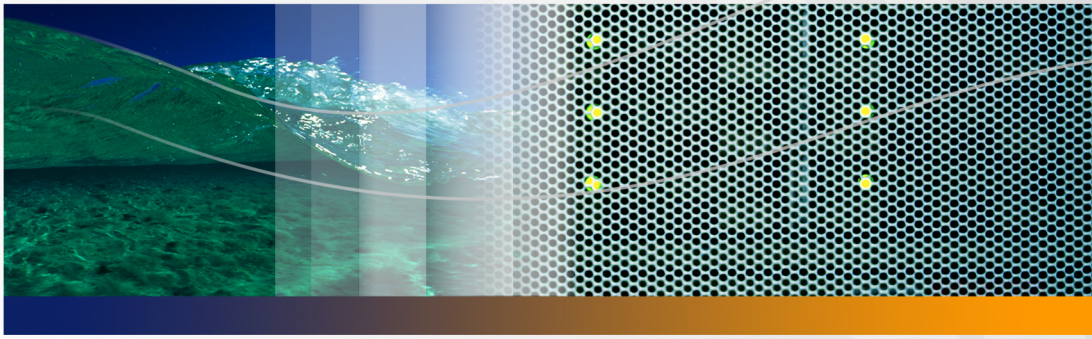
Product Documentation

Peregrine Systems, Inc.

BI Portal 5.2



Administration Guide

Part No. DBNI-52-EN04

Peregrine SYSTEMS

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 5.2 of the licensed program.

Peregrine Systems, Inc.
3611 Valley Centre Drive San Diego, CA 92130
858.481.5000
Fax 858.481.1751
www.peregrine.com

PEREGRINE

Contents

PEREGRINE

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 section	Describes
Chapter 1, Peregrine OAA Architecture Overview	Information about the Peregrine Open Application Architecture.
Chapter 2, Customizing the Peregrine Portal	How to customize the Peregrine Portal.
Chapter 3, Using the Peregrine Portal	How to use the Peregrine Portal.
Chapter 4, Using the OAA Administration Module	How to use the OAA Administration module.
Chapter 5, Security	Security options for the portal.
Chapter 6, BI Portal Administrator Functions	How to use the BI Portal Administration functions.
Chapter 7, Troubleshooting	Troubleshooting suggestions.
Appendix A, BI Portal and ServiceCenter Synchronization	Manually synchronizing new BI Portal users with the ServiceCenter database.
Appendix B, BI Portal and AssetCenter Synchronization	Manually synchronizing new BI Portal users with the AssetCenter database.
Appendix C, Copyright Notices	Additional copyright information.

Related Documentation

In addition to this guide, the following documentation is available for the BI Portal product and for WebIntelligence. Unless otherwise noted, the documentation is available at *http://support.peregrine.com*.

Manual	Description
BI Portal User Guide	Provides base reports and describes how to create and work with both base and custom reports.
BI Portal Installation Guide	Describes how to install and configure the application and Web servers for BI Portal.
RDS for ServiceCenter Administration Guide	Provides information about customizing the RDS for ServiceCenter.
RDS for AssetCenter Administration Guide	Provides information about customizing the RDS for AssetCenter.
BI Portal Release Notes	Includes last-minute enhancements, known issues, and closed issues.
WebIntelligence User's Guide	Describes how to use WebIntelligence for building and running queries, reporting, and analysis. This is available using the Help button of the WebIntelligence Java Report Panel, which is accessed when creating or editing reports.

Typographical conventions

This guide uses typeface conventions to indicate special terms and actions.

Convention	Meaning
Bold	Information that you must type exactly as shown appears in bold. The names of buttons, menus, and menu options also appear in **bold**.
Italics	Variables and values that you must provide are in *italics*. New terms and book titles also are in *italics*.

`Monospace`	Code or script examples, output, and system messages are in a `monospace` font.
	`var msgTicket = new Message( "Problem" );`
	…
	`msgTicket.set( "_event", "epmc" );`
	
	An ellipsis (…) indicates that portions of a script have been omitted because they are not needed for the current topic. Samples of code are not entire files, but they are representative of the information discussed in a particular section.
	Filenames, such as `login.asp`, appear in a `monospace` font.

Special elements

This guide uses special elements to help you locate information. These special elements and their uses are in the following table.

Element	Usage
Important:	Information that is required to complete a task
Note:	Information that is of general interest
Tip:	Information that can make a task easier or faster
Warning:	Information that is needed when there is a risk of losing data

Need further assistance?

For further information and assistance with this release, you can download documentation or schedule training.

Customer Support

For further information and assistance, 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 your answer. The first place to search is the KnowledgeBase, which contains informational articles about all categories of Peregrine products.
4. 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 on the Peregrine Customer Support Web.

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 using 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.

CHAPTER 1

Peregrine OAA Architecture Overview

Peregrine Open Application Architecture (OAA) 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 overview

Peregrine OAA is the underlying architecture for many Peregrine products, including, but not limited to, the Get-It suite of Employee Self-Service products.

OAA Product	Description
AssetCenter Web	Web-based application that enables access to the AssetCenter database to all users without having to install the AssetCenter client.
BI Portal	Web-based reporting tool for creating and executing queries against ServiceCenter and AssetCenter data; and for generating reports and graphs based on that data.
Get-Answers	Web-based, knowledge management application that enables you to capture and store knowledge in a database, and to search for that knowledge when you need it. Using Get-Answers, you can improve the quality and accuracy of the knowledge that people in your company use to perform their jobs, and help them avoid calls to the service desk.

OAA Product	Description
Get-Resources™	Web-based solution that integrates with AssetCenter Procurement, AssetCenter Portfolio, or ServiceCenter Request Management to enable employees to create requests for resources and to streamline the approval workflow of those requests throughout the organization.
Get-Services™	Web-based extension of ServiceCenter that enables users to report problems in the work environment by opening problem tickets in Get-Services and then store them in the ServiceCenter back-end system. This allows users to view tickets from Get-Services and ServiceCenter. Modules include Service Desk and Change Management.

Peregrine OAA 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 Peregrine OAA are monitored and maintained.

The base of Peregrine OAA includes:

Component	Description
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	Peregrine OAA 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.

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

Component	Description
Adapters	Enables connection to the back-end system database. The adapter required by your Web application is deployed during the installation.
OAA Persistence (Get-Answers only)	Provides a general purpose database that is used by certain Peregrine Web applications. OAA Persistence provides data persistence to a database.

Component	Description
OAA Workflow (Get-Answers only)	Enables workflow capabilities used by some Peregrine OAA Web applications.
Notification Services (Get-Answers only)	A centralized service for sending and receiving notifications through multiple communication devices and for tracking the status of these notifications.

Separate documentation for Notification Services is provided with the Web applications that use this feature.

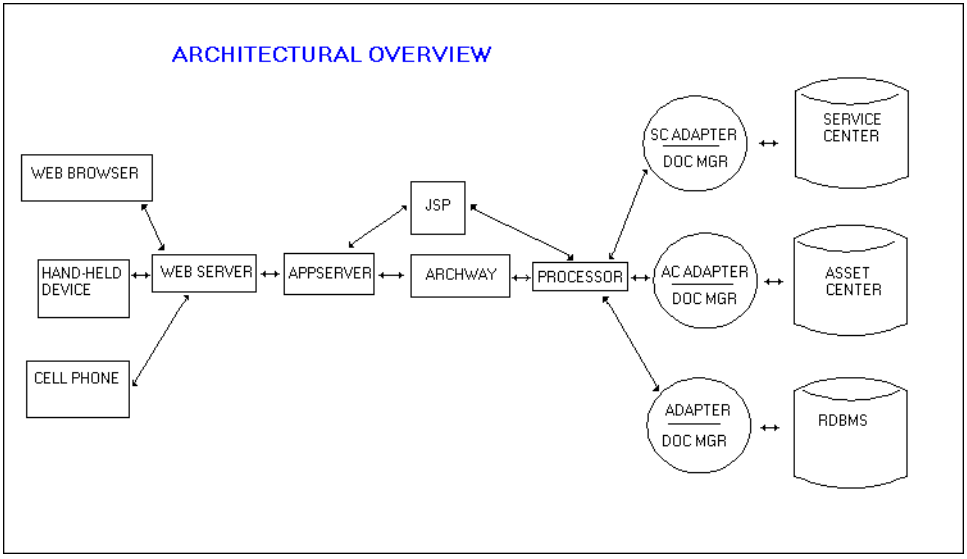
Peregrine OAA architecture

Peregrine OAA 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 supports Apache Tomcat, WebSphere, and WebLogic.
Common clients	Applications can be deployed with Web browsers (for example, IE, Netscape, and Mozilla), 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 can contact Archway and supply it with a new purchase request to be entered into the database.

All requests and responses are formatted using XML, such as the following problem ticket expressed in XML.

```
<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/*.

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, except BizDocAdapter, use `DLLs` (or `.so` files on Unix) 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/oaa/servlet/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 `/oaa/servlet` mapping assumes that you are using the default URL mapping that BI Portalautomatically 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/oaa/servlet/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 `/oaa/servlet` 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/oaa/servlet/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 `/oaa/servlet` 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:

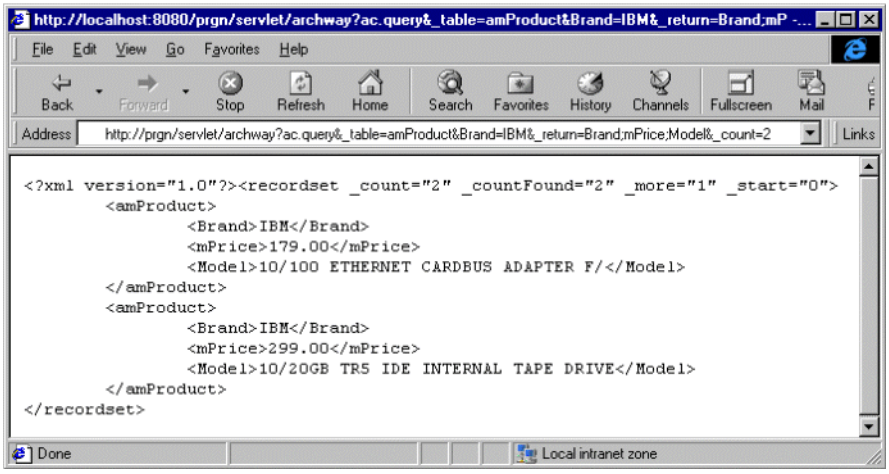
- *host name/oaa/servlet/archway?sc.query&_table=probsummary&priority.code=1*

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

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

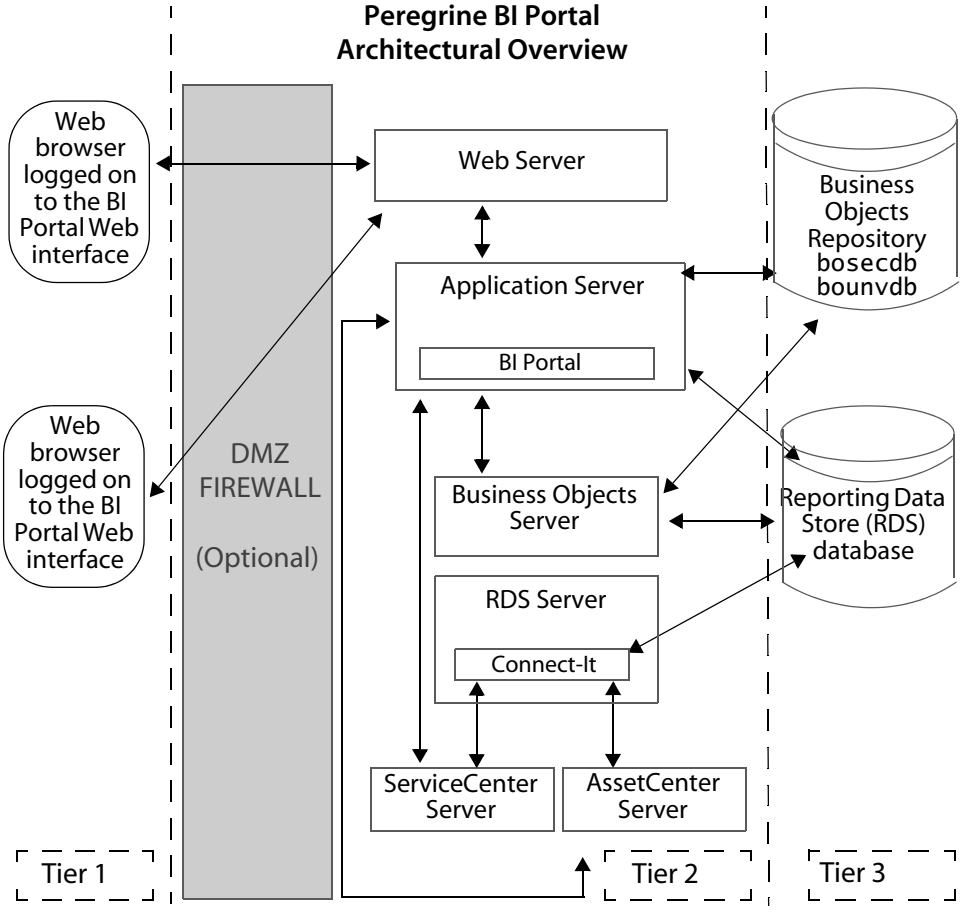
  This sends a query request to AssetCenter for the first two records in the `amProduct` table. Only the **Brand**, **mPrice**, and **Model** fields are returned for each record.

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



BI Portal architecture

The following figure illustrates the BI_Portal architecture.



CHAPTER 2 Customizing the Peregrine Portal

Peregrine 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 BI 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
- Creating script extensions

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 screen shots 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:

Theme	Description
Accessible	Makes the screen available to users who need high contrast colors or better accessibility support. It provides 508 compliance.
Baja	Adds southwestern green and beige hues to the Classic design.
Quicksilver	Adds silver and blue hues to the Classic design.
Sierra	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\Portal\image\images\skins\classic`

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/oaa/admin.jsp`) as the system administrator.

2 Click **Settings** > **Themes.** Change the following parameters:

- In the **Default skin/Theme** field, change the parameter to the name of the theme you want to use (for example, *Baja*).
- In the **Default style sheet** field, change the parameter to the appropriate name for the CSS file (for example, `baja.css`).
- In the **Default XSL templates** 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 Click the **Control Panel** link on the Admin Settings menu.

5 When the Control Panel opens, click **Reset Peregrine Portal**.

6 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 BI 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 on page 30.

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 on page 36.

2 Save your custom header graphic to the following location:

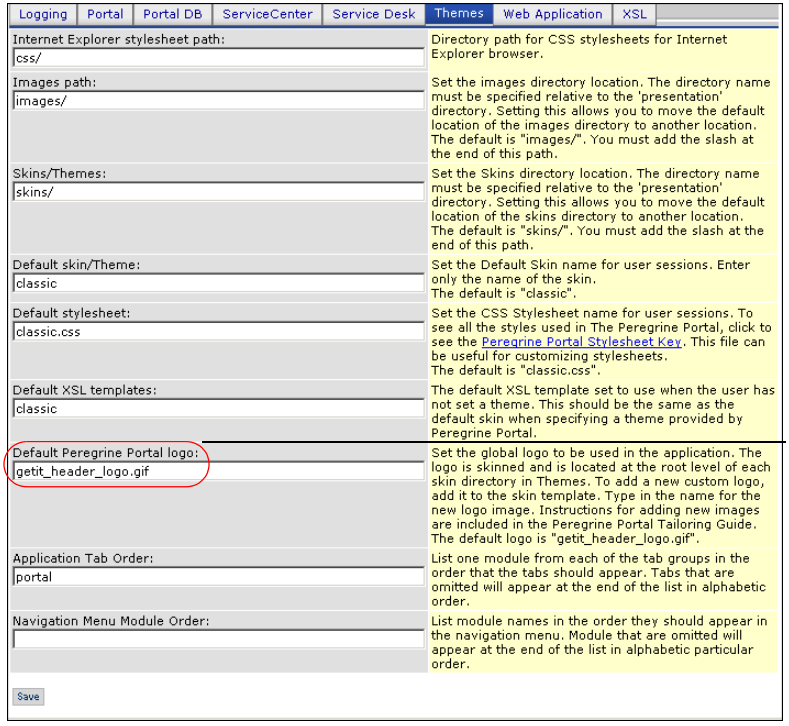
```
C:<AppServer>\webapps\oaa\images\skins\classic
```

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, type the name of your custom header logo.



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

7 Click the **Control Panel** link on the Admin Settings menu.

8 When the Control Panel opens, click **Reset Peregrine Portal**.

9 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, style sheets, and XSL templates. The default path for these files is:

File type	Location
Images	C:\Program Files\Peregrine\Portal\image\images \skins\<a_theme>
Style sheets	C:\Program Files\Peregrine\Portal\image \css\<a_theme>.css
XSL templates	C:\Program files\Peregrine\Portal\image \WEB-INF\templates\<a_theme>

2 Paste and then rename the folders for the classic theme to a new name. For example:

Images	C:\Program Files\Peregrine\Portal\image\images \skins\myTheme
Style sheets	C:\Program Files\Peregrine\Portal\image \css\myTheme.css
XSL templates	C:\Program files\Peregrine\Portal\image \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 `myTheme.css` file in your new theme.

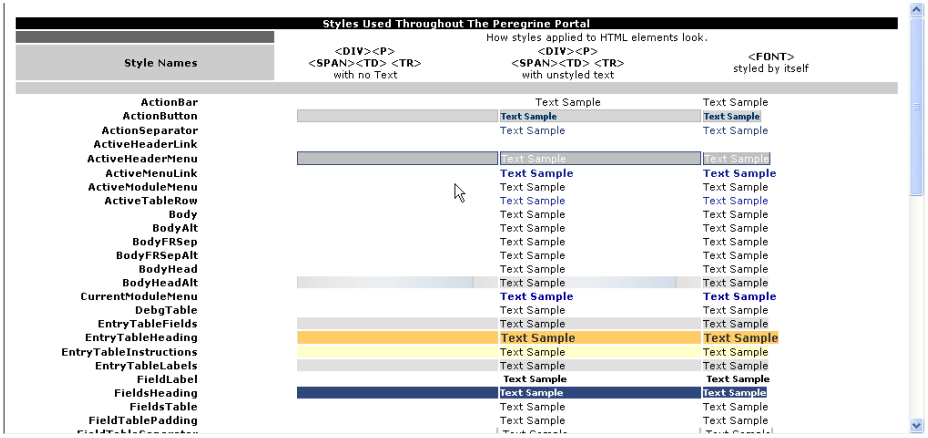
The following table lists some of the more commonly modified styles.

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

Note: You can see a detailed style sheet key in the themes Administration section of the Portal. To access the style sheet key, locate the Default style

sheet field on the Themes tab of the Admin Settings page and click the **Peregrine Portal Stylesheet Key** link.



5 Save your theme style sheet with the same name as your new theme. For example, `C:\Program Files\Peregrine\Portal\image\css\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, see Layers properties on page 34.

7 Open and edit any XSL style sheets you want to change.

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

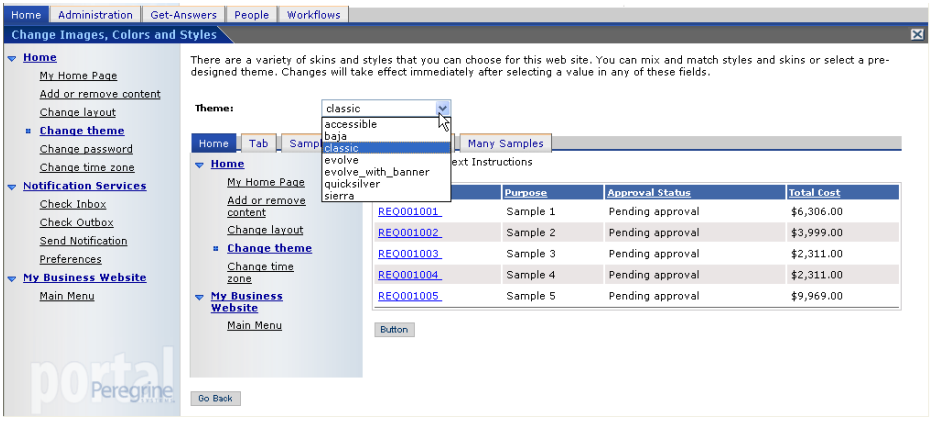
The XSL style sheets determine how BI Portal displays form components in the main portal frame.

The following table lists the XSL style sheets you can change.

To change	edit this XSL stylesheet
Attachment picker	attachments.xsl
HTML form generation	basic-form.xsl
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 checkbox 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;">
<img name="logo" border="0" src="<%= logo %>" alt="logo"></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%"> </td>
<td nowrap width="3" align="right" valign="top">
<img src="<%= Archway.getSkinImagePath("backgrounds/rt_l.gif",
user ) %>">
</td>
<td nowrap align="right" valign="top" width="100%"
background="<%=
Archway.getSkinImagePath("backgrounds/rt_tile.gif", user ) %>">
<img src="<%=
Archway.getSkinImagePath("backgrounds/rt_tile.gif", user ) %>">
</td>
<td nowrap><font class="userBarText" size="1" face="Arial,
Helvetica, sans-serif"><%=userTitle%></font>  </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;"> 
</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\Portal\images\skins\<mytheme>`.

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. Open the browser-specific frameset file `frames_<xx>.jsp` in a text editor (where `<xx>` is `ie` for Internet Explorer).
2. Modify the frameset properties.
3. Save the file.

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

frames_ie.jsp

```
<%@ include file="../../../jspheader_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>
```

admin_frames_ie.jsp

```
<%@ include file="../../../jspheader_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_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>
```

Creating script extensions

By creating ECMA script extensions, you can modify the actions of the out-of-box script without changing the original script. Extension scripts are added to the `jscriptextensions` directory under `WEB-INF/apps/<component>`, where `<component>` is the name of an application module (for example, `common`, `portal`, and so on).

When adding extension scripts, you must:

- Preserve the hierarchy (path) of the out-of-box script under the `jscriptextensions` directory.
- Use only one extension per OAA `.js` file.

The extension file can declare new functions as well as functions that override functions of the same name in the out-of-box file. The object created to represent the out-of-box file is configured as the *prototype* object of the extension object.

You can call original function implementations from a function that overrides the original by appending `proto` to the function reference. For example, to call the out-of-box implementation of `login.login()`, use `proto.login.login(msg);` from the `login()` method declared in the extension file.

The following example writes a message to the archway log when the user logs in.

