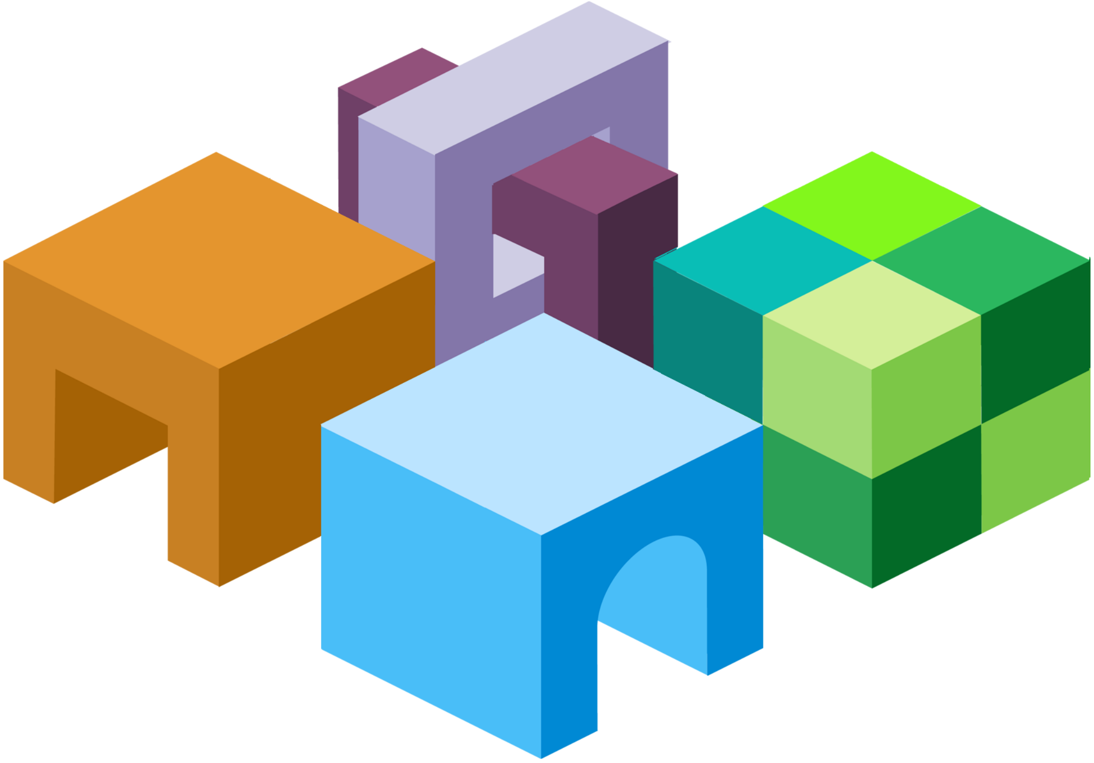


HYPERION® PORTAL INTEGRATION TOOLKIT

RELEASE 11.1.2

SETUP GUIDE

ORACLE®
ENTERPRISE PERFORMANCE
MANAGEMENT SYSTEM

Portal Integration Toolkit Setup Guide, 11.1.2

Authors: EPM Information Development Team

Contents

Documentation Accessibility . . . 9

Chapter 1. Portal Integration Toolkit Installation . . . 11

Portal Integration Toolkit Overview . . . 11

Functionality Limitations . . . 11

Financial Reporting . . . 12

Interactive Reporting . . . 12

Performance Scorecard . . . 12

Web Analysis . . . 12

How Portal Integration Toolkit Is Installed . . . 13

Deployment and Setup Procedures . . . 13

Configuring files for Server Component . . . 13

Configuring EPM Workspace Server on WebSphere for Portlets . . . 14

Portal Setup Procedures . . . 14

General Security Recommendations . . . 15

Quirks and Strict Modes and EPM System Portlets . . . 15

Chapter 2. WebSphere Portal Setup . . . 17

Deploying the EPM System Portlet for WebSphere . . . 17

Assigning Privileges and Owners . . . 19

Changing the Producer Preference Setting for WebSphere . . . 19

Configuring EPM System Portlet SSL for WebSphere . . . 20

Disabling Content Caching for the EPM System Portlet in WebSphere . . . 20

Changing the Portlet Title . . . 21

Choosing a WebSphere 6.0 Portal Theme . . . 21

Setting Up Pages for WebSphere Portals . . . 22

IBM Websphere Portal SSO Implementation . . . 22

Chapter 3. SAP NetWeaver 2004s Portal Setup . . . 23

Resetting the SAP Portal for ABAP Authentication . . . 23

Deploying the EPM System Portlet for SAP NetWeaver . . . 24

Adding Portal Content . . . 26

Changing the Producer Preference Setting for SAP NetWeaver . . . 30

Configuring the EPM System Portlet SSL for SAP NetWeaver 31
Setting Up Pages for SAP Portals 32

Chapter 4. SharePoint Portal 2003 Setup 39
Hyperion WebPart and SharePoint Portal 2003 39
SharePoint Portal 2003 Installation Prerequisites 39
SharePoint Portal 2003 Installation Package Contents 40
Installing the EPM System WebPart Application for SharePoint Portal 2003 41
Configuring Single Sign-On (SharePoint Portal 2003) 41
Installing the Hyperion WebPart ProxyPage Web Application (SharePoint Portal 2003) 43
Installing Hyperion WebPart ResourceHttpHandler (SharePoint Portal 2003) 50
Creating key container for Hyperion WebPart Encryptor 53
Installing Hyperion WebPart Encryptor 53
Customizing the Database Creation Script for SharePoint Portal 2003 58
Installing WebPart for SharePoint Portal 2003 59
Updating Web.config (SharePoint Portal 2003) 60
Customizing Hyperion WebPart app.config (SharePoint Portal 2003) 61
Configuring Default Permissions for EPM System WebPart (SharePoint Portal 2003) 61
Updating the Hyperion WebPart Application (SharePoint Portal 2003) 62
Updating Hyperion WebPart ProxyPage Web Application and Hyperion WebPart ResourceHttpHandler (SharePoint Portal 2003) 62
Updating the Web Part Installation (SharePoint Portal 2003) 63
Uninstalling the Hyperion WebPart Application (SharePoint Portal 2003) 63
Removing the Hyperion Web Part (SharePoint Portal 2003) 63
Removing SSO Data (SharePoint Portal 2003) 64
Removing Hyperion WebPart Encryptor 64
Removing key container for Hyperion WebPart Encryptor 65
Removing Hyperion WebPart ResourceHttpHandler (SharePoint Portal 2003) 65
Removing Hyperion WebPart ProxyPage (SharePoint Portal 2003) 65
SSL Support (SharePoint Portal 2003) 66
SSO Implementation 67
Support Activities (SharePoint Portal 2003) 67
Tips and Troubleshooting: SharePoint Portal 2003 68
Configuring Log Storage (SharePoint Portal 2003) 68
Customizing Hyperion WebPart app.config (SharePoint Portal 2003) 68
Error Messages (SharePoint Portal 2003) 69
Other Error Messages (SharePoint Portal 2003) 71

Chapter 5. SharePoint Portal 2007 Setup . . . 75
Hyperion WebPart and Microsoft SharePoint Portal 2007 . . . 75
Installation Prerequisites (SharePoint Portal 2007) . . . 75
Installation Package Contents (SharePoint Portal 2007) . . . 76
Installing the EPM System WebPart Application (SharePoint Portal 2007) . . . 77
Configuring Single Sign-On (SharePoint Portal 2007) . . . 77
Installing the Hyperion WebPart ProxyPage Web Application (SharePoint Portal 2007) . . . 79
Installing Hyperion WebPart ResourceHttpHandler (SharePoint Portal 2007) . . . 85
Customizing the Database Creation Script (SharePoint Portal 2007) . . . 88
Installing WebPart for SharePoint Portal 2007 . . . 88
Updating Web.config (SharePoint Portal 2007) . . . 88
Configuring Default Permissions for EPM System WebPart (SharePoint Portal 2007) . . . 90
Updating the Hyperion WebPart Application (SharePoint Portal 2007) . . . 90
Updating physical folders of Hyperion Web Part ProxyPage and Hyperion Web Part ResourseHttpHandler . . . 90
Customizing Database Update Script . . . 91
Updating Web.config . . . 91
Running UpdateWebPart.bat . . . 91
Updating app.config . . . 91
Removing Hyperion WebPart . . . 91
Removing the Web Part (SharePoint Portal 2007) . . . 92
Removing SSO Data (SharePoint Portal 2007) . . . 92
Removing Hyperion WebPart ResourceHttpHandler (SharePoint Portal 2007) . . . 92
Removing Hyperion WebPart ProxyPage (SharePoint Portal 2007) . . . 92
SSL Support: SharePoint Portal 2007 . . . 93
Support Activities (SharePoint Portal 2007) . . . 94
Tips and Troubleshooting: SharePoint Portal 2007 . . . 94
Configuring Log Storage (SharePoint Portal 2007) . . . 94
Customizing Hyperion WebPart app.config (SharePoint Portal 2007) . . . 95
Error Messages (SharePoint Portal 2007) . . . 96
Other Error Messages (SharePoint Portal 2007) . . . 98

