Admin Settings page where you can reset the server.

BI tab

The BI tab displays all of the configuration settings for BI Portal on a single page. On this page you can reset any of the settings and then click Save at the bottom of the page to update the settings. This page is useful for viewing the current settings and quickly seeing settings that may be incorrect. The following figures show settings on the BI tab.

To access the BI tab

- 1 Click **Settings** under the Admin Activity menu.
- 2 Click the **BI** tab.

The BI tab opens.

BI	Common	E-mail	Logging	Portal	Portal DB	ServiceCenter	Themes	Web Application	XSL
BI/targets:									
sc									
Business Objects Admin Settings									
Business Entity Name:		Please enter the business entity name. Click for default: []							
prgn									
BI Portal Group Name:		Name of the BO Group for BI Portal Click for default: []							
prgnbip									
BO Document Domain Name:		Please enter Name of the Document Domain in BO. Click for default: []							
docdomain									
BO ORB CLUSTER NAME:		Please enter Name of the BO Cluster. Click for default: [mycluster]							
my_cluster									
BO Supervisor Name:		Please enter the BO Repository Supervisor User name. Click for default: []							
bisupervisor									
BO Supervisor Password:		Please enter the BO Repository Supervisor User's Password. Click for default: [*****]							

BO Designer User Name:		Name of the BO User with Designer Profile for BI Portal Click for default: []							
bidesigner									
BO Designer Password:		Password of the BO User with Designer Profile for BI Portal Click for default: [*****]							

BroadCastAgent (BCA) Name:		Please enter the BO Repository BroadCastAgent User name. Click for default: []							
bca									
BroadCastAgent (BCA) Password:		Please enter the BO Repository BroadCastAgent's Password. Click for default: [*****]							

Enable BCAScheduler:		A 'true' or 'false' value. A true value indicates BCA Scheduler is enabled.							
<input type="radio"/> Yes <input checked="" type="radio"/> No									
Enable Security Indicator:		A 'true' or 'false' value. A true value indicates Data Level Security is on.							
<input type="radio"/> Yes <input checked="" type="radio"/> No									
BI Portal SC Application Settings									
GroupName:		Name of the BO Group for ServiceCenter Application. Click for default: []							
sc									

Business Objects(BO) Repository (Security) Database Settings

BO Security Database Type: Oracle	Name of the Database Management System on which BO security repository database exists.
BO Security Database User Name: bisecurity	User name to log into the BO security repository database. Click for default: [bisecurity]
BO Security Database User Password: *****	Password for the BO Security Repository Database User. Click for default: [*****]
JDBC Driver: oracle.jdbc.driver.OracleDriver	JDBC Driver Class for BO Security Repository Database. For example: <ul style="list-style-type: none"> Oracle "oracle.jdbc.driver.OracleDriver" DB2 "COM.ibm.db2.jdbc.app.DB2Driver" MSSQLServer Driver "com.microsoft.jdbc.sqlserver.SQLServerDriver" Sprinta Driver "com.inet.tds.TdsDriver"
JDBC URL: jdbc:oracle:thin:@bi-repo:1521:birepo	JDBC URL for BO Security Repository Database. For example: <ul style="list-style-type: none"> Oracle Native Driver Url "jdbc:oracle:oci8:@TNS_ALIS" Oracle Thin Driver Url "jdbc:oracle:thin:@HOSTNAME:1521:SERVICE_NAME" DB2 Driver Url "jdbc:db2:DB2_ALIAS" MSSQLServer Driver Url "jdbc:microsoft:sqlserver://HOSTNAME:1433;datasename=DATABASE_NAME" Sprinta Driver Url "jdbc:inetdae7:HOSTNAME:PORT?database=DATABASE_NAME" Click for default: [jdbc:oracle:thin:@HOSTNAME:1521:SERVICE_NAME]

RDS Database Settings

RDS Database Type: Oracle	Name of the Database Management System on which Reporting Data Store exists.
RDS Database User Name: rds_dba	User name to log into the RDS database.
RDS Database User Password: *****	Password for the RDS Database User. Click for default: [*****]
JDBC Driver: oracle.jdbc.driver.OracleDriver	JDBC Driver Class for RDS Database. For example: <ul style="list-style-type: none"> Oracle "oracle.jdbc.driver.OracleDriver" DB2 Driver "COM.ibm.db2.jdbc.app.DB2Driver" MSSQLServer Driver "com.microsoft.jdbc.sqlserver.SQLServerDriver" Sprinta Driver "com.inet.tds.TdsDriver"
JDBC URL: jdbc:oracle:thin:@bi-repo:1521:birepo	JDBC URL for RDS Database. For example: <ul style="list-style-type: none"> Oracle Native Driver Url "jdbc:oracle:oci8:@TNS_ALIS" Oracle Thin Driver Url "jdbc:oracle:thin:@HOSTNAME:1521:SERVICE_NAME" DB2 Driver Url "jdbc:db2:DB2_ALIAS" MSSQLServer Driver Url "jdbc:microsoft:sqlserver://HOSTNAME:1433;datasename=DATABASE_NAME" Sprinta Driver Url "jdbc:inetdae7:HOSTNAME:PORT?database=DATABASE_NAME" Click for default: [jdbc:oracle:thin:@HOSTNAME:1521:SERVICE_NAME]

BI Portal Settings

User Synchronization Interval: 900	A value in seconds. RDS database is polled for modified users to update their roles in Business Objects Repository.
RDS Log Table Purge Interval: 3600	A value in seconds. RDS's log table is purged periodically, at the specified interval.
Data Security Refresh Interval: 300	A value in seconds. BO Data Security Definition is extracted and saved into RDS repository, at the specified interval. Click for default: [3600]
BO Admin Server Refresh Interval: 1800	A value in seconds. BO Administration Session is refreshed periodically, at the specified interval.
<input type="button" value="Save"/>	

5 Security

CHAPTER

This chapter describes the different security configuration options available in BI Portal. Topics in this chapter include:

- *Password encoding methods* on page 78
- *User registration* on page 79
- *Authenticating users* on page 80
- *Default security configuration* on page 80
- *Custom JAAS configuration* on page 81
- *Standard Sun Microsystems JAAS configuration* on page 90
- *Integrated Windows Authentication* on page 91
- *Integrating with single sign-on tools* on page 100
- *Contact-based authentication* on page 105
- *Creating an alternate login page* on page 114
- *BI Portal security overview* on page 116

Password encoding methods

By default, BI Portal does not encode passwords sent over the network. BI Portal sends plain text passwords to the authenticating back-end databases and stores plain text passwords in a browser cookie if the user selects to **enable automatic login**. If you want to secure your BI Portal passwords, you have three options:

- Enable Secure Sockets Layer (SSL) on your Web server
- Configure BI Portal to use a directory service such as LDAP
- Enable your Web server to use Windows NT Challenge/Response

In order to use SSL, you need to acquire a digital certificate. If your Web server has a certificate, then your BI Portal login URL must include the **https** protocol indicator. After the user browser has made a secure connection to the Web server, all data transferred is encrypted. Refer to your Web server documentation for information on configuring SSL.

BI Portal also supports authentication via a directory service such as LDAP. When you authenticate to a directory service, BI Portal passes SHA hash encoding passwords to the service. For instructions configuring a directory service see *Custom JAAS configuration* on page 81.

BI Portal also supports Integrated Windows Authentication. When this form of authentication is used, passwords are not actually exchanged between the browser and Web server, and the authentication process is kept secure. However, Integrated Windows Authentication is only supported by Internet Explorer browsers on Windows systems. For instructions configuring Integrated Windows Authentication see *Integrated Windows Authentication* on page 91.

User registration

All BI Portal users need a login account. If a user is attempting to log in for the first time, the user is prompted for certain default information as shown in the following page. The first four fields are required, as indicated by the arrows to the right of each field.

When the user clicks **Register**, the information is stored in the appropriate database.

Basic registration information and login scripts are stored in the `.../oaa/apps/common/jscript/` directory. Login scripts are in the `login.js` file. If you want to make changes to the registration process, such as changing the way a user's password is defined, you can change the scripts in this directory.

After the user is registered, that user in ServiceCenter must be given BI capabilities in order access to the BI Reporting module. BI capabilities are `BI_Access`, which is mandatory and one of the following: `BI_Admin`, `BI_Create`, `BI_View`.

Authenticating users

You can configure the Peregrine OAA Platform to use one of five security authentication options:

- Use the default configuration to authenticate users against Peregrine adapters. See *Default security configuration* on page 80.
- Use a custom configuration to authenticate users against user-defined adapters such as LDAP or JDBC compliant databases. See *Custom JAAS configuration* on page 81.
- Use a standard JAAS configuration to authenticate users against the Sun Microsystem's standard Java Authentication and Authorization Service (JAAS). See *Standard Sun Microsystems JAAS configuration* on page 90.
- Use Integrated Windows authentication to authenticate users and pass the information to the Web application. See *Integrated Windows Authentication* on page 91.
- Use an alternate login page and authenticate users against any of the other login options. See *Creating an alternate login page* on page 114.

Once a user is authenticated, the modules to which the user has access are defined by the back-end system. If you are using ServiceCenter for the back-end system, the user must have the appropriate capability words set in the Operator record in ServiceCenter in order to see the corresponding module in the web application.

Default security configuration

The default configuration authenticates users against a set of pre-configured JAAS login modules. By default, one JAAS login module is configured for each registered Peregrine adapter. For example, if you are using both AssetCenter and ServiceCenter, then BI Portal creates login modules for *both* the ACAdapter and the SCAdapter.

These login modules are *only* used to authenticate users. User access rights are derived from user profile records in the back-end systems (for example, ServiceCenter or AssetCenter). User access rights determine which modules the user can access and what tasks they can perform within those modules. For example, one user can open tickets only, while another has rights to approve tickets as well.

You do not have to do any additional configuration to use the default security configuration. BI Portal automatically generates login modules for each Peregrine adapter installed on the system.

The default login module settings are:

- loginModule=com.peregrine.OAA.security.OAALoginModule
- control flag=OPTIONAL
- options=<none>

Custom JAAS configuration

A custom JAAS configuration authenticates users against a set of JAAS LoginModules you define in a `local.xml` file. This file contains the settings to use for each JAAS LoginModule. A `<jaas_config>` entry in `local.xml` has the following format.

```
<jaas_config>

  <jaasConfiguration>CustomConfig</jaasConfiguration>
  <CustomConfig>adapter1;adapter2</CustomConfig>

  <adapter1>
    <loginModule>Java class of login module</loginModule>
    <controlFlag>authentication behavior</controlFlag>
    <options>semicolon separated list of options</options>
  </adapter1>

  <adapter2>
    <loginModule>Java class of login module</loginModule>
    <controlFlag>authentication behavior</controlFlag>
    <options>semicolon separated list of options</options>
  </adapter2>

</jaas_config>
```

The following table describes how to use the XML tags and assign appropriate values.

Important: XML is case sensitive.

Use these XML tags	To do this
<pre><jaas_config> </jaas_config></pre>	Define a custom JAAS configuration. All JAAS configuration settings must be between these two tags.
<pre><jaasConfiguration> </jaasConfiguration></pre>	Define the name of your custom JAAS LoginModule. The value of this tag determines the tag name to use for the next tag. For example, if you create a custom configuration with the value <code>CustomConfig</code> , then you must use the tags <code><CustomConfig></code> and <code></CustomConfig></code> to define the list of adapters used.
<pre><CustomConfig> </CustomConfig></pre> <p><i>This is a user definable tag</i></p>	Define the list of <i>all</i> adapters that you want to use for authentication. Use semicolons between entries to specify multiple adapters. If the adapter name you list does not match a registered AdapterPool, then BI Portal assumes the name is the logical name of a non-OAA LoginModule. BI Portal attempts to authenticate users against each adapter you list. The values listed in this tag determine the tags names to use for each adapter. For example, if you create two adapters <code>adapter1</code> and <code>adapter2</code> , then you must use the tags <code><Adapter1></code> , <code></Adapter1></code> , <code><Adapter2></code> , and <code></Adapter2></code> to define your adapters.
<pre><adapter1> </adapter1> <adapter2> </adapter2></pre> <p><i>These are user definable tags</i></p>	Define the JAAS LoginModule settings for each adapter. Each adapter <i>must</i> have both <code><loginModule></code> and <code><controlFlag></code> tags defined for it.

Use these XML tags	To do this
<code><loginModule> </loginModule></code>	<p>Define the fully qualified class name of the JAAS LoginModule.</p> <p>This is <i>required</i> only when authenticating against non-OAA LoginModules (adapters). The default value is <code>com.peregrine.oaa.archway.security.OAALoginModule</code>.</p> <p>This is <i>optional</i> only when authenticating against Peregrine back-ends.</p>
<code><controlFlag> </controlFlag></code> This tag is <i>optional</i> .	<p>Define the authentication behavior of this LoginModule. The default value is REQUIRED.</p> <p>See <i>JAAS LoginModule control flags</i> on page 83 for a description of available options.</p>
<code><options> </options></code>	<p>Define the list of authentication options. Use semicolons between entries to specify multiple options. This is an <i>optional</i> setting for each JAAS LoginModule you use. See <i>JAAS configuration options</i> on page 86 for a description of available options.</p>

JAAS LoginModule control flags

The following table lists the possible settings for the `<controlFlag>` tag. A JAAS LoginModule can have one of four behaviors:

Control flag	Authentication behavior
REQUIRED	If the user cannot be authenticated against the adapter, the login fails. Whether it succeeds or fails, authentication continues to the next LoginModule in the list.
REQUISITE	If the user cannot be authenticated against the adapter, the login fails. If it succeeds, authentication continues to the next LoginModule in the list.

Control flag	Authentication behavior
SUFFICIENT	Authentication can proceed even if this LoginModule fails. If it succeeds, authentication does not continue to the next LoginModule in the list. If it fails, authentication continues to the next LoginModule in the list.
OPTIONAL	Authentication can proceed even if this LoginModule fails. Whether it succeeds or fails, authentication continues to the next LoginModule in the list. This is the default behavior.

Note: The controlFlag settings are case insensitive.

The overall authentication succeeds only if all Required and Requisite LoginModules succeed. If a Sufficient LoginModule is configured and succeeds, then only the Required and Requisite LoginModules prior to that Sufficient LoginModule need to have succeeded for the overall authentication to succeed. If no Required or Requisite LoginModules are configured for an application, then at least one Sufficient or Optional LoginModule must succeed.

By default, the controlFlag setting of all BI Portal Web applications LoginModules is Optional. For most enterprises, this is the desired configuration.

The following table shows some sample scenarios and how the login process works.

Module Name	Status	Scenario 1	Scenario 2	Scenario 3
LoginModule1	required	pass	pass	fail
LoginModule2	sufficient	fail	fail	fail
LoginModule3	requisite	pass	pass	pass
LoginModule4	optional	pass	fail	fail
Final Authentication		pass	pass	fail

In Scenario 1, authentication succeeds even though LoginModule2 fails. This is because the Required loginModule takes precedence over the sufficient loginModule.

In Scenario 2, authentication succeeds because the loginModules that failed are only Sufficient and Optional.

Scenario 3 authentication fails because a loginModule with a status of Required failed.

JAAS configuration options

The following tables list the possible settings for the <options> tag.

Standard JAAS Options

The following table lists the standard JAAS options available for all adapters.