```
function login( msg )
{
  env.log("*** YOUR MESSAGE GOES HERE*** ");
  return proto.login.login(msg);
}
```

Note: The relative path of the example extension file is `..\WEB-INF\apps\common\jscriptextensions\login.js`.

If the out-of-box method calls other functions that are also overridden in the extension file, use the following technique to ensure that the new implementations of the secondary functions are called:

```
proto.login.login.apply(this, arguments);
```

where `arguments` is an implicit variable that exists in the context of an ECMA Script function.

```
function login( msg )
{
  env.log("*** YOUR MESSAGE GOES HERE*** ");
  return proto.login.login.apply(this, arguments);
}
```

CHAPTER 3 Using the Peregrine Portal

The BI 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.

Topics in this chapter include:

Logging in to the Peregrine Portal

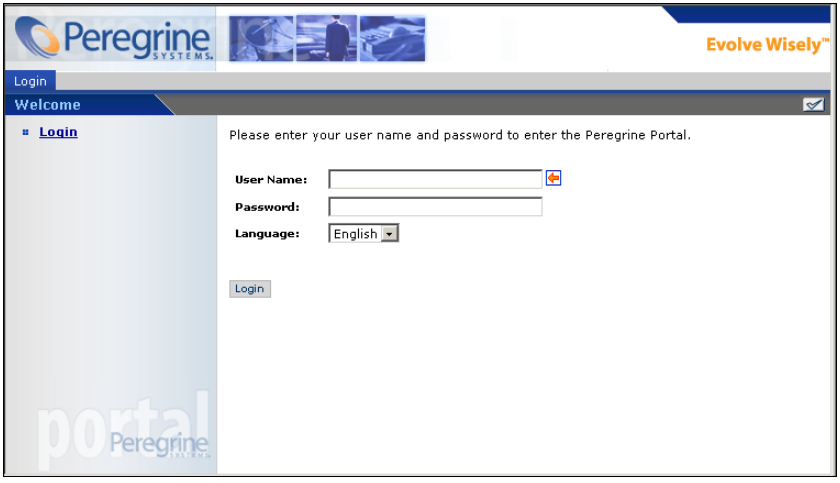
There are two login screens that provide access to the Peregrine Portal:

Login screen	URL
User login	*http://<server>/oaa/login.jsp*
Administrator login	*http://<server>/oaa/admin.jsp*

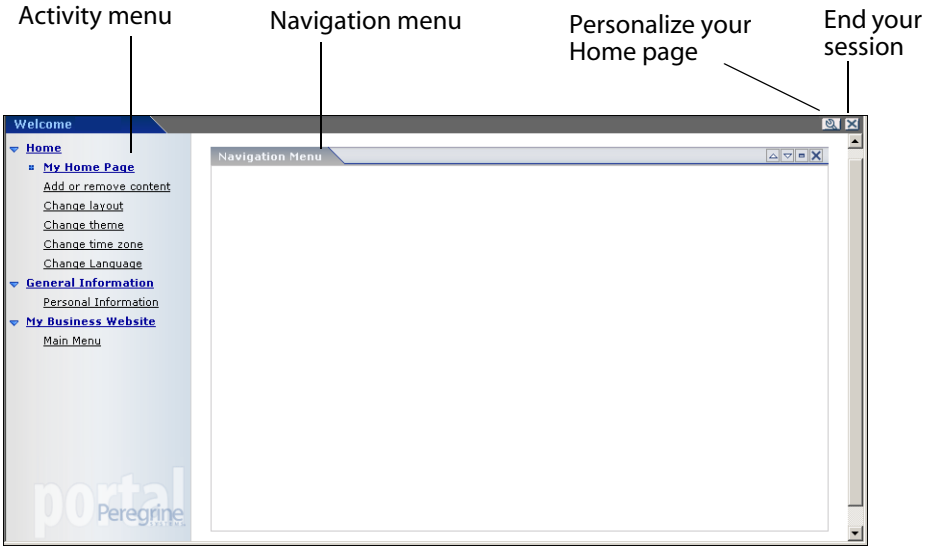
Note: An alternative to this login method is the Integrated Windows Authentication. See the Security chapter of this guide.

Note: 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. Enter your user name and password. In the Language pull-down list select the language that you want the Peregrine Portal to display. English is the default login language, but you can enable other languages in the Settings page of the Administration Control Panel. For more information about enabling login languages, see the section Choosing a Login Language.



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 BI 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.

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 6.0+.

Administration components

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

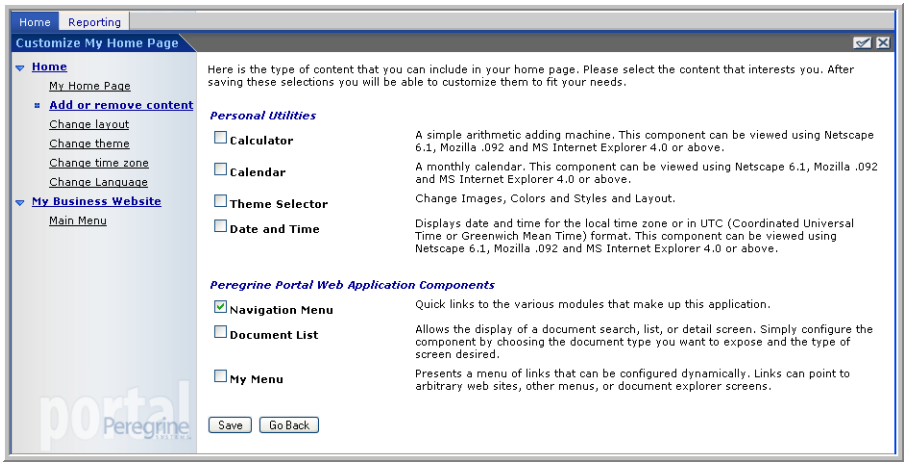
This component	Provides
Connection Status	A list of the adapters currently registered in this server and their connection status.
Control Panel	A button to reset the server and all its connections.
Page Hits / Minute	A list of the total number of pages accessed per minute.
Adapter Transactions / Minute	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 with a list of the components available for customizing.



2 Select the components you want to either add or remove from 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**.

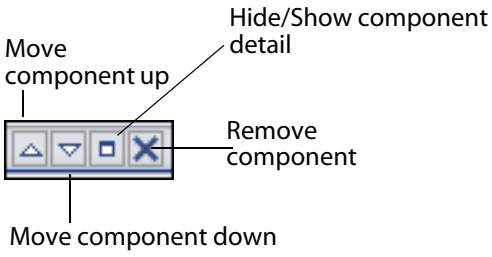
When you return to the Peregrine Portal, the new components appear in the Peregrine Portal. The following example shows the .

Changing the layout

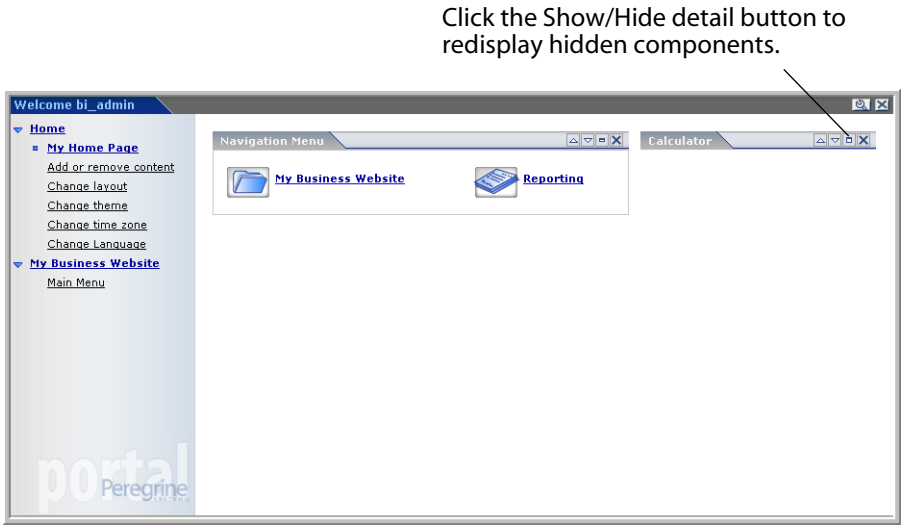
The following sections contain procedures for changing the location of the components or removing them from the Peregrine Portal. Your Web browser determines the procedure you use.

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.



The following screen shows the Calculator hidden or minimized.

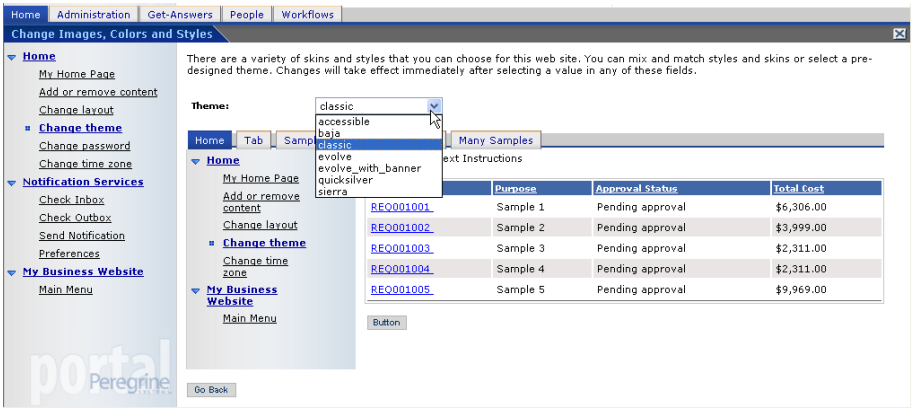


Changing themes

You can choose from a number of themes to change the look of your Web pages. The out-of-box installation provides several themes from which you can choose. If you want to deploy additional themes, refer to Customizing the Peregrine Portal.

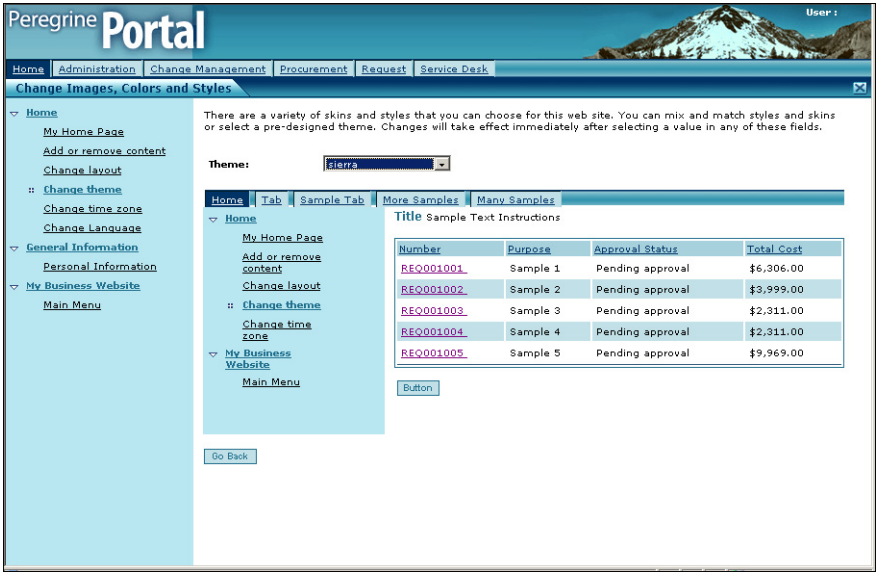
To change the theme:

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



2 Choose a theme 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.



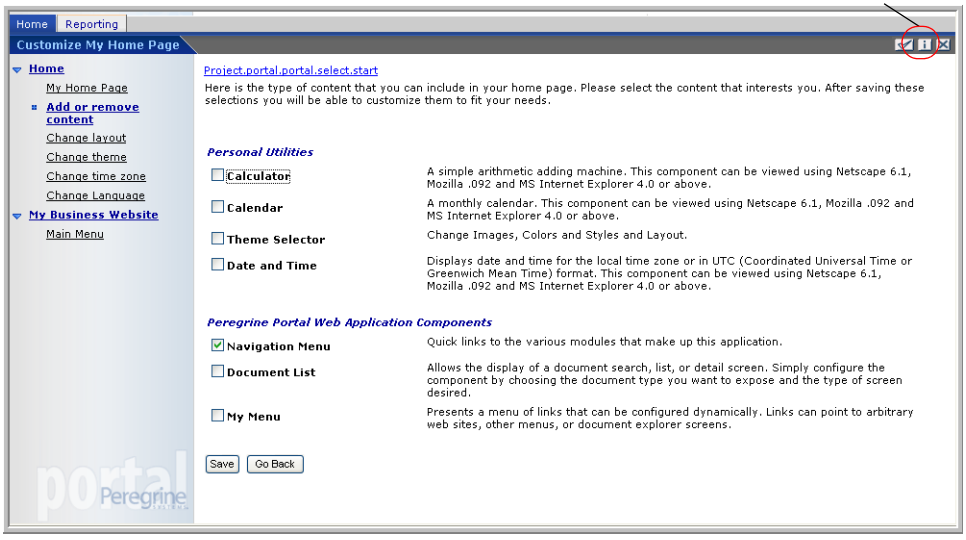
This new configuration remains through subsequent work sessions for the user until changed by the user.

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.



CHAPTER 4 Using the OAA Administration Module

This chapter includes instructions for administering your BI Portal system.

Topics in this chapter include:

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 or AssetCenter user with **getit.admin** rights to access the Admin module and administer the BI Portal integration with ServiceCenter and/or AssetCenter. 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.

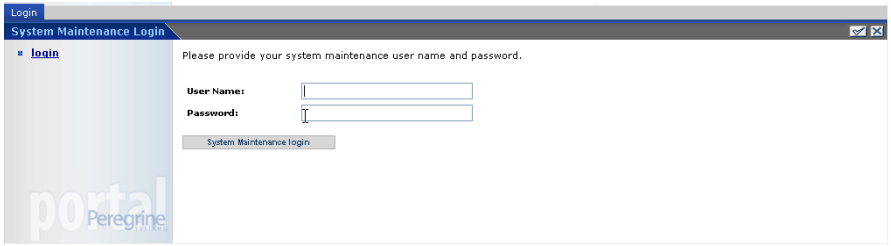
Important: When you change parameters using the Admin module, a `local.xml` file is created in the `\<AppServer>\WEB-INF` directory (where `AppServer` is the path to your application server) to store these parameters.

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:

   ```
   http://<hostname>:<port>/oaa/admin.jsp
   ```

3 Press Enter to open the Portal administrator login page.

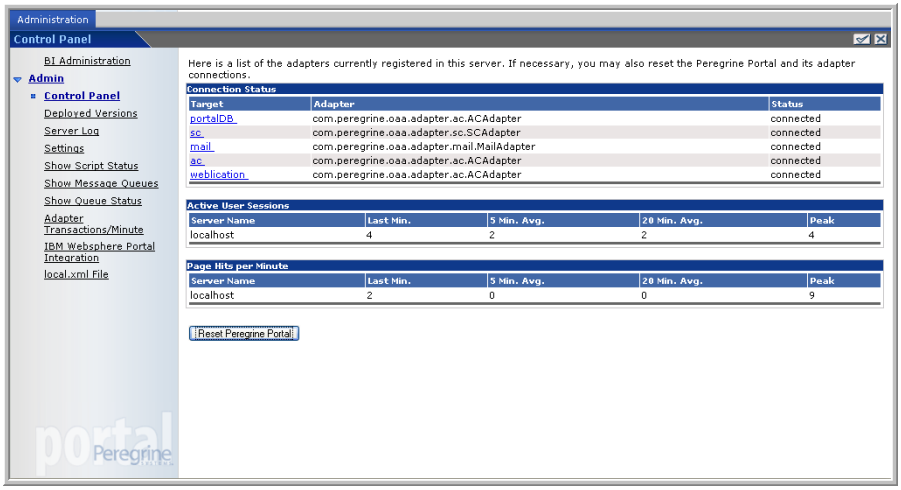


4 In the Name field, type **System**.

No password is required on initial login.

5 Click **System Maintenance login.**

6 Click **Control Panel** to open the Control Panel page.



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 application 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
local.xml File	Download the local.xml file

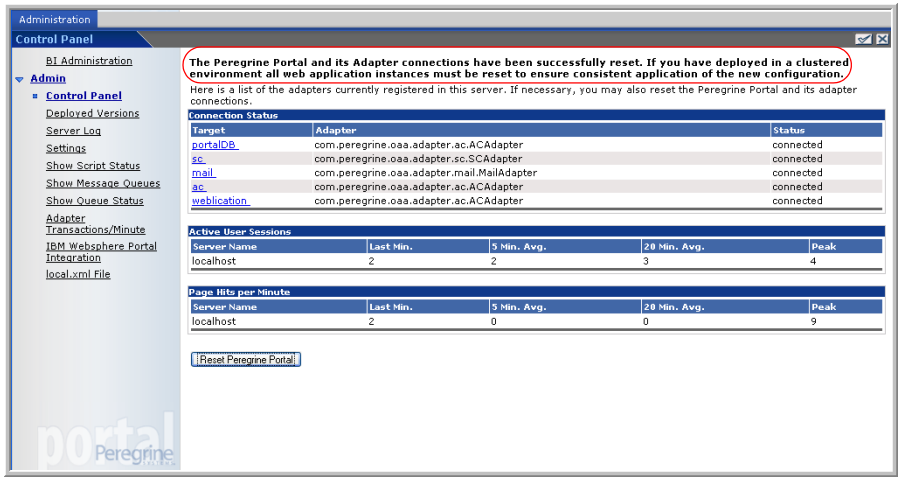
Using the Control Panel

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 Peregrine Portal.**

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



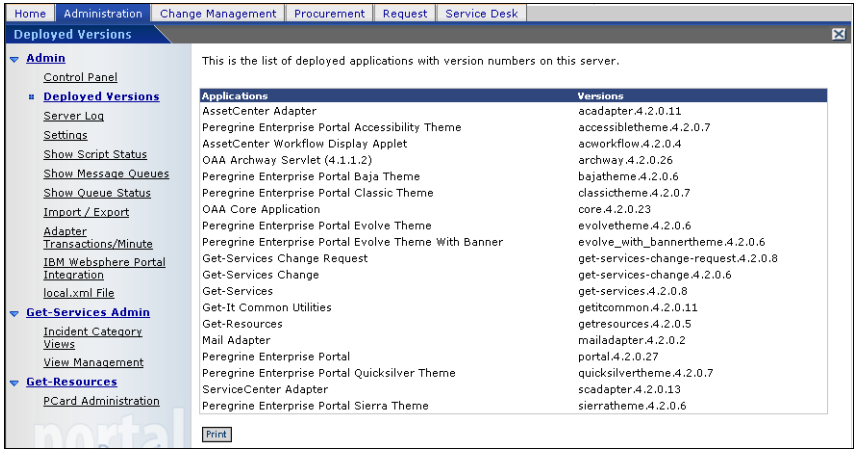
Viewing the Deployed Versions

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**.

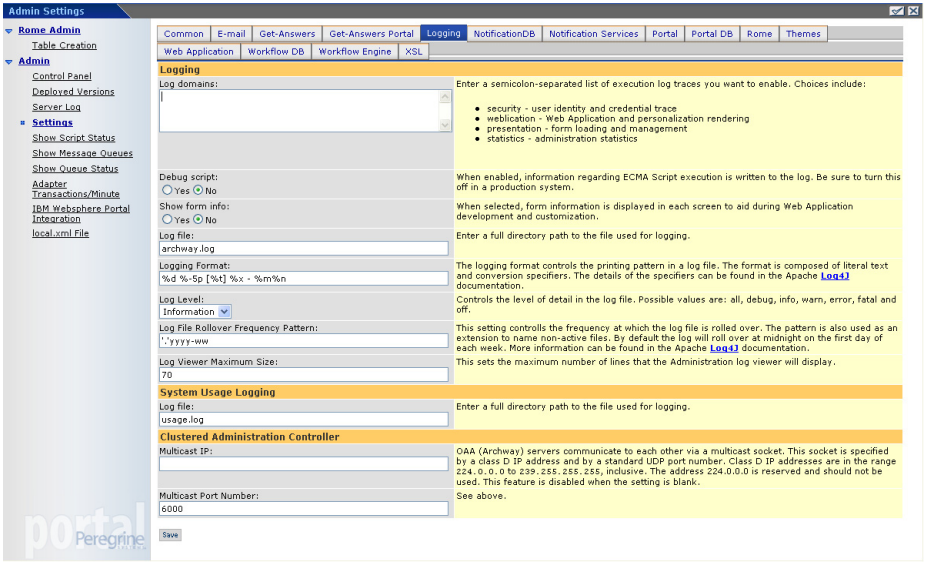
A list of the installed packages opens.



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

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`. A sample list appears in the text describing the Log domain text box.



The valid debug domains include the following:

acadapter	AssetCenter adapter (authentication, authorization, and adapter services)
scadapter	ServiceCenter adapter (authentication, authorization, and adapter services)
mailadapter	used for email
trigger	schema object trigger subsystem
bizdocadapter	BizDoc adapter (authentication, authorization, and adapter services)
presentation	how personalizations are delivered
personalization	wrench icon
weblication	personalization operations
archway	Archway services

ProcessorFactory	OAA internal request handling system (script, database and administration)
AdminController	Administrative request handling object
security	JAAS login modules to authenticate users
statistics	fundamental OAA statistics (moving averages)
oaaworkflow	workflow processes
templateengine	workflow templates
notificationservices	periodic script pollers that check for workflow assignments and workflow-related email notifications

The Log Level parameter allows you to specify the level of detail for the log information written to the log file. The All setting captures the most detail and the other settings specify various degrees or types of information collected for the specified Log domains. Possible values are: all, debug, info, warn, error, fatal and off in reverse order of detail. Typically this setting should be left at warn or error so the logs indicate any significant problems encountered during production use. The more verbose settings of debug and info should be used during tailoring or problem isolation.

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	Used to output the category of the logging event. The category conversion specifier can be optionally followed by *precision specifier*, which is a decimal constant in brackets. 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. For example, for the category name "a.b.c" the pattern %c{2} is output as "b.c".
C	Used to output the fully qualified class name of the caller issuing the logging request. This conversion specifier can be optionally followed by *precision specifier*, which is a decimal constant in brackets. 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. For example, for the class name "org.apache.xyz.SomeClass", the pattern %C{1} is output as "SomeClass". **Note:** Generating the caller class information is slow. Avoid it unless execution speed is not an issue.

d	Used to output the date of the logging event. The date conversion specifier may be followed by a *date format specifier*, which is enclosed in braces, such as
	`%d{HH:mm:ss,SSS}`
	or
	`%d{dd MMM yyyy HH:mm:ss,SSS}`
	If no date format specifier is given then ISO8601 format is assumed.

F	Used to output the file name where the logging request was issued. **Note:** Generating caller location information is extremely slow. Avoid it unless execution speed is not an issue
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 *extremely* slow. Avoid it unless execution speed is not an issue.

Conversion character	Effect
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.
X	Used to output the MDC (mapped diagnostic context) associated with the thread that generated the logging event. The X conversion character *must* be followed by the key for the map placed between braces, as in: `%X{clientNumber}` where `clientNumber` 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

The Apache DailyRollingFileAppender class determines the log file rollover frequency.

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.

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.

Using the Settings page

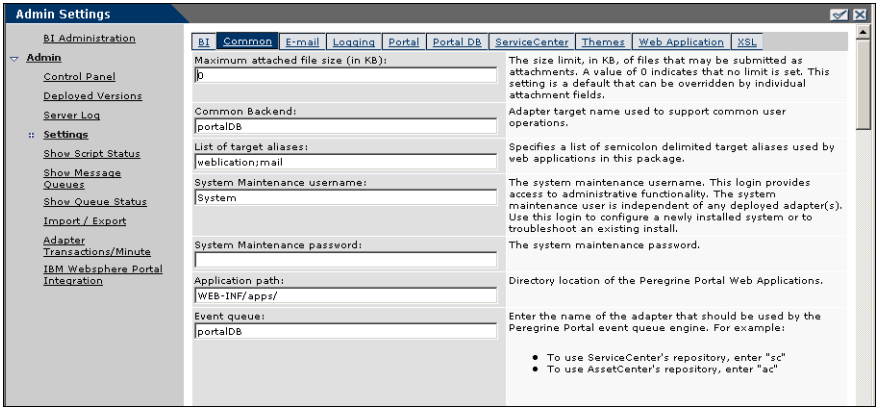
On the Activity menu, click **Settings** to open the current parameter settings. The Settings page is divided into tabs. The tabs that you see depend on the Web applications that you installed and the adapters that you use. The Common tab is available for all installations.

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. Use the E-mail tab to configure E-mail, so that users are notified by E-mail of their password when users have access to self-registration (see User self-registration on page 73).

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.



Setting parameters using the Admin module

When you make changes using the Admin Settings page, a `local.xml` file is created in the `C:\<AppServer>\WEB-INF` directory. All changes to property

settings are stored in this file. Restart the application server after making changes that are stored in `local.xml`.

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.

3 From the Activity menu, click **Control Panel** > **Reset Peregrine Portal**.

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.

Note: You can only enable additional languages if the language packs are deployed.

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.

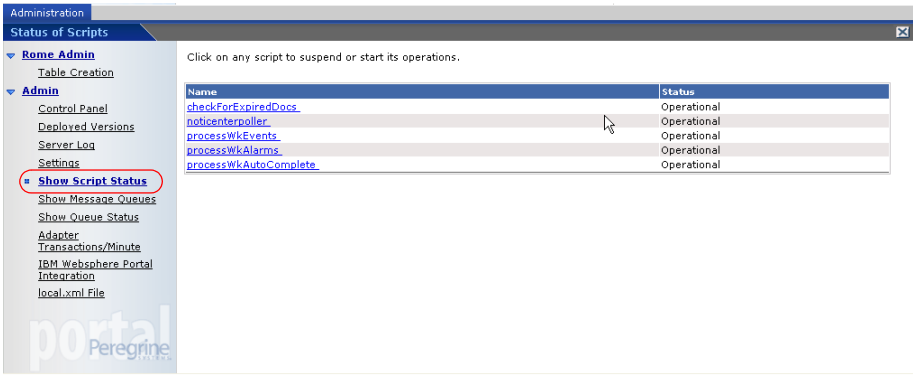
4 Make sure that **Yes** is specified for **Enable Logout**. This is important because you need to log out of the Peregrine Portal and log back in for your changes to take effect.

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.



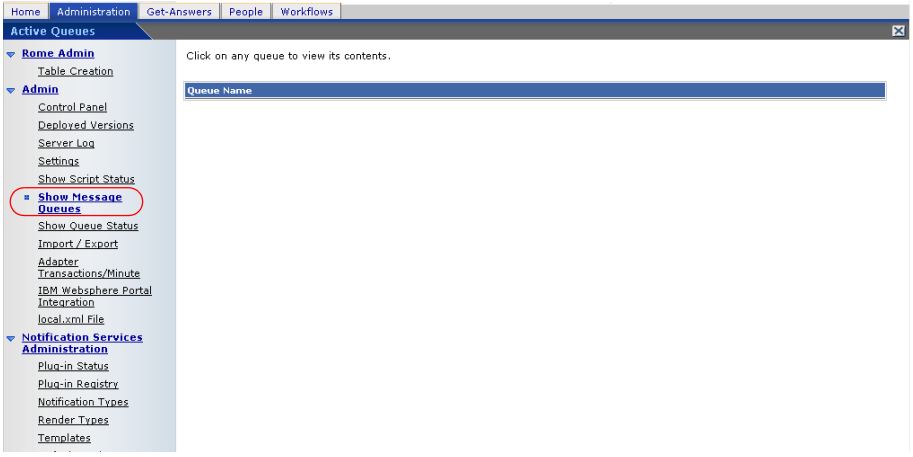
2 Click on the script to suspend it.

Displaying Message Queues

The Message Queues display 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.



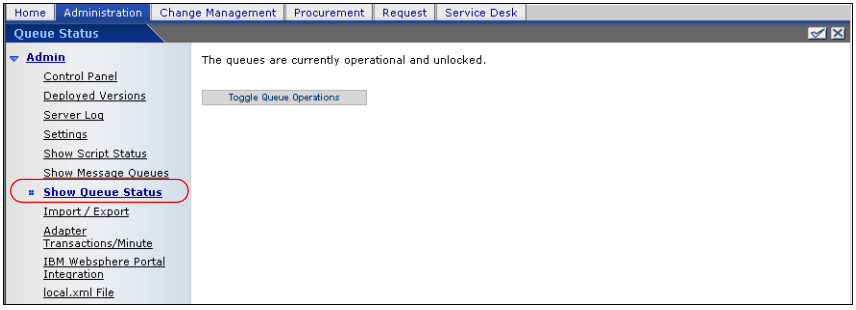
2 Click the queue name in the list to view the contents of a queue.

Showing Queue Status

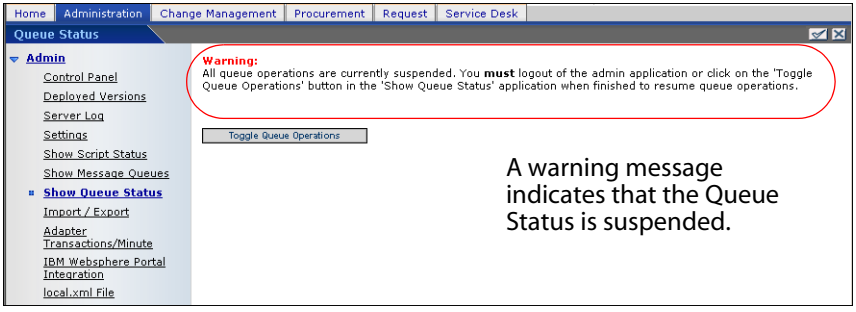
Use the Show Queue Status option to verify or change the status of the message queues.

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**.



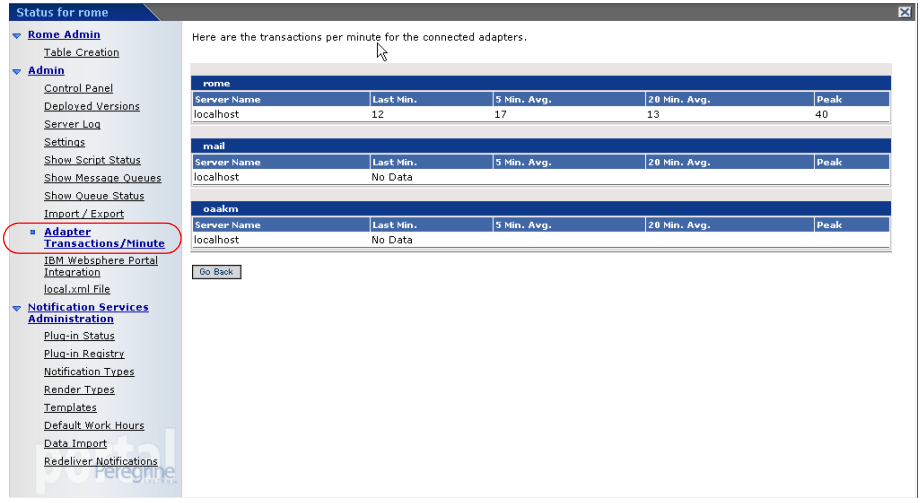
3 Click **Toggle Queue Operations** to return to the operational status.

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.

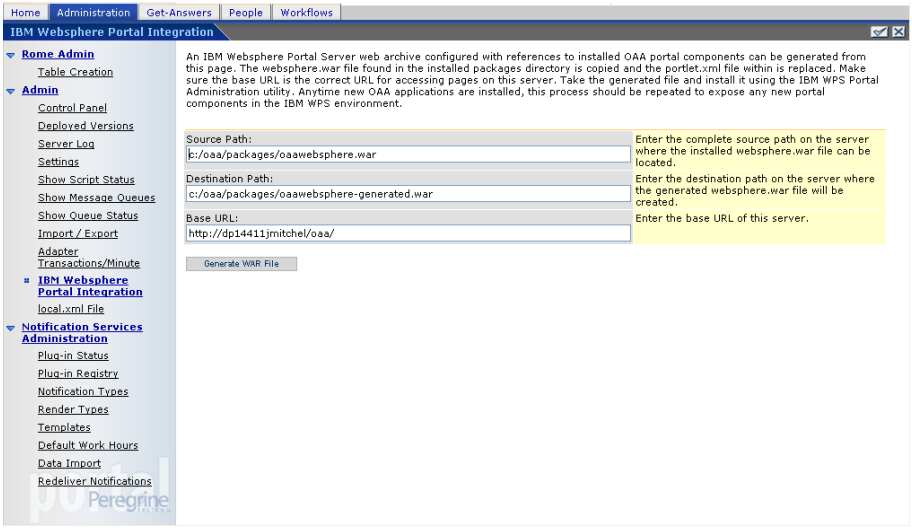


Using the IBM WebSphere Portal

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.



2 Enter the following information:

- source path
- destination path
- base URL

3 Click **Generate WAR File**.

Downloading the local.xml file

When you change parameters using the Admin module, a `local.xml` file is created in the `\<AppServer>\WEB-INF` directory (where `AppServer` is the path to your application server) to store these parameters. You can download the `local.xml`to preserve your settings if you want to test other settings and then replace the `local.xml` file your test created with your original `local.xml`.

To download the local.xml file:

1. From the Activity menu, click **local.xml File** to open the Download local.xml File page.
2. Click **Download**.
3. In the File Download dialog box, select **Open** or **Save**.
4. If you selected Save, specify the save location for the `local.xml` 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:

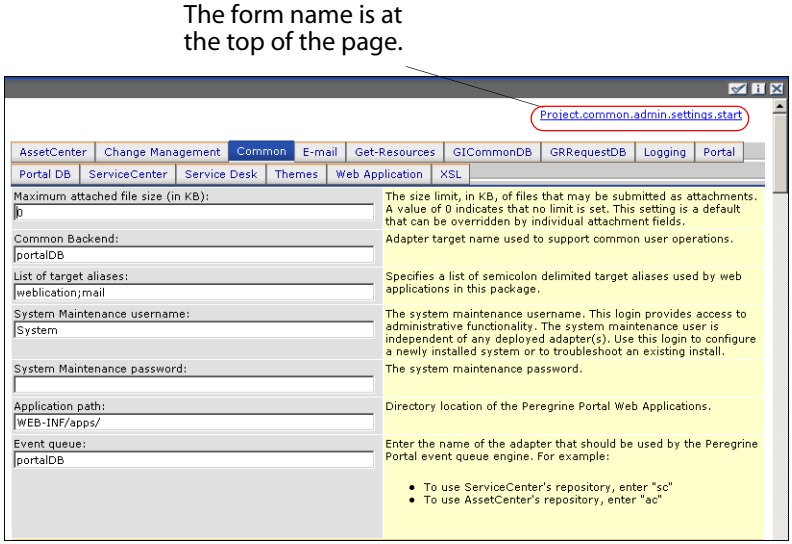
1. From the Admin module, click **Settings** > **Logging**.

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

3 Click **Save**.

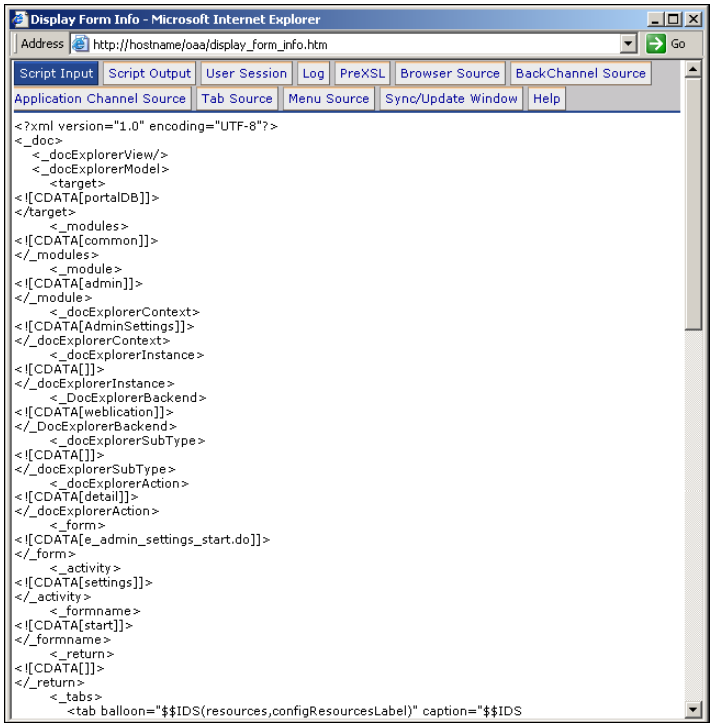
4 For this particular setting, it is not necessary to Reset Peregrine Portal.

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



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.



This is a partial example of the contents in the PortalDB tab.

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

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.

This tab	Contains
Application Channel Source	HTML source code for the shared applications.
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.

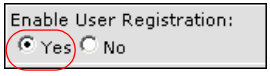
User self-registration

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 or AssetCenter database. In ServiceCenter, BI Portal creates an operator and contact record for the new user with basic user login rights. In AssetCenter, BI Portal transforms this data into a Profile record that then passes to your AssetCenter system. An amEmplDept record is created with the user-supplied data and the default Profile `getit.default` is assigned. 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 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 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 Documentation for instructions.

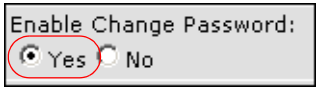
Changing passwords

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**.



Click Yes to give users the ability to change their own passwords.

3 Click **Yes**.

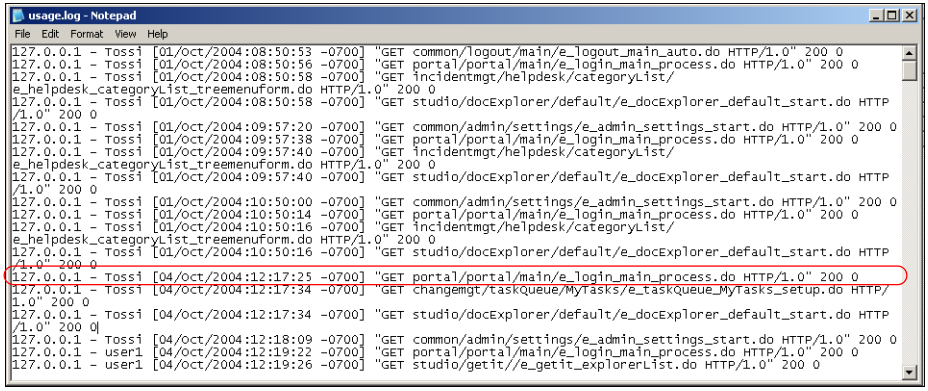
Logging and monitoring user sessions

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.