Chapter 6. WebLogic Portal Setup . . . 103
Deploying the EPM System Portlet for WebLogic . . . 103
Assigning Privileges for WebLogic . . . 105
Resetting the Producer Preference in WebLogic . . . 105
Configuring the EPM System Portlet SSL for WebLogic . . . 106
Changing the EPM System Portlet Title . . . 106

Choosing Look and Feel 106

Setting Up Pages for WebLogic Portal 107

SSO Implementation 107

Chapter 7. Oracle 10g Portal Setup 109

Configuring Server Components for SSO 109

Oracle Portal Security Recommendations 110

Deploying the EPM System Portlet for Oracle 110

Configuring Parallel Page Engine 112

Assigning Privileges for Oracle 112

Changing the Producer Preference Setting for Oracle 113

Configuring the EPM System Portlet SSL for Oracle 113

Setting Up Pages for Oracle 114

Tips and Troubleshooting: Oracle Portal 114

SSO Implementation 115

Chapter 8. Oracle® Web Center 10g (10.1.3.4.0) Setup 117

Configuring Server Components for SSO 117

Oracle WebCenter Security Recommendations 118

Deploying the Hyperion Portlet for Oracle WebCenter 118

Changing the Producer Preference Setting in Oracle WebCenter 120

Configuring Hyperion Portlet SSL for Oracle WebCenter 121

Setting Up Pages for Oracle WebCenter 121

Navigational parameters 121

SSO Implementation 122

Interactive Reporting Page Parameter Wiring Feature in Oracle Web Center 122

Chapter 9. Oracle® Web Center 11g (11.1.1) Setup 127

Configuring Server Components for SSO 127

Oracle WebCenter 11 Security Recommendations 127

Deploying the Hyperion Portlet for Oracle WebCenter 11 128

Changing the Producer Preference Setting in Oracle WebCenter 11 129

Configuring Hyperion Portlet SSL for Oracle WebCenter 11 130

Setting Up Pages for Oracle WebCenter 11 130

Navigational Parameters 131

SSO Implementation 131

Chapter 10. Web Analysis Portlets 133

Subscription Controls Functional in Portlets 133

Designer Components Not Supported in Portlets 133

Launch Out to EPM Workspace 134

Points of View, Personal Variables, and Subscription Controls 134

Web Analysis Portlet External POV feature from End User Perspective 134

Chapter 11. Performance Scorecard Portlet Pages 137

About Performance Scorecard Portlets 137

Creating Portlet Pages 137

Measure Trending Table 139

Measure Chart 140

Annotations 140

Scorecard Trending Table 140

Scorecard Detail 141

Scorecard Chart 141

Documentation Accessibility

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

Access to Oracle Support for Hearing-Impaired Customers

Oracle customers have access to electronic support through My Oracle Support or by calling Oracle Support at 1.800.223.1711. Hearing-impaired customers in the U.S. who wish to speak to an Oracle Support representative may use a telecommunications relay service (TRS). Information about the TRS is available at http://www.fcc.gov/cgb/consumerfacts/trs.html/, and a list of telephone numbers is available at http://www.fcc.gov/cgb/dro/trsphonebk.html. International hearing-impaired customers should use the TRS at +1.605.224.1837. An Oracle Support engineer will respond to technical issues according to the standard service request process.

1 Portal Integration Toolkit Installation

In This Chapter

Portal Integration Toolkit Overview 11
Functionality Limitations 11
How Portal Integration Toolkit Is Installed 13
Deployment and Setup Procedures 13
General Security Recommendations 15
Quirks and Strict Modes and EPM System Portlets 15

Portal Integration Toolkit Overview

Oracle's Hyperion® Portal Integration Toolkit gives you access to Oracle's Hyperion Reporting and Analysis information from Enterprise Information portals. This release of Portal Integration Toolkit supports these portals:

- IBM WebSphere 5.1.0.1
- IBM WebSphere 6.0
- SAP NetWeaver 2004 and 2004s
- Microsoft SharePoint Portal 2003 and 2007
- WebLogic 9.2 and 10
- Oracle Application Server Portal 10g Release 2 (10.1.4)
- Oracle WebCenter 10.1.3.4
- Oracle WebCenter 11

Portal Integration Toolkit has two parts:

- Server component—Part of the Reporting and Analysis server and is installed with it.
- Client component—Runs on the Enterprise Information portal and must be installed on it.

Functionality Limitations

The following limitations exist for product functionality in the portlets.

Financial Reporting

Reports and report features available in the portlet are similar to those in Oracle Enterprise Performance Management Workspace, Fusion Edition. The following features are not supported in the portlet:

- POV Changes — You cannot change the report or grid POV settings.
- Prompts — Report prompts are not supported. If a report with prompts is selected, the default members are used.
- Related Content — All related content links (including cell documents) are disabled.
- Annotations — Annotations are not supported.
- Locked Grid Headers — Locked headings are only supported in Firefox.

Interactive Reporting

The following features are not supported in the portlet:

- Page navigation and section navigation
- Dashboard functionality — Dashboard controls with scripting, client-side JS, embedded browser, hyperlink only supported through new window
- No corner tab images on Pivot
- View only and no support for context menus
- Variable limits dialog, Alert dialog, Exception dialog, Database Logon dialog not supported
- State information of current selection not maintained

Performance Scorecard

The following features are not supported in the portlet:

- Reports are displayed completely expanded, retaining grouping information and cannot be collapsed.
- You cannot specify custom colors for charts.
- Custom reports are not available.
- Maps are not available.

Web Analysis

The following features are not supported in the portlet:

- Presentations and database connections are not supported and cannot be selected as a target document.
- Slider Subscription and Tab Group Subscription are not supported
- EIS Drill-through reports are not supported.

- Drill-linking is not supported.
- Portlet only renders report design components allowed by HTML subset. Some report design elements are not supported.
- All right-click functions are not supported.
- Portlet requires preferable size to be specified in the Edit mode.
- Reports with SAP BW data sources with mandatory SAP BW variables without default values specified are not rendered,

How Portal Integration Toolkit Is Installed

Portal Integration Toolkit installation is selected by default when you install Oracle's Hyperion Reporting and Analysis Framework, Oracle's Hyperion® Interactive Reporting, or Oracle's Hyperion® Web Analysis. Oracle's Hyperion Enterprise Performance Management System Configurator installs Portal Integration Toolkit when an application server is deployed. Although no installation procedures are required, you must complete several other procedures before the portlets can be used.

Deployment and Setup Procedures

The Oracle Hyperion Enterprise Performance Management System portlet gives you access to other portlets where you can display reports. You must deploy the EPM System portlet before users can add it to portal pages so they can use the other portlets. You repeat the procedure only when you need an updated version of the EPM System portlet.

Configuring files for Server Component

To configure client components to connect to a particular server component (producer), update the URL in client modules with the actual location of your Reporting and Analysis deployment server.

Table 1 Configuring files for Server Components

Portal	File	Configuration File Path
WebSphere Portal	`ibm-avaproxy.war`	`ibm-avaproxy.war\WEB-INF\portlet.xml`
SAP NetWeaver 2004s Portal	`com.hyperion.portlet.proxy.ProxyPortlet.par`	`com.hyperion.portlet.proxy.ProxyPortlet.par\PORTAL-INF\portalapp.xml`
SharePoint Portal 2003	`HyperionWebPart.zip`	`HyperionWebPart.zip\HyperionWebPartProxyPage\Web.Config`
SharePoint Portal 2007	`HyperionWebPart2007.zip`	`HyperionWebPart2007.zip\ HyperionWebPartProxyPage\Web.config`

Portal	File	Configuration File Path
WebLogic Portal	`bea-avaproxy.zip`	`bea-avaproxy.zip\WEB-INF\portlet.xml`
Oracle 10g Portal	`oracle-avaproxy.war`	`oracle-avaproxy.war\WEB-INF\portlet.xml`
Oracle® Web Center 10g	`oracle-avaproxy.ear`	`oracle-avaproxy.ear\oracle-avaproxy.war\ WEB-INF \portlet.xml`
Oracle® Web Center 11g	`oracle-avaproxy11.ear`	`oracle-avaproxy11.ear\oracle-avaproxy.war\WEB-INF \portlet.xml`

➤ To configure files for server components:

1 **Unzip configuration file from corresponding client package into a temporary folder.**

2 **Replace all occurrences of the following strings in the configuration file:**

Table 2 String Replacement Values

String to Replace	New Value
`$GET(appServerProps.workspaceHost)`	Host name of your Reporting and Analysis deployment
`$GET(httpServerProps.httpServerPort)`	HTTP server port number of your Reporting and Analysis deployment

For example:

`http://$GET(appServerProps.workspaceHost): $GET(httpServerProps.httpServerPort)/raframework/wsrp4j/ WSRPBaseService"` should be changed to "`http://myhost:7777/raframework/ wsrp4j/WSRPBaseService`

3 **Repack updated configuration file into corresponding client package.**

4 **Use updated client package in your deployment and setup procedures.**

Configuring EPM Workspace Server on WebSphere for Portlets

If you have WebSphere Application Server 5.1 earlier than Release 5.1.1.10 or WebSphere Application Server 6 earlier than Release 6.0.2.9, complete these steps:

1. Remove the `client-config.wsdd` file from the `%WEBSPHERE_HOME%/lib/wsif.jar` file.
2. Restart the application server.