Option	Use	Description
debug=true	optional	Instructs a LoginModule to output debugging information. The OAALoginModule logs debugging information to stdout and not to archway.log .
tryFirstPass=true	optional	The first LoginModule in the list saves the password entered and this password is used by subsequent LoginModules. If authentication fails, the LoginModules prompt for a new password and repeats the authentication process.
useFirstPass=true	optional	The first LoginModule in the list saves the password entered and this password is used by subsequent LoginModules. If authentication fails, LoginModules do not prompt for a new password.
storePass=true	optional	Stores the password for the user being authenticated.
clearPass=true	optional	Clears the password for the user being authenticated.

Peregrine JndiLoginModule options

The following table lists the options available to custom JAAS LoginModules using the Peregrine JndiLoginModule.

Note: The Peregrine JAAS LoginModule `com.peregrine.oaa.security.JndiLoginModule` is modeled after Sun's `JndiLoginModule`. The main difference is that an RFC 2307 (NIS over LDAP) compliant schema is not required. User must have “uid” and “userPassword” properties defined.

Option	Use	Description
<code>user.provider.url</code>	required	<p>Use this option to provide the URL to the starting point in your directory service where you want to search for users.</p> <p>For example, <code>ldap://server/dc=peregrine,dc=com</code></p> <p>Note: This option corresponds to the Java constant <code>Context.PROVIDER_URL</code>.</p>
<code>security.principal</code>	optional	<p>Use this option to specify which directory service user you want to use to authenticate non-anonymous queries of your directory service. Use the DN of the directory service user. For example, <code>uid=user,dc=peregrine,dc=com</code></p> <p>Tip: To prevent user passwords from being visible to users, you should only set this option if you are using a directory server such as IPlanet where user passwords are SHA hashed by default.</p> <p>Note: This option corresponds to the Java constant <code>Context.SECURITY_PRINCIPAL</code>.</p>

Option	Use	Description
security.credentials	optional	<p>Use this option to define the password for the <code>security.principal</code> user. This option should only be used in conjunction with the <code>security.principal</code> option.</p> <hr/> <p>Important: If you are using a simple security authentication protocol, then this password may be passed as plain text.</p> <hr/> <p>Tip: To safeguard this password, either enable SSL (set the <code>security.protocol=ssl</code> option) or use an <code>security.authentication</code> that protects passwords.</p> <p>Note: This option corresponds to the Java constant <code>Context.SECURITY_CREDENTIALS</code>.</p>
security.protocol	optional	<p>Use this option to enable or disable an SSL connection between the JndiLoginModule and your directory server. This option has two possible values:</p> <ul style="list-style-type: none"> ■ <code>simple</code> (Default setting) ■ <code>ssl</code> <p>Note: This option corresponds to the Java constant <code>Context.SECURITY_PROTOCOL</code></p>
security.authentication	optional	<p>Use this option to enable or disable anonymous binding to your directory service. Typically, this option has one of two values:</p> <ul style="list-style-type: none"> ■ <code>none</code> (Default setting) ■ <code>simple</code> <p>Note: If you do not specify a value for <code>security.principal</code> then <code>security.authentication</code> defaults to a value of <code>none</code>. Likewise, if you set <code>security.authentication</code> to <code>simple</code> but <code>security.credentials</code> is omitted or has zero length, then <code>security.authentication</code> resets to <code>none</code>.</p> <p>Note: This option corresponds to the Java constant <code>Context.SECURITY_AUTHENTICATION</code>.</p>

Option	Use	Description
<code>user.search.scope</code>	optional	<p>Use this option to specify the number of levels to descend when searching for the user being authenticated by <code>user.provider.url</code>. This value must be an integer. The default value is 1.</p> <p>Note: This option corresponds to the Java constant <code>SearchControls.ONELEVEL_SCOPE</code>.</p>
<code>group.provider.url</code>	optional	<p>Use this option to provide the URL to the starting point in your directory service where you want to search for groups.</p> <p>For example, <code>ldap://server/dc=peregrine,dc=com</code></p> <p>Note: This option corresponds to the Java constant <code>Context.PROVIDER_URL</code>.</p>
<code>group.search.scope</code>	optional	<p>Use this option to specify the number of levels to descend when searching for a group. This option should only be used with <code>group.provider.url</code>. This value must be an integer. The default value is 1.</p> <p>Note: This option corresponds to the Java constant <code>SearchControls.ONELEVEL_SCOPE</code>.</p>
<code>group.search.objectClass</code>	optional	<p>Use this option to specify the name of the LDAP group objectClass. Valid values are:</p> <ul style="list-style-type: none"> ■ <code>groupOfNames</code> (Default value) ■ <code>groupOfUniqueNames</code>. ■ <code>groupOfUrls</code> <p>Note: Either <code>groupOfNames</code> or <code>groupOfUniqueNames</code> can be used to define static groups in LDAP, but they may not be used together.</p> <p>If you choose the <code>groupOfUrls</code> option, then you are configuring dynamic groups. No additional configuration settings are required to recognize dynamic groups.</p>
<code>storeIdentity=true</code>	optional	Use this option to store a reference to the User being authenticated.
<code>clearIdentity=true</code>	optional	Use this option to clear a reference to the User being authenticated.

Example: Defining an LDAP custom configuration

The following XML code is an example of how to define a loginModule to authenticate users against an LDAP directory service.

Note: LDAP is not an adapter and does not imply any other functionality.

```
<jaas_config>
  <jaasConfiguration>myConfig</jaasConfiguration>
    <myConfig>ldap</myConfig>

  <ldap>
    <loginModule>
      com.peregrine.oaa.security.JndiLoginModule
    </loginModule>
    <options>
      user.provider.url=ldap://server/dc=peregrine,dc=com;
      group.provider.url=ldap://server/dc=peregrine,dc=com
    </options>
  </ldap>
</jaas_config>
```

Standard Sun Microsystems JAAS configuration

The standard JAAS configuration option authenticates users against the Sun Microsystems formatted JAAS configuration. To enable the standard JAAS configuration, you must edit the local.xml file and add the following lines:

```
<jaas_config>
  <useStandardJAASConfiguration>true</useStandardJAASConfiguration>
</jaas_config>
```

If you choose to use the standard JAAS configuration, then you must also do one of the following two things:

- Specify the appropriate JAAS command line options when the container is started
- or—
- Configure the java.security file in \$JAVA_HOME/jre/lib/security for JAAS.

Command line options

The command line properties required for use of the standard file-based configuration are as follows:

```
java -classpath <list of jars> \
  -Djava.security.manager \
  -Djava.security.policy==java2.policy \
  -Djava.security.auth.policy==jaas.policy \
  -Djava.security.auth.login.config==jaas.config \
  <MyMainClass>
```

For <list of jars>, enter the list of jars used by your JAAS-enabled Java application.

For <MyMainClass>, enter the fully qualified class name of the Java main program class.

Integrated Windows Authentication

Windows Integrated Authentication (known as NT/Challenge Response in previous versions of Windows) is one of the ways Windows facilitates the authentication of users on a Web server. The process consists of a secure handshake between Internet Explorer (IE) and the Internet Information Server (IIS) Web server. The handshake lets the Web server know exactly who the user is, based on how they logged in to their workstation. This allows the Web server to restrict access to files or applications based on who the user is. Applications running on the Web server can use this information to identify users without requiring them to log in.

BI Portal uses Integrated Windows Authentication as follows:

- The user logs in to a Windows XP/2000/NT workstation.
- The user starts the IE browser and navigates to the `login.asp` page.
- IE automatically sends user authentication information to IIS. The user's password is not transferred, but the Integrated Windows Authentication handshake between IE and IIS is enough for the server to recognize the user.
- The Web application login automatically detects the user by using the Integrated Windows Authentication/IIS server data.
- The user is logged in without requiring that a name and password be entered.

During this process, the back-end database authenticates and impersonates the Windows user with each of its adapters.

The following circumstances are exceptions to the normal Integrated Windows Authentication login process:

- The Windows user has already registered with a back-end database adapter. When this occurs, BI Portal asks the user to register and enter profile information. BI Portal then lets the user log in and stores this information for future login attempts.
- The Windows user name is not already registered as an Administrator in the back-end system. When this occurs, the web application does not proceed with automatic login. The user is presented with another login screen and is asked to verify their password. This step is an added security measure to prevent a user from accidentally logging in with administrative rights.

Setting up Integrated Windows Authentication

This section describes how to configure BI Portal to use IIS for Integrated Windows Authentication while using Apache as the primary Web server. You can also follow these instructions if you use IIS as your primary Web server.

It is a seven-step process:

Step 1 Verify that all users have an Operator record in the appropriate back-end database. See *Creating an Operator record* on page 93.

Step 2 Install and configure BI Portal with Apache and Tomcat. See *Preparing to configure Integrated Windows Authentication* on page 93.

Note: Tomcat/Apache is the preferred configuration for BI Portal.

Step 3 Set Web server properties for the `login.asp` file. See *Setting Web server properties for the login.asp file* on page 93.

Step 4 Set Web server properties for the `e_login_main_start.asp` file. See *Setting Web server properties for the e_login_main_start.asp file* on page 95.

Step 5 Set Web server properties for the `loginverify.asp` file. See *Setting Web server properties for the loginverify.asp file* on page 98.

- Step 6** Set the **Require Windows NT Challenge/Response Authentication** parameter, and optionally the **Default User Login Name** and **Default Login User Password** parameters from the BI Portal administration page. See *Setting the Admin parameters* on page 99.
- Step 7** Optionally, define the **LogoutURL** from the BI Portal administration page. This step is necessary when BI Portal and IIS reside on different servers. See *Setting up the LogoutURL* on page 100.

The following procedures illustrate how to setup Integrated Windows Authentication using Windows 2000 as an example. If you are using Windows XP, the overall procedure is the same. The IIS Management Console is called Internet Information Services.

Creating an Operator record

All users must have a back-end database Operator record. Contact your AssetCenter or ServiceCenter administrator to verify that users have Operator records. Create an Operator record as needed.

Preparing to configure Integrated Windows Authentication

Note: If you are not using the preferred Tomcat/Apache configuration, skip this section.

- 1 Install and configure BI Portal with Apache and Tomcat, and verify that you can log in through `login.jsp`.
- 2 On a server running IIS, create a virtual directory named `oaa`.
This virtual directory must have read access and permission to run scripts.
- 3 From the BI Portal deployment directory, copy the following files to the `oaa` virtual directory on the IIS server:
 - `login.asp`
 - `loginverify.asp`
 - `e_login_main_start.asp`

The default BI Portal deployment directory is:

`C:\Program Files\Peregrine\Common\Tomcat4\webapps\oaa`

Setting Web server properties for the login.asp file

Note: If you are using IIS for your Web server, go directly to step 3.

- 1 On the IIS server, edit `login.asp` using a text editor.

Edit <FORM... action...> and change it from login.jsp to the absolute URL of login.jsp on the Apache server.

For example, change from:

```
<FORM name="f" action="login.jsp" method="post">
```

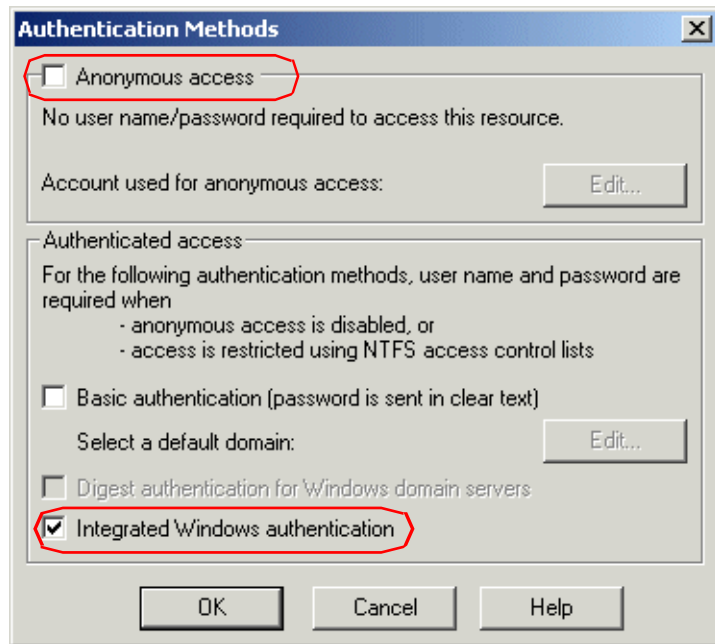
to:

```
<FORM name="f" action="
"http://<apacheserver.mycompany.com>/oaa/login.jsp" method="post">
```

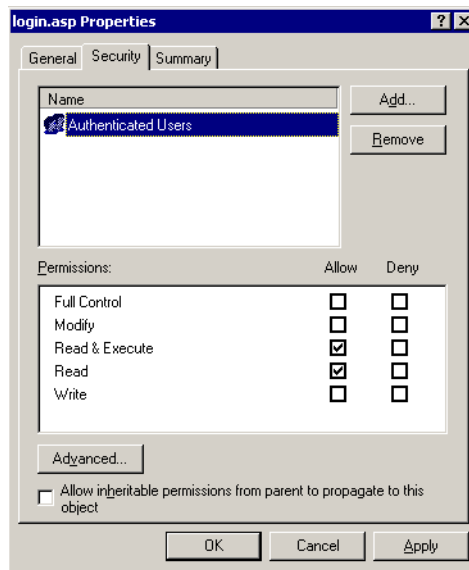
- 2 Open the IIS Management Console (**Start>Programs>Administrative Tools>Internet Information Services**).
- 3 Click on the oaa virtual directory.
- 4 Right-click on login.asp and select **Properties**.
- 5 Select the **File Security** tab.
- 6 Click **Edit** in the **Anonymous Access and Authentication Control** section and set the permissions as follows:
 - a Disable **Anonymous** access.
 - b Require **Integrated Windows** authentication.

Clear the Anonymous access check box.

Select the Integrated Windows authentication check box.



- 7 Click **OK** on all windows displayed until you return to the Microsoft Management Console.
- 8 From Windows Explorer, update the following properties to **login.asp**.
 - a Add the **Authenticated Users** group to the list of authorized users.
 - b Grant the following **Permissions** to the Authenticated Users group:
 - **Read & Execute** – Allow
 - **Read** – Allow



Setting Web server properties for the e_login_main_start.asp file

Note: If you are using IIS for your Web server, go directly to step 3.

- 1 On the IIS server, edit **e_login_main_start.asp** using a text editor. Edit `<FORM... action...>` and change it from **e_login_main_start.do** to the absolute URL of **e_login_main_start.do** on the Apache server.

For example, change from:

```
<FORM name="f" action="e_login_main_start.do" method="post">
```

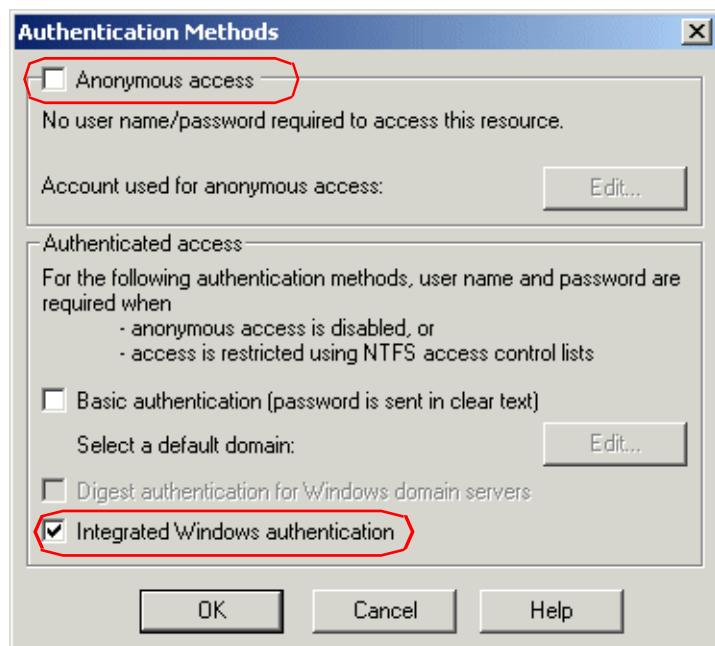
to:

```
<FORM name="f" action="http://<apacheserver.mycompany.com>/oaa/e_login_main_start.do" method="post">
```

- 2 Open the IIS Management Console (Start>Programs>Administrative Tools>Internet Information Services).
- 3 Click on the oaa virtual directory.
- 4 Right-click on e_login_main_start.asp and select Properties.
- 5 Select the File Security tab.
- 6 Click **Edit** in the **Anonymous Access and Authentication Control** section and set the permissions as follows:
 - a Disable **Anonymous** access.
 - b Require **Integrated Windows authentication**.