```
127.0.0.1 - Tossi [04/Oct/2004:12:17:25 -0700] "GET portal
/portal/main/e_login_main_process.do 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
127.0.0.1	-	Tossi	[04/Oct/ 2004:12:17 :25 -0700]	"GET portal/portal /main/e_login_main_ process.do 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.
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 to sett the PortalDB, Web Application, and Portal adapters to support the deployed BI Portal environment.

You log in to the Admin module of the BI Portal Web interface to configure BI Portal. You must change the adapters and the BI Portal Session Timeout interval.

The default administrator, **System**, gives you access to the Admin module.

To access the Peregrine Portal administrator login page:

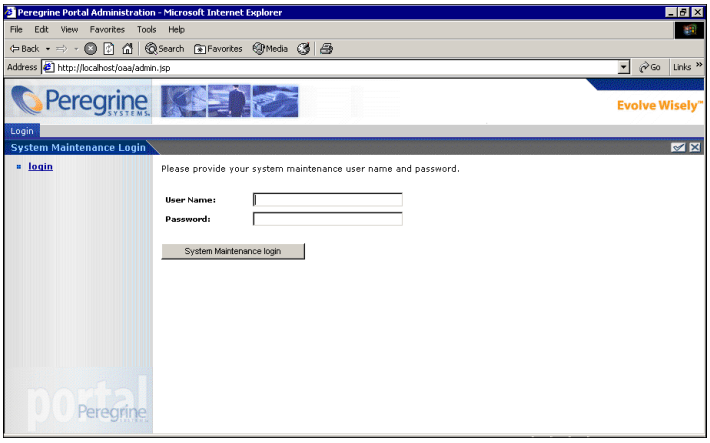
1 Restart the Business Objects server.

Note: Make sure the Business Objects server has started before you proceed.

2 Restart the application server. Refer to your application server documentation.

3 In your Web browser Address field, type: *<hostname>/oaa/admin.jsp*.

4 Click **Go** to open the Portal administrator login page.



Type your hostname to connect to your local server.

System is the default administrator name.

5 In the User Name field, type **System**.

No password is required for initial login.

You then set the PortalDB, Web Application, and Portal adapters to support the deployed BI Portal environment. The following table indicates the settings for AssetCenter, ServiceCenter, and multiple data source deployment.

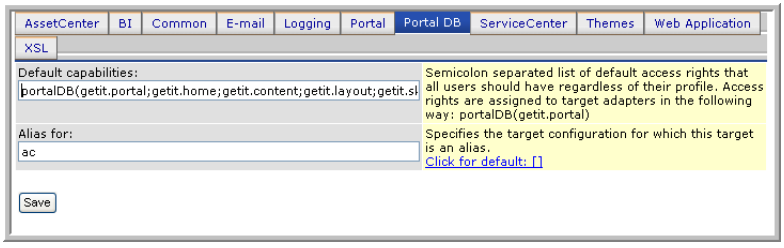
If the data source is…	Then use these settings in the Alias for and List of target aliases fields…	
AssetCenter only	PortalDB	`ac`
	Web Application	`ac`
	Portal	`PortalDB`

If the data source is…	Then use these settings in the Alias for and List of target aliases fields…	
ServiceCenter only	PortalDB	sc
	Web Application	sc
	Portal	PortalDB
AssetCenter and ServiceCenter (multiple data source)	PortalDB	ac or sc
	Web Application	ac or sc
	Note: PortalDB and Web Application must use the same data source because this is where the user login is authenticated.	
	Portal	PortalDB;ac;sc

To set the adapters for AssetCenter:

1 From the Peregrine Portal Admin module, click **Settings**.

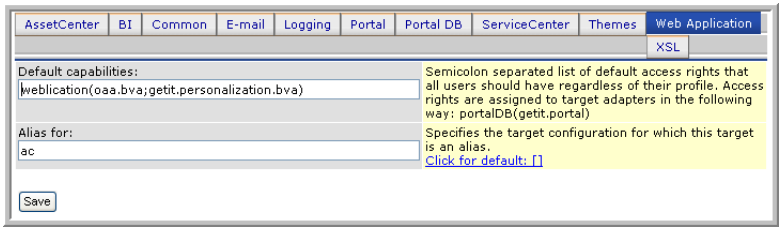
2 At the top of the page, click the **Portal DB** tab to display the Portal Database settings page.



a In the **Alias for** field, type **ac**.

b Click **Save**.