Portal Setup Procedures

You must also perform other setup procedures before portlets can be used. The deployment and setup procedures depend on your application server.

- For WebSphere procedures, see Chapter 2, "WebSphere Portal Setup"
- For SAP procedures, see Chapter 3, "SAP NetWeaver 2004s Portal Setup"
- For SharePoint Portal 2003 procedures, see Chapter 4, "SharePoint Portal 2003 Setup"
- For SharePoint Portal 2007 procedures, see Chapter 5, "SharePoint Portal 2007 Setup"
- For WebLogic procedures, see Chapter 6, "WebLogic Portal Setup"
- For Oracle Portal procedures, see Chapter 7, "Oracle 10g Portal Setup"
- For Oracle WebCenter procedures, see Chapter 8, "Oracle® Web Center 10g (10.1.3.4.0) Setup"

General Security Recommendations

The point-to-point communication between the EPM System portlet and Reporting and Analysis must be secured. You can provide the necessary security by ensuring that one of the following statements is true:

- The Reporting and Analysis Framework Web application is not exposed to an untrusted network.
- SSL is being used between the EPM System portlet and the Reporting and Analysis Framework Web application

Quirks and Strict Modes and EPM System Portlets

Browsers can use quirks mode or strict mode to interpret cascading style sheets (CSS). The mode that is used to render an HTML page is defined in the document type declaration for the page. Portals differ in the HTML code that they use during page construction. Some portals use table-based layout, and others using div elements to position portal content. Some portals use quirks mode DocType specifications, and others use strict mode.

EPM System portlets produce complex HTML code that relies on quirks rendering mode in the browser. If you try to display the content of a EPM System portlet in a portal with a strict mode DocType specification, formatting problems (such as excess white space, alignment issues, truncation, and so forth) and JavaScript console errors and warnings may occur when a page is rendering. To avoid such problems ensure that your portal renders pages with EPM System portlets on them in quirks mode, not strict mode; remember to specify quirks mode when customizing a portal.

Ensure that other portlets on the same page as a EPM System portlet are rendered correctly in quirks mode. If they do not, place them on a separate page using strict mode.

Strict mode support is planned for future releases of Portal Integration Toolkit.

For more information about quirks and strict mode, go to `http://www.quirksmode.org/css/quirksmode.html`.

2

WebSphere Portal Setup

In This Chapter

Deploying the EPM System Portlet for WebSphere 17

Assigning Privileges and Owners 19

Changing the Producer Preference Setting for WebSphere 19

Configuring EPM System Portlet SSL for WebSphere 20

Disabling Content Caching for the EPM System Portlet in WebSphere 20

Changing the Portlet Title....................21

Choosing a WebSphere 6.0 Portal Theme....................21

Setting Up Pages for WebSphere Portals....................22

IBM Websphere Portal SSO Implementation....................22

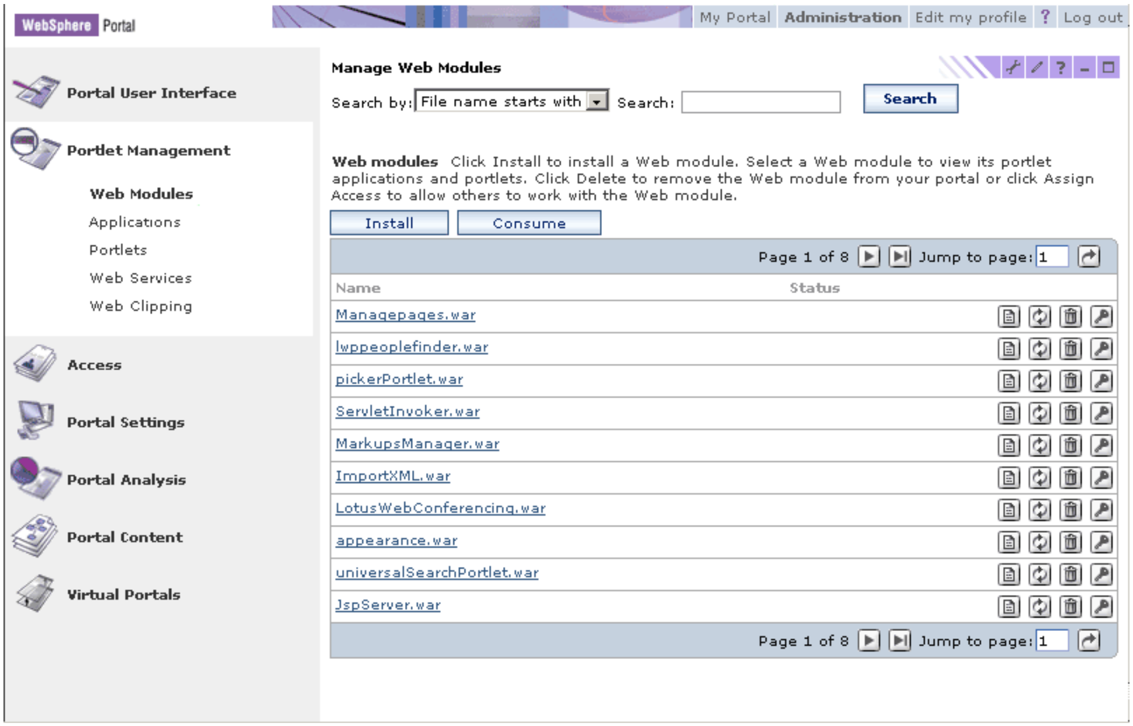
Note: All procedures in this chapter assume that you are logged on to WebSphere as a portal administrator.

Deploying the EPM System Portlet for WebSphere

You can deploy the EPM System portlet for WebSphere 5.1.0.1 or 6.0.

➤ To deploy the EPM System portlet for WebSphere:

1. On the WebSphere toolbar, click **Administration.**
2. In the left pane, select **Portlet Management**, then **Web Modules.**



Manage Web Modules

Search by: File name starts with Search:

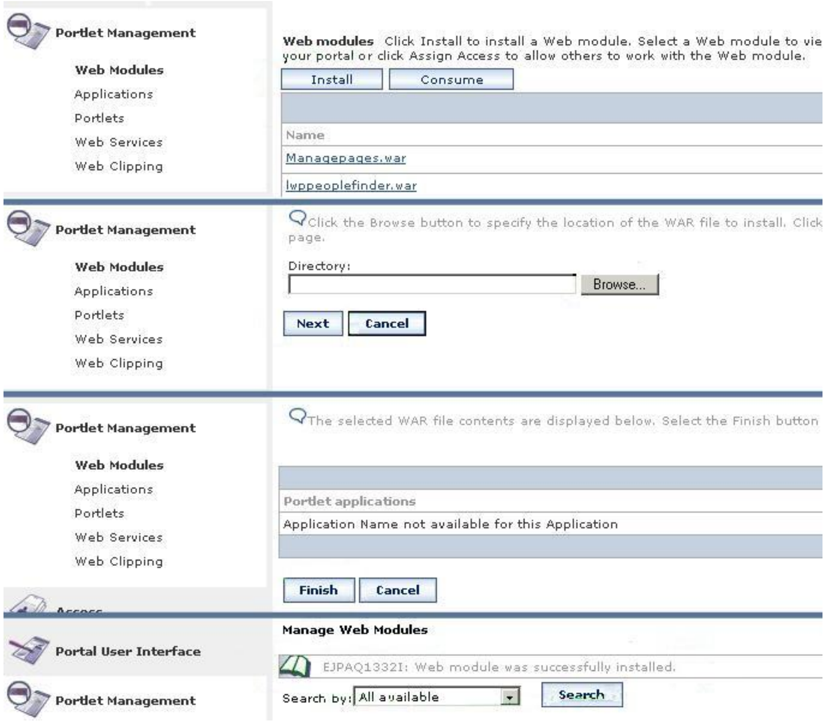
Web modules Click Install to install a Web module. Select a Web module to view its portlet applications and portlets. Click Delete to remove the Web module from your portal or click Assign Access to allow others to work with the Web module.