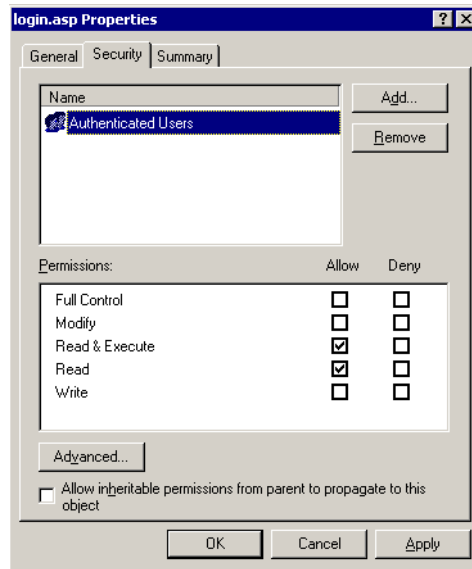
Clear the Anonymous access check box.

Select the Integrated Windows authentication check box.



- 7 Click **OK** on all windows displayed until you return to the Microsoft Management Console.
- 8 From Windows Explorer, update the following properties to e_login_main_start.asp.
 - a Add the **Authenticated Users** group to the list of authorized users.
 - b Grant the following **Permissions** to the **Authenticated Users** group:
 - **Read & Execute – Allow**

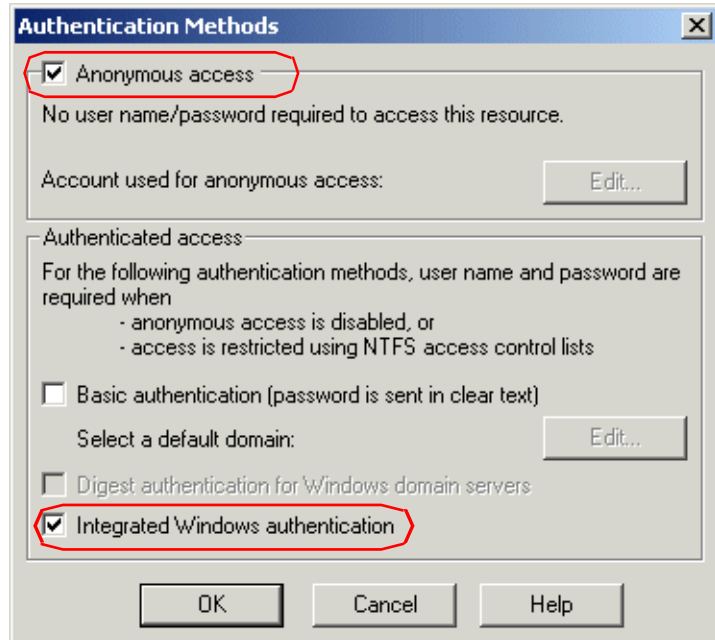
- Read – Allow



Setting Web server properties for the loginverify.asp file

- 1 Open the IIS Management Console (Start>Programs>Administrative Tools>Internet Information Services).
- 2 Click on the oaa virtual directory.
- 3 Right-click on loginverify.asp and select Properties.
- 4 Select the File Security tab.
- 5 Click **Edit** in the **Anonymous Access and Authentication Control** section.

Select the Anonymous access check box.



Select the Integrated Windows authentication check box.

- 6 Verify that **Anonymous access** and **Integrated Windows authentication** have a check.
- 7 Click **OK** on all windows displayed until you return to the Microsoft Management Console.
- 8 Close the Management Console.

Setting the Admin parameters

You must set the **Require Windows NT Challenge/Response Authentication** parameter to **Yes** if you want only users who have a Windows account to log in. Users without Windows authentication can still have login capabilities by assigning a **Default Login User Name**.

Warning: The default login user has whatever capabilities you assign in the ServiceCenter or AssetCenter back-end. When you enable this feature, anyone can log in. Assign minimal user rights to this user.

To set Windows NT Challenge/Response Authentication

- 1 Open a Web browser.
- 2 Enter the following URL: `http://<webserver>/<oaa>/admin.jsp` in the browser address field (where `<webserver>` is the name of your Web server and `<oaa>` is the name of the virtual directory created during installation).
- 3 Login using the administrator name and password.
- 4 From the Administration Home page, click **Settings**.

Select the **Yes** option in **Require Windows NT Challenge/Response Authentication** to allow only Windows users to log in.

The screenshot shows the 'Admin Settings' interface. On the left is a navigation tree with 'Settings' selected. The main area contains various configuration fields. The 'Require Windows NT Challenge/Response Authentication' field is highlighted with a red circle, showing the 'Yes' radio button selected. Other visible fields include 'Logout URL', 'Server URL', 'Message URL Prefix', 'Help URL Prefix', 'Loginverify.asp URL prefix', 'Default Login User Name' (set to 'Harte'), and 'Default Login User Password'. The right side of the page provides detailed descriptions for each field.

- 5 From the **Common** tab, set the **Require Windows NT Challenge/Response Authentication** parameter to **Yes**.
- 6 To allow users without Windows authentication to login, assign a **Default Login User Name**, and optionally a password.
- 7 Click **Save**, then click **Reset Server**.

Setting up the LogoutURL

Note: This step is necessary when BI Portal and IIS reside on different servers.

- 1 From the Administration home page (see *To set Windows NT Challenge/Response Authentication* on page 99), click **Settings**.
- 2 From the **Common** tab, set the **LogoutURL** setting to the URL you want users to go to if Integrated Windows Authentication fails or is not possible due to the user's current browser.
- 3 Click **Save**, then click **Reset Server**.

Testing the settings

Log in to your Peregrine Web application to make sure the access permissions are set correctly. The Integrated Windows Authentication settings are activated when you log in through a special login page named **login.asp**. Accessing your applications through the standard **login.jsp** page results in the users needing to log on as usual.

To test the settings:

- 1 Open a Web browser.
- 2 Enter the following URL: **http://<webserver>/<oaa>/login.asp** in the browser address field (where *<webserver>* is the name of your Web server and *<oaa>* is the name of the virtual directory created during installation).
- 3 Verify that access to BI Portal is what you expected based on the settings you chose for the **login.asp** and **loginverify.asp** files.

Integrating with single sign-on tools

You can integrate BI Portal with a single sign-on tool such as SiteMinder to eliminate displaying the BI Portal login screen. When you integrate with a single sign-on tool, BI Portal users browse to a special URL that obtains their user information from the sign-on tool and then automatically logs them in if the sign-on tool validates them. The following steps are for integrating BI Portal with a third-party single sign-on tool. If you want to use Integrated Windows Authentication as your single sign-on tool, refer to *Integrated Windows Authentication* on page 91.

To integrate with a single sign-on tool

- 1 Choose or create one user record for each single sign-on user you want to access BI Portal. Each user record must have a password and a list of capability words or user rights.

Important: The back-end database user record is required to determine what portions of the BI Portal interface the user can access.

- 2 Open a text editor such a NotePad.
- 3 Create a new JSP file to be the target of your automatic login URL.

You can use the following code as a template:

<p>Add JSP code here to obtain the user name of the person that the single sign-on tool has authenticated _____</p>	<pre><%@ include file="jspheader.jsp" %> <% // Add JSP code that obtains proper user name from // the third party single-sign on tool // ... // Replace "user" with the user name obtained above String sUser = "user"; // Turn on OAA pre-authentication user.setPreAuthenticated(true); %></pre>
<p>Replace the value _____ "user" with the user name obtained from your single sign-on tool</p>	<pre><HTML> <BODY> <FORM name="f" action="login.jsp" method="post"> <INPUT type="hidden" name="loginuser" value="<%=sUser%>" /> </FORM> </BODY> </HTML> <SCRIPT LANGUAGE="JavaScript"> self.document.forms[0].submit() </SCRIPT></pre>

- 4 Add any necessary JSP code to query your single sign-on tool for the name of the user who has been pre-authenticated.

Typically, these tools use HTTP headers to submit this information. See your single sign-on tool API documentation for details.

- 5 Save the file as `autologin.jsp` in your application server's presentation folder. For example:

C:\Program Files\Peregrine\Common\Tomcat4\webapps\oaa\autologin.jsp

Note: The name you choose for the JSP file will be the file name required in the URL.

Testing access to BI Portal from a single sign-on tool

You can use the following steps to test access to BI Portal from your single sign-on tool.

To test your single sign-on settings

- 1 Login to your single sign-on tool.
- 2 Open a browser and go to the following URL:

`http://<server_name>/oaa/autologin.jsp`

If you configured the login settings correctly you will be authenticated and redirected automatically to the BI Portal home page.

Note: If you saved the automatic login page with a different file name, then use that file name instead of `autologin.jsp`.

Authentication models

The following sections discuss:

- *ServiceCenter authentication components*
- *OAA contact and operator associations*
- *Regular operator authentication*
- *Contact-based authentication*

ServiceCenter authentication components

There are two components of the ServiceCenter authentication model: the **Operator** file and the **Contacts** file.

The **Operator** file contains the following keys:

- The `name` field is the primary key (unique and indexed).
- The `full.name` field is a foreign key to the contact table. It represents the contact associated with the operator. It is indexed, it can be empty, and several operators can have the same value for this field. The value of the `full.name` field, when not empty, represents the value of the `contact.name` field in one of the records in the contacts file.

The **Contacts** file contains the following keys:

- The `contact.name` field is the primary key; it is unique and indexed.
- The `user.id` field is indexed and is a “no duplicate” field; it can be null, but must be unique if not null. When contact-based authentication is enabled, the `user.id` field is the key used to look up contacts.

OAA contact and operator associations

OAA approaches contact and operator handling by allowing ServiceCenter administrators to customize their **Contacts** and **Operator** files, and to use **Contacts** and **Operator** associations that differ from OAA defaults.

The OAA schemas allow flexibility in defining associations between records in the **Contacts** and **Operator** files. These OAA schemas provide a logical view that is “wrapped around” their physical implementations. OAA provides attribute names that correspond to each type of lookup operation. Therefore, for an administrator, customizing the lookup is as simple as creating a schema extension on the **Profile** or the **Contact** schema. For more information about schemas refer to the “Schemas” chapter in this guide.

Regular operator authentication

Name and password pairs are validated against the existing operator in the operator table. In addition, the presence of a contact that corresponds to the operator's contact is queried based on the fields mentioned below.

Note: If a contact for the corresponding operator’s contact is not found, OAA creates a contact automatically.

Algorithm for looking up contacts

The Contact schema has the following attributes:

Logical name	Mapping in profile schema	Mapping in contact schema
OperatorContactKey1	full.name	contact.name
OperatorContactKey2	Name	user.id

Using these attributes, the lookup algorithm is the following:

- 1 Read the values for OperatorContactKey1 and OperatorContactKey2 in the Profile schema whose UserName equals the UserName (login) of the operator who is logged in.
- 2 Search the Contact schema for a record whose Id is the value of OperatorContactKey1.
- 3 If exactly one record is found, return this contact's Id.
- 4 If no record, or more than one record, is found, search the Contact schema for a record whose Id equals the value of OperatorContactKey2.
- 5 If exactly one record is found, return this contact's Id.
- 6 If no record, or more than one record, is found, return null and attempt to create the contact. (See the section *Contact creation* below.)

Contact creation

All the information from the Profile record for the logged in operator is used to create a record in the Contact schema. Therefore, all the Profile values that have a corresponding attribute in the Contact schema are saved in the database. In addition, the ProfileId record in the Contact schema (see below for mapping) is assigned the value of the Profile record's Id in order map the Contact to the Profile. The following tables describe both the logical and physical mappings of particular fields of interest during contact creation.

Logical mapping

Logical name in Profile schema	Logical name in Contact schema
Id	ProfileId
UserName	UserName
FullName	Id

Physical mapping

Logical name in Profile schema	Logical name in Contact schema
Name	operator.id
name	user.id
full.name	contact.name

Contact-based authentication

This section describes an alternate authentication scheme that automatically verifies Windows users as ServiceCenter contacts.

You can configure BI Portal to automatically log in specific groups of authenticated Windows users as one or more pre-defined Operators in ServiceCenter. Each group of Windows users has its own login page.

Note: The authentication scheme described below requires that both the user who is logged into the machine running the client browser *and* the IIS server reside either in the same domain, or in different domains that have a trusted relationship.

Perform the following steps:

- Step 1** Look up the contact at login. See *Looking up the contact at login* on page 106.
- Step 2** Choose or create one Operator record in ServiceCenter for each group of Windows users you want to authenticate. See *Creating an Operator record in ServiceCenter* on page 107.
- Step 3** Create a contact record in ServiceCenter for each Windows user who you want to be able to log in. See *Creating a contact record* on page 108.
- Step 4** From the Windows domain server, add a Windows group for each Operator that you defined in step 2. Refer to your Windows documentation for more information on adding groups. See *Adding groups* on page 108.
- Step 5** Create a login ASP file for each Operator defined in step 2. See *Configuring the login ASP file* on page 108.
- Step 6** Configure each login ASP file to be exclusive to each Windows group defined in step 4. See *Setting properties for the login ASP file* on page 109.
- Step 7** On the BI Portal Admin module Settings page, click the Common tab, scroll down to the Encoding, Locales, and Sessions section, and make sure that **Require Windows NT Challenge/Response Authentication** is set to **No**.
- Step 8** Edit *local.xml* in <application server>\oaa\WEB-INF to define the passwords for each Operator defined in step 4. See *Editing the local.xml file* on page 111.
- Step 9** Modify *rds_user* Scenario and restart the scenario to re-synchronize the user data. See *Modifying rds_user scenario* on page 112.

Looking up the contact at login

OAA uses the ServiceCenter the *user.id* field in the contacts file to look up a contact for contact-based authentication. However, some administrators use this field to hold employee IDs (such as numeric employee IDs, badge number, and Social Security number) rather than network names (which are applicable when Integrated Windows Authentication is enabled). *UserName* is the logical name in the Contact schema for the *user.id* field. Through a schema extension, administrators can customize this to point to a different field or a newly defined field.

Logical name	Mapping in Contact schema
<i>UserName</i>	<i>user.id</i>

The contact lookup algorithm ensures that there is only one match for a given UserName. Otherwise, authentication is denied.

Creating an Operator record in ServiceCenter

Choose or create one Operator record for each group of users or role you want to access BI Portal. Each Operator must have a password and a list of capability words. For example, you can define one Operator with default access (`scdefault`) and one Operator with manager access (`scmgr`). Refer to your ServiceCenter documentation for more information on adding Operator records.

The following procedures describe how to use `scdefault` and `scmgr` as the Operators.

Using Operator records in ServiceCenter

- 1 Create two Operator records: `scdefault` and `scmgr`.