3 At the top of the page, click the **Web Application** tab to display the Web application settings page.

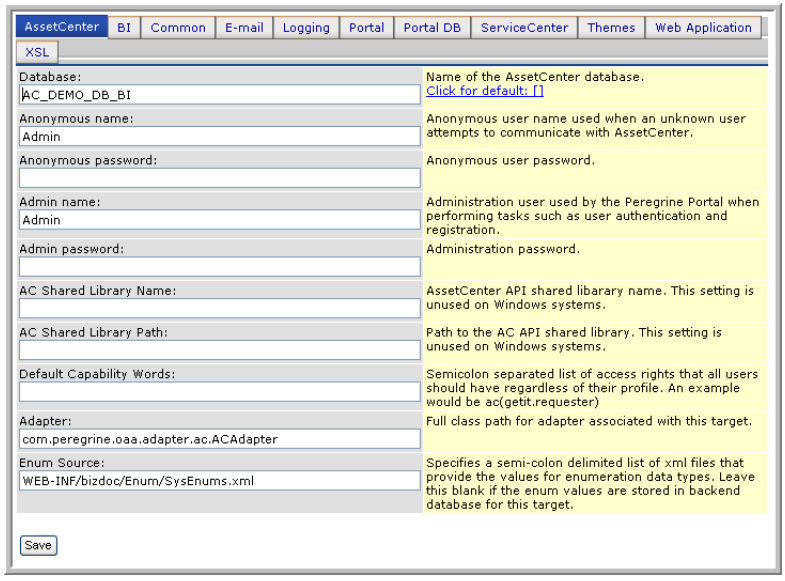


a In the **Alias for** field, type **ac**.

b Click **Save**.

Note: When using only AssetCenter as the data source, you do not need to set the Portal tab.

4 At the top of the Settings page, click the **AssetCenter** tab to display the AssetCenter settings.

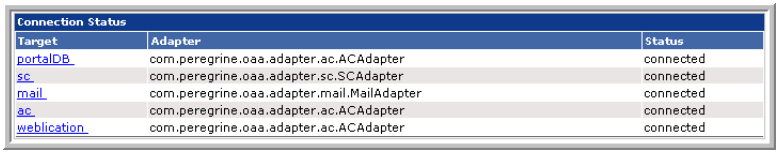


a Enter the database name of the AssetCenter server.

b Click **Save**.

5 From the Administration menu, click **Control Panel**, then click **Reset Peregrine Portal**.

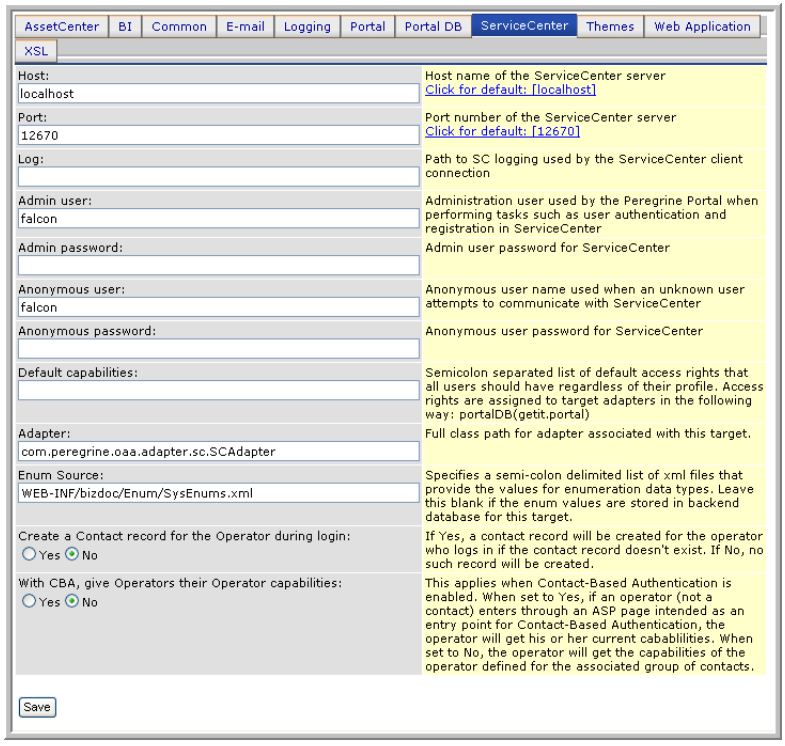
6 When the operation completes, verify that the adapter is `com.peregrine.oaa.adapter.ac.ACAdapter` for the **portalDB**, **ac**, and **weblication** targets and displays **Connected** in the Connection Status.



To set the adapters for ServiceCenter:

1 From the Peregrine Portal Admin module, click **Settings**.

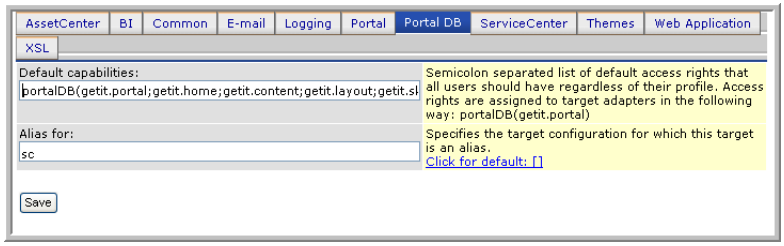
2 At the top of the Settings page, click the **ServiceCenter** tab to display the ServiceCenter settings.



a Enter the host name of the ServiceCenter server and the port number that ServiceCenter uses.

b Click **Save**.

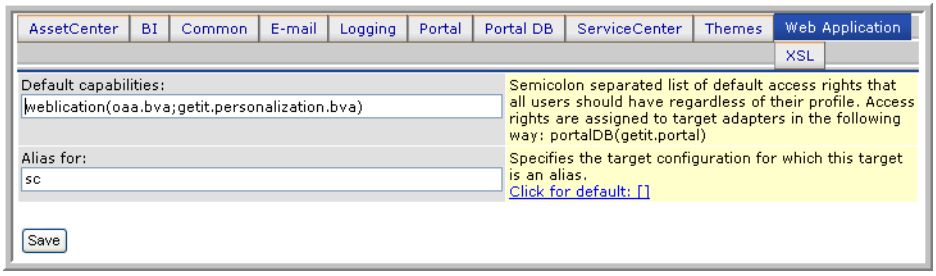
3 At the top of the page, click the **Portal DB** tab to display the Portal Database settings page.



a In the **Alias for** field, type **sc**.

b Click **Save**.

4 At the top of the page, click the **Web Application** tab to display the Web application settings page.



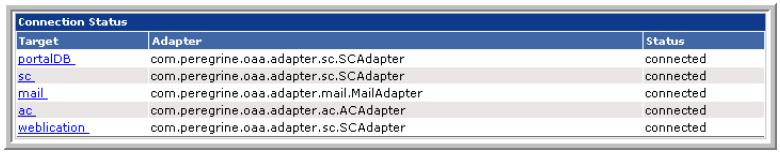
a In the **Alias for** field, type **sc**.

b Click **Save**.

Note: When using only ServiceCenter as the data source, you do not need to set the Portal tab.

5 From the Administration menu, click **Control Panel**, then click **Reset Peregrine Portal**.

6 When the operation completes, verify that the adapter is `com.peregrine.oaa.adapter.sc.SCAdapter` for the **portalDB**, **sc**, and **weblication** targets and displays **Connected** in the Connection Status.



Connection Status

Target	Adapter	Status
portalDB	com.peregrine.oaa.adapter.sc.SCAdapter	connected
sc	com.peregrine.oaa.adapter.sc.SCAdapter	connected
mail	com.peregrine.oaa.adapter.mail.MailAdapter	connected
ac	com.peregrine.oaa.adapter.ac.ACAdapter	connected
weblication	com.peregrine.oaa.adapter.sc.SCAdapter	connected

To set the adapters for both AssetCenter and ServiceCenter (multiple data source):

1 From the Peregrine Portal Admin module, click **Settings**.

2 At the top of the Settings page, click the **AssetCenter** tab to display the AssetCenter settings.

   a Enter the database name of the AssetCenter server.

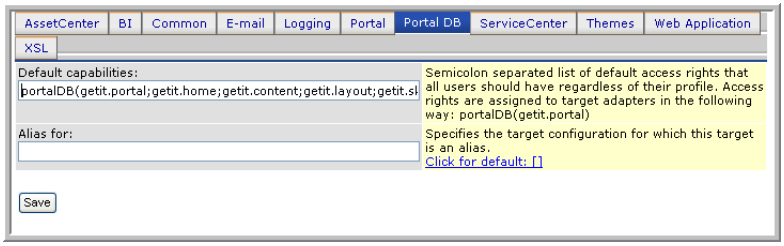
   b Click **Save**.

3 At the top of the Settings page, click the **ServiceCenter** tab to display the ServiceCenter settings.

   a Enter the host name of the ServiceCenter server and the port number that ServiceCenter uses.

   b Click **Save**.

4 At the top of the page, click the **Portal DB** tab to display the Portal Database settings page.

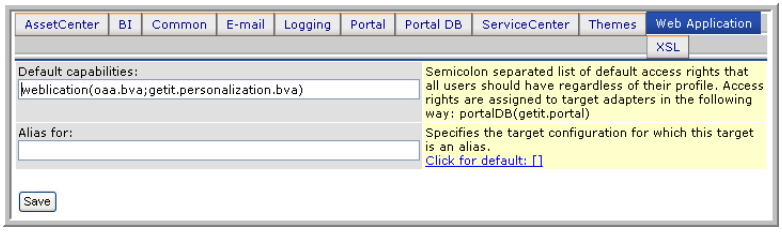


a In the **Alias for** field, type **ac** or **sc**.

Note: This depends on whether you want to authenticate users with ServiceCenter or AssetCenter. You must use the same data source in both PortalDB and Web Application because this is where the user login is authenticated.

b Click **Save**.

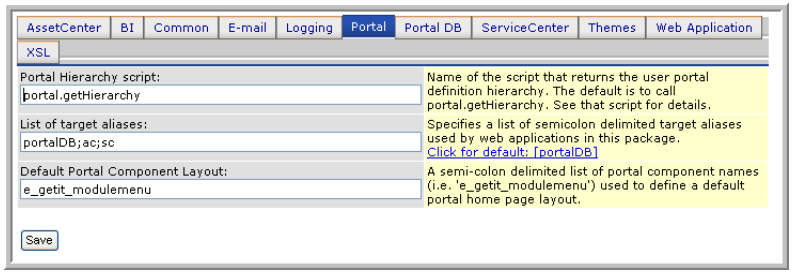
5 At the top of the page, click the **Web Application** tab to display the Web application settings page.



a In the **Alias for** field, type **ac** or **sc**.

b Click **Save**.

6 At the top of the page, click Portal to display the Portal settings page.



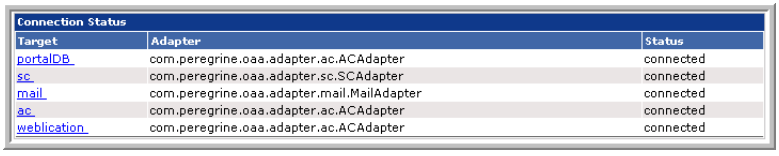
a In the **List of target aliases** field, type **portalDB;ac;sc**.

b Click **Save**.

7 From the Administration menu, click **Control Panel**, then click **Reset Peregrine Portal**.

8 When the operation completes, verify that:

- The connection status is **Connected.**
- The **ac** adapter is `com.peregrine.oaa.adapter.ac.ACAdapter`.
- The **sc** adapter is `com.peregrine.oaa.adapter.sc.SCAdapter`.
- The **portalDB** and **weblication** adapters are the same (either `com.peregrine.oaa.adapter.ac.ACAdapter` or `com.peregrine.oaa.adapter.sc.SCAdapter`).



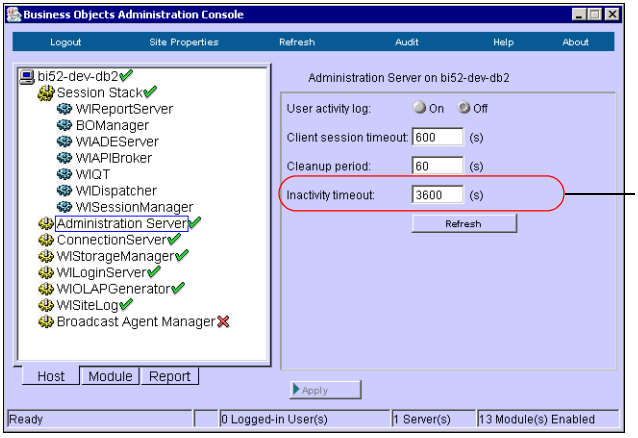
To proceed with the configuration, make sure that the BI Portal **Session timeout** interval is equal to or greater than the **Inactivity timeout** interval set in the Business Objects Administration Server.

To change the session timeout interval:

1 View the interval of the Business Objects Administration server **Inactivity timeout**.

a Log on to the Business Objects Administration Console as a supervisor.

b Highlight the Administration Server to view the interval set for the Inactivity timeout.

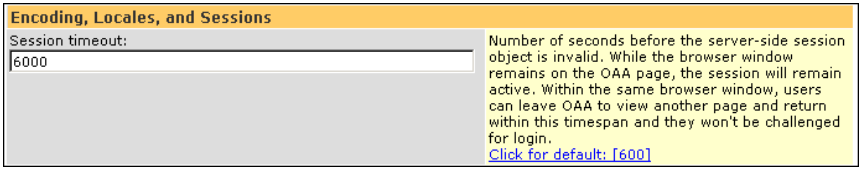


The BI Portal Session timeout must be equal to or greater than the Inactivity timeout on the Business Objects Administration Server.

2 Change the **Session timeout** interval from the BI Portal Admin settings to be equal to or greater than the interval set in Business Objects.

a From the Peregrine Portal Admin module, click **Settings**.

b Scroll to the **Encoding, Locales, and Sessions** section of the Common tab.



c Change the interval in the Session timeout to a number equal to or greater than the Inactivity timeout parameter in Business Objects.

d Click **Save**.

e From the Administration menu, click **Control Panel**, then click **Reset Peregrine Portal**.

Using the BI Portal Administration page

You can setup and configure the connections to Business Objects (BO) with ServiceCenter and AssetCenter 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 and AssetCenter. 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.

Button	Description
Test	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	Restore all settings to the values that were last saved.
Save	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.

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

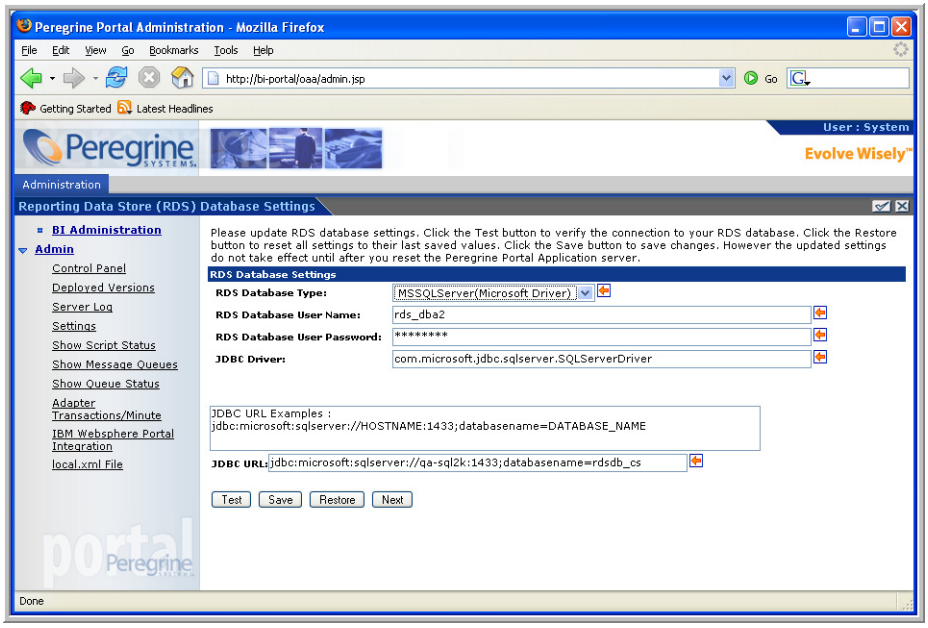
To access the BI administration functions:

1 Login to the Peregrine Portal Admin page.

`http://hostname/oaa/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.

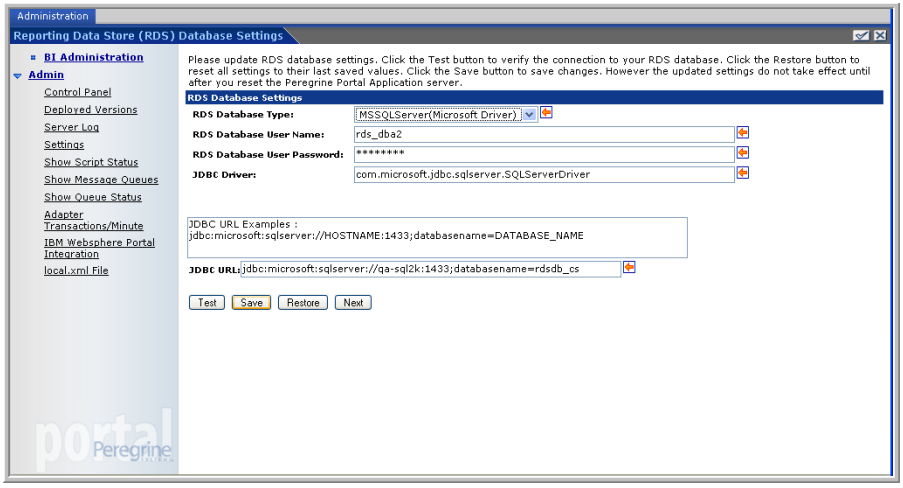
6 Click **Test** to test the connection to the RDS database.

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.

Type the BO Security Database User Name. (required)

10 Type the BO Security Database User Password. (required)

11 Type the JDBC Driver. (required)

12 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.

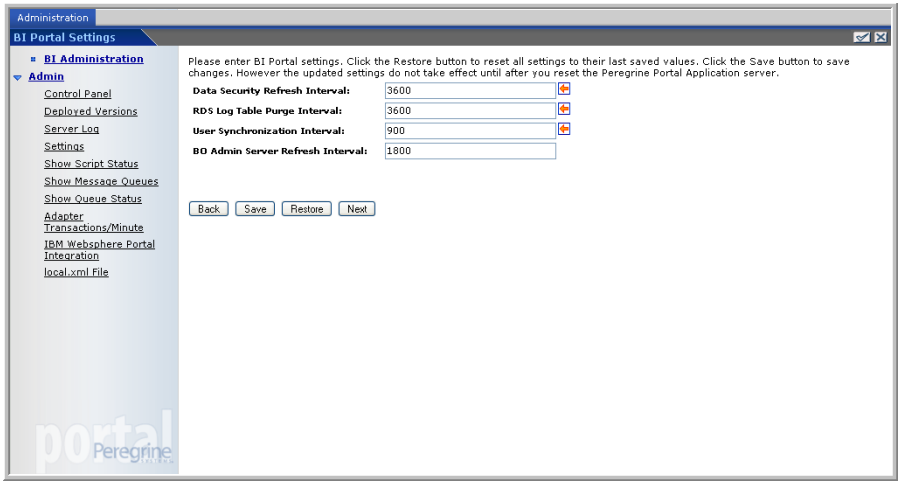
13 Click **Test** to test the connection to the specified database.

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.

14 Click **Save** if you wish to save your settings at this point in the process.

15 Click **Next**.

The BI Portal Settings page opens.



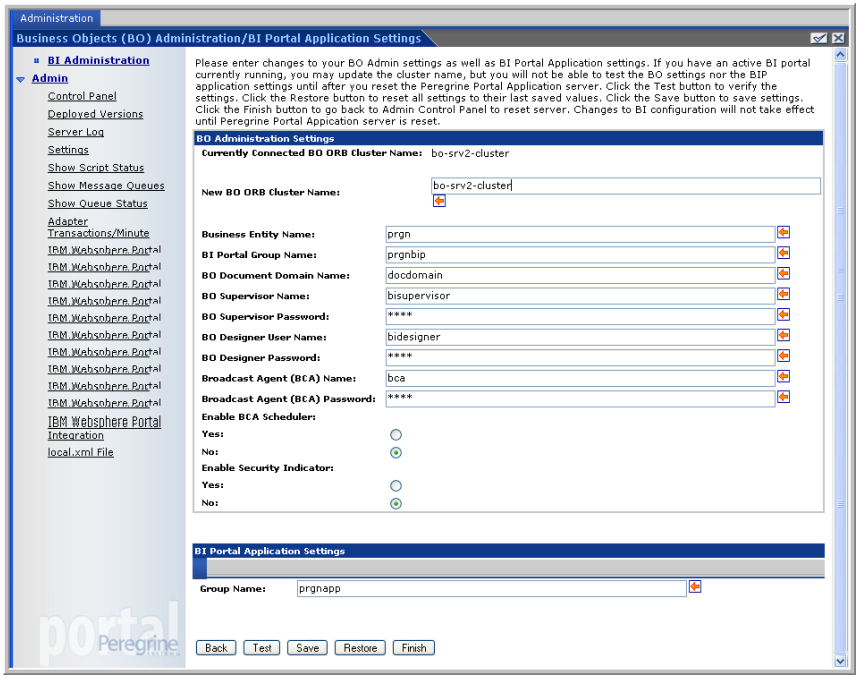
16 Enter numeric values for the following fields. An entry is required for each field.