Page 1 of 8 Jump to page: 1

Name	Status
Managepages.war	
lwppeoplefinder.war	
pickerPortlet.war	
ServletInvoker.war	
MarkupsManager.war	
ImportXML.war	
LotusWebConferencing.war	
appearance.war	
universalSearchPortlet.war	
JspServer.war	

Page 1 of 8 Jump to page: 1

3 Install `ibm-avaproxy.war`:



Web modules Click Install to install a Web module. Select a Web module to vie your portal or click Assign Access to allow others to work with the Web module.

Name
Managepages.war
lwppeoplefinder.war

Click the Browse button to specify the location of the WAR file to install. Click page.

Directory:

The selected WAR file contents are displayed below. Select the Finish button

Portlet applications
Application Name not available for this Application

Manage Web Modules

EJPAQ1332I: Web module was successfully installed.

Search by: All available

a. Click **Install**.

b. Using the **Browse** button, locate and select **`ibm-avaproxy.war`**.

Default location: `*Hyperion*\products\biplus\InstallableApps\portlets`, where *Hyperion* is the Reporting and Analysis home directory.

c. Click **Next**.

4 Click **Finish**.

Assigning Privileges and Owners

After deploying the EPM System portlet for WebSphere, you assign privileges for the Administrator role and specify an owner for the portlet.

➤ To assign privileges for the Administrator role:

1 In the left pane, select **Portlet Management**, then **Portlets**.

2 Find and select the EPM System portlet:

   a. Select **Title starts with** from the **Search by** list in the lower half of the page.

   b. Type **Hyperion** in the **Search** box.

   c. Click **Search**.

   d. Click **Hyperion**.

3 On the **Portlet Management** page, change the privileges for the portlet:

   a. Click 🔑, **Assign access to portlet**.

   b. In the **Administrator** row, click **Edit Role**.

   c. Click + Add, and then select **All Authenticated Portal Users**.

   d. Click **OK**.

4 In WebSphere 6.0, repeat step 3 for the **Hyperion Credential Manager** portlet.

➤ To specify an owner for the portlet:

1 Click **Display/Modify Owner**.

2 Select **All Authenticated Portal Users**.

3 Click **Done**.

Changing the Producer Preference Setting for WebSphere

The EPM System portlet contains the `wsrp_producer_url` setting, which points to the Reporting and Analysis Framework instance, or producer, that contains all the other portlets. The default producer is set when EPM System Configurator installs the EPM System portlet. To use a different producer, you must change the preference setting.

➤ To change the producer preference setting:

1 In the left pane, select **Portlet Management**, then **Portlets**.

2 Find and select the **Hyperion** portlet:

a. Select **Title starts with** from the **Search by** list in the lower half of the page.

b. Type **Hyperion** in **Search**.

c. Click **Search**.

d. Click **Hyperion**.

3 Click, 🔧.

4 On the **Parameters and Values** page:

a. Click , ✎, for **`wsrp_producer_url`**.

b. Delete the entry in the **Value** column.

c. In the **Value** column, enter the URL for the producer that you want to use. (Example: `http://`*`ComputerName`*`:`*`Port`*`/raframework/wsrp4j`).

Configuring EPM System Portlet SSL for WebSphere

Configuring SSL for the EPM System portlet for WebSphere involves these tasks:

- Changing the producer preference setting to point to the SSL address of the Hyperion server (which usually has the prefix `https://`)
- Importing the public EPM System server certificate into the trusted certificates list

  For example, you can import the certificate into the cacerts key store, which is usually in the `%WAS_HOME%\java\jre\lib\security\` folder, using the IBM iKeyman utility. The default key store password is changeit. For details about managing digital certificates, see `http://publib.boulder.ibm.com/infocenter/wasinfo/v5r1/index.jsp?topic=/com.ibm.websphere.base.doc/info/aes/ae/tsec_mngcert.html`.

Disabling Content Caching for the EPM System Portlet in WebSphere

For the EPM System portlet to work correctly, content caching for the portlet must be disabled. EPM System portlet content caching is disabled by default. You can enable it by changing the cache expiration setting.

➤ To ensure that content caching for the EPM System portlet is disabled:

1 In the left pane, select **Portlet Management**, then **Portlets.**

2 Find and select the **Hyperion** portlet:

a. Select **Title starts with** from the **Search by** list in the lower half of the page.

b. Type **`Hyperion`** in Search.

c. Click **Search**.

d. Click **Hyperion**.

3 Click **Configure Portlet**, 🔧.

4 Under **Cache Expiration**, ensure that**Portlet cache always expires** is selected.

5 Click **OK**.

Changing the Portlet Title

Users with Administrative privileges can change the title of the portlet. For example, you can change it from Hyperion (the default name) to Primary.

Note: Procedures in this guide use the default title for the EPM System portlet.

➤ To change the portlet title :

1 In the left pane, select **Portlet Management**, then **Portlets.**

2 Find and select **Hyperion**:

a. Type **Hyperion** in the **Search** box.

b. Click **Search**.

c. Click **Hyperion**.

3 Click 🔧.

4 On the **Parameters and Values** page, click **I want to set titles and descriptions.**

5 Edit the title, and then click **OK.**

Choosing a WebSphere 6.0 Portal Theme

To ensure that the HTML content of a EPM System portlet is correctly displayed, ensure that you are using the appropriate portal theme, which triggers the quirks layout mode in browser. The default theme for WebSphere Portal 6.0 uses standards compliance (strict mode), which is incompatible with the complex HTML content of EPM System portlets.

If you do not have another quirks-mode theme, you can use the theme that is bundled with EPM System applications. It is in `websphere-portal-6-quirks-theme.zip` file for illustrative purpose only. Default location: *`Hyperion`*`\\products\biplus\\InstallableApps\portlets\unconfigured`, where *`Hyperion`* is a Reporting and Analysis application home directory.

After installing a theme, you can use it when creating portal pages for EPM System portlets.

➤ To install a quirks-mode theme:

1 Copy the `quirks` folder and its contents from `websphere-portal-6-quirks-theme.zip` to the `was_profile_root/installedApps/cellname/wps.ear/wps.war/themes/html` folder.

2 Log on to WebSphere Portal as an administrator.

3 Select **Product Links**, then **Administration.**

4 In the left pane, select **Portal User Interface**, then **Themes and Skins.**

5 Click **Add new theme.**

6 In **Theme name and default locale title**, enter a name for the theme.

7 In **Theme directory name**, type `quirks`.

8 Select skins for the new theme.

9 Click **OK.**

Setting Up Pages for WebSphere Portals

You must set up a page before you can work with portlets in WebSphere. You can then navigate to the page, switch any portlet to Edit Mode, and select a report to display.

➤ To set up a page:

1 Log on as a regular user.

2 Create a page:

a. click **New Page** link.

b. Enter a name for the page.

c. Specify additional properties for the page or accept the defaults.

d. Click **OK**.

3 Navigate to the page that you created in the preceding step.

4 On the **Edit Layout** page, click **Add Portlets.**

5 Find and select **Hyperion**:

a. Type **Hyperion** in the **Search** box.

b. Click **Search**.

c. Click **Hyperion**.

6 Click **OK.**

7 Click **Done.**

IBM Websphere Portal SSO Implementation

IBM Credential Vault is used to store mapping between portal user credentials and EPM system credentials. When you display the proxy portlet for the first time, the system prompts for EPM System user credentials. On subsequent calls, the EPM System user credentials are used to authenticate requests from a particular user.

3

SAP NetWeaver 2004s Portal Setup

In This Chapter

Resetting the SAP Portal for ABAP Authentication 23

Deploying the EPM System Portlet for SAP NetWeaver..24

Adding Portal Content 26

Changing the Producer Preference Setting for SAP NetWeaver......................................30

Configuring the EPM System Portlet SSL for SAP NetWeaver..31

Setting Up Pages for SAP Portals..32

Resetting the SAP Portal for ABAP Authentication

You can use an SAP NetWeaver Application Server (AS) Advanced Business Application Programming (ABAP) authentication for user management data. To do this, you must reset the SAP portal to use the ABAP authentication database before deploying the EPM System portlet for SAP NetWeaver.

➤ To reset the SAP portal to use the ABAP authentication database:

1 Start the SAP portal.

2 Open Start the Config tool with the program configtool.bat/sh (**<directory of the J2EE Installation>**\<SID>\JC<inst. no.>\j2ee\configtool\configtool.bat/sh).