Refer to your ServiceCenter documentation for information on adding Operator records.

- 2 Add the BI Portal capability words you want users assigned to this Operator to have. For example:

Operator	Capability words
<code>scdefault</code>	<code>getit.service</code> <code>getit.personalization.default</code> <code>BI_Access</code> <code>BI_View</code>
<code>scmgr</code>	<code>getit.service</code> <code>getit.itemployee</code> <code>getit.itmanager</code> <code>getit.personalization.default</code> <code>BI_Access</code> <code>BI_View</code>

Note: Each Operator will use its own login page.

In this example, users who log in to `logindefault.asp` have the capabilities of the `scdefault` Operator in ServiceCenter. Users who log in to `loginmgr.asp` have the capabilities of the `scmgr` Operator in ServiceCenter.

- 3 Assign a password to each Operator.

Note: The password must match the password defined in *Editing the local.xml file* on page 111.

Creating a contact record

Create a contact record for each Windows user who you want to be able to log in. The Employee ID field of the contact record must match the Windows user name exactly, including upper- and lower-case.

For more information about creating contact records, see the *Service Center System Administration Guide*.

Adding groups

You must have an equivalent Windows group for each Operator that you want to authenticate. For example:

Operator	Suggested group
scdefault	Authenticated Users (default Windows group)
scmgr	Managers (created on domain server)

Refer to your Windows documentation for adding groups to Windows.

Configuring the login ASP file

You must configure or create a separate login ASP file for each Operator you define (see *Creating an Operator record in ServiceCenter* on page 107). Each file needs a unique name.

Two sample login ASP files, `logindefault.asp` and `loginmgr.asp` are in the BI Portal deployment directory: `<application server>\oaa`

To configure the login ASP file

- 1 Create a unique login file for each Operator.
 - For example, create `logindefault.asp` for `scdefault` and create `loginmgr.asp` for `scmgr`.
 - a Copy `logindefault.asp` from the deployment folder: `<application server>\oaa`
 - b Paste the file in the same folder and rename the copied file.

Note: Whatever file name you choose becomes part of the URL users enter to access BI Portal. For example, if the file name is `mylogin.asp`, the URL is: `http://yourhostname/oa/mylogin.asp`.

- 2 Edit the value of the OPERATOR form input to match the Operator you defined in *Creating an Operator record in ServiceCenter* on page 107.

```

...
<FORM name="f" action="login.jsp" method="post">
  <INPUT type="hidden" name="AUTH_TYPE" value="<%=sType%>" />
  <INPUT type="hidden" name="AUTH_USER" value="<%=sUser%>" />
  <INPUT type="hidden" name="AUTH_KEY" value="<%=sKey%>" />
  <INPUT type="hidden" name="OPERATOR" value="scdefault" />
</FORM>
...

```

The value of the OPERATOR must match the Operator name.

- 3 Save and close the file.

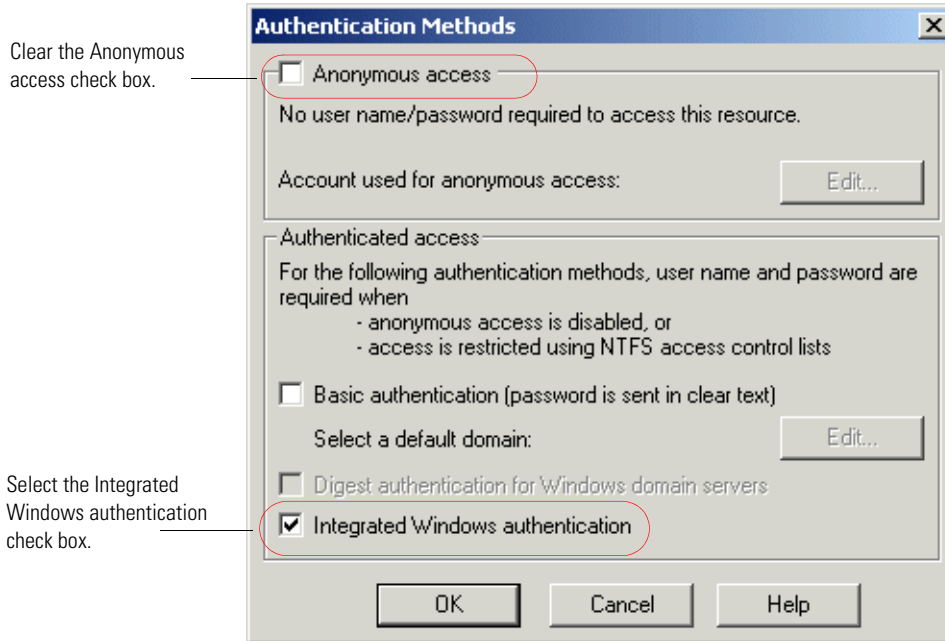
Setting properties for the login ASP file

You must configure each login ASP file to be exclusive to each Windows group. This requires changing the authentication method in IIS and setting the file security properties in Windows.

To change the authentication method in IIS

- 1 Open the IIS Management Console (**Start > Programs > Administrative Tools > Internet Information Services**).
- 2 Navigate to the `oa` virtual directory.
- 3 For each Operator, navigate to the ASP file that you created in *Configuring the login ASP file* on page 108.
For example, navigate to `logindefault.asp` for `scdefault`; navigate to `loginmgr.asp` for `scmgr`.
- 4 Right-click on the file and select **Properties**.
- 5 Select the **File Security** tab.
- 6 Click **Edit** in the **Anonymous Access and Authentication Control** section and set the permissions as follows:
 - a Disable **Anonymous** access.

b Require Integrated Windows authentication.

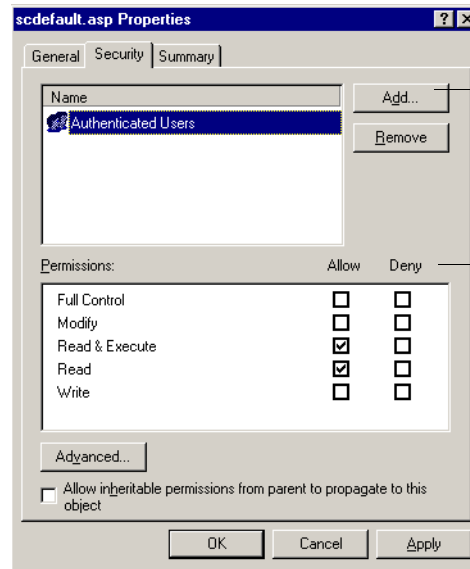


- 7 Click OK on all windows displayed until you return to the Microsoft Management Console.

To set the file security properties in Windows

- 1 Open Windows Explorer.
- 2 Browse to your deployment folder: <application server>\oaa
- 3 Update the following login ASP properties.
 - a Right-click on your login ASP file; for example, scdefault.asp, and click **Properties**.

- b Add the user group associated with this Operator; for example, **Authenticated Users**.



Click Add to open the Select Users, Computers, or Groups dialog box and select the Windows group associated with this Operator.

Set Permissions to Allow for the Read & Execute option and the Read option.

- c Grant the following **Permissions** to the **Authenticated Users** group:

- **Read & Execute** – Allow
- **Read** – Allow

- d Click **OK**.

- 4 Repeat step 3 for each login ASP file.
- 5 On the BI Portal Admin module Settings page, click the Common tab, scroll down to the Encoding, Locales, and Sessions section, and make sure that **Require Windows NT Challenge/Response Authentication** is set to **No**.

Editing the local.xml file

You must identify the password for each Operator that you defined in the local.xml file. This file is located at:

<application server>\oaa\WEB-INF\local.xml.

To edit the local.xml file:

- 1 Using a text editor, edit local.xml.

The default location is:

C:\Program Files\Peregrine\Common\Tomcat4\webapps\oaa\WEB-INF.

2 Add an XML entry for each Operator.

The tag has the format: `<[operator name]password>`

For example, for operators `scmgr` and `scdefault`, add the following inside the `<settings> ... </settings>` tags:

```
<scmgr>scmgr</scmgr>
<scmgrPassword>scmgr_password</scmgrPassword>
<scdefault>scdefault</scdefault>
<scdefaultPassword>scdefault_password</scdefaultPassword>
```

where `scmgr_password` is the ServiceCenter password assigned to operator `scmgr`, and `scdefault_password` is the ServiceCenter password assigned to operator `scdefault`.

Important: The password must match the Operator password in ServiceCenter.

3 Restart your application server for your changes to take effect.

Modifying `rds_user` scenario

In order for the BI Portal to work properly in an environment that is a contact-based authentication environment, you must edit the `rds_user` scenario and turn the flag for transferring contact data into RDS. This causes both Contact and Operator data to be pushed to RDS (`RDS_USER` table).

Note: The Operator option in the `rds_user` scenario must never be turned off. Only the Contact option can be turned on or off.

To edit the `rds_user` scenario

- 1 Open up the Connect-It Service Console
Start>Programs>Peregrine>Connect-It>Service Console.
- 2 Select the `rds_user` scenario on top.
- 3 Click the **Stop** button.
- 4 Double-click `rds_user.scn` file in `RDS/cit` directory on your RDS server.
- 5 Click **Scenario>Open all connectors** and wait until the system finishes opening all the connectors.
- 6 Select the “ServiceCenter” connector from the scenario diagram pane.
- 7 Click the **Document type** tab on the Details of the connector pane, which is below it.

- 8 Check the box for “contacts (contactsSrc)”.
- 9 Select “Mapping-RDSUSER” connector from the scenario diagram pane.
- 10 Click the Mappings tab on the Details of the connector pane, which is below it.
- 11 Check the box for “contacts-RDS_USER”.
- 12 Use **File>Save** to save the scenario.
- 13 Delete the rds_user.ini file from RDS/cit directory on your RDS server.
- 14 On the CIT Service Console, click the Start button to restart the rds_user scenario.

This re-synchronizes all users (operators and contacts) from ServiceCenter into the RDS_USER table.

If you decide to change your environment from contact-based authentication to non-contact-based authentication, then steps 1 to 14 should be done. You will be un-checking the box in step 4 and 6. In addition, the records in the RDS_USER table should be manually deleted before step 14, which restarts the scenario.

If you decide to change their environment from non-contact-based authentication to contact-based authentication, you should follow steps 1 to 14 above.

In a contact-based authentication environment, the RDS_USER table has both **Contacts** and **Operators** data in it. Therefore, the portal users are:

- **Operators** who appear with their user name as usual; for example, Admin.
- **Contacts** who appear with a suffix of the operator name they belong to. For example, if the Operator name is Admin and the Contact name is also Admin, then the user list in the portal shows the following information.

User name	Description
Admin	This is the Operator.
Admin(Admin)	This is the Contact and the Operator it belongs to is indicated in parenthesis after the Contact name; for example: contact_name(operator_name).

Creating an alternate login page

If you do not want to use the default Peregrine OAA login page, you can create your own login page that authenticates users and redirects them to the proper start page. Creating an alternate login page requires two basic steps:

- Step 1** Create a login Web page with the necessary authentication parameters. See the following section, *Creating a login Web page*.
- Step 2** Edit the `local.xml` file to specify the HTTP authentication method you want to use. See *Specifying an alternate authentication method* on page 115.

Creating a login Web page

Your custom login web page can be any HTML form that prompts for the following required parameters:

- Username
- Password

In addition, you can include optional login parameters such as:

- Display Language and Locale
- Time format
- Theme

A sample HTML login form, `login_sample.htm` is in the OAA deployment folder of your application server:

```
<application server>\WEB-INF\oaa\
```

Customize this sample HTML form using the following guidelines:

- Whatever custom login file you create becomes part of your login URL. For example, if you create a custom page called `my_login.htm`, then the login URL is `http://<server>:<port>/oaa/my_login.htm`
- You must specify the `basicauth` servlet in the form action. For example, `action="http://<server>:<port>/oaa/servlet/basicauth"`
- Users who fail to be successfully authenticated should see the page that is specified in the `_failURL` value. This can simply point to your login page so that the user can re-attempt login.

- The `basicauth` servlet does not encrypt usernames and passwords during login. You must enable HTTPS if you are concerned about password security on your intranet.
- There are no specific Administration page settings needed to set up a custom login page. You must define all login parameters in your custom login page.
- The following login parameters are available:

Login parameters Description

Login parameters	Description
<code>loginuser</code>	This is a required login parameter specifying the user name. You must specify a form input for this parameter.
<code>loginpass</code>	This is a required login parameter specifying the login password. You must specify a form input for this parameter.
<code>_locale</code>	This is an optional login parameter specifying the user's locale and regional display settings.
<code>_timezone</code>	This is an optional login parameter specifying the user's timezone.
<code>_theme</code>	This is an optional login parameter specifying which theme should be displayed in the Peregrine OAA Portal

Specifying an alternate authentication method

By default, Peregrine OAA uses HTTP basic authentication provided by the `HttpBasicAuthenticationManager` class. If you create a custom login page, you need to specify the alternate authentication method in the `local.xml` file.

To specify an alternate HTTP authentication method:

- 1 Stop your application server.
- 2 Using a text editor, open the `local.xml` file located at:

```
<application server>\webapps\oaa\WEB-INF\
```
- 3 Add the following entry to `local.xml` below the `<settings>` element (if the entry does not already exist):

```
<HTTPAuthClass>HttpAlternateAuthenticationManager</HTTPAuthClass>
```
- 4 Save the file.
- 5 Modify the `web.xml` file.

You will need to enable the `AuthController` servlet to establish a proxy for HTTP basic authentication.

- a Using a text editor, open the `web.xml` file located at:
`<application server>\webapps\oaa\WEB-INF.`
- b Add the following lines at the end of the last `<servlet>` definition:

```
<servlet>
  <servlet-name>AuthController</servlet-name>
  <display-name>AuthController</display-name>
  <description>A controller (decorator) servlet that can be used to enable
  configurable auth protection of any resource.</description>

  <servlet-class>com.peregrine.oaa.archway.AuthControllerServlet
</servlet-class>
  <load-on-startup>2</load-on-startup>
</servlet>

<servlet-mapping>
  <servlet-name>AuthController</servlet-name>
  <url-pattern>/servlet/basicauth/*</url-pattern>
</servlet-mapping>
<servlet-mapping>
  <servlet-name>AuthController</servlet-name>
  <url-pattern>/servlet/auth/*</url-pattern>
</servlet-mapping>
```

- c Save the file.
- 6 Restart your application server.

Warning: Changing the HTTP authentication setting to the Alternate Authentication Manager exposes queries (including login names and passwords) in the URL. If you want to protect URL queries, then you must restrict access to this information through your Web server.

BI Portal security overview

In addition to the security features discussed in the previous section, BI Portal also provides the following security mechanisms to manage application security, report and document group security, and data level security.

Note: See the *BI Portal Administration Guide, Chapter 6*, for a detailed description of how to use these security features.

Security groups

There are three types of security groups:

- Role-level security groups
- Group-level security groups
- Data-level security groups

For additional information about groups, see *Chapter 6, BI Portal Administration Functions* in the *BI Portal Administration Guide*.

Out-of-box role-level security groups

The out-of-box “role-level” security groups are automatically created. These are:

- prefix_BI_ADMIN
- prefix_BI_CREATE
- prefix_BI_VIEW

Note: The prefix in BI_ADMIN refers to the BI Portal group name.

These groups appear in the Portal Group Management screen in the System-Defined Group list. Users cannot rename or delete a role-level security group using the BI Portal. These groups also appear in the User Management screen. They do not appear in the Document Management, Upload, Publish, or the list of Corporate Documents in the Document Groups screens.