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 database at the specified interval defined by this setting. (For additional information see Chapter 6 - BI Portal Administrator Functions, Viewing and synchronizing data security.)
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
User Synchronization Interval	900	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 from RDS to the Business Objects repository automatically. (For additional information see Chapter 6 - BI Portal Administrator Functions, Synchronizing users.)
BO Admin Server Refresh Interval	1800	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.

17 Click **Save** if you wish to save your settings at this point in the process.

18 Click **Next**.

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



19 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
- BO Supervisor Password

- BO Designer User Name
- BO Designer Password
- Broadcast Agent (BCA) Name
- Broadcast Agent (BCA) Password

20 Select Yes or No for Enable BCA Scheduler.

21 Select Yes or No for Enable Security Indicators.

22 In the BI Portal Applications Setting section type the Group Name for your application.

Note: This name must match the name you used when creating this group in the Business Objects Supervisor tool.

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

You may see status messages at the top of the page after you test your configuration settings. Some of these messages may indicate that something went wrong with the Business Objects server. 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 a state that only can be corrected by a restart.

24 Click **Finish**.

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

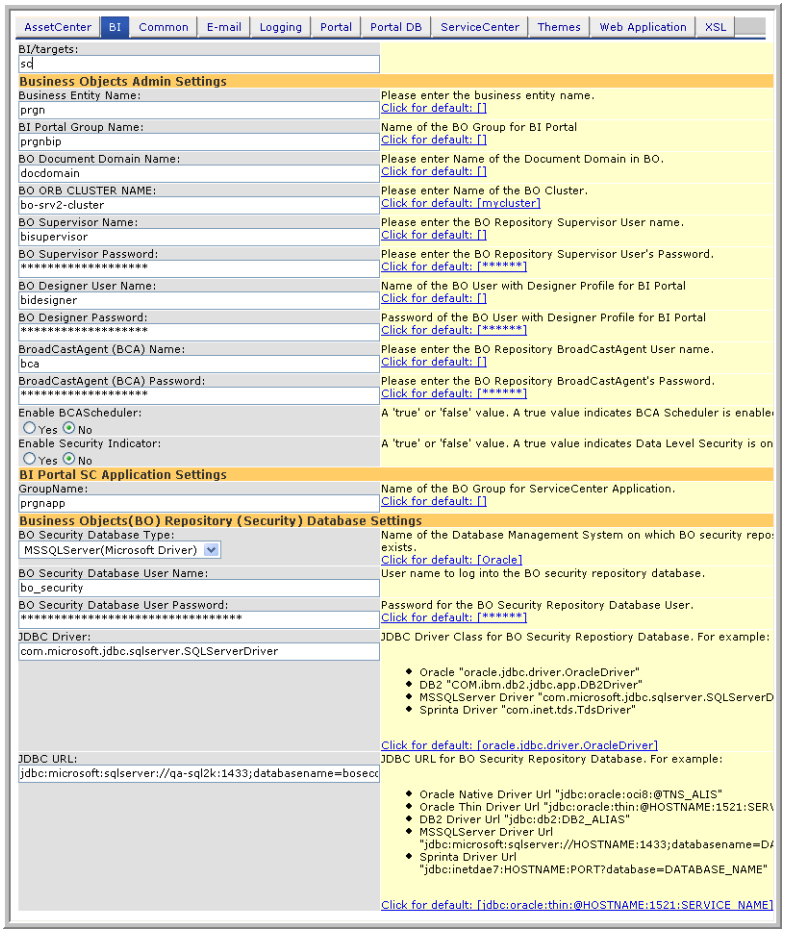
The BI tab displays all of the configuration settings for BI Portal on a single page. On this page you can reset any of the settings and then click Save at the bottom of the page to update the settings. This page is useful for viewing the current settings and quickly seeing settings that may be incorrect.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

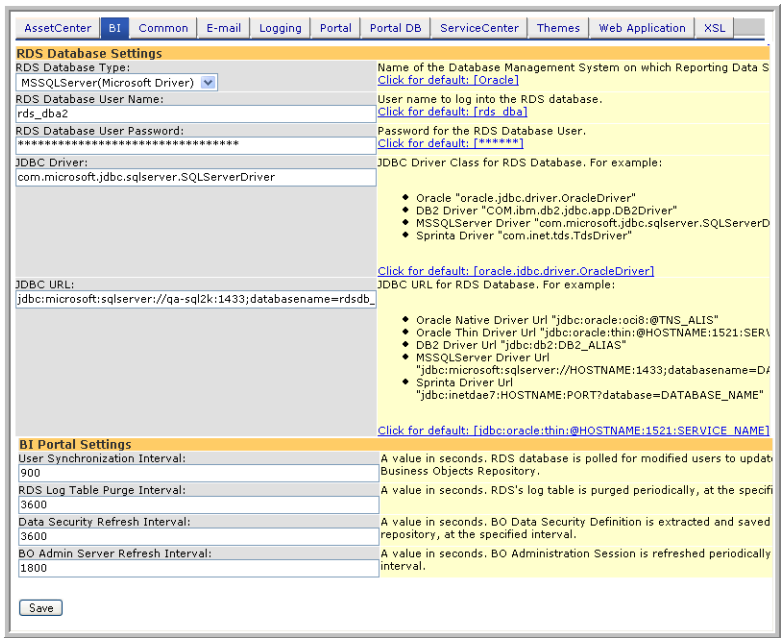
To access the BI tab:

1 Click **Settings** under the Admin Activity menu.

2 Click the **BI** tab.

The BI tab opens.




AssetCenter
BI
Common
E-mail
Logging
Portal
Portal DB
ServiceCenter
Themes
Web Application
XSL
RDS Database Settings
RDS Database Type:
MSSQLServer(Microsoft Driver)
Name of the Database Management System on which Reporting Data S
Click for default: [Oracle]
RDS Database User Name:
rds_dba2
User name to log into the RDS database.
Click for default: [rds_dba]
RDS Database User Password:
Password for the RDS Database User.
Click for default: [******]
JDBC Driver:
com.microsoft.jdbc.sqlserver.SQLServerDriver
JDBC Driver Class for RDS Database. For example:
Oracle "oracle.jdbc.driver.OracleDriver"
DB2 Driver "COM.ibm.db2.jdbc.app.DB2Driver"
MSSQLServer Driver "com.microsoft.jdbc.sqlserver.SQLServerD
Sprinta Driver "com.inet.tds.TdsDriver"
Click for default: [oracle.jdbc.driver.OracleDriver]
JDBC URL:
jdbc:microsoft:sqlserver://qa-sql2k:1433;databasename=rdsdb_
JDBC URL for RDS Database. For example:
Oracle Native Driver Url "jdbc:oracle:oci8:@TNS_ALIS"
Oracle Thin Driver Url "jdbc:oracle:thin:@HOSTNAME:1521:SER
DB2 Driver Url "jdbc:db2:DB2_ALIAS"
MSSQLServer Driver Url "jdbc:microsoft:sqlserver://HOSTNAME:1433;databasename=D
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 updat
Business Objects Repository.
RDS Log Table Purge Interval:
3600
A value in seconds. RDS's log table is purged periodically, at the specifi
Data Security Refresh Interval:
3600
A value in seconds. BO Data Security Definition is extracted and saved
repository, at the specified interval.
BO Admin Server Refresh Interval:
1800
A value in seconds. BO Administration Session is refreshed periodically
interval.
Save

5 Security

CHAPTER

This chapter describes the different security configuration options available in BI Portal. Topics in this chapter include, password and access rights for Health Insurance Portability and Accountability Act (HIPAA) support, default and custom security configurations, authentication, and alternate login pages.

By default, BI Portal does not encode passwords sent over the network; however, passwords are stored in SHA-1 format (encrypted format) in the database. 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 Integrated Windows Authentication

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 107.

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 116.

Back-end system security

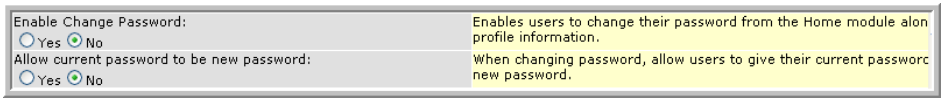
This section includes information about how BI Portal authenticates users and stores personalization changes in the ServiceCenter, AssetCenter, or Rome back-end system.

User account and password management

This section describes how the Administrator can manage user accounts and setup password formatting rules.

General administrative options

There are administrative options that apply to all the back-end adapters. These options are listed on the Common tab of the Administration page.



Enable Change Password: The **Yes** option enables the display of the **Change Password** portal component for user accounts that are granted with the `getit.password` capability. The **No** option requires the administrator to change passwords for all users.

Allow current password to be new password: The **No** option gives administrators the ability to require users to enter a new password that is different from the current password when they are using the Change Password options.

Refer to the corresponding ServiceCenter and AssetCenter guides for the options that are available for managing user accounts and password format rules.

Authentication with ServiceCenter or AssetCenter

When a user logs on to BI Portal, the user name and password are validated against a corresponding operator record in ServiceCenter or the Employee table in AssetCenter. When a user logs on, the back-end validates the user password, account status, and the password expiration according to the rules defined in each respective system. A generic error appears when a user fails to authenticate to any of the back-ends.

```
Sorry, your password has expired in at least one of the
supported targets. Please reset your password before you enter
the Peregrine Portal.
```

More back-end specific errors may be available in the `archway.log` file.

When one adapter returns an expired password code, the system redirects the user to the Change Password screen.

The user cannot log on to the system unless the user successfully resets the password.

Both the **Current Password** and **New Password** are sent to the back-end adapters. The back-end is responsible for verifying the current password and making sure that the new password complies with the rules and format for the password.

Generic error messages are displayed when a user has failed to reset the password. These messages can be customized by modifying the properties in the portal language string file in order to specify password format restrictions if desired.

Specific error messages may be found in the `archway.log`.

ServiceCenter capability words and AssetCenter user right keywords

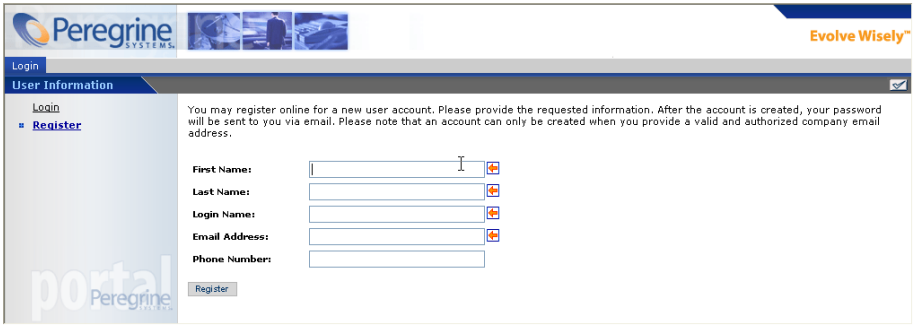
Following is a list of available capability words and user rights keywords for BI Portal functionality that can be assigned to a record in ServiceCenter or a profile in AssetCenter.

Access	Description
getit.admin	Provides access to the OAA Admin module.
	Can view the OAA home page and portal components. Note: Individual portal components are further restricted by the following capability words, which are described below: getit.home, getit.content, getit.layout, getit.skins, and getit.password.
getit.home	Grants access to the My Home Page portal component. Lets users view a defined home page.
getit.content	Grants access to the Add or Remove Content portal component, where users can add content to, or remove it from, their home pages.
getit.language	Grants access to the Change Language portal component, where users can change the preferred language.
getit.layout	Grants access to the Change Layout portal component, where users can change the layout of the My Home Page view.
getit.skins	Grants access to the Change Theme portal component, where users can change the portal's appearance.
getit.password	Grants access to the Change Password portal component, where users can change their passwords. This requires that the Administration setting is "Enable Change Password" option on the Common tab is set to "Yes."
getit.timezone	Grants access to the Change time zone portal component, where users can change the preferred time zone setting.
oaa.forbidden	Reserved capability word to prevent access to all OAA users (cannot be granted to any user).

User registration

Self-registration is only allowed if the **Enable User Registration** option is set to **Yes** on the Admin page. All BI Portal users need a login account in the back-end database providing authentication. For example, if you are using ServiceCenter as your back-end database, then the appropriate capability words must be defined in the user's Operator record. In AssetCenter, the appropriate user rights are defined in the user's Profile. Similar access rights can be defined in any back-end system that you are using. The user login is automatically authenticated in the back-end system.

If a user is attempting to log in for the first time without back-end authentication, 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. In AssetCenter, BI Portal transforms this data into a Profile record that then passes to your AssetCenter system. An amEmplDept record is created with the user-supplied data and the default Profile `getit.default` is assigned. In ServiceCenter, BI Portal creates an operator and contact record for the new user.

Note: The appropriate back-end system adapter must be defined before the capability words are recognized. For example, if no adapter is defined for ServiceCenter, the ServiceCenter capability words are not used.

Basic registration information and login scripts are stored in the `.../WEB-INF/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 or change the HIPPA security settings in the Rome database.

After the user is registered, that user in ServiceCenter must be given BI capabilities to access the BI Portal Reporting module. BI capabilities are `BI_Access`, which is mandatory and one of the following: `BI_Admin`, `BI_Create`, `BI_View`. For AssetCenter, you must import script files to give users the appropriate user rights and profiles.

When a user account is created, the back-ends automatically populate the fields required by the account and password management. For example, the Rome back-end automatically calculates the Password Expiration Date.

Enabling the E-mail adapter

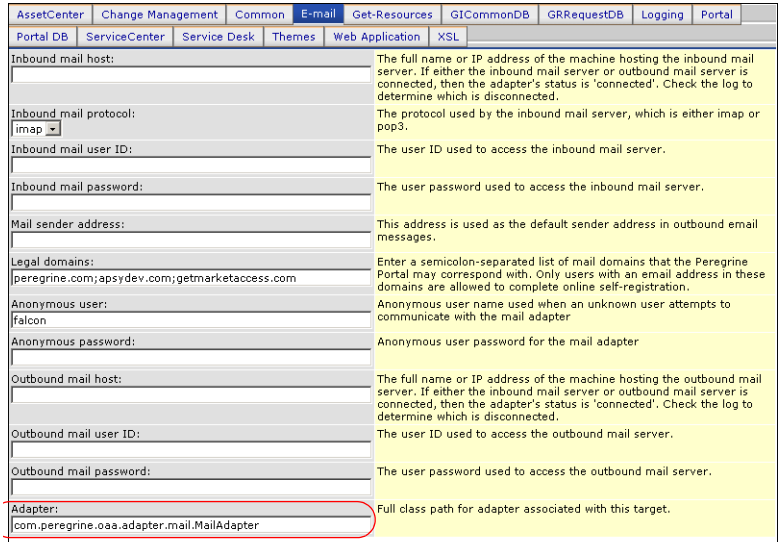
If users have the ability to self-register, you must make sure that the E-mail tab from the BI Portal Admin module Settings page contains the MailAdapter name.

The MailAdapter is an implementation of JavaMail API 1.2 and supports the following mail protocols:

- POP3 for inbound mail
- IMAP for inbound mail
- SMTP for outbound mail

The MailAdapter also supports MIME type attachments in outbound e-mail.

Set the following parameters, as needed, on the E-mail tab of the Admin module Settings page.



Type the name of your MailAdapter in the Adapter field.

Troubleshooting the MailAdapter connection

You can check the status of the MailAdapter connection on the Control Panel. If the adapter shows as *disconnected*, check that the settings on the E-mail tab of the Settings page are correct. If you are still unable to connect, contact your system administrator for verification of the parameter values.

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 106.
- Use a custom configuration to authenticate users against user-defined adapters such as LDAP or JDBC compliant databases. See Custom JAAS configuration on page 107.

- 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 115.
- Use Integrated Windows authentication to authenticate users and pass the information to the Web application. See Integrated Windows Authentication on page 116.
- Use an alternate login page and authenticate users against any of the other login options. See Creating an alternate login page on page 140.

Once a user is authenticated, the modules to which the user has access are defined by the back-end system. For example, if you are using AssetCenter and a user does not have access rights to a particular table in AssetCenter, the user cannot access the corresponding module in the Web application. 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:

Default Setting
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
`<jaas_config> </jaas_config>`	Define a custom JAAS configuration. All JAAS configuration settings must be between these two tags.
`<jaasConfiguration>` `</jaasConfiguration>`	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 `CustomConfig`, then you must use the tags `<CustomConfig>` and `</CustomConfig>` to define the list of adapters used.
`<CustomConfig>` `</CustomConfig>` This is a user definable tag.	Define the list of *all* 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 adapter1 and adapter2, then you must use the tags `<Adapter1>`, `</Adapter1>`, `<Adapter2>`, and `</Adapter2>` to define your adapters.
`<adapter1> </adapter1>` `<adapter2> </adapter2>` These are user definable tags.	Define the JAAS LoginModule settings for each adapter. Each adapter *must* have both `<loginModule>` and `<controlFlag>` tags defined for it.
`<loginModule> </loginModule>`	Define the fully qualified class name of the JAAS LoginModule. This is *required* only when authenticating against non-OAA LoginModules (adapters). The default value is `com.peregrine.oaa.archway.security.OAALoginModule.` This is *optional* only when authenticating against Peregrine back-ends.

Use these XML tags	To do this
`<controlFlag> </controlFlag>` This tag is optional.	Define the authentication behavior of this LoginModule. The default value is `REQUIRED`. See JAAS LoginModule control flags on page 109 for a description of available options.
`<options> </options>`	Define the list of authentication options. Use semicolons between entries to specify multiple options. This is an *optional* setting for each JAAS LoginModule you use. See JAAS configuration options on page 110 for a description of available options.

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.
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.

Option	Use	Description
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
user.provider.url	required	Use this option to provide the URL to the starting point in your directory service where you want to search for users. For example, `ldap://server/dc=peregrine,dc=com` **Note:** This option corresponds to the Java constant `Context.PROVIDER_URL`.
security.principal	optional	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, `uid=user,dc=peregrine,dc=com` **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. **Note:** This option corresponds to the Java constant `Context.SECURITY_PRINCIPAL`.

Option	Use	Description
security.credentials	optional	Use this option to define the password for the `security.principal` user. This option should only be used in conjunction with the `security.principal` option. **Note:** If you are using a simple security authentication protocol, then this password may be passed as plain text. **Tip:** To safeguard this password, either enable SSL (set the `security.protocol=ssl` option) or use an `security.authentication` that protects passwords. **Note:** This option corresponds to the Java constant `Context.SECURITY_CREDENTIALS`.
security.protocol	optional	Use this option to enable or disable an SSL connection between the JndiLoginModule and your directory server. This option has two possible values: `simple` (Default setting) `ssl` **Note:** This option corresponds to the Java constant `Context.SECURITY_PROTOCOL`
security.authentication	optional	Use this option to enable or disable anonymous binding to your directory service. Typically, this option has one of two values: **none** (Default setting) **simple** **Note:** If you do not specify a value for `security.principal` then `security.authentication` defaults to a value of none. Likewise, if you set `security.authentication` to `simple` but `security.credentials` is omitted or has zero length, then `security.authentication` resets to none. **Note:** This option corresponds to the Java constant `Context.SECURITY_AUTHENTICATION`.
user.search.scope	optional	Use this option to specify the number of levels to descend when searching for the user being authenticated by `user.provider.url`. This value must be an integer. The default value is 1. **Note:** This option corresponds to the Java constant `SearchControls.ONELEVEL_SCOPE`.