3 Connect to the default database.

4 Enter these settings:

Key	Custom Value
`ume.login.guest_user.uniqueids`	A user name that is entered in the property `ume.login.guest_user.uniqueids` This user name must not exist in the new AS ABAP system. **Caution!** These requirements must be met for AS Java to start after you change the database settings.
`ume.persistence.data_source_configuration`	`dataSourceConfiguration_r3.xml`
`ume.r3.connection.master.ashost`	Application server host address Example: `server02.mycompany.com`

Key	Custom Value
`ume.r3.connection.master.client`	SAP System client Example: 100
`ume.r3.connection.master.sysnr`	SAP System number Example: 12
`ume.r3.connection.master.user`	User ID in the SAP system with which the connection to the SAP system is set up. This user must be authorized to use RFC and to create, change, and delete users in the SAP system.
`ume.r3.connection.master.passwd`	Password for the SAP System user

Note: The Custom Value and Default Cell values are empty for key `ume.r3.mastersystem`.

5 In the left pane, select **UME LDAP data.**

6 On the **Additional LDAP properties** tab, select **`dataSourceConfiguration.r3.xml`**` from **Data source configuration file.**

7 Click **Apply Changes** and close **Config Tool.**

Note: On Windows, you might need to modify the `%WINDOWS%\system32\drivers\etc\services` file and add next services: `sapdp00-3200/tcp, sapdp01-3201/tcp, sapdp02-3202/tcp`, and so on.

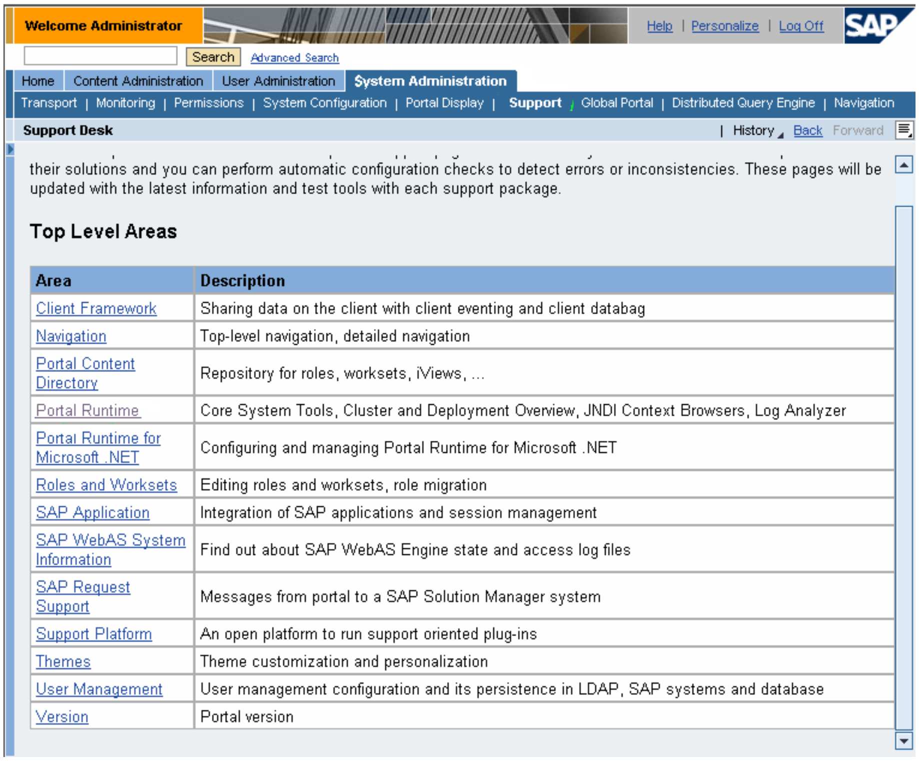
8 Restart the SAP portal and verify that ABAP users are listed in **User Management.**

Deploying the EPM System Portlet for SAP NetWeaver

You need an SAP portal certificate when configuring Oracle's Hyperion® Shared Services to work with portlets using an SAP portal. For the SAP portal to list EPM System portlet, the `SAP.certificate` file from Shared Services must be in the `SAP\lib` folder on the computer running the Web application in order to have Portlet shown in SAP Portal.

➤ To deploy the EPM System portlet for SAP NetWeaver:

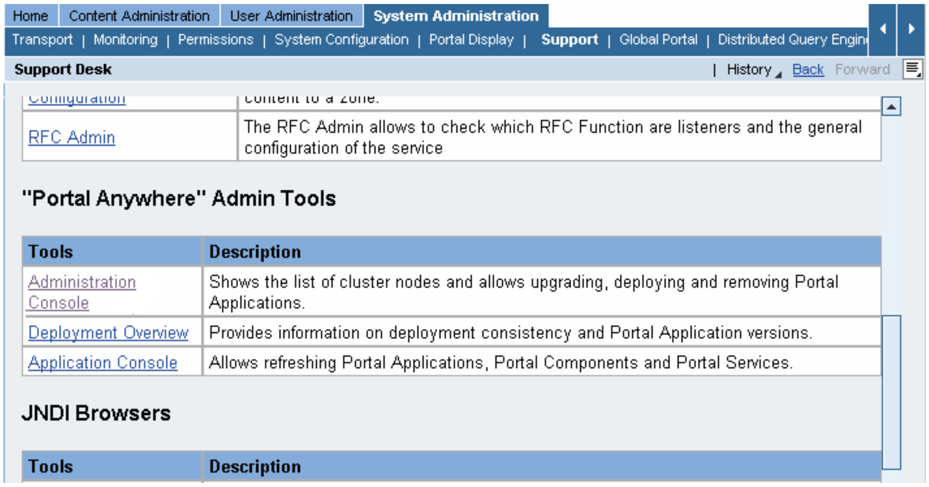
1 Log on to SAP as an administrator and navigate to **System Administration — Support — Portal Runtime — Administration Console.**


Welcome Administrator
Help | Personalize | Log Off
SAP
Search
Advanced Search
Home | Content Administration | User Administration | System Administration
Transport | Monitoring | Permissions | System Configuration | Portal Display | Support | Global Portal | Distributed Query Engine | Navigation
Support Desk
History | Back Forward

their solutions and you can perform automatic configuration checks to detect errors or inconsistencies. These pages will be updated with the latest information and test tools with each support package.

Top Level Areas

Area	Description
Client Framework	Sharing data on the client with client eventing and client databag
Navigation	Top-level navigation, detailed navigation
Portal Content Directory	Repository for roles, worksets, iViews, ...
Portal Runtime	Core System Tools, Cluster and Deployment Overview, JNDI Context Browsers, Log Analyzer
Portal Runtime for Microsoft .NET	Configuring and managing Portal Runtime for Microsoft .NET
Roles and Worksets	Editing roles and worksets, role migration
SAP Application	Integration of SAP applications and session management
SAP WebAS System Information	Find out about SAP WebAS Engine state and access log files
SAP Request Support	Messages from portal to a SAP Solution Manager system
Support Platform	An open platform to run support oriented plug-ins
Themes	Theme customization and personalization
User Management	User management configuration and its persistence in LDAP, SAP systems and database
Version	Portal version


Home | Content Administration | User Administration | System Administration
Transport | Monitoring | Permissions | System Configuration | Portal Display | Support | Global Portal | Distributed Query Engin
Support Desk
History | Back Forward

Configuration	content to a zone.
RFC Admin	The RFC Admin allows to check which RFC Function are listeners and the general configuration of the service

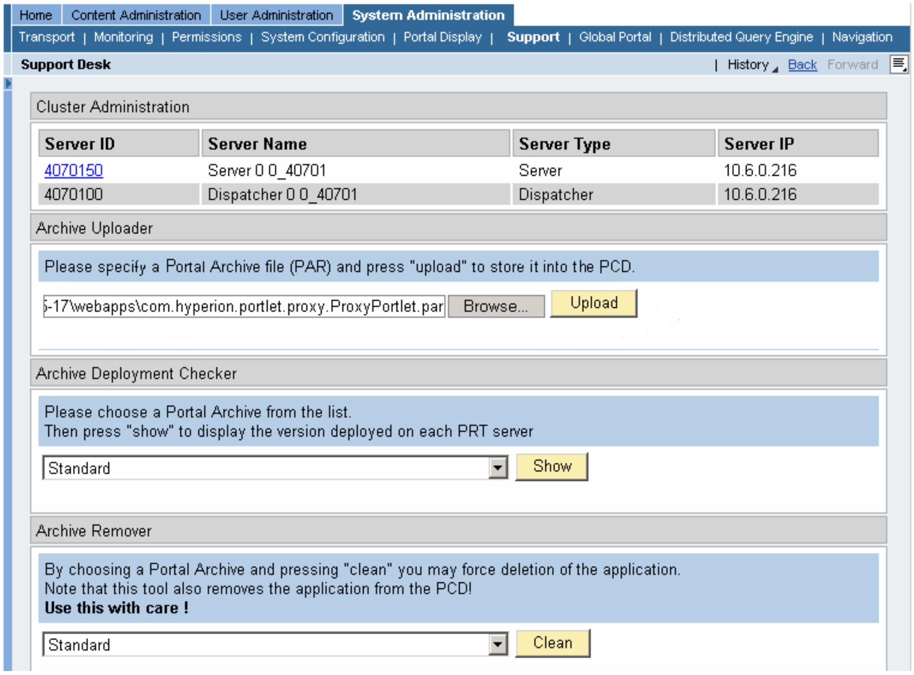
"Portal Anywhere" Admin Tools

Tools	Description
Administration Console	Shows the list of cluster nodes and allows upgrading, deploying and removing Portal Applications.
Deployment Overview	Provides information on deployment consistency and Portal Application versions.
Application Console	Allows refreshing Portal Applications, Portal Components and Portal Services.