BI Portal users are automatically assigned to these groups by the user synchronization process that occurs on a scheduled basis.

Out-of-box group-level security groups for ServiceCenter

Out-of-box “group-level” security groups are automatically created. These are:

- prefix_Change Management
- prefix_Incident Management
- prefix_Inventory Management
- prefix_Root Cause Analysis

- prefix_Service Level Management
- prefix_Service Management

These groups appear in the BI Portal Group Management screen under the System-Defined Group list. These groups also appear in the BI Portal User Management, Document Management, Upload, and Publish screens or in the Corporate Documents list on the Document Groups screen.

Users are assigned to these groups using the BI Portal User Management function.

Data-level security groups

The data-level security groups must only be created by an administrator using the Business Objects Supervisor tool. The data-level security groups must be created under the SC application group. No prefix is required, and the security groups can have any name.

Data-level security groups only appear on the BI Portal Group Management and User Management screens. These groups do not appear on the Upload, Document Management, and Publish screens or in the Document Groups list on the Corporate Documents screen.

Data-level security groups appear under the System-Defined Group list on the Group Management screen. Users are assigned to these groups using the BI Portal User Management function.

Row and object level security

Row-level and object-level security are applied to data-level security groups using the Business Objects Supervisor tool. Users are assigned to a data-level security group by using the BI Portal User Management screen.

Any group created by the user under the SC group using the Business Objects Supervisor tool is assumed to be a data-level security group and therefore appears under the System-Defined Group list on the BI Portal Group Management screen.

ALL groups other than data-level security groups must be created using the Portal Group Management screen. Any groups created using the Business Objects Supervisor tool (but not under the SC group) do not appear in the BI Portal.

6 BI Portal Administrator Functions

CHAPTER

This chapter explains how to use the functions available in the BI Portal. You can use these functions to both administer the BI Portal and use the BI Portal to access report data. Some of these functions are available to both the BI Portal administrator and BI Portal users. This chapter discusses the following topics:

- *Uploading*
- *Group management* on page 123
- *Capability words* on page 127
- *User management* on page 130
- *Document management* on page 131
- *Synchronizing users* on page 132
- *Publishing sample documents* on page 133
- *Scheduling automatic data synchronization* on page 135
- *Restricting report data access* on page 138

Overview

Before users can begin using BI Portal, you should complete the following administrative tasks to ensure that all users are able to use BI Portal effectively:

- Review the BI Portal capability words to determine which BI Portal users should have what access rights.

- Assign BI Portal users the appropriate BI capability (done in ServiceCenter).
- Use the Synchronize Users function to synchronize the BI Portal users capabilities with those defined for the users in ServiceCenter.
- Assign users to document groups as required.
- Add security groups as required to restrict access to various reports or data in the reports.

Uploading

You can send a PDF file or Excel spreadsheet from your hard drive to the BI Portal and publish it as a corporate document.

To upload reports

- 1 Log in to BI Portal.
- 2 From the Reporting module activity menu, click **Upload**.

Upload as corporate document

Enter the document name:

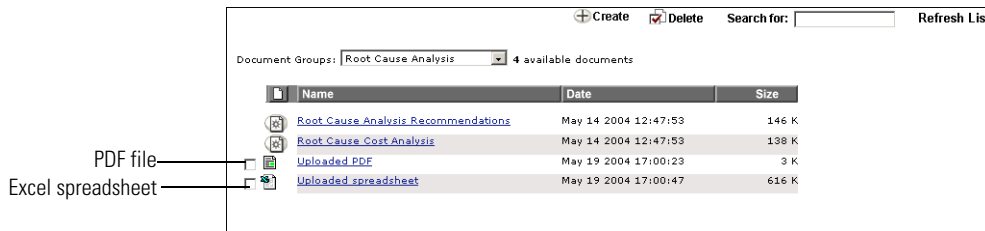
Overwrite the document

Select the destination doc groups: Change Mgmt
Incident Mgmt
Inventory Mgmt
Root Cause Analysis
Service Level Mgmt

Enter the file location (.PDF or .XLS):

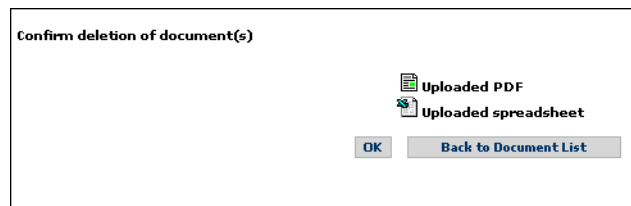
- 3 In the **Enter the document name** field, type the name of the file to upload. You have the option to overwrite the document if it already exists.
- 4 In the **Select the destination doc groups** field, select which group to store the file.
- 5 In the **Enter the file location (.PDF or .XLS)** field, type, or browse and select, the file name.
- 6 Click **Publish**.

The uploaded files appear in the document group list.



7 To delete the files, select the check box next to the file and click **Delete**.

- Click **OK** to delete the file.



You see the message status: Documents successfully deleted at the bottom of the form.

8 Click **Back to Document List** to return to the main menu.

Group management

In BI Portal, report data is organized and grouped to facilitate the management of reports and report data. There are system-defined groups and user-defined groups.

Note: You must have BI_Admin capability to use this function.

Note: Group names must contain at least one alpha character.

The system-defined groups are pre-set (out-of-box), and you cannot add, delete, or rename any of the system-defined groups. These groups are based on the ServiceCenter applications. The system-defined groups are:

- Change Management
- Incident Management
- Inventory Management

- Root Cause Analysis
- Service Level Management
- Service Management
- sc

Important: The `sc` group is a name used for the Peregrine Systems ServiceCenter application and is user-defined on the Admin page.

The `sc` group contains all of the BI Portal users in ServiceCenter. These groups are based on the hierarchy defined in the Peregrine repository in Business Objects (BO). BI Portal uses these groups to manage the reports and data. For a complete description of the repositories in Business Objects, see the Business Objects documentation.

If you name or rename the ServiceCenter group name in the Supervisor tool with a prefix that is the same as the BI Portal group name, then the ServiceCenter group name that appears in the Portal truncates the prefix part of the name. For example, using the Supervisor tool, you call the BI Portal group name `BIPortal` and the ServiceCenter group name `BIPortal_SC`. The ServiceCenter group name in the portal is `SC` because the prefix is truncated.

The Group Management function in BI Portal enables you to manage the user-defined groups. With the Group Management function, you can create new groups, delete groups, or rename groups. Once you have created these groups, you can add users and documents to these groups.

Note: You must have `BI_Admin` capability to use this function.

In BI Portal, each report is assigned to a group. All the sample reports are assigned to pre-defined groups. In addition, you can create new groups and assign reports to them. When you assign each user to one or more groups, you control the reports that the user can execute and view.

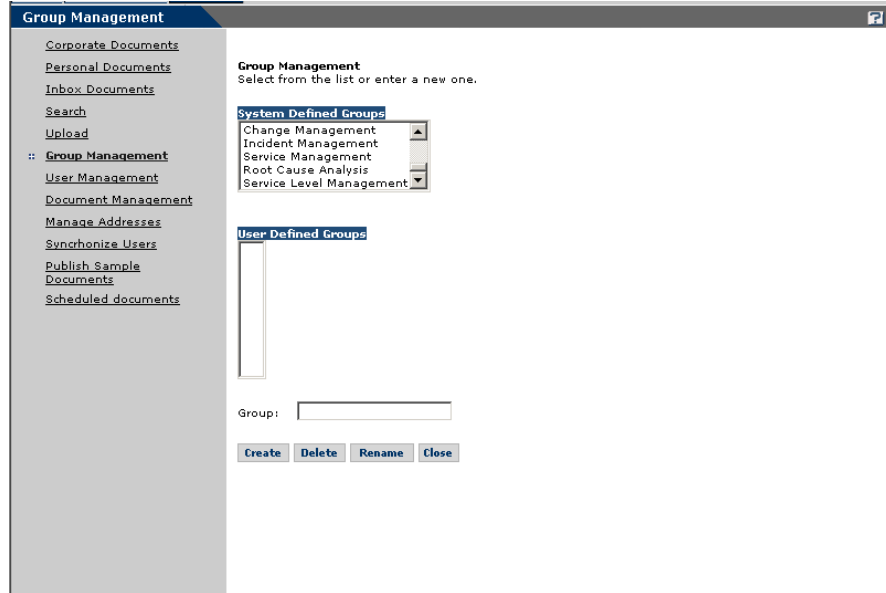
The following table lists the reports and data that are available for querying and viewing by users assigned various groups.

This group...	Provides a view to these reports...
Change Management	All reports and data related to Change Management. See the section <i>Sample Reports for Change Management</i> in the <i>BI Portal User Guide</i> for more information.
Incident Management	All reports and data related to Incident Management. See the section <i>Sample Reports for Incident Management</i> in the <i>BI Portal User Guide</i> for more information.
Inventory Management	All reports and data related to Inventory Management. See the section <i>Sample Reports for Inventory Management</i> in the <i>BI Portal User Guide</i> for more information.
Root Cause Analysis	All reports and data related to Root Cause Analysis. See the section <i>Sample Reports for Root Cause Analysis</i> in the <i>BI Portal User Guide</i> for more information.
Service Level Management	All reports and data related to Service Level Management. See the section <i>Sample Reports for Service Level Management</i> in the <i>BI Portal User Guide</i> for more information.
Service Management	All reports and data related to Service Management. See the section <i>Sample Reports for Service Management</i> in the <i>BI Portal User Guide</i> for more information.

To create a group

- 1 Log into BI Portal.
- 2 From the Reporting module activity menu, click **Group Management**.

The Group Management form opens.



- 3 In the **Group** field, type the name of the new group.
- 4 Click **Create** to add the new document group to the **User Defined Groups** list.

The name of the group you created appears in the **User Defined Groups** list.

To delete a user defined group

- 1 Log into BI Portal.
- 2 From the Reporting module activity menu, click **Group Management**.
The Group Management form opens.
- 3 In the **User Defined Groups** list, select the group you want to delete.
- 4 Click **Delete**.

The group you selected is removed from the list.

To rename a user defined group

- 1 Log into BI Portal.
- 2 From the Reporting module activity menu, click **Group Management**.
The Group Management form opens.
- 3 In the **User Defined Groups** list, select the group you want to rename.

- 4 In the **Group** field, type the new name of the group.
- 5 Click **Rename**.

The group you selected is renamed in the list.

Capability words

It is the ServiceCenter capability words that control the level of access allowed for each BI Portal user. As a minimum, all BI Portal users must have **BI_Access** assigned to them in ServiceCenter to access the BI Portal. It is the capability words assigned in ServiceCenter to BI Portal users that control access to the various reporting functions available in BI Portal.

Note: All individual BI users should only be assigned to a BI user capability group (**BI_Admin**, **BI_Create**, **BI_View**) from ServiceCenter.

The following table summarizes the functions that each capability allows.

This capability... Access level Allows the user to...

BI_Access	Required	<ul style="list-style-type: none"> ■ Gain access to the WebIntelligence Reporting module <p>Note: Each user needs BI_Access capability simply to access the WebIntelligence Reporting module. In addition, each user need one of the following capabilities in order to perform querying and reporting functions.</p>
BI_View	3	<ul style="list-style-type: none"> ■ Manage personal documents and categories ■ Read corporate and inbox documents ■ Run and refresh documents ■ Use and refresh list of values ■ Work in drill mode ■ Schedule documents ■ Send documents to users within and outside of the user's own group

This capability...	Access level	Allows the user to...
BI_Create	2	<p>Perform the same functions as a user assigned BI_View capability; and:</p> <ul style="list-style-type: none"> ■ Download Zero Administration Business Objects ■ Create and edit documents ■ Format the toolbar ■ Perform a transparent drill outside the cube ■ View SQL <hr/> <p>Warning: Users who have BI_Create user capability have full access to all data in the rds universe file when creating reports and ad hoc queries in the Reporting module; however, full access can be limited for some users when object level and row level security access restrictions apply.</p>
BI_Admin	1 (Highest)	<p>Perform the same functions as a user assigned BI_View and BI_Create capabilities; and:</p> <ul style="list-style-type: none"> ■ Change list display and default Web site ■ Change, view, and edit technology options ■ Access Group Management ■ Access the Document Management ■ Access the User Management ■ Delete published documents ■ Publish sample and corporate documents ■ Synchronize users ■ Perform uploads <hr/> <p>Warning: Users who have BI_Admin user capability have full access to all data in the rds universe file when creating reports and ad hoc queries in the Reporting module.</p>

If a user is assigned multiple capabilities, the lowest-level capability overrides other, higher-level capabilities. Therefore, ServiceCenter administrators should assign only one capability that is appropriate to the functions that the user needs to perform tasks in BI Portal.

BI Capabilities

The following table outlines the capabilities available in the BI Portal to each BI user capability group (BI_Admin, BI_Create, BI_View).

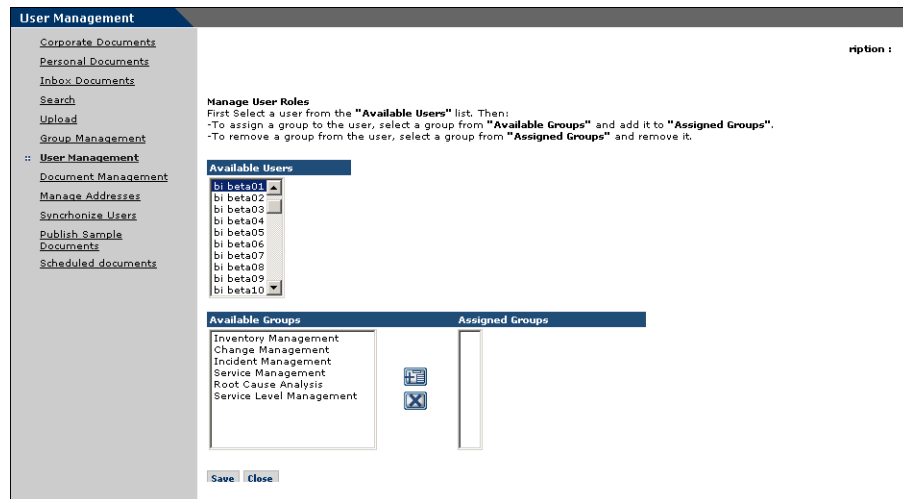
	BI_Admin	BI_Create	BI_View
Create	X	X	
Delete (published documents)	X		
Document Management	X		
Download	X	X	X
Drill	X	X	X
Edit	X	X	
Group Management	X		
Manage Addresses	X	X	X
Manage Inbox Documents	X	X	X
Manage Personal Documents	X	X	X
Maximize	X	X	X
Page or Draft Mode	X	X	X
Publish (or save to Corporate Documents)	X		
Publish Sample Documents	X		
Read Corporate Documents	X	X	X
Refresh	X	X	X
Refresh List	X	X	X
Save (to Personal Documents)	X	X	X
Scheduled Documents	X	X	X
Search	X	X	X
Send	X	X	X

	BI_Admin	BI_Create	BI_View
Synchronize Users	X		
Upload	X		
User Management	X		
View in PDF/HTML	X	X	X

User management

The User Management function allows you to assign each user to as many document groups as required.

Note: You must have BI_Admin capability to use this function.



To assign a user to a document group

- 1 Log into BI Portal.
- 2 From the Reporting module activity menu, click User Management.
- 3 Click a user in the Available Users list to highlight the user's name.
- 4 In the Available Groups list, double-click a group to move it to the Assigned Groups list.