Option	Use	Description
group.provider.url	optional	Use this option to provide the URL to the starting point in your directory service where you want to search for groups. For example, `ldap://server/dc=peregrine,dc=com` **Note:** This option corresponds to the Java constant `Context.PROVIDER_URL`.
group.search.scope	optional	Use this option to specify the number of levels to descend when searching for a group. This option should only be used with `group.provider.url`. This value must be an integer. The default value is 1. **Note:** This option corresponds to the Java constant `SearchControls.ONELEVEL_SCOPE`.

group.search.objectClass	optional	Use this option to specify the name of the LDAP group objectClass. Valid values are:
		`groupOfNames` (Default value)
		`groupOfUniqueNames`
		`groupOfUrls`
		Note: Either `groupOfNames` or `groupOfUniqueNames` can be used to define static groups in LDAP, but they may not be used together.
		If you choose the `groupOfUrls` option, then you are configuring dynamic groups. No additional configuration settings are required to recognize dynamic groups.

storeIdentity=true	optional	Use this option to store a reference to the User being authenticated.
clearIdentity=true	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.

```
<settings>
  <jaas_config>
      <jaasConfiguration>myConfig</jaasConfiguration>
      <myConfig>ldap;ac;sc;rome</myConfig>
      <ldap>
        <loginModule>com.peregrine.oaa.security.JndiLoginModule</loginModule>
          <controlFlag>requisite</controlFlag>
           <options>
              setPreAuthenticated=true;
              user.provider.url=ldap://myldapserver:389/
                  ou=people,dc=mycompany,dc=com
           </options>
      </ldap>
  </jaas_config>
</settings>


Example with additional user capabilities stored in LDAP, see group.provider.url
option:

<settings>
  <jaas_config>
      <jaasConfiguration>myConfig</jaasConfiguration>
      <myConfig>ldap;ac;sc;rome</myConfig>
      <ldap>
          <loginModule>com.peregrine.oaa.security.JndiLoginModule</loginModule>
          <controlFlag>requisite</controlFlag>
           <options>
              setPreAuthenticated=true;
              user.provider.url=ldap://myldapserver:389/
                 ou=people,dc=mycompany,dc=com
              group.provider.url=ldap://myldapserver:389/
                 ou=groups,dc=mycompany,dc=com
           </options>
      </ldap>
  </jaas_config>
</settings>

Notes:
1) Character comparisons are case-sensitive. Be sure to match cases for all XML
tags and values.

2) Strip out all extraneous white space from with the values of elements. For
example, do not specify:
          <loginModule>
               com.peregrine.oaa.security.JndiLoginModule
          </loginModule>
Rather, use:
          <loginModule>com.peregrine.oaa.security.JndiLoginModule</loginModule>

White spaces are allowed only between semi-colon separated options within the
<options></options> tags.

Tip: To ensure your local.xml file contains valid XML formatting, open it using
InternetExplorer or some other XML viewing tool.
```

Standard Sun Microsystems JAAS configuration

The standard JAAS configuration option authenticates users against the Sun Microsytems 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 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 circumstance is an exception to the normal Integrated Windows Authentication login process:

- The Windows user name is not already registered in the back-end system. When this occurs, the Web application does not proceed with automatic login. This only occurs for users when the **Require Integrated Windows Authentication** option on the Admin page is set to No. The user sees another login screen and is asked for password verification. 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 an eight-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 118.

Step 2 Install and configure BI Portal with Apache and Tomcat (refer to the Installation Guide). See Preparing to configure Integrated Windows Authentication on page 118.

Step 3 Set Web server properties for the `login.asp` file. See Setting Web server properties for the login.asp file on page 118.

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 121.

Step 5 Set Web server properties for the `loginverify.asp` file. See Setting Web server properties for the loginverify.asp file on page 123.

Step 6 Set the **Require Integrated Windows 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 124.

Step 7 Set the settings on the Common tab from the BI Portal administration page. See Updating the Common tab URL settings on page 120.

Step 8 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 125.

The following procedures illustrate how to setup Integrated Windows Authentication using Windows 2000 as an example. 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 Get-Answers, AssetCenter, or ServiceCenter administrator to verify that users have Operator records. Create an Operator record as needed.

Preparing to configure Integrated Windows Authentication

This section describes how to configure Integrated Windows Authentication if you use Tomcat as your application server, Apache as your Web server, and IIS for authentication.

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: `<AppServer>\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. From the deployment server, edit `login.asp` using a text editor. The default location is: `C:\Program Files\Peregrine\Portal\image.`

   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">
```

Note: If you are not using the default port (80), you must specify the port number on the URL.

2 Open the IIS Management Console (**Start>Programs>Administrative Tools>Internet Information Services**).

3 Click on the `oaa` virtual directory.

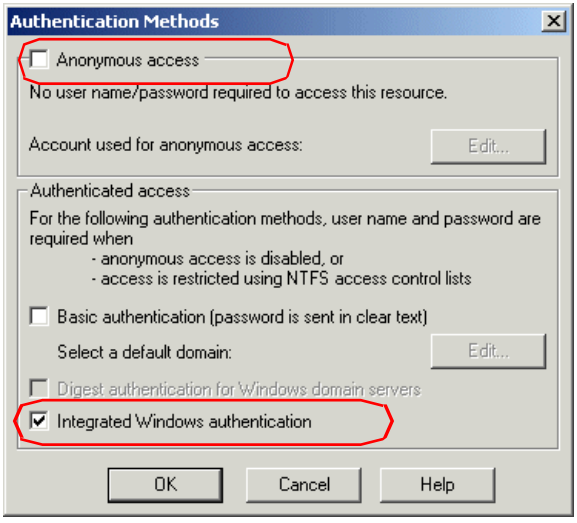
4 Right-click on `login.asp` and select **Properties**.

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.

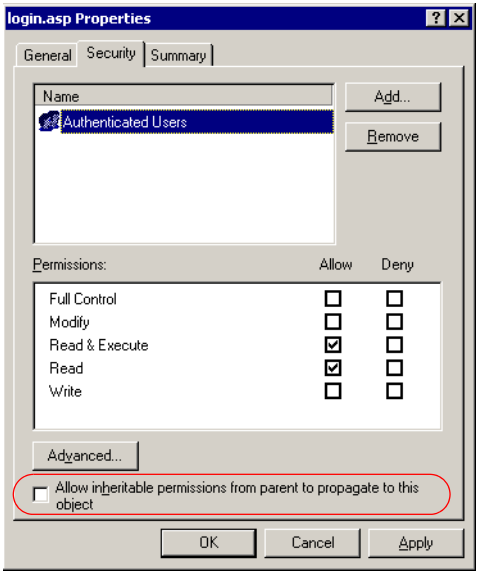
7 Click **OK** on all windows displayed until you return to the Microsoft Management Console.

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



Make sure that only the Authenticated Users group is in this list.

Verify that the **Allow inheritable permissions from parent to propagate to this object** option is not checked.

c Clear the check box beside the **Allow inheritable permissions from parent to propagate to this object** option, then click **OK**.

Updating the Common tab URL settings

You need to set the Server URL and Login Verify URL parameters on the Common tab of the Admin Settings page.

To set the URL settings:

1 Log on the Peregrine Portal as a system administrator.

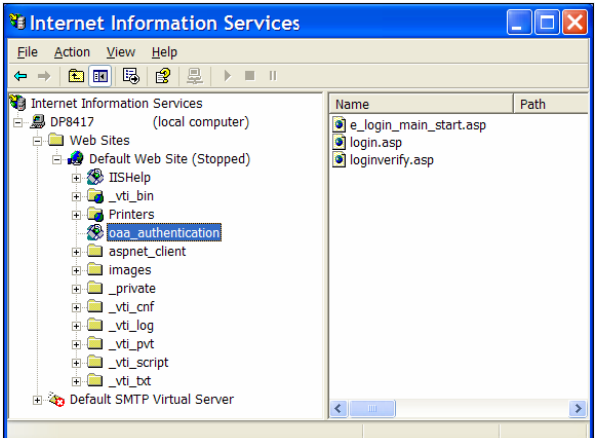
2 Click the **Administration** tab.

3 Click the **Settings** link.

4 On the Common tab, set the following parameters:

- Server URL - This must be the fully qualified Apache Web server / IIS server URL to the OAA virtual directory. The URL must include the port number if it is not 80.
- Login Verify URL - This must be the fully qualified IIS server URL to the OAA virtual directory. The URL must include the port number if it is not 80.

  Example: `http://DP8417:87/oaa_authentication`



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 From the deployment server, edit `e_login_main.start.asp` using a text editor. The default location is:
`C:\Program Files\Peregrine\Portal\image.`

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">
```

Note: If you are not using the default port (80), you must specify the port number on the URL.

2 Open the IIS Management Console (click **Start** > **Programs** > **Administrative Tools** > **Internet Information Services**).

3 Click on the `oaa` virtual directory.

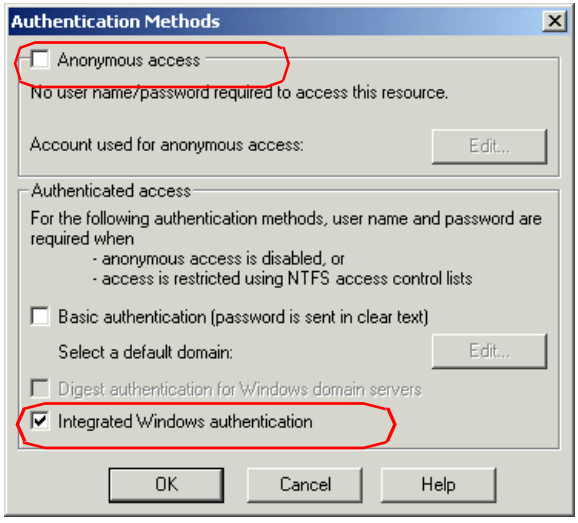
4 Right-click on `e_login_main_start.asp` and select **Properties**.

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.

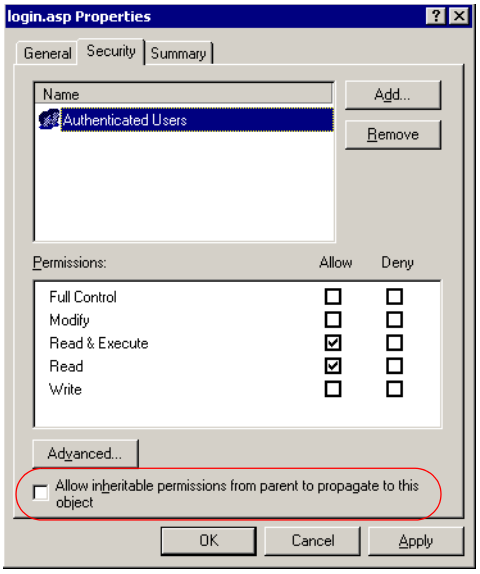
7 Click **OK** on all windows displayed until you return to the Microsoft Management Console.

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



Make sure that only the Authenticated Users group is in this list.

Verify that the **Allow inheritable permissions from parent to propagate to this object** option is not checked.

c Clear the check box beside the **Allow inheritable permissions from parent to propagate to this object** option, then click **OK**.

Setting Web server properties for the loginverify.asp file

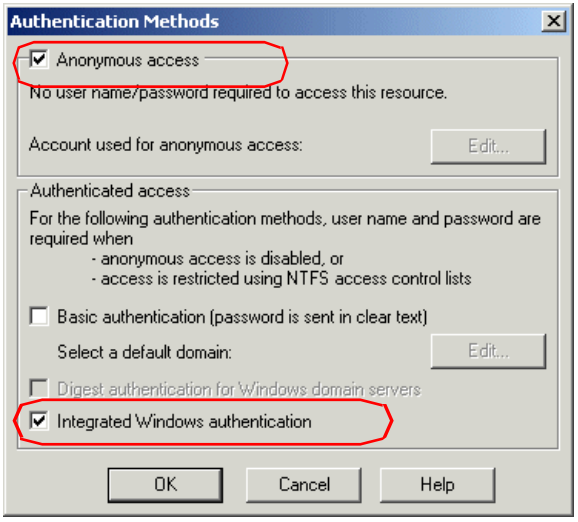
1 Open the IIS Management Console (Start > Programs > Administrative Tools > Internet Information Services).

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 Integrated Windows 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.

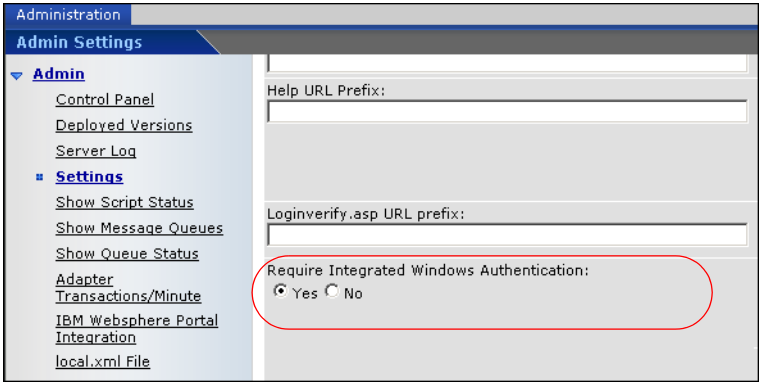
To set Integrated Windows Authentication:

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**.



5 From the **Common** tab, set the **Require Integrated Windows 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 Peregrine Portal**.

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 Setting the Admin parameters on page 124), 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 Peregrine Portal**.

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>:<port>/<oaa>/login.asp* in the browser address field (where `<webserver>` is the name of your Web server, and `:<port>` is only required if it is other than port 80, 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.

Once you have verified this setting, all the users authenticated by Integrated Windows Authentication should now access BI Portal with the `login.asp` URL.

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 116.

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:

```
<%@ 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);
%>

<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>
```

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: `<AppServer>\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

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

The `Operator` file contains the following keys.

Key	Description
name field	This is the primary key (unique and indexed).
full.name field	This 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.

Key	Description
contact.name field	This is the primary key; it is unique and indexed.
user.id field	This 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, see the Schemas chapter in this guide.

Important: If you create schema extensions for either the Contact schema or the Profile schema, ensure that their corresponding fields in the Contacts file and the Operator file are both unique (no duplicates) and indexed to maintain adequate performance during table look ups.

Regular operator authentication

In ServiceCenter, name and password pairs are validated against the existing operator in the operator table. In addition, the presence of the operator's contact is queried based on the fields mentioned below.

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 name) of the logged in operator.

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, if required. (See the following Contact creation section.)

Contact creation

If an operator's contact record is not found during contact lookup, OAA does not create a contact automatically. A setting in the BI Portal Admin module under the ServiceCenter tab controls this behavior: `Create a Contact record for the Operator during login`. The default setting is No, which does not create a contact record for the operator during login. When set to Yes, a contact record is created for the operating during login if the contact record does not already exist.

All the information from the Profile record for the logged in operator is used to create a Contact record. Therefore, all the Profile values that have a corresponding attribute in the `Contact` schema are saved in the database. In addition, the Contact record's ProfileId (see Logical mapping) is assigned the value of the Profile record's Id to establish a mapping from the Contact back 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

Physical name in Profile schema	Physical name in Contact schema
name	operator.id
name	user.id
full.name	contact.name

Contact-based authentication for ServiceCenter users

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

When logging in through `loginContactBased.asp` or one of its copies, the user will be logged in if a contact exists for this user in ServiceCenter. The user gets the ServiceCenter profile and capability words from a ServiceCenter operator. The same operator performs all ServiceCenter operations on behalf of the user.

The setting of the `With CBA, give Operators their Operator capabilities` attribute under the ServiceCenter tab controls how the operator is determined.

Setting option	What the setting determines
Yes	The operator defined on the contact record in ServiceCenter is used. If no operator is defined in the contact record, the default operator defined in `local.xml` is used.
No (default setting)	The default operator set in the `local.xml` file (see Editing the local.xml file on page 136) is used.

Note: The following authentication scheme 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.

Setting up contact-based authentication

Perform the following steps to set up your server:

Step 1 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 133.

Step 2 Choose or create one Operator record in ServiceCenter that will be the default operator. See Creating a default Operator record in ServiceCenter on page 133.

Step 3 Configure each login ASP file for Integrated Windows Authentication. See Changing the authentication method in IIS on page 134.

Step 4 Verify the Integrated Windows Authentication setting on the BI Portal Admin module Settings page. See Verifying the BI Portal Admin setting on page 135.

Step 5 Edit `local.xml` in `<application server>\oaa\WEB-INF` to define the passwords for the default operator. The step is optional; do this only if you want to set up a default operator. See Editing the local.xml file on page 136.

Step 6 Modify the `rds_user` Scenario and restart the scenario to resynchronize the user data. See Modifying the rds_user scenario on page 137.

Step 7 Restart the application server.

Creating a contact record

Create one contact record for each Windows user who you want to log in. The Employee ID (userid) 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 ServiceCenter Application Administration online help.

Creating a default Operator record in ServiceCenter

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

Assign the BI Portal capability words that you want your users to have by default.

Changing the authentication method in IIS

You must configure `loginContactBased.asp` or its copies. This requires changing the authentication method in IIS.

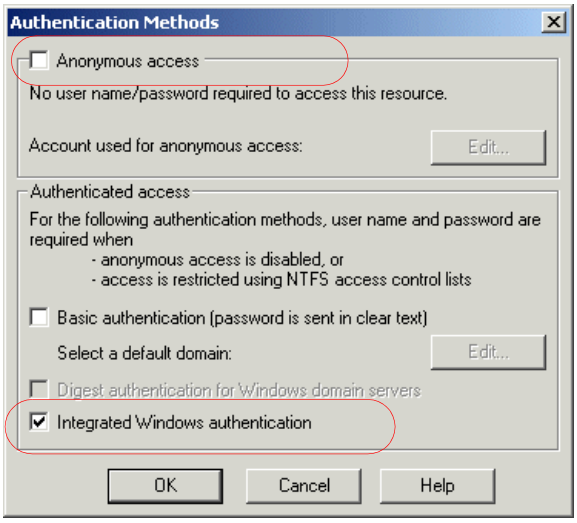
To change the authentication method in IIS:

1. Open the IIS Management Console (click **Start** > **Programs** > **Administrative Tools** > **Internet Information Services**).
2. Navigate to the `oaa` virtual directory.
3. Navigate to `loginContactBased.asp`.
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**.



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.

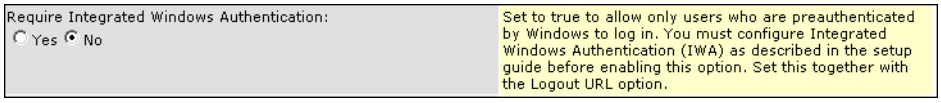
Verifying the BI Portal Admin setting

From the BI Portal Admin module, you must verify that the **Require Integrated Windows Authentication** option is set to No. If set to Yes, users accessing `login.jsp` directly might be logged in with no access to ServiceCenter or the login might fail.

1 Log in to the BI Portal Admin module, click Settings, then click the Common tab.

2 Scroll to the Encoding, Locales, and Sessions section.

3 Make sure that the option **Require Integrated Windows Authentication** is set to **No**.



Editing the local.xml file

In the `local.xml` file, you must specify the operator name and password for the scdefault alias. This file is located at:
`<application server>\oaa\WEB-INF\local.xml`.

To edit the local.xml file:

1 Using a text editor, open `local.xml`.

2 Add two XML entries.

The tags have the format:

```
<scdefault>operator</scdefault>
```

and

```
<scdefaultPassword>password</scdefaultPassword>
```

For example, for operator `Tossi` and `scdefault`, add the following inside the `<settings> ... </settings>` tags.

```
<scdefault>Tossi</scdefault>
<scdefaultPassword>Tossi_password</scdefaultPassword>
```

where `Tossi_password` is the ServiceCenter password assigned to operator `Tossi`.

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

Modifying the rds_user scenario

For 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 **Stop**.
4. Double-click the `rds_user.scn` file in the `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.
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
11. Check the box for **contacts-RDS_USER**.
12. Click **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 **Start** to restart the rds_user scenario.

This resynchronizes all users (operators and contacts) from ServiceCenter into the RDS_USER table.

If you change your environment from contact-based authentication to non-contact-based authentication, then do steps 1 to 14. You need to clear the box in step 4 and step 6. In addition, manually delete the records in the RDS_USER table before step 14, which restarts the scenario.

If you change the environment from non-contact-based authentication to contact-based authentication, follow step 1 to step 14.

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).

Restarting the application server

You must restart the application server for your changes to take effect.

Tailoring contact-based authentication

OAA uses the ServiceCenter 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 numbers, and Social Security numbers) rather than network names (network names 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.

Similarly, the Profile schema defines UserName to maintain data integrity and facilitate customization. Creating a schema extension for this usually is not necessary. For more information, see the Schemas chapter of this guide.

Schema type	Logical name	Physical name
Contact	UserName	user.id
Profile	UserName	name

Important: If you create a schema extension for UserName for either the Contact schema or the Profile schema, ensure that their corresponding fields in the Contacts file and Operator file are both unique and indexed to maintain adequate performance during table look ups.

AssetCenter authentication

BI Portal can authenticate users using either NT or LDAP authentication. However, the two mechanisms are not entirely dependent.

Integrated Windows authentication with AssetCenter

If your AssetCenter user is not set up for integrated Windows authentication, you can still use integrated Windows authentication in BI Portal, but you will need an employee for your user. (See Integrated Windows Authentication on page 116.) The employee's UserLogin is either: the NT user's name (the default); or the domain and user name in the format `<Domain>\<UserName>` if the `stripNtLoginDomain` entry in the `local.xml` file is set to False.

If your AssetCenter deployment is set up for integrated Windows authentication, BI Portal cannot authenticate the user directly through AssetCenter. The BI Portal user needs to be pre-authenticated by a trusted third party source. This source can be (and usually is) integrated Windows authentication. In any case, the user name of the third-party source must be the full NT name in this format: `<Domain>\<UserName>`. Further, the `stripNtLoginDomain` entry in the `local.xml` file must be set to False.

LDAP authentication with AssetCenter

BI Portal can also authenticate users using LDAP. The mechanism is different from the way AssetCenter authenticates users with LDAP.

If your AssetCenter deployment is not set up for LDAP, you can still use LDAP authentication in BI Portal. The login name for BI Portal is the uid of a person; further, this uid *must* correspond to the UserName of a record in the amEmplDept (Employee) table in order to be able to perform the transactions in AssetCenter.

If your AssetCenter deployment is set up for LDAP, you need not use the LDAP authentication in BI Portal because BI Portal will use the AssetCenter LDAP authentication mechanism. The LDAP interface DLL, `nsldap32v50.dll`, which is delivered with AssetCenter, must be either in the startup directory of your Web Application Server (WebSphere, or Tomcat), or in your system wide path.

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 142.

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
`loginuser`	This is a required login parameter specifying the user name. You must specify a form input for this parameter.
`loginpass`	This is a required login parameter specifying the login password. You must specify a form input for this parameter.
`_locale`	This is an optional login parameter specifying the user's locale and regional display settings.
`_timezone`	This is an optional login parameter specifying the user's timezone.
`_theme`	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.