JNDI Browsers

Tools	Description

2 Upload **`com.hyperion.portlet.proxy.ProxyPortlet.par`**, which is in *`EPM_ORACLE_HOME\products\biplus\InstallableApps\portlets\unconfigured\`* by default.


Home
Content Administration
User Administration
System Administration
Transport | Monitoring | Permissions | System Configuration | Portal Display | Support | Global Portal | Distributed Query Engine | Navigation
Support Desk
History
Back
Forward

Cluster Administration

Server ID	Server Name	Server Type	Server IP
4070150	Server 0 0_40701	Server	10.6.0.216
4070100	Dispatcher 0 0_40701	Dispatcher	10.6.0.216

Archive Uploader

Please specify a Portal Archive file (PAR) and press "upload" to store it into the PCD.

5-17\webapps\com.hyperion.portlet.proxy.ProxyPortlet.par

Archive Deployment Checker

Please choose a Portal Archive from the list.
Then press "show" to display the version deployed on each PRT server

Standard

Archive Remover

By choosing a Portal Archive and pressing "clean" you may force deletion of the application.
Note that this tool also removes the application from the PCD!
Use this with care !

Standard

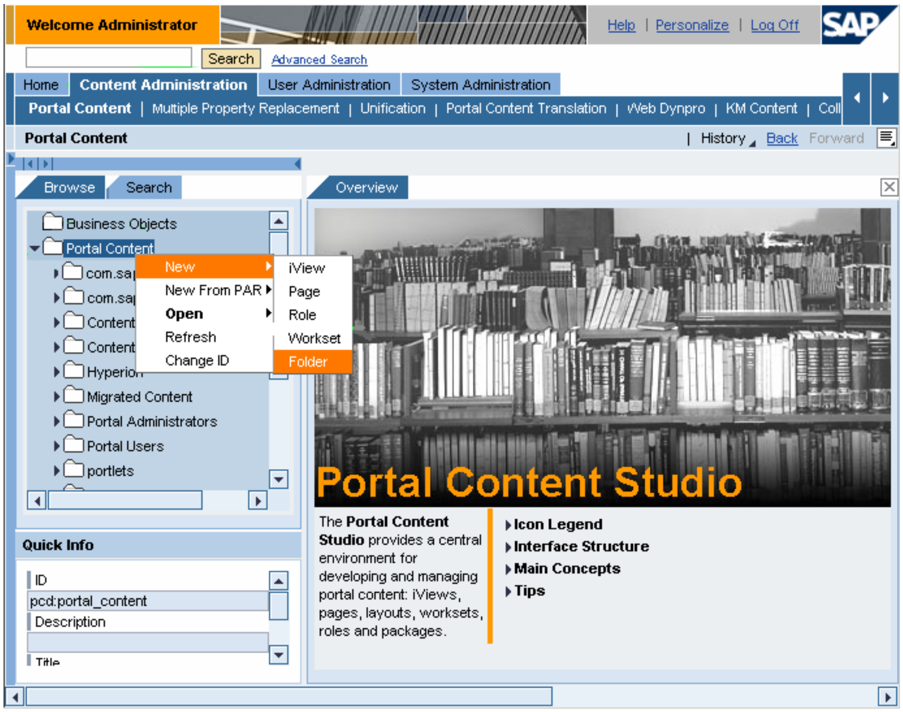
Adding Portal Content

After uploading the EPM System portlet for a portal, you create a folder, a page, and an iView for the portal.

➤ To add portal content:

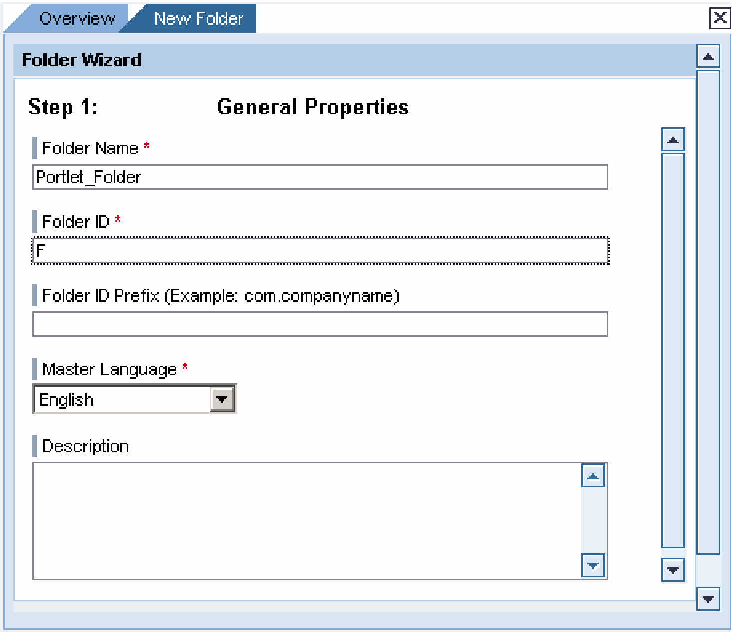
1 Navigate to **Content Administration – Portal Content.**

2 Create a new folder in the **Portal Content** folder.



ID
pcd:portal_content
Description
Title

The **Portal Content Studio** provides a central environment for developing and managing portal content: iViews, pages, layouts, worksets, roles and packages.



Folder Wizard

Step 1: General Properties

Folder Name *
Portlet_Folder

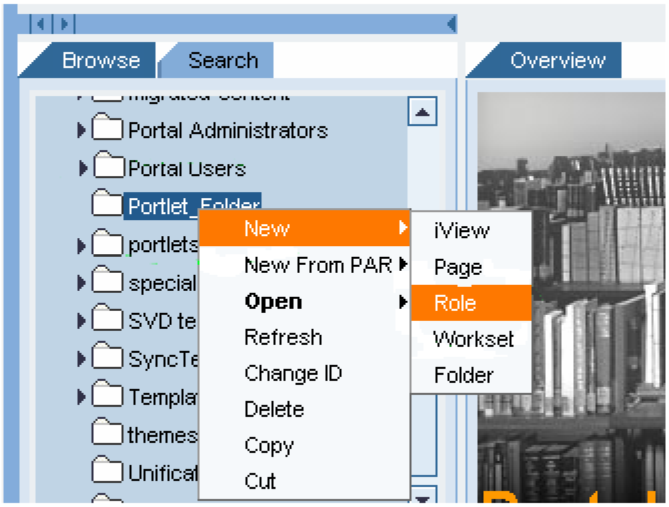
Folder ID *
F

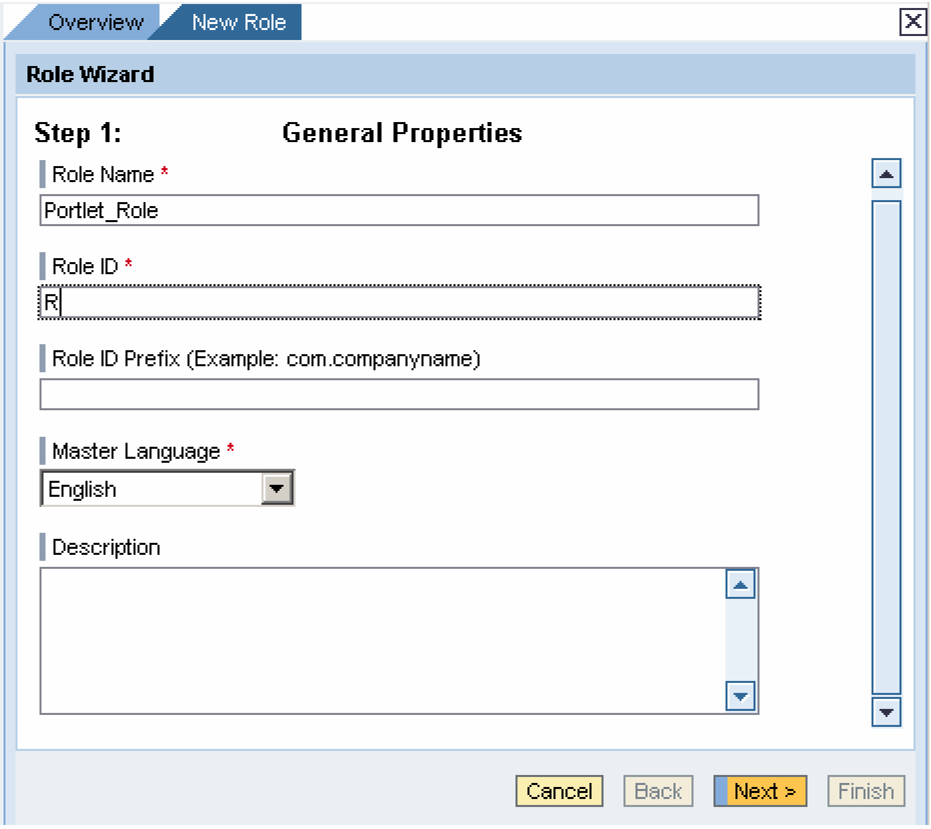
Folder ID Prefix (Example: com.companyname)