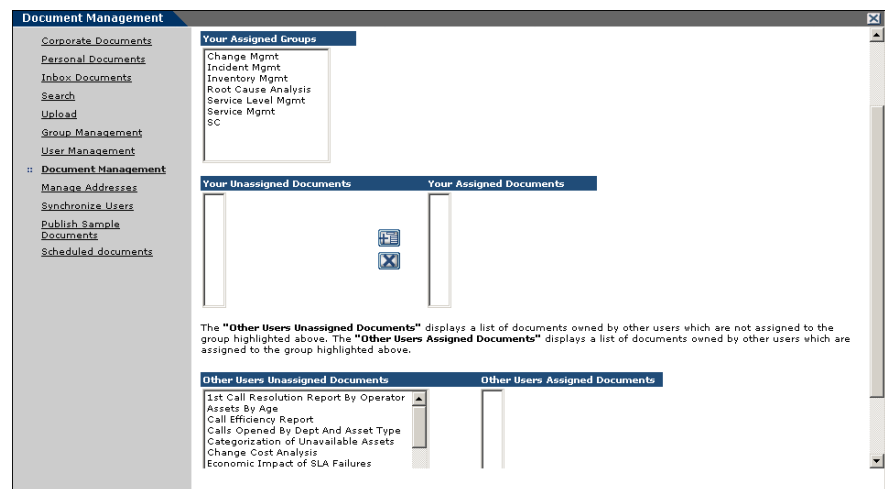
You can also click a group in the Available Groups list and click the Add button to move the group to the Assigned Groups list.

- 5 To remove a user from a group, double-click the group in the **Assigned Groups** list to move it to the **Available Groups** list.
- ✕ You can also click the group in the **Assigned Groups** list and click the **Remove** button to move the group to the **Available Groups** list.
- 6 Click **Save** to commit the group assignments.

Document management



The Document Management function allows you to assign unassigned documents to a group so that the document is available to all users in that group. This form displays the list of groups that you are allowed to assign documents to and your lists of unassigned and assigned documents. You can also view the documents of other users that are unassigned. However, you are not allowed to change these documents since you are not the author.

Note: You must have BI_Admin capability to use this function.



To assign a user to a group

- 1 Log in to BI Portal.
- 2 From the Reporting module activity menu, click **Document Management**.
- 3 Click a group in **Your Assigned Groups** to highlight the group.
- 4 In **Your Unassigned Documents**, double click a document to move it to **Your Assigned Documents**.

-  You can also click a document in **Unassigned Documents** and click the **Add** button to move the document to **Your Assigned Documents**.
- 5 To remove a document from **Your Assigned Documents**, double-click the document in the list to move it to **Your Unassigned Documents**.
-  You can also click the document in **Your Assigned Documents** and click the **Remove** button to move the document to **Your Unassigned Documents**.
- 6 Click **Save** to commit the document assignments.

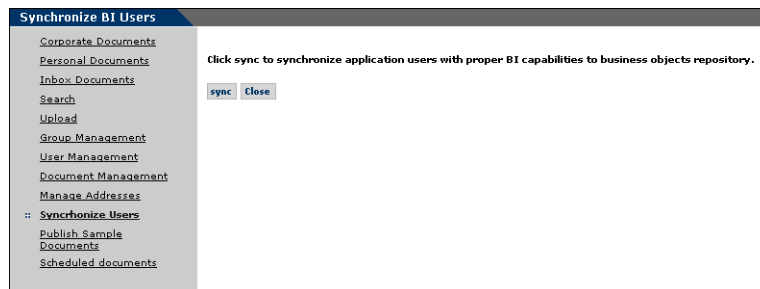
Synchronizing users

The Synchronize Users function allows you to synchronize application users with the appropriate BI capabilities between the RDS database and the Business Objects repository. User synchronization is for on-demand synchronization, and normally, user data is synchronized automatically for a predefined interval defined by the value specified in **User Synchronization Interval** on the BI Portal Setting page of the BI Administration function.

Note: You must have **BI_Admin** capability to use this function.

To synchronize users

- 1 Log in to BI Portal.
- 2 From the Reporting module activity menu, click **Synchronize Users**.

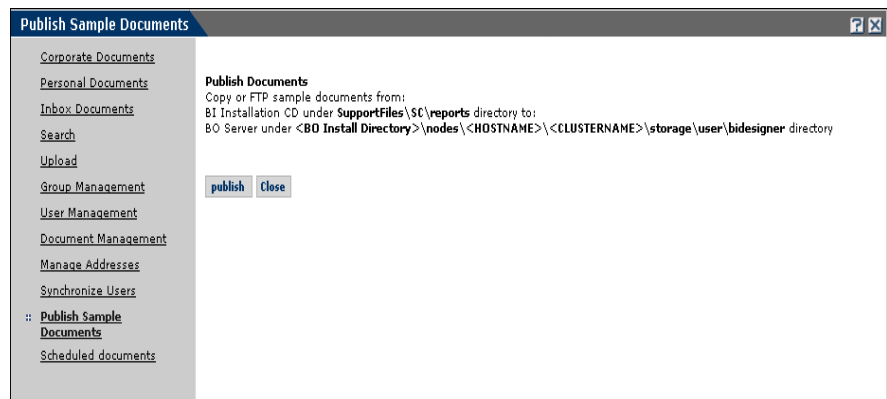


- 3 Click **sync**.
You see the message
Success: Synchronize Users request is submitted and will be processed immediately.
at the top of the form.
- 4 Click **Close** to return to the main menu.

Publishing sample documents

The out-of-box version of BI Portal provides a set of sample documents that you can publish. When you publish these documents, you make them available in the Corporate Documents to all BI Portal users. Use the Publish Sample Documents link on the Reporting module activity menu to publish the sample documents.

Note: You must have BI_Admin capability to use this function.



To publish the sample documents

- 1 Log in to BI Portal.
- 2 If this is the first time the sample documents are being published, you must copy the sample documents from:

BI Installation CD under SupportFiles\SC\reports

to:

BO Server under <BO Install

Directory>\nodes\<hostname>\<clustername>\storage\user\<BO designer user name>

- 3 From the Reporting module activity menu, click **Publish Sample Documents**.

The Publish Documents window opens.

- 4 Click **Publish**.

You see confirmation messages.

```

Success: Connecting to WebIntelligence Server ...
Finished Connecting to WebIntelligence Server.
Finished Logging in.
Publishing Document : "Change Cost Analysis" Category: "PRGN_BIP_Change Mgmt"
Publishing Document : "Failed Changes" Category: "PRGN_BIP_Change Mgmt"
Publishing Document : "Tasks Under Change" Category: "PRGN_BIP_Change Mgmt"
Publishing Document : "Incident Closure Analysis" Category: "PRGN_BIP_Incident Mgmt"
Publishing Document : "Incident Cost Analysis" Category: "PRGN_BIP_Incident Mgmt"
Publishing Document : "Incident Management Ad Hoc Crosstab" Category: "PRGN_BIP_Incident Mgmt"
Publishing Document : "Assets By Age" Category: "PRGN_BIP_Inventory Mgmt"
Publishing Document : "Categorization of Inavailable Assets" Category: "PRGN_BIP_Inventory Mgmt"
Publishing Document : "Recurrent Outages" Category: "PRGN_BIP_Inventory Mgmt"
Publishing Document : "Root Cause Analysis Recommendations" Category: "PRGN_BIP_Root Cause Analysis"
Publishing Document : "Root Cause Cost Analysis" Category: "PRGN_BIP_Root Cause Analysis"
Publishing Document : "1st Call Resolution Report By Operator" Category: "PRGN_BIP_Service Mgmt"
Publishing Document : "Call Efficiency Report" Category: "PRGN_BIP_Service Mgmt"
Publishing Document : "Calls Opened By Dept And Asset Type" Category: "PRGN_BIP_Service Mgmt"
Publishing Document : "Service Management Ad Hoc Crosstab" Category: "PRGN_BIP_Service Mgmt"
Publishing Document : "Economic Impact of SLA Failures" Category: "PRGN_BIP_Service Level Mgmt"
Publishing Document : "Service Contract Cost Analysis" Category: "PRGN_BIP_Service Level Mgmt"
Publishing Document : "SLA Availability Successes" Category: "PRGN_BIP_Service Level Mgmt"
Publishing Document : "SLA Response Time Successes" Category: "PRGN_BIP_Service Level Mgmt"
Finished Processing Documents. Available Documents: 19 Published Documents: 19

Publish Documents
Copy or FTP sample documents from:
BI Installation CD under SupportFiles\SC\reports directory to:
BO Server under <BO Install Directory>\nodes\<HOSTNAME>\<CLUSTERNAME>\storage\user\bi_designer directory

publish Close

```

5 Click Close to return to the document list.

Scheduling automatic data synchronization

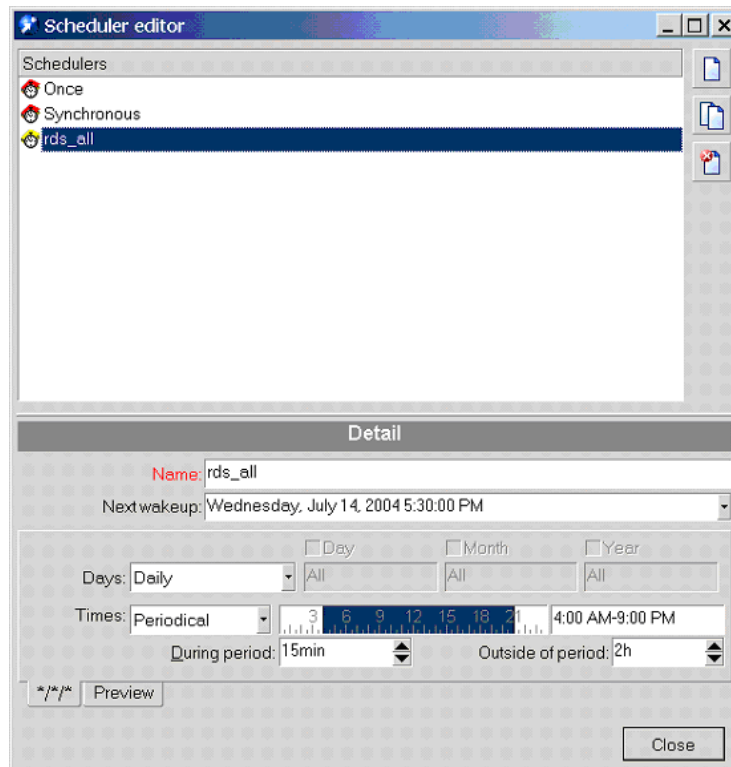
The Reporting Data Store (RDS) has set of pre-defined Connect-It scenario schedulers to run different synchronization tasks.

Because some of the synchronization tasks require more system resources than others, Peregrine recommends that they not be re-configured to occur more frequently than the default time intervals.

To schedule synchronization, you use the Connect-It Scheduler Editor.

To open the Connect-It Scheduler Editor

- 1 Click **Start > Programs > Peregrine > Connect-It > Service Console**.
- 2 Select either `rds_user` or `rds_sc` scenario.
- 3 Click **Scheduling** to open the Connect-It Scheduling window.
- 4 Click the **Edit Schedulers** button to open the Connect-It Scheduler Editor.



The following scheduler defines a synchronization schedule for the `rds_sc` scenario.

Scheduler:	Description:
<code>rds_all</code>	Synchronizes new and updated records at the default intervals of once a day at midnight.

Note: If the ServiceCenter database is large, the default synchronization intervals may need to be increased to accommodate the time it takes to synchronize a large database.

Each data synchronization cycle only picks up records with system modification timestamp value that is earlier than or equal to the current synchronization time. Any record that has a system modification timestamp value that is greater than the current synchronization time is not picked up until the next data synchronization cycle. This is more likely to happen on tables that are frequently updated by ServiceCenter background processes. Potentially, the number of records that the RDS should have for a specific table may be less than the number of records for the table in the ServiceCenter database.

Due to the records modification timestamp discrepancy problem, for reports that were generated from a RDS database that is populated base on ServiceCenter 5.1 database, sometimes the reports may contain less records than they should have. The reports will most likely reflect the correct content the next time the RDS data synchronization takes place.

The following scheduler defines a synchronization schedule for the `rds_user` scenario.

Scheduler:	Description:
<code>rds_user</code>	Synchronizes new and updated operator records at the default intervals of 15 minutes within the defined period and 1hours (1h) outside of that period.

The `rds_user` interval can be changed; however, if this interval is changed, the “BIP user sync interval” must also be changed to match the `rds_user` interval. The “BIP user sync interval” is changed using BI Administration in the Administration module of BI Portal. Refer to *Using the BI Portal Administration page* on page 65.

For more information about using the Connect-It Scheduler Editor, see the Connect-It documentation.

Restricting report data access

This section explains how to use the Business Objects Supervisor to set row and object level security for users. You can use row level security and object level security to restrict the access that some users have to view or create reports or to view (or query for) some of the data in a report. The best way to manage this is to create a group or groups that have specific data access limits and then assign users to these groups depending upon their access requirements. For example, you might want to create a group that limits access to information in the device table. Then you can place users in this group that have no need to access the specified information in the device table.

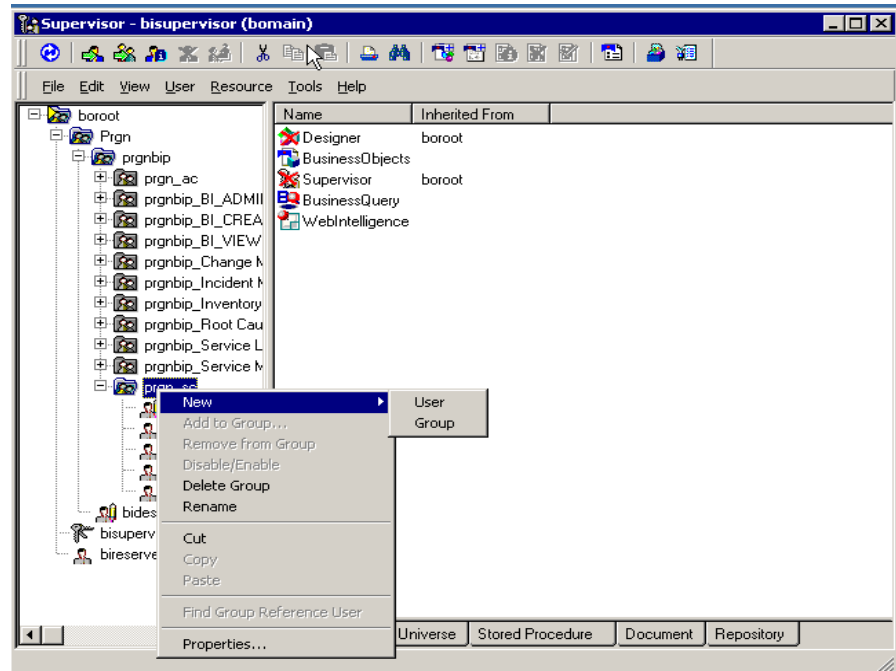
Example: To manage and control access to specific reports or data in a report you should:

- Step 1** Create a new group (PRGNBIP_SEC_NOSLM).
- Step 2** Apply object level security restrictions to the group (PRGNBIP_SEC_NOSLM).
- Step 3** Assign users to the group (PRGNBIP_SEC_NOSLM).
- Step 4** Create a new group (PRGNBIP_SEC_COMPUTER).
- Step 5** Apply row level security restrictions to the group (PRGNBIP_SEC_COMPUTER).
- Step 6** Assign users to the group (PRGNBIP_SEC_COMPUTER).
- Step 7** View current object and row level restrictions.