CHAPTER 6 BI Portal Administrator Functions

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:

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

- Review the BI Portal capability words and user rights to determine which BI Portal users should have what access rights.
- Assign BI Portal users the appropriate BI capability (done in ServiceCenter and AssetCenter).

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

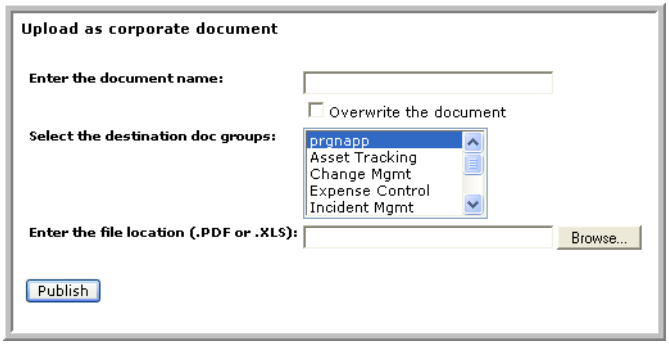
Uploading

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**.



3 In the **Enter the document name** field, type the name of the file to upload.

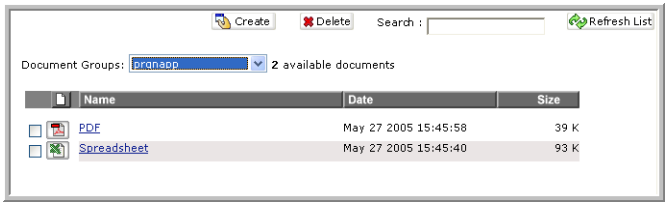
You have the option to overwrite the document if it already exists.

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.

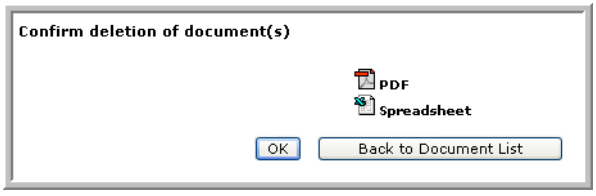
6 Click **Publish**.

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.

After you upload a document, you may see a pop-up window when you click the document name in BI Portal to open the document. To avoid getting a pop-up window which prompts you whether or not to open the document, edit the file type options in Windows Explorer.

To set Windows Explorer options to prevent a pop-up window:

1 In Windows Explorer, go to **Tools** > **Folder Options**.

2 Click the **File Types** tab.

3 Highlight the PDF or XLS file type from the list.

4 Click the **Advanced** button.

5 Clear the **Confirm Open after download** option.

6 Click **OK** twice to close all dialog boxes.

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.
Group names must contain at least one alpha character.

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

- Asset Tracking
- Change Mgmt
- Expense Control
- Incident Mgmt
- Inventory Mgmt
- prgnapp
- Root Cause Analysis
- Service Level Mgmt
- Service Mgmt

Important: The `prgnapp` group is a name used for Peregrine applications and is entered on the Admin page. The `prgnapp` group name must match the name you used when you created this group in BO Supervisor tool.

The `prgnapp` group contains all of the BI Portal users in ServiceCenter or AssetCenter. 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.

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 base 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 available for querying and viewing by users assigned various groups.

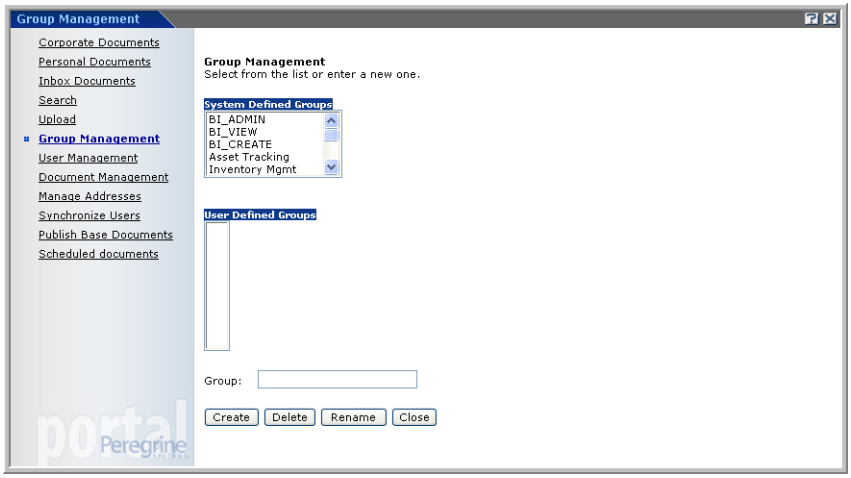
Group	Application	Description
Asset Tracking	AssetCenter	All reports and data related to Asset Tracking. See the Base Reports for Asset Tracking in the BI Portal User Guide for more information.
Change Mgmt	ServiceCenter	All reports and data related to Change Management. See the Base Reports for Change Management in the BI Portal User Guide for more information.
Expense Control	AssetCenter	All reports and data related to Expense Control. See the Base Reports for Expense Control in the BI Portal User Guide for more information.
Incident Mgmt	ServiceCenter	All reports and data related to Incident Management. See the Base Reports for Incident Management in the BI Portal User Guide for more information.
Inventory Mgmt	ServiceCenter	All reports and data related to Inventory Management. See the Base Reports for Inventory Management in the BI Portal User Guide for more information.
Root Cause Analysis	ServiceCenter	All reports and data related to Root Cause Analysis. See the Base Reports for Root Cause Analysis in the BI Portal User Guide for more information.

Group	Application	Description
Service Level Mgmt	ServiceCenter	All reports and data related to Service Level Management. See the Base Reports for Service Level Management in the BI Portal User Guide for more information.
Service Mgmt	ServiceCenter	All reports and data related to Service Management. See the Base Reports for Service Management in the BI Portal User Guide for more information.

To create a group:

1 Log into BI Portal.

2 From the Reporting module activity menu, click **Group Management** to open the Group Management form.



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.

In the **User Defined Groups** list, select the group you want to rename.

3 In the **Group** field, type the new name of the group.

4 Click **Rename**.

The group you selected is renamed in the list.

Capability words and user rights

It is the ServiceCenter capability words and AssetCenter user rights 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 either ServiceCenter or AssetCenter to access the BI Portal. It is the ServiceCenter capability words and AssetCenter user rights assigned to BI Portal users that control access to the various reporting functions available in BI Portal.

Note: All individual BI users must be assigned to a BI user capability group (`BI_Admin`, `BI_Create`, `BI_View`) from ServiceCenter or AssetCenter.

Important: The `rds_ac.scn` scenario creates `BI_Connector` as the user who accesses the AssetCenter database. The user rights for `BI_Connector` allow for deletion of `amOutputEvent` records. If you want to use a different user other than `BI_Connector`, make sure that the designated user has `BI_Admin` rights assigned. This is necessary to ensure that processed event records are properly deleted from the AssetCenter `amOutputEvent` table.

The following table summarizes the functions that each capability or right allows.

Capability or right	Access level	Allows the user to...
`BI_Access`	Required	Gain access to the WebIntelligence Reporting module **Note:** Each user needs `BI_Access` capability simply to access the WebIntelligence Reporting module. In addition, each user needs one of the following capabilities to perform querying and reporting functions.
`BI_View`	3	■ 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

Capability or right	Access level	Allows the user to...
BI_Create	2	■ Perform the same functions as a user assigned BI_View capability; and: ■ Download Zero Administration Business Objects ■ Create and edit documents ■ Format the toolbar ■ Perform a transparent drill outside the cube ■ View SQL 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.
BI_Admin	1 (Highest)	■ Perform the same functions as a user assigned BI_View and BI_Create capabilities; and: ■ 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 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.

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

BI capabilities and rights

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

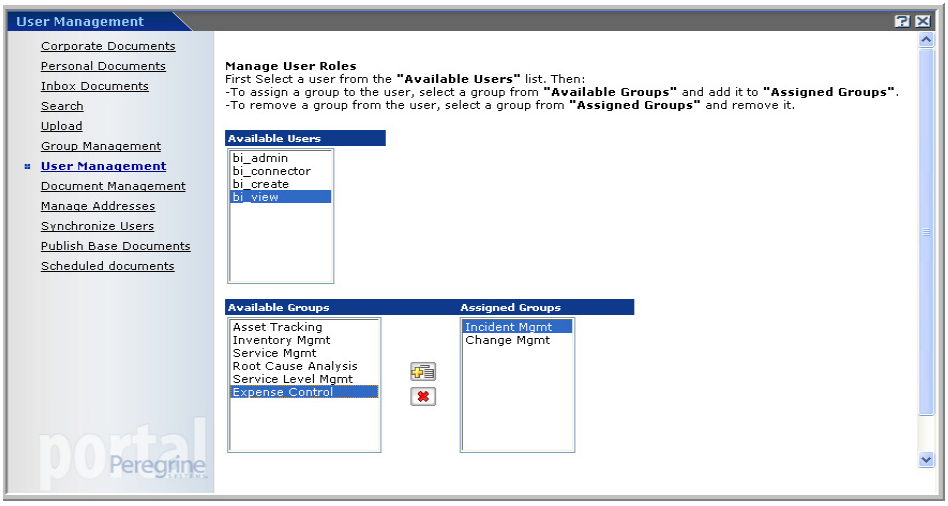
	BI_Admin	BI_Create	BI_View
Create	X	X	
Delete (published documents)	X		
Document Management	X		
Download	X	X	X
Drill	X	X	X
Edit	X	X	
Group Management	X		
Manage Addresses	X	X	X
Manage Inbox Documents	X	X	X
Manage Personal Documents	X	X	X
Maximize	X	X	X
Page or Draft Mode	X	X	X
Publish (or save to Corporate 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
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. You also can publish documents to more than one group.

In the following scenario, a document is published to both the **Change Management** and **Incident Management** groups. When a user who belongs to the Change Management group but not to the Incident Management group tries to see the document in the Incident Management group, the document in discussion will be displayed even though the user does not have rights to see the documents in the Incident Management group. This is because the document is attached to multiple groups: Change Management and Incident Management. Since the user can see the documents in the Change Management group, the document will be displayed to the user.

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. 

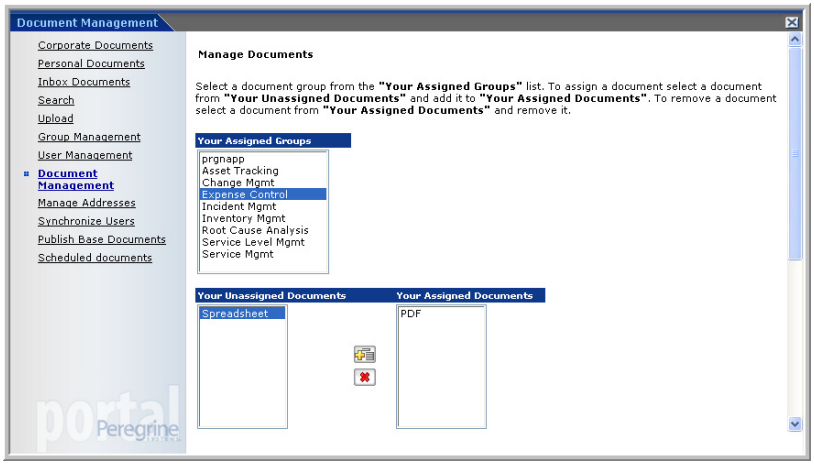
6 Click **Save** to commit the group assignments.

Document management

The Document Management function allows you to assign unassigned Corporate documents to a group so that the document is available to all users in that group. Documents that the user already published shows up in the Document Management page. The user can then assign these documents to different groups using this screen.

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 document 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 Document**s 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

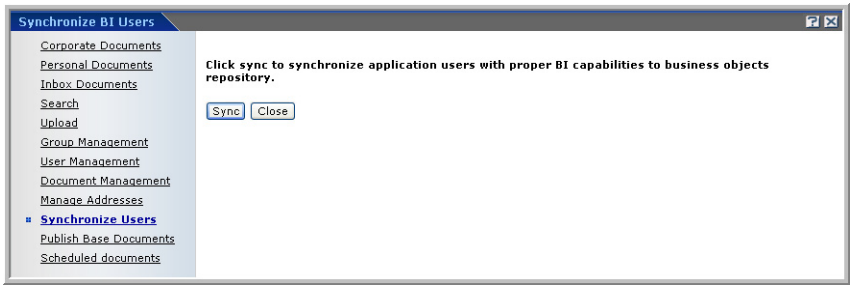
The Synchronize Users function allows you to synchronize application users with the appropriate BI capabilities between the RDS database and the Business Objects repository. User synchronization is for on-demand synchronization, and normally, user data is synchronized automatically for a predefined interval 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**.

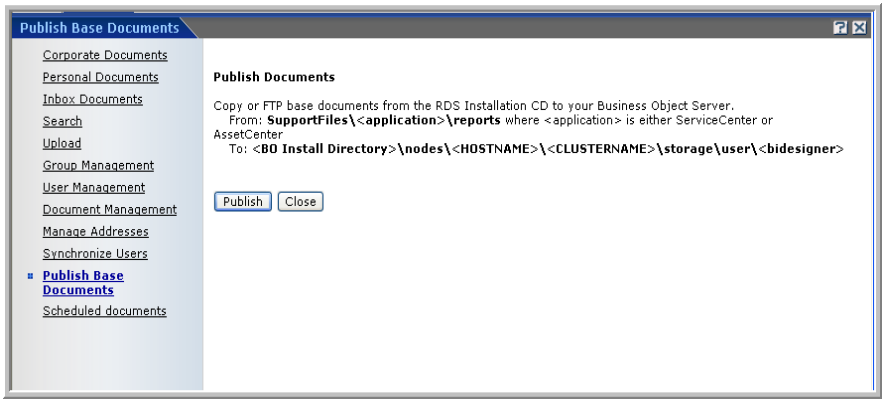
You see the message
`Success: Synchronize Users request is submitted and will be processed immediately.`
at the top of the form.

4 Click **Close** to return to the main menu.

Publishing base 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 Base Documents link on the Reporting module activity menu to publish the base documents.

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



To publish the base documents:

1 Log in to BI Portal.

2 If this is the first time you are publishing the base documents, you must copy the documents from the RDS for AssetCenter or RDS for ServiceCenter Installation CD.

Application	Copy from this location
AssetCenter	`SupportFiles\AssetCenter\reports`
ServiceCenter	`SupportFiles\ServiceCenter\reports`

3 Paste to the Business Objects server.

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

4 From the Reporting module activity menu, click **Publish Base Documents**.

5 Click **Publish**.

You see confirmation messages.

6 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.

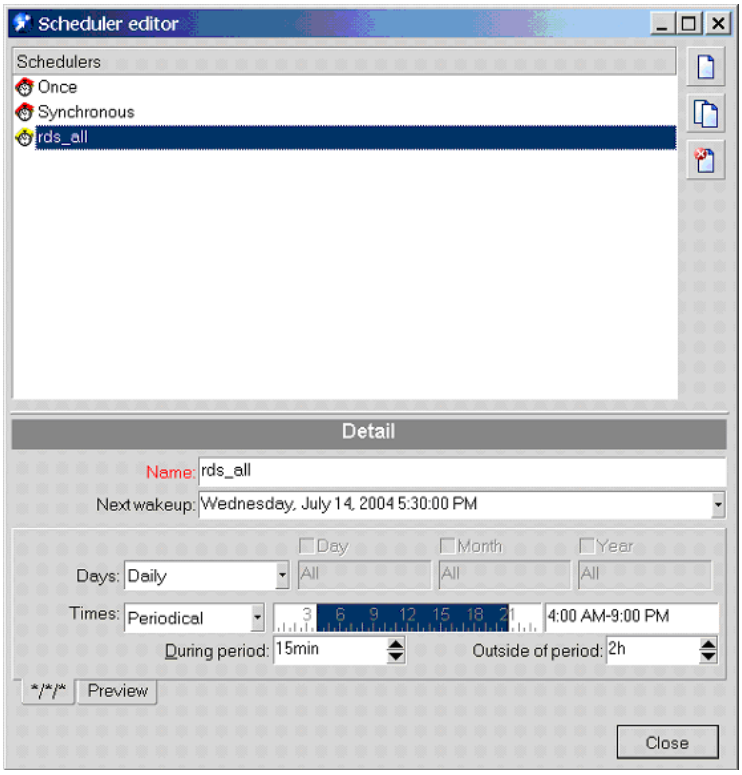
Because some of the synchronization tasks require more system resources than others, Peregrine recommends that they not be re-configured to occur more frequently than the default time intervals.

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_acuser`, `rds_user`, `rds_ac`, 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` and `rds_ac` scenario.

Scheduler	Description
`rds_all`	Synchronizes new and updated records at the default intervals of once a day at midnight.

Note: If the AssetCenter or 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:
`rds_user`	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. Use BI Administration in the Administration module of BI Portal to the **BIP user sync interval**. See Using the BI Portal Administration page on page 87.

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`).

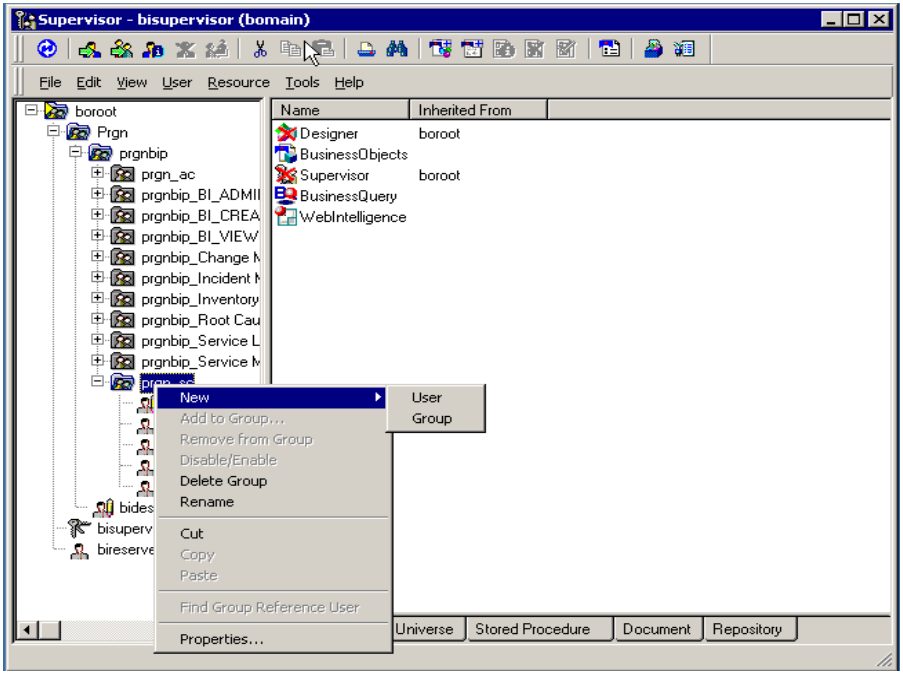
Step 6 Assign users to the group (`PRGNBIP_SEC_COMPUTER`).

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. With 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 can assign users and modify the security attributes to the new group.

To add object level security to a group:

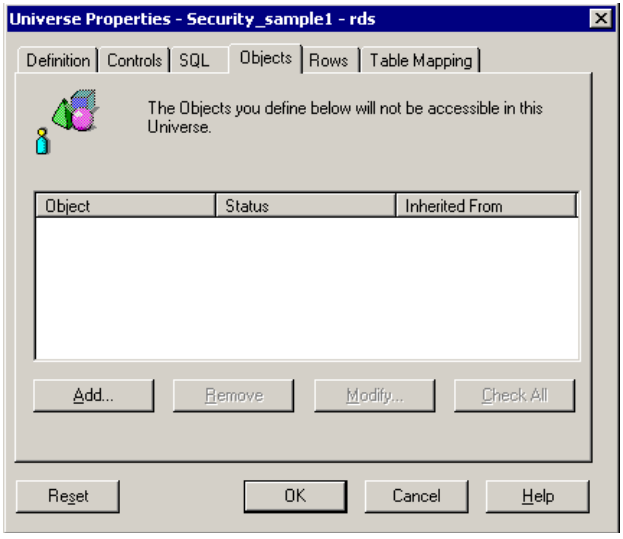
1 From the Business Objects Supervisor select the Universe tab.

A list of Universe files displays. 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.

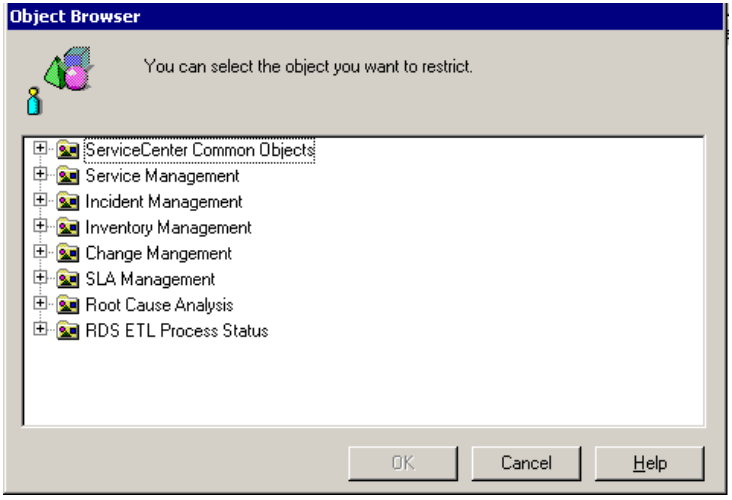


4 Click the **Objects** tab.

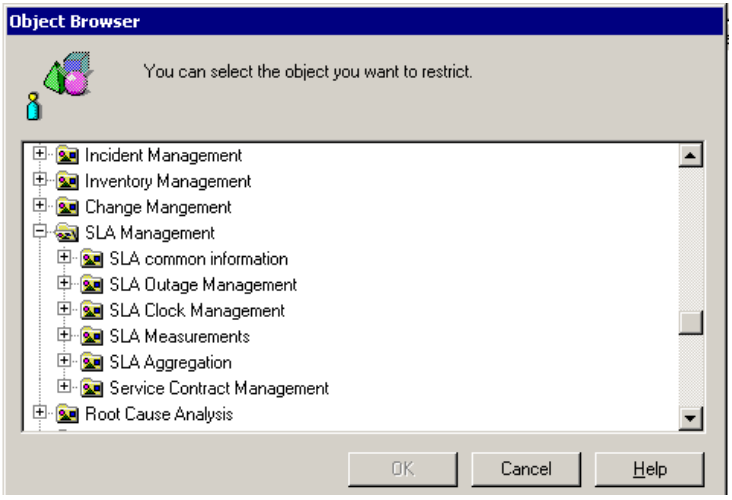
5 Click **Add** on the Objects tab, which lists all the classes and objects available in the universe.