Master Language *
English

Description

3 Create a role in the new folder.





Role Wizard

Step 1: General Properties

Role Name *
Portlet_Role

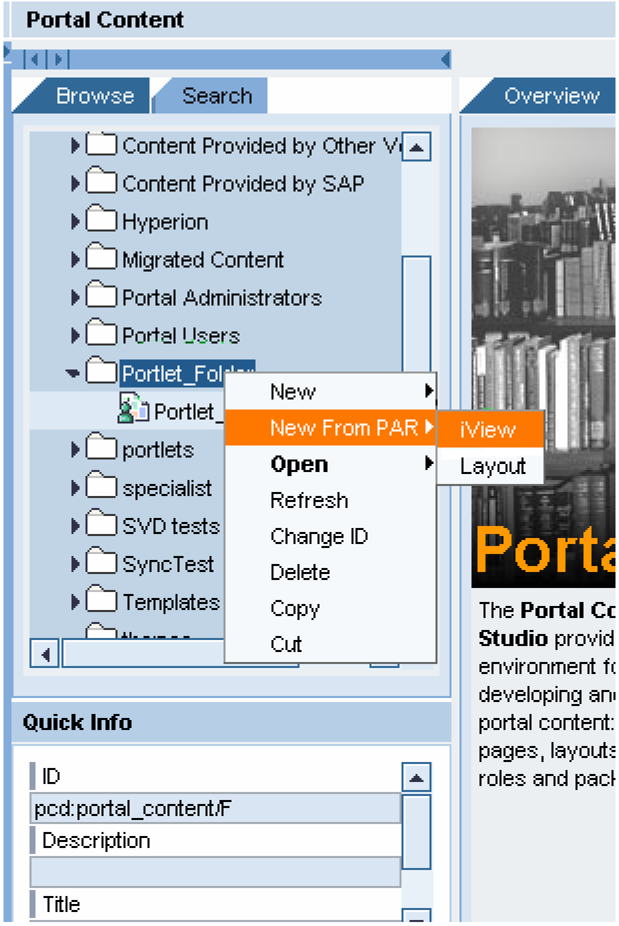
Role ID *
R

Role ID Prefix (Example: com.companyname)

Master Language *
English

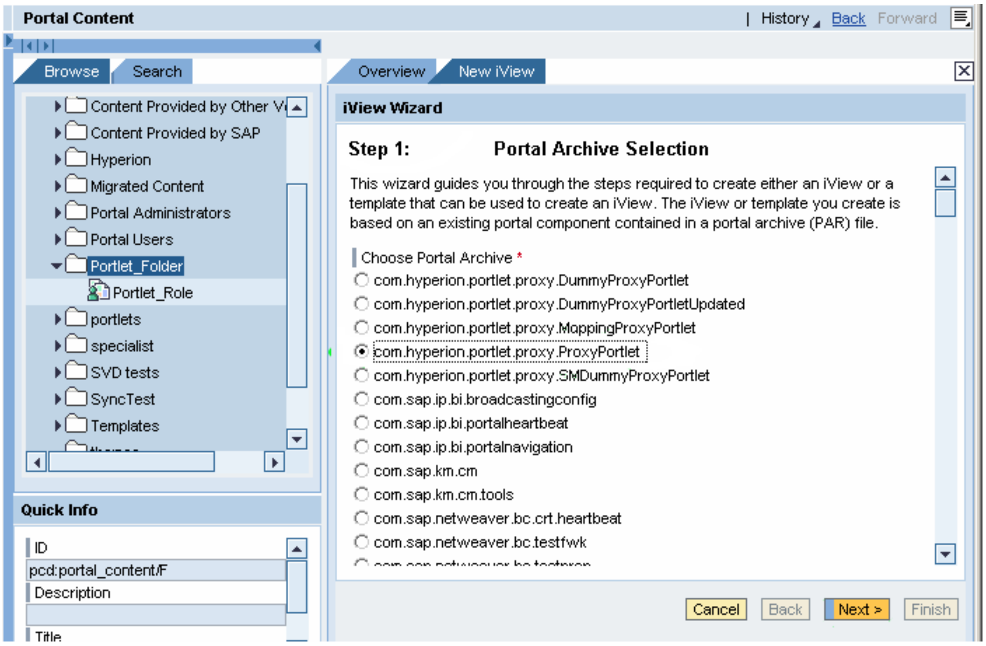
Description

4 In the same folder, create an iView from PAR.



5 In the **iViewWizard**:

a. Select **com.hyperion.portlet.proxy.ProxyPortlet**.



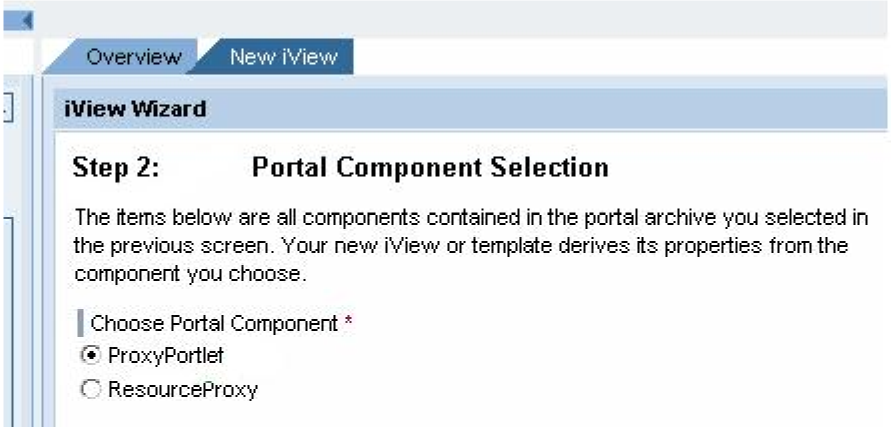
Step 1: Portal Archive Selection

This wizard guides you through the steps required to create either an iView or a template that can be used to create an iView. The iView or template you create is based on an existing portal component contained in a portal archive (PAR) file.

Choose Portal Archive *

○ com.hyperion.portlet.proxy.DummyProxyPortlet
○ com.hyperion.portlet.proxy.DummyProxyPortletUpdated
○ com.hyperion.portlet.proxy.MappingProxyPortlet
● com.hyperion.portlet.proxy.ProxyPortlet
○ com.hyperion.portlet.proxy.SMDummyProxyPortlet
○ com.sap.ip.bi.broadcastingconfig
○ com.sap.ip.bi.portalheartbeat
○ com.sap.ip.bi.portalnavigation
○ com.sap.km.cm
○ com.sap.km.cm.tools
○ com.sap.netweaver.bc.crt.heartbeat
○ com.sap.netweaver.bc.testfwk

b. Select **ProxyPortlet**.