Object level security

To create a new group

- 1 From the Business Objects Supervisor select the SC application group. In this example, create the group, PRGN_SEC_NOSLM in the SC application group. While you have the folder selected, right-click to display a drop-down menu.



- 2 Click **New > Group** in the drop-down menu.

A new folder appears in the list.

- 3 Type the name of the group in the folder label; for example, PRGN_SEC_NOSLM.

You have now created a new group to which you can assign users and modify the security attributes.

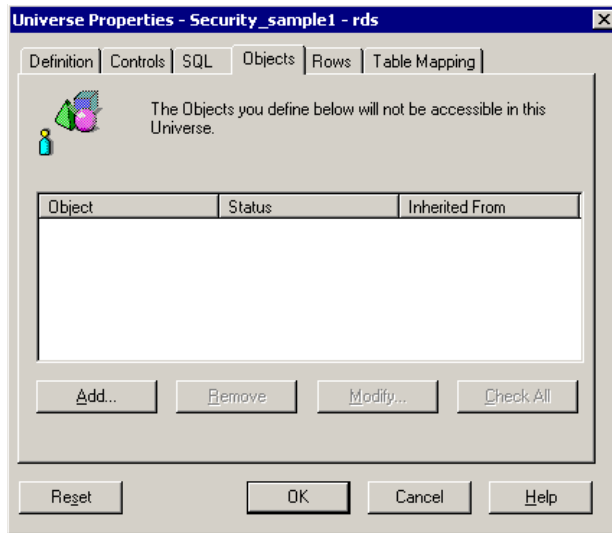
To add object level security to a group

- 1 From the Business Objects Supervisor select the Universe tab.

A list of Universe files display. In this example, rds is the only universe file defined.

- 2 Select the group folder, PRGN_SEC_NOSLM, to which you want to add object level security. While you have the folder selected, right-click on the rds file in the Universe tab.
- 3 Click **Properties** in the drop-down menu.

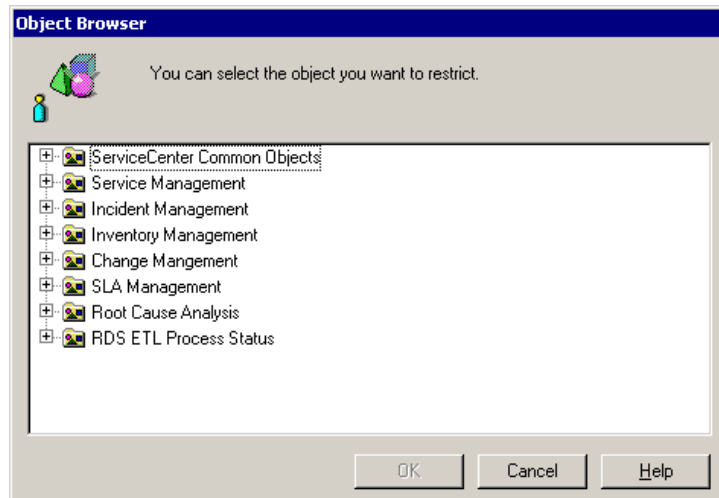
The Universe Properties window opens for the PRGN_SEC_NOSLM group.



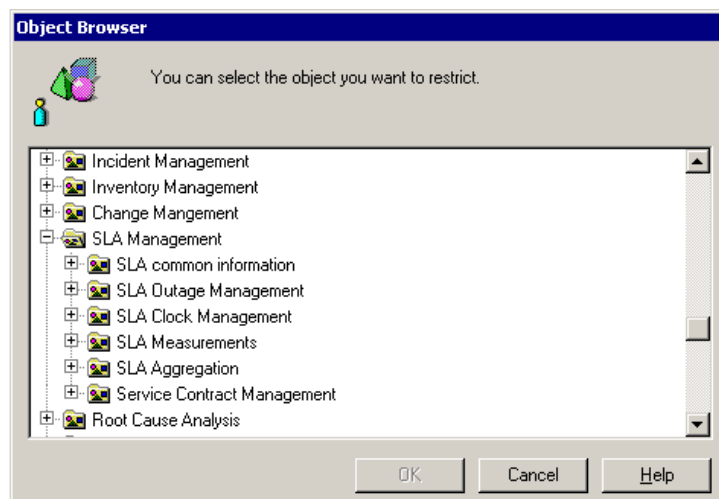
- 4 Click the **Objects** tab.
- 5 Click **Add** on the Objects tab, which lists all the classes and objects available in the universe.

The New Restricted Objects window opens.

- Click **Select** to display a list of objects to which the user's access will be restricted.



You can now select which objects you want to restrict access to. You can select either the entire object or expand the object to select only some of the elements of the object. For this example, select SLA Management.

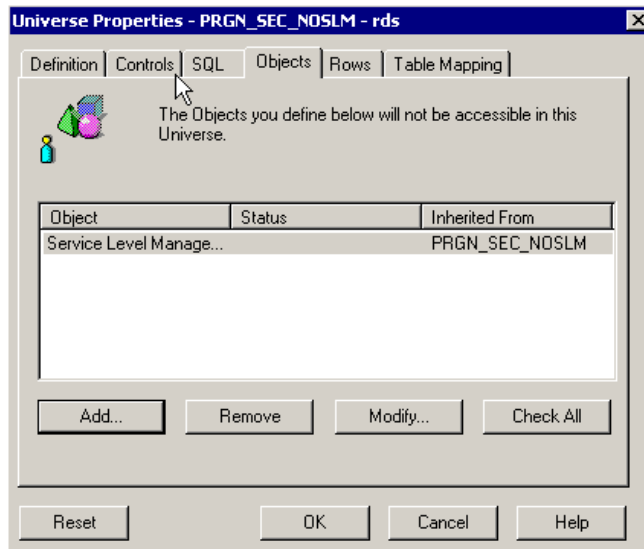


- After you make your selection, click **OK**.

The **New Restricted Object** window opens and displays the name of the object you selected.

8 Click OK.

The Universe Properties window opens and displays the object you selected.



- 9 You can continue adding restricted objects by repeating steps 5 thru 8.
- 10 Click OK when you have added all of the objects to which you wish to restrict access for the selected group (PRGN_SEC_NOSLM).

To verify that you have correctly set object level security restrictions

- 1 Login to BI Portal as a user who has bi_admin capability.
- 2 From the Navigation Menu, click **Reporting**.
- 3 From the Activity menu, click **User Management**.
- 4 In the Available Users list, select a user who has bi_create capability and assign this user to the group PRGNBIP_SEC_NOSLM you created.
- 5 Login to BI Portal as the user you selected in step 4.
- 6 While logged in as this user, attempt to create or edit a report.
You should not see the Service Level Management Object in the create or edit report panel.

Note: When object level security is applied to a user for data security to restrict access, the Group assignment for that user should match the data security. For example, if you assign object level security to a user to restrict that user from the Change Management data, then the you should also make sure that this user does not have Change_Management group assigned to him. In BI Portal, this is done with the User Management function.

Row level security

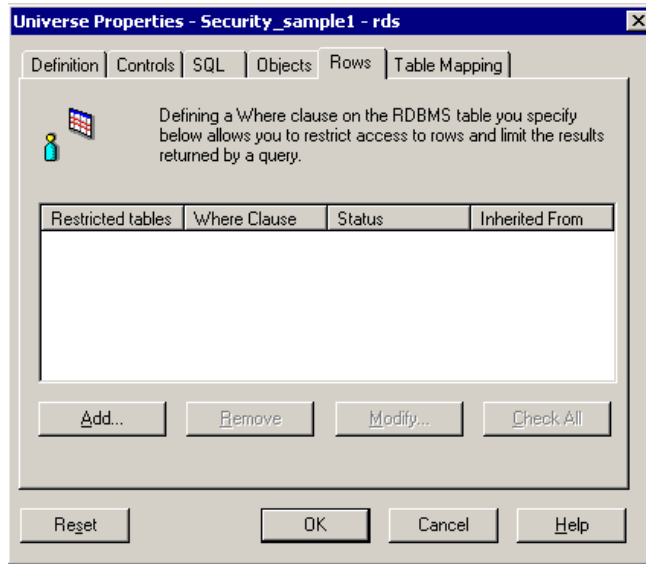
This example shows you how to use row level security to create the following conditions:

- A user (user1) who can view all the data in the DEVICE_D database table.
- A user (user2) who can view the data where the value, for typeprgn, in the DEVICE_D table is 'computer'.
- A user (user3) who can only view 'Desktops' in 'computers' from the table DEVICE_D. This user cannot view other types of 'computers' such as laptops or handheld computers.

To set row level security conditions

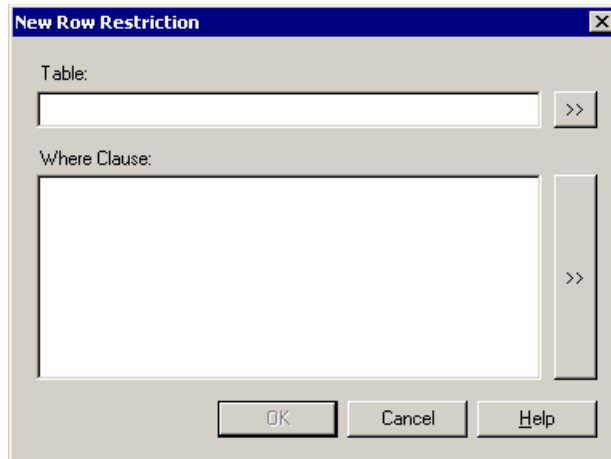
- 1 Start the Business Objects Supervisor tool.
- 2 Create a group PRGNBIP_SEC_COMPUTER under the SC application group.
- 3 Select the group you created (PRGNBIP_SEC_COMPUTER), and from right-hand pane select the universe tab.
- 4 Select the rds universe file and while selected, right click to select the properties menu.

- In the Properties dialog box, select the Rows tab.

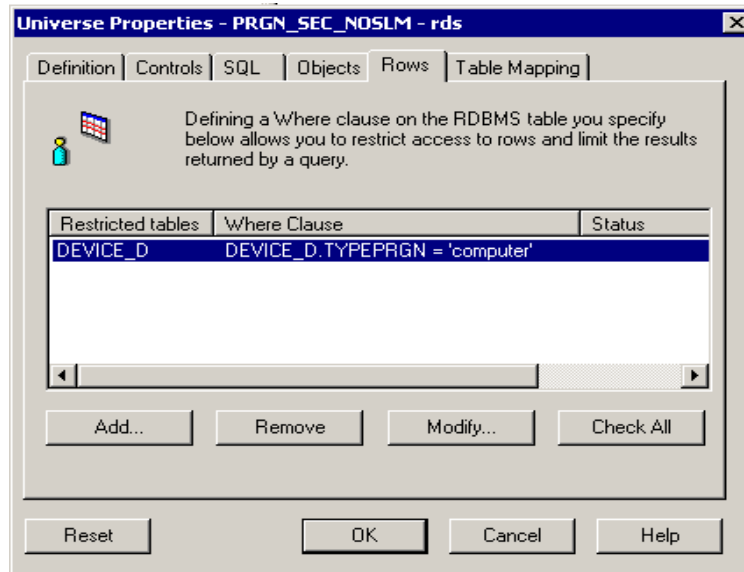


- Click Add.

The New Row Restriction window opens.



- Select the table, `DEVICE_D`, from the list box.
- In the Where Clause creator, choose the column `typeprgn` and from the operator list choose '='. Type the value 'computer'.



You should see the where clause displayed as `DEVICE_D.typeprgn = 'computer'`.

- 9 Click OK.
- 10 Repeat the steps 2 - 9 to create another group, `PRGNBIP_SEC_DESKTOP`. Use the following where clause:
`DEVICE_D.subtype = 'Desktop'`

Note: Sometimes, when adding row level security, the BO Supervisor's response is very slow. Peregrine has identified an issue with databases using Oracle. Business Objects recommends upgrading to Oracle 9.2.0.4 for the database server and Oracle client.

To verify the row level security settings

- 1 Login to BI_PORTAL with bi_admin capability.
- 2 Create a simple report, from Asset Objects. (See the *BI Portal User Guide* for additional information.)
 - a Choose the fields name, type, and subtype fields.
 - b Save the report to the Inventory Management group.
 - c Call this document 'mylist'.
- 3 From the Activity menu in BI Portal, click User Management.

- 4 Add user2 to the group PRGNBIP_SEC_COMPUTER and user3 to the groups PRGNBIP_SEC_COMPUTER and PRNGBIP_SEC_DESKTOP.
- 5 Use User Management to verify that all the users (user1, user2, user3) are in the Inventory Management group.
- 6 Log in to BI Portal as user1.
- 7 Open the report, mylist, and verify that this user is able to see all the data in DEVICE_D table. (Report should consists of type of computer, softwarelicenses, network, hub etc.)
- 8 Log in to BI Portal as user2 and open the report, mylist, to verify that this user is restricted to viewing report data of type 'computer' only. This user is able to see all subtypes like 'Desktop', 'laptop', 'handheld computers' or any subtype.
- 9 Log in to BI Portal as user3 and open the report, mylist, to verify that this user is further restricted to see data of type 'computer' and subtype 'Desktop'.

Once you have created a security group and specified the access restrictions for that group you can add users to the group. The group access restrictions are inherited by all users assigned to the group.

Viewing and synchronizing data security

With row level and object level restrictions scattered in various locations and various groups it can be difficult for an administrator to know what are the restrictions for a user on a particular table or what are the restrictions for a user on any table. BI Portal, at regular intervals as defined in the BI Administration Page, polls the Business Objects Security Databases and gathers row and object level related information and populates it into the following three tables.

- *rdsgroups* - By searching this table, an administrator can determine to what groups a user belongs.
- *rdconditions* - By searching this table, an administrator can determine, what conditions are defined for a group or user.
- *rdsoversecurity* - By searching this table, an administrator can know exactly what filter conditions will be applied for a user. This table is useful when a user belongs to many groups with various conditions defined on each group.

7 Troubleshooting

CHAPTER

This section offers solutions when trying to resolve administration problems.

This chapter covers the following topics:

- *Browser issues* on page 147
- *Tomcat issues* on page 148
- *WebSphere Portal Server issues* on page 149
- *BI Portal fails to start* on page 149
- *BO Administration settings on BI Portal Administration page fail verification* on page 150
- *“BI Initialization Failed” after server reset* on page 154
- *Reports do not return any data* on page 154
- *“BI Server Not Available” message* on page 154
- *Duplicate groups appear in BI Portal or the Business Objects Supervisor tool* on page 155

Browser issues

The following problems can result from the Internet browser you use to view BI Portal.

Navigation Issue

When logged in to BI Portal, using the browser Back, Forward, and Refresh buttons can cause unexpected behavior of BI Portal forms.

Solution Do not use the browser navigation or Refresh buttons with BI Portal forms displayed.

Issue When using the Microsoft Internet Explorer 5.5 browser, the following can occur:

- Icons fail to display in dataset results.
- You cannot personalize Collections and Subdocuments.
- JavaScript errors appear during login (apparent only if the option to display JavaScript errors is turned on for the browser).

Solution Upgrade to Internet Explorer 6.

Issue After changing a theme using the Change Themes page, clicking the Go Back button does not return you to the Home page.

Solution On the Activity menu in the sidebar, click My Home Page.

Issue Using the Back button intermittently produces a page expired error message. This error most often appears when you attempt to return to a list screen from a detail screen.

Solution Create a new search to regenerate your list. BI Portal does not cache what is on the screen.