The New Restricted Objects window opens.

6 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.

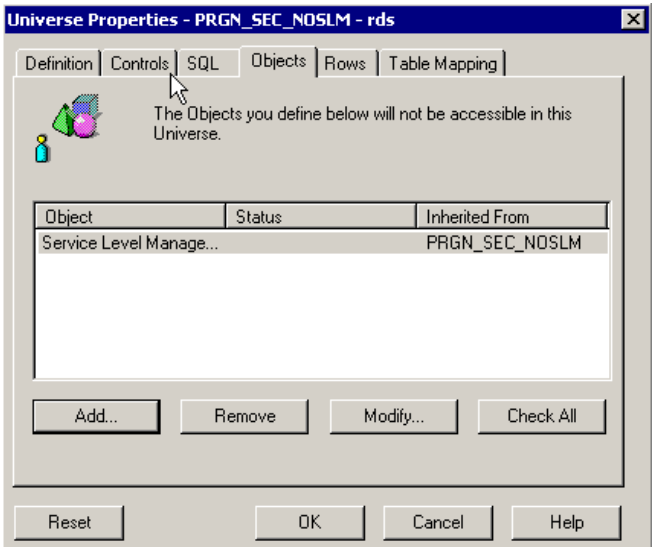


7 After you make your selection, click **OK**.

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 through 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:

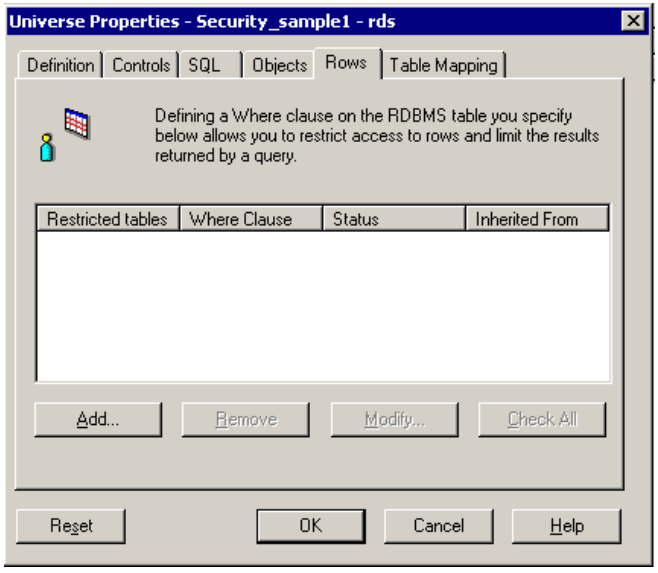
1 Start the Business Objects Supervisor tool.

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.

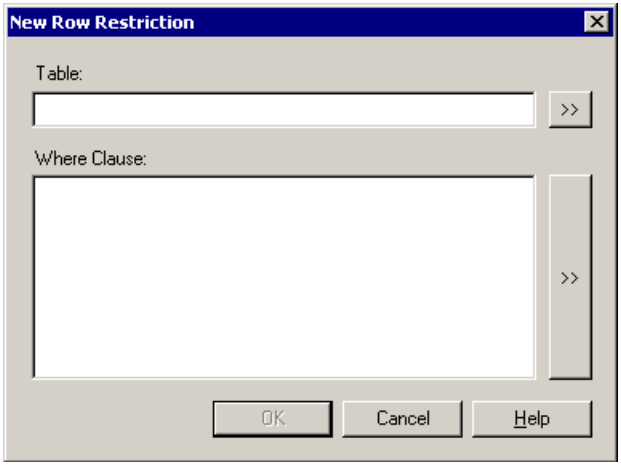
4 Select the **rds** universe file and while selected, right click to select the properties menu.

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



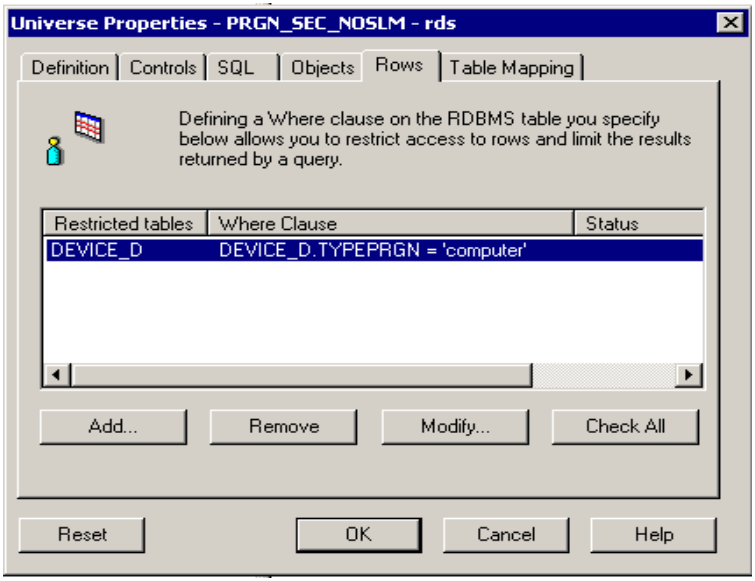
6 Click **Add**.

The New Row Restriction window opens.



7 Select the table, **DEVICE_D**, from the list box.

8 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 the restrictions are for a user on a particular table or what the restrictions are 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.

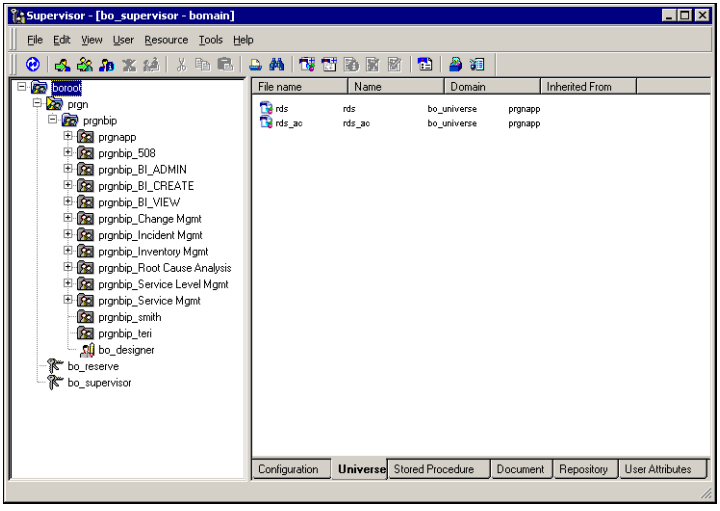
Table	Description
rdsgroups	By searching this table, an administrator can determine to what groups a user belongs.
rdsconditions	By searching this table, an administrator can determine, what conditions are defined for a group or user.
rdsopersecurity	By searching this table, an administrator can know 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.

Supporting multiple data sources

BI Portal supports AssetCenter and ServiceCenter as multiple data sources. The Business Objects repository contains an RDS universe for each data source.

To set up the Business Objects repository for multiple data sources:

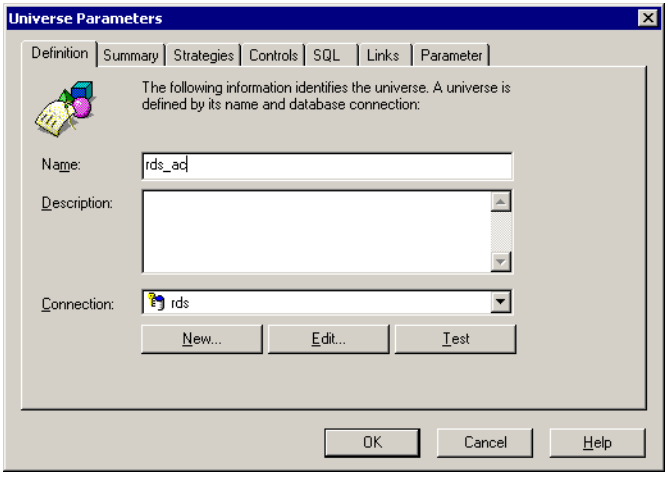
1 Export the `rds_ac.unv` to the `prgnapp` group (see Exporting the universe in the Installation Guide).



2 Rename the ServiceCenter universe, do one of the following.

- From the Business Objects Designer, open the `rds.unv` (from the BI Portal 5.1 ServiceCenter universe).

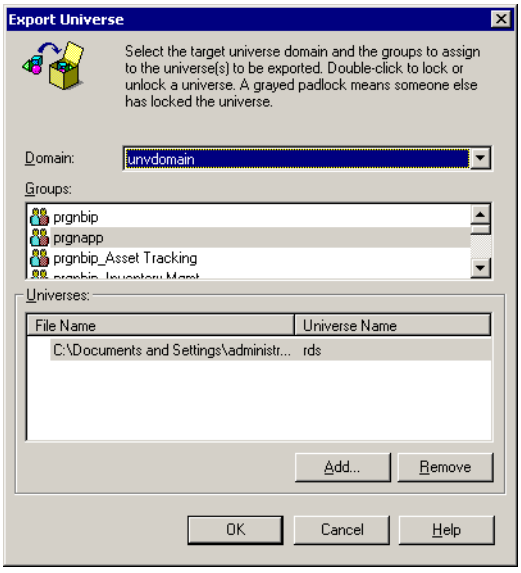
  Click File > Parameters.
  Change the universe name to `rds_sc`.



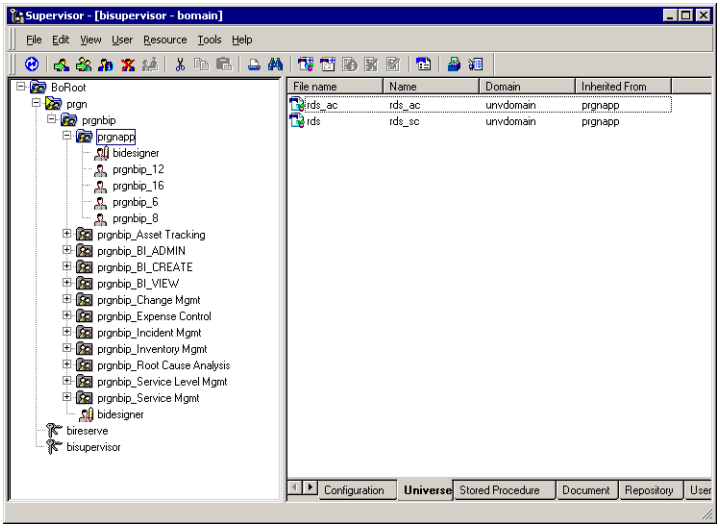
- From Business Objects Designer, export `rds_sc.unv` as `rds.unv` to the

prgnapp group to reorganize the Business Objects repository.

- Click File > Export.



- Go to Business Objects Supervisor.
- Highlight the prgnapp group.
- Click the Universe tab to see the following screen.



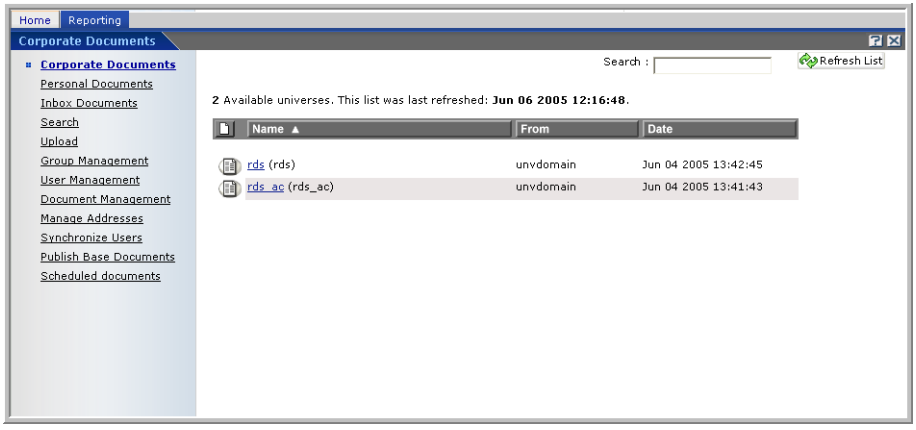
3 Delete the Business Objects universe cache.

a Navigate to

```
<BO_INSTALLATION_DIR>\nodes\<nodename>\<clustername>\universe
```

b Delete all files and folders under the `universe` directory.

4 Login to BI Portal and click **Create** to see both universes.



Note: For more information about limiting users for the control of accessing universe, objects or modules, see Restricting report data access on page 164.

Generating expense lines with AssetCenter

If you are using AssetCenter with BI Portal, when using the reports to project expenses, you must configure the AssetCenter server to generate expense lines. This is required for the Future Contract Expenses report, and is a good general practice for projecting expenses.

To configure the AssetCenter server to generate expense lines:

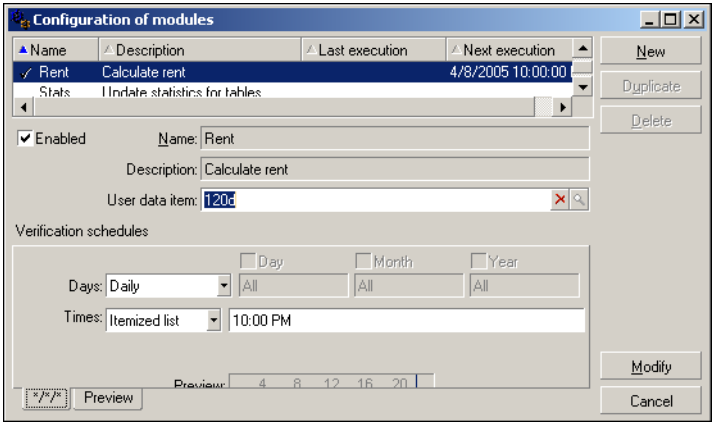
1 From a Windows environment, click **Start** > **Programs** > **Peregrine** > **AssetCenter** > **AssetCenter Server** to open AssetCenter Server.

2 Click **File** > **Connect to database** to connect to the server.

3 Click **Tools** > **Configure modules**.

4 Select **Rent** from the list.

5 Set **User data item** to 120d, then click **Close**.



6 Calculate the rent.

- To manually set rents to calculate, click **Action** > **Activate**, check **Calculate rent**, then click **OK**.
- To automatically calculate, keep the server running until the scheduled time passes.

7 Troubleshooting

CHAPTER

This section offers solutions when trying to resolve administration problems.

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

Issue	Solution
Navigation: When logged in to BI Portal, using the browser Back, Forward, and Refresh buttons can cause unexpected behavior of BI Portal forms.	Do not use the browser navigation or Refresh buttons with BI Portal forms displayed. Instead, use the Back link and Refresh link on the Portal.
When using the Microsoft Internet Explorer 5.5 browser, the following can occur: Icons fail to display in data set results. JavaScript errors appear during login (apparent only if the option to display JavaScript errors is turned on for the browser).	Upgrade to Internet Explorer 6.
After changing a theme using the Change Themes page, clicking the Go Back button does not return you to the Home page.	On the Activity menu in the sidebar, click My Home Page.

The following issues relate to the universe.

Issue	Solution
When you click the `rds` or `rds_ac` universe from the Portal to create an ad hoc report or edit a report, the universe does not open. You see the error message: `WebIntelligence cannot connect to the server. Please see your administrator.`	To open the universe after an error message: 1 Navigate to your Business Objects installation. `\Business Objects \BusinessObjects Enterprise 6 \nodes\<servername> \<clustername>\universes` 2 Delete all files and folders under the `\universes` directory. 3 Log off the portal.

APPENDIX A

BI Portal and ServiceCenter 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 user 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_SC installation root directory and verify that the *user* table has been synchronized.

   Alternatively, open the `RDS_USER` table in the RDS database and ensure users are added to this table.

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.

APPENDIX B

BI Portal and AssetCenter Synchronization

Manually synchronize new BI Portal users with AssetCenter database

In general, users defined in the operator table of AssetCenter are synchronized with BI Portal by the `rds_acuser` scenario at pre-defined intervals. By default, this interval is set to 15 minutes. This means that if a new AssetCenter 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_acuser` scenario.

To initiate a data synchronization using the rds_acuser scenario:

1. From CIT Service console window, stop the **rds_acuser** scenario.
2. Delete the file, `rds_acuser.ini`, in the `cit` sub-directory under the `RDS` installation root directory.
3. From the CIT Service console window, start the `rds_acuser` scenario.

4 Open the log file, `rds_acuser.log` in the logs sub-directory under the `RDS_AC` installation root directory and verify that the *user* table has been synchronized.

   Alternatively, open the `RDS_USER` table in the RDS database and ensure users are added to this table.

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 AssetCenter user now has access to BI Portal:

- Log in to BI Portal as the new AssetCenter user.

APPENDIX C

Copyright Notices

Peregrine Systems acknowledges the copyrights belonging to the following third parties. (This appendix constitutes a continuation of the copyright page.)

Notices

iso-relax.jar

The following software may be included in this product: `iso-relax.jar` v2002/07/07; This software may be obtained under the terms of the license below:

MIT license

Copyright © Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR

IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE

relaxngDatatype.jar

The following software may be included in this product: `relaxngDatatype.jar` v1.0; This software may be obtained under the terms of the license below:

Copyright © 2001, Thai Open Source Software Center Ltd, Sun Microsystems. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the names of the copyright holders nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Jcrypt.java

This product includes software developed by Eric Young (*eay@mincom.oz.au*).

JAXP

See the W3C license and the Apache version 2 license below.

W3C

W3C IPR SOFTWARE NOTICE

Copyright © 2000 World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University). All Rights Reserved.

The DOM bindings are published under the W3C Software Copyright Notice and License. The software license requires “Notice of any changes or modifications to the W3C files, including the date changes were made.” Consequently, modified versions of the DOM bindings must document that they do not conform to the W3C standard; in the case of the IDL binding, the pragma prefix can no longer be 'w3c.org'; in the case of the Java binding, the package names can no longer be in the 'org.w3c' package.

Note: The original version of the W3C Software Copyright Notice and License could be found at
http://www.w3.org/Consortium/Legal/copyright-software-19980720

Copyright © 1994-2000 World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University). All Rights Reserved.
http://www.w3.org/Consortium/Legal/

This W3C work (including software, documents, or other related items) is being provided by the copyright holders under the following license. By obtaining, using and/or copying this work, you (the licensee) agree that you have read, understood, and will comply with the following terms and conditions:

Permission to use, copy, and modify this software and its documentation, with or without modification, for any purpose and without fee or royalty is hereby granted, provided that you include the following on ALL copies of the software and documentation or portions thereof, including modifications, that you make:

1. The full text of this NOTICE in a location viewable to users of the redistributed or derivative work.

2. Any pre-existing intellectual property disclaimers, notices, or terms and conditions. If none exist, a short notice of the following form (hypertext is preferred, text is permitted) should be used within the body of any redistributed or derivative code: "Copyright © [$date-of-software] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University). All Rights Reserved. *http://www.w3.org/Consortium/Legal/*"

3. Notice of any changes or modifications to the W3C files, including the date changes were made. (We recommend you provide URIs to the location from which the code is derived.)

THIS SOFTWARE AND DOCUMENTATION IS PROVIDED "AS IS," AND COPYRIGHT HOLDERS MAKE NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE SOFTWARE OR DOCUMENTATION WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS.

COPYRIGHT HOLDERS WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF ANY USE OF THE SOFTWARE OR DOCUMENTATION.

The name and trademarks of copyright holders may NOT be used in advertising or publicity pertaining to the software without specific, written prior permission. Title to copyright in this software and any associated documentation will at all times remain with copyright holders.

Apache Version 1.1

The Apache Software License, Version 1.1

Copyright © 1999 The Apache Software Foundation. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment:

> "This product includes software developed by the Apache Software Foundation (*http://www.apache.org/*)."

Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

4. The names "Xalan" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact *apache@apache.org*.

5. Products derived from this software may not be called "Apache", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation and was originally based on software copyright © 1999, Lotus Development Corporation., *http://www.lotus.com*. For more information on the Apache Software Foundation, please see *<http://www.apache.org/>*.

Apache Version 2

Apache License, Version 2.0, January 2004, *http://www.apache.org/licenses/*

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. **Definitions.**

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works

shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. **Grant of Copyright License**. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. **Grant of Patent License**. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. **Redistribution**. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. **Submission of Contributions**. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. **Trademarks**. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. **Disclaimer of Warranty.** Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. **Limitation of Liability**. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. A**ccepting Warranty or Additional Liability**. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own

identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.Copyright [yyyy] [name of copyright owner]Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0 Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

See the License for the specific language governing permissions and limitations under the License.

PEREGRINE

Index

S

T

U

W