Tomcat issues

The following problems involve issues with Tomcat as the application server.

Issue Tomcat fails to launch after a new version of the JDK is installed.

Solution When installing a new JDK, you must copy the JAR files from C:\Program Files\Peregrine\oaa\external (or to the installation location you specified) to the new JDK jre\lib\ext directory.

Issue Tomcat and Apache do not automatically start after a UNIX upgrade.

Solution Restart OAA by executing the command:
`/usr/local/peregrine/bin/oaactl restart`

WebSphere Portal Server issues

The following problems occur when using WebSphere Portal Server.

Issue The Web browser displays runtime errors when you view BI Portal inside a WebSphere Portal Server page. This occurs with Internet Explorer version 5.50.4807.2300 SP2, but could also appear with other older browsers.

Solution Upgrade to the latest version of your Web browser.

Issue WebSphere Portal Server does not display the results of the BI Portal form in a new maximized window.

Solution To see form results in a maximized window, maximize the WebSphere portlet first and then submit the form. The results appear in the same portlet.

Issue If a user times out while in a maximized WebSphere Portal Server portlet, clicking on any link returns the user to `http://<server-name>/oaa/login.jsp` instead of the WebSphere Portal Server interface.

Solution Change the default time out parameter.

Issue There are various rendering errors when viewing BI Portal portlets in WebSphere Portal Server when using Netscape 7.0 or Mozilla 1.0+. These errors are due to a known Mozilla bug. See Bugzilla Bug 67903 for additional details.

Solution Use a supported version of Internet Explorer to view WebSphere Portal Server portlets.

BI Portal fails to start

Issue BI Portal fails to start and display the login page.

Solution To correct this problem, perform the following checks:

- Verify all components that are needed by BI Portal 5.1 are properly installed and configured. Refer to *BI Portal 5.1 Installation Guide* for more detail.
- Verify that the Business Objects (BO) server (WebIntelligence service) has started.
- Verify that the ServiceCenter server is running.
- Use BI Administration user interface to test the configuration to ensure the following:
 - The Reporting Data Store (RDS) database and Business Object server database are accessible and that BI Portal can connect to them.
 - Business Objects administration settings verified successfully.

BO Administration settings on BI Portal Administration page fail verification

Issue One or more of the Business Objects Administration setting failed verification.

Solution To correct this problem, perform the following checks:

- Verify that your cluster configuration file (for example, `mycluster.cfg`) that you configured during Business Object installation was copied to the correct location known to the Peregrine BI Portal server.
- Verify that Business Objects server (WebIntelligence service) has started.

Example: ping `[businessobjects]` server

If the response is unknown host or host not found, add the IP address of `[businessobjects]` server system in the `/etc/hosts` file in the case of Unix.

In the case of Windows, you need to add in the IP address of `[businessobjects]` server system in `C:\WINNT\system32\drivers\etc`

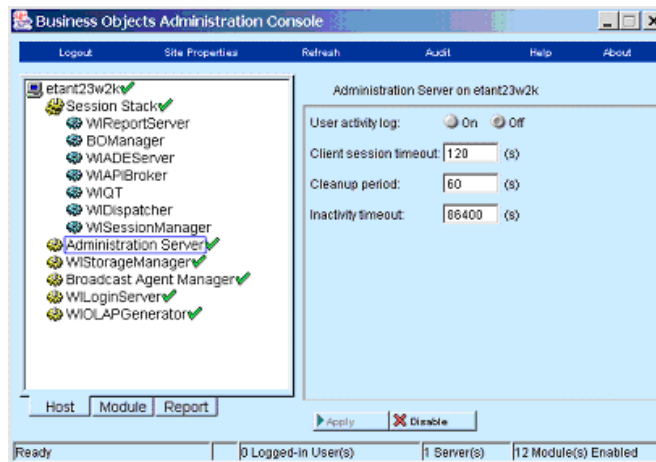
After editing the appropriate file, use the ping command to verify that BI Portal system is able to communicate with BO WebIntelligence System.

Use the ping command to verify that BI Portal is able to communicate with the database hosts also.

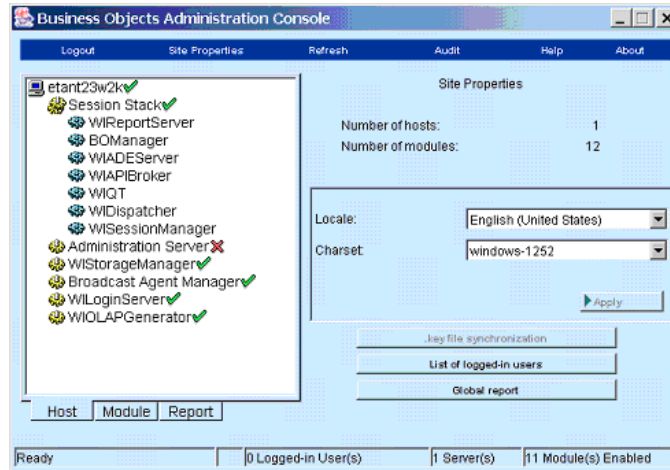
- If it is already running, then verify whether or not the Business Objects Administration server is running. The Business Objects Administration server may have timed out. If that is the case, try to disable and then enable the Business Objects Administration server. After the Business Objects Administration server is running, retry the verification using the BI Administration page.

Use the following steps to re-enable Business Objects Administration server:

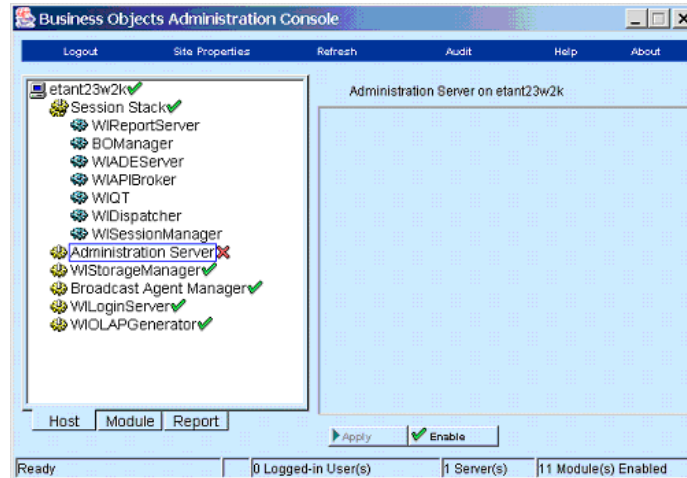
- Log in to the Business Objects Administration Console with a known supervisor user name and password.
- Although it may appear that the server is running, in fact, it may have timed out. Select the Administration Server component in the Business Objects Administration Console window, as shown:



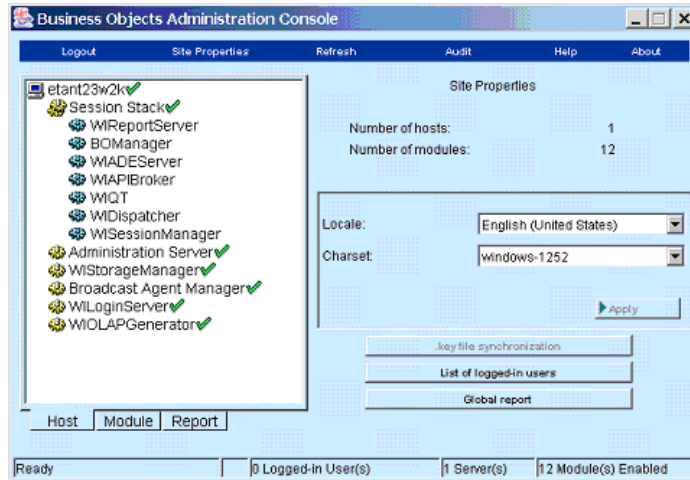
- Click the **Disable** button to disable the currently running Administration Server.



- Select the Administration Server again, and click the **Enable** button to enable the Administration Server session.



- The Administration Server should now be running.



- If the verification still fails, then save all the setting. Restart the Business Objects server. Once the Business Objects server starts successfully, restart the BI Portal application server.
- You should now log in to the *Admin.jsp* page and go to BI Administration and redo the verifications.
- If the verification still fails, then contact Peregrine Technical support for further assistance.

Note: For additional information, refer to the Business Objects documentation.

“BI Initialization Failed” after server reset

If you inadvertently save the wrong settings in the BI Administration screens and then do a reset server, and then go back to BI Administration and correct the settings, save them, and do a reset server; you will get a “BI Initialization Failed” message when you try to access to the Reporting module. You will also see the following message in the archway.log file:

```
BIPortal.Connect(): Exception: WebIntelligence SDK / JSP Exception --- Number
:19001 --- javaError : org.omg.CORBA.OBJECT_NOT_EXIST:
IT_POA:SERVANT_NOT_FOUND minor code: 1230243073 completed: No ---
Description : Common CORBA error 2004-07-22 13:43:53,703 ERROR
[TP-Processor3] System(61A922F2F71BEE1ECDD56B6373DD3E8C) - BIPortal
Initialization Failed.
```

To correct this problem, you must restart the Peregrine Tomcat server. Then you can log in to BI Portal and access the Reporting module.

Reports do not return any data

To have reports return with data

- 1 Create a new connection using the Business Objects Designer tool for the rds database.

File > Parameters.

- 2 Remove the old connection.
- 3 Export the universe again.
- 4 Log on to BI Portal.

The reports should now return data.

“BI Server Not Available” message

If you receive this message when trying to access the Reporting module in BI Portal, you must perform the following steps.

- 1 Restart the Business Objects server.

Make sure the Business Objects server has completely started by viewing the red dot on the Business Objects server icon on the Task Bar. When the red dot is not blinking, the server has completely started.

- 2 Restart your application server.
- 3 Log on to BI Portal.
- 4 Click the **Reporting** icon.

Duplicate groups appear in BI Portal or the Business Objects Supervisor tool

To correct this problem

- 1 Access the Business Objects Supervisory tool.
- 2 Click **Tools > Repository**.
- 3 Select Businessobjects Security and click the **Scan** button.
- 4 In the Scan and Repair window that opens, click the **Repair & Compact** button.
- 5 Click **Close**.
- 6 Select the document domain name and click the **Scan** button.
- 7 In the Scan and Repair window, click **Repair**.
- 8 Click **Close**.
- 9 Restart the Business Objects server.
- 10 Restart your application server.

A BI Portal and ServiceCenter APPENDIX Synchronization

Manually synchronize new BI Portal users with ServiceCenter database

In general, users defined in the operator table of ServiceCenter are synchronized with BI Portal by the `rds_user` scenario at pre-defined intervals. By default, this interval is set to 15 minutes. This means that if a new ServiceCenter operator is added and given access to BI Portal before the Reporting Data Store (RDS) user synchronization interval elapses, this new user does not exist in the `RDS_USER` table of the RDS database until after the next data synchronization cycle completes. In this situation, this user cannot log in to BI Portal until the user becomes a known RDS user.

This section summarizes the steps you can take to initiate an immediate data synchronization using the `rds_user` scenario.

To initiate a data synchronization using the `rds_user` scenario

- 1 From CIT Service console window, stop the `rds_user` scenario.
- 2 Delete the file, `rds_user.ini`, in the `cit` sub-directory under the RDS installation root directory.
- 3 From the CIT Service console window, start the `rds_user` scenario.
- 4 Open the log file, `rds_user.log` in the `logs` sub-directory under the RDS installation root directory and verify that the `user` table has been synchronized.

- 5 Log in to BI Portal as a user with bi_admin capabilities.
- 6 Click **Reporting**.
- 7 From the Reporting tab, click **Synchronize Users** in the Activity menu.
- 8 Click **sync**.
A confirmation message reports the status of your request.

To verify the new ServiceCenter user now has access to BI Portal

- ▶ Log in to BI Portal as the new ServiceCenter user.

Index

A

- Activity menu 35
- adapter transactions, viewing 58
- Admin module
 - changing Settings 49
 - Control Panel 46
 - displaying message queues 56
 - generating web archive files 59
 - importing and exporting personalizations 58
 - message queues 56
 - script status 56
 - Server Log 55
 - Settings page 48
 - showing queue status 57
 - verifying script status 56
 - viewing adapter transactions 58
- Archway architecture
 - building blocks 12
 - clients 14
 - diagram 13
 - requests 16
 - XML 14
- assign users to document groups 130, 131
- assigned documents 131
- authentication
 - contact-based 105
 - models 103
 - overriding the login script 114
 - regular operator 104
 - users 80

B

- BI_Admin capability 124, 130, 132, 133

C

- changing passwords 63
- changing the Peregrine Portal layout 38
- changing themes 40
- components
 - adding Portal 36
 - creating new 35
- contact based authentication 113
- Control Panel 46
- CSS files, editing 25
- customer support 9

D

- deploying themes 22
- document groups 123, 130, 131
 - assigning users to 127
- document management 131–132

E

- Excel format
 - upload reports 122
- exporting personalized pages 58

F

- form details 61
- form details, displaying 61
- Form Info, displaying 59
- form information, displaying 42

framesets, changing 30

G

getit.admin user rights 44
 group management
 add a user-defined group 125
 delete a user-defined group 126
 pre-defined groups 124
 rename a user-defined group 126
 groups
 document 123

H

header graphic, changing 23

I

IBM Websphere portal 59
 importing personalized pages 58
 Info button 61
 Integrated Windows Authentication
 configuring 91
 security 78

J

JAAS
 authentication 80
 login modules 81

L

language
 login 49
 layers, changing 27
 layout, changing
 MSIE 39
 Netscape Navigator 39
 LDAP 78
 Lightweight Directory Access Protocol 78
 local.xml file 44, 48
 log, form details 61
 Logging 50
 file format 51
 file rollover 54
 logging user sessions 63
 login authentication 80
 login language 49

login modules, JAAS 81
 login script, overriding 114
 login.asp 100

M

message queues 56
 message queues, displaying 56
 monitoring user sessions 63
 moving personalized pages 58

O

overriding the login script 114

P

parameters, defining 49
 password, changing 63
 passwords
 protecting 78
 PDF format
 upload reports 122
 Peregrine Portal
 adding components 36
 personalizing 36
 Peregrine Portal, tailoring 21
 Peregrine Systems customer support 9
 personalized pages
 moving 58
 personalizing
 portal 36–41
 personalizing the Peregrine Portal 36
 Portal Components, creating new 35
 pre-defined groups 124
 preXSL, form details 61
 publish
 sample reports 133

Q

queue status, displaying 57

R

rds
 security 113
 reports
 upload 122
 resetting the server 46

S

- sample reports
 - publish 133
- scalability
 - OAA 14
- schemas
 - testing from a URL 17
- script input, form details 61
- script output, form details 61
- script status 56
- script status, verifying 56
- scripts
 - testing from a URL 16
- Secure Sockets Layer 78
- security 113
 - alternate login authentication 114
 - user authentication 80
 - Windows Integrated Authentication 91
- self-registration 62
- server log 55
- Settings page 49
- SSL 78
- synchronize users 132
- system-defined groups 123

T

- tailoring themes 21
 - changing framesets 30
 - changing layers 27
 - changing stylesheets 25
 - changing the header graphic 23
 - deploying themes 22
- technical support 9
- themes
 - deploying 22
 - tailoring 21
- themes, changing 40
- themes, creating 25

U

- unassigned documents 131
- upload reports 122
- URL
 - querying scripts and schemas from 16
- user management 130

- user registration 62
- user rights
 - getit.admin 44
- user session 61
- user sessions, logging 63
- user.log file 63
- user-defined groups 123

W

- web archive (war) files 59
- Websphere portal 59