iView Wizard

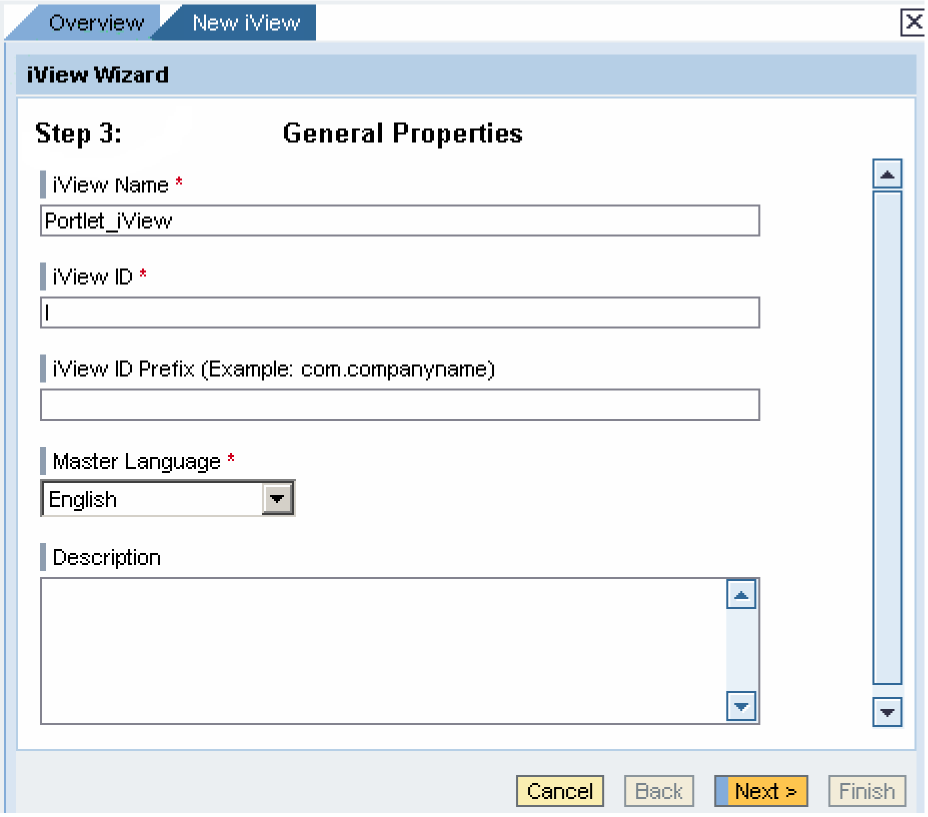
Step 2: Portal Component Selection

The items below are all components contained in the portal archive you selected in the previous screen. Your new iView or template derives its properties from the component you choose.

Choose Portal Component *

● ProxyPortlet

○ ResourceProxy



iView Wizard

Step 3: General Properties

iView Name *: Portlet_iView

iView ID *: I

iView ID Prefix (Example: com.companyname):

Master Language *: English

Description:

Changing the Producer Preference Setting for SAP NetWeaver

The EPM System portlet contains the `wsrp_producer_url` setting, which points to the Reporting and Analysis Framework instance, or producer, that contains all the other portlets. The default producer is set when EPM System Configurator installs the EPM System portlet. To use a different producer, you must change the preference setting.

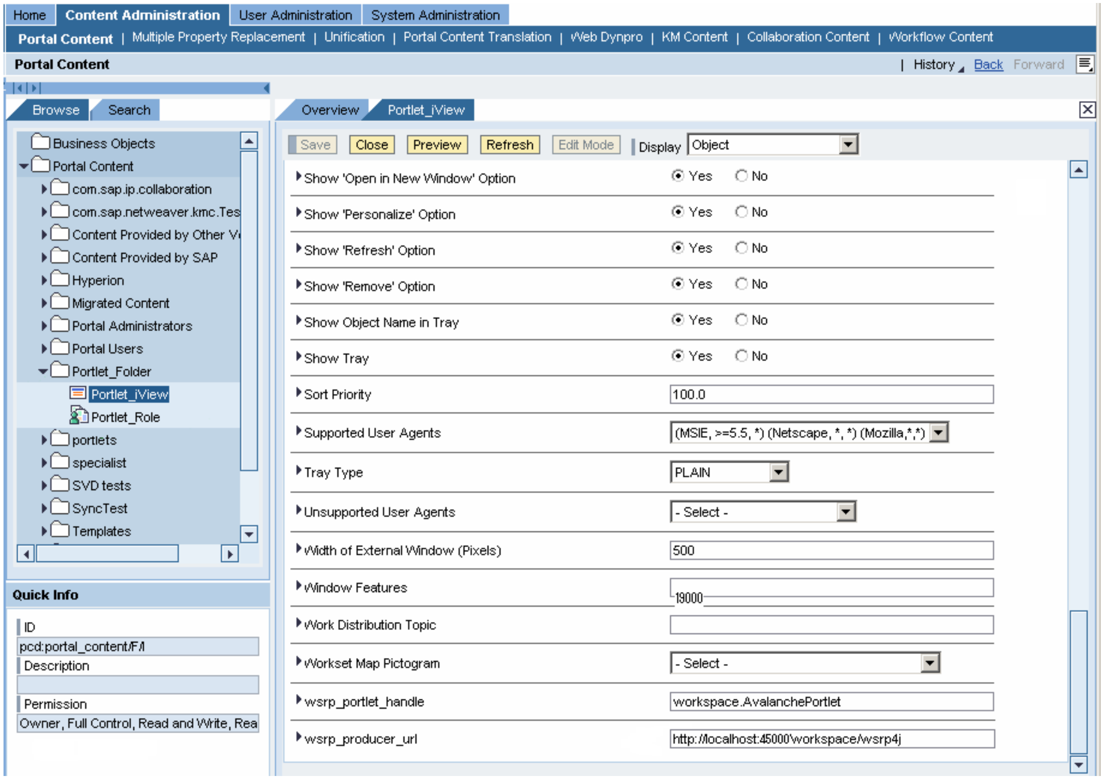
➤ To change the producer preference setting:

1 **Open the iView that you created in “Adding Portal Content” on page 26.**

2 Select **Show All** from the **Property Category** list.

3 Select **`wsrp_producer_url`**, which is at the bottom of the list

4 Enter a new value; for example, `http://`*`ComputerName`*`:`*`Port`*`/raframework/wsrp4j`.



ID
pcd:portal_content/F/l

Description

Permission
Owner, Full Control, Read and Write, Rea

Display: Object

Show 'Open in New Window' Option	● Yes ○ No
Show 'Personalize' Option	● Yes ○ No
Show 'Refresh' Option	● Yes ○ No
Show 'Remove' Option	● Yes ○ No
Show Object Name in Tray	● Yes ○ No
Show Tray	● Yes ○ No
Sort Priority	100.0
Supported User Agents	(MSIE, >=5.5, *) (Netscape, *, *) (Mozilla,*,*)
Tray Type	PLAIN
Unsupported User Agents	- Select -
Width of External Window (Pixels)	500
Window Features	
Work Distribution Topic	
Workset Map Pictogram	- Select -
wsrp_portlet_handle	workspace.AvalanchePortlet
wsrp_producer_url	http://localhost:45000\workspace/wsrp4j

Configuring the EPM System Portlet SSL for SAP NetWeaver

Configuring SSL for the EPM System portlet for SAP NetWeaver involves these tasks:

- Changing the producer preference setting to point to the SSL address of the EPM System server (which usually has the prefix `https://`)
- Importing the public EPM System server certificate into the SAP Portal key store

➤ To import the public EPM System server certificate into the SAP Portal key store:

1 **Specify these startup Java parameters in Config Tool for your SAP Portal server instance:**

`-Djavax.net.ssl.trustStore=`*`PATH_TO_KEYSTORE`*

`-Djavax.net.ssl.trustStorePassword=`*`KEYSTORE_PASSWORD`*

where *`PATH_TO_KEYSTORE`* is the path to the Java key store file with the public EPM System server certificate and *`KEYSTORE_PASSWORD`* is a password for the key store.

2 **Save the new parameters.**

3 **Restart the portal instance.**

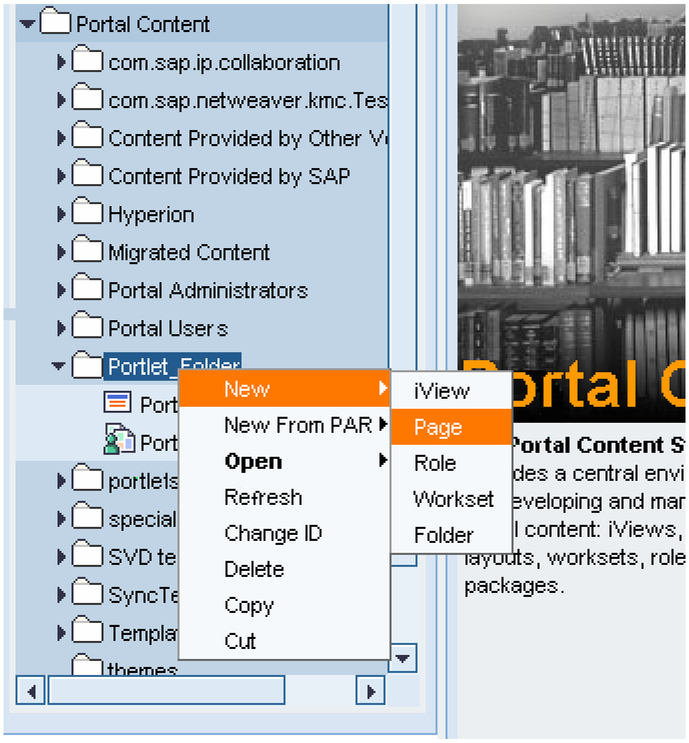
See `http://help.sap.com/saphelp_nw04/helpdata/en/4e/d1cf8d09a94ae79319893c2537d3a0/frameset.htm` for details about using Config Tool.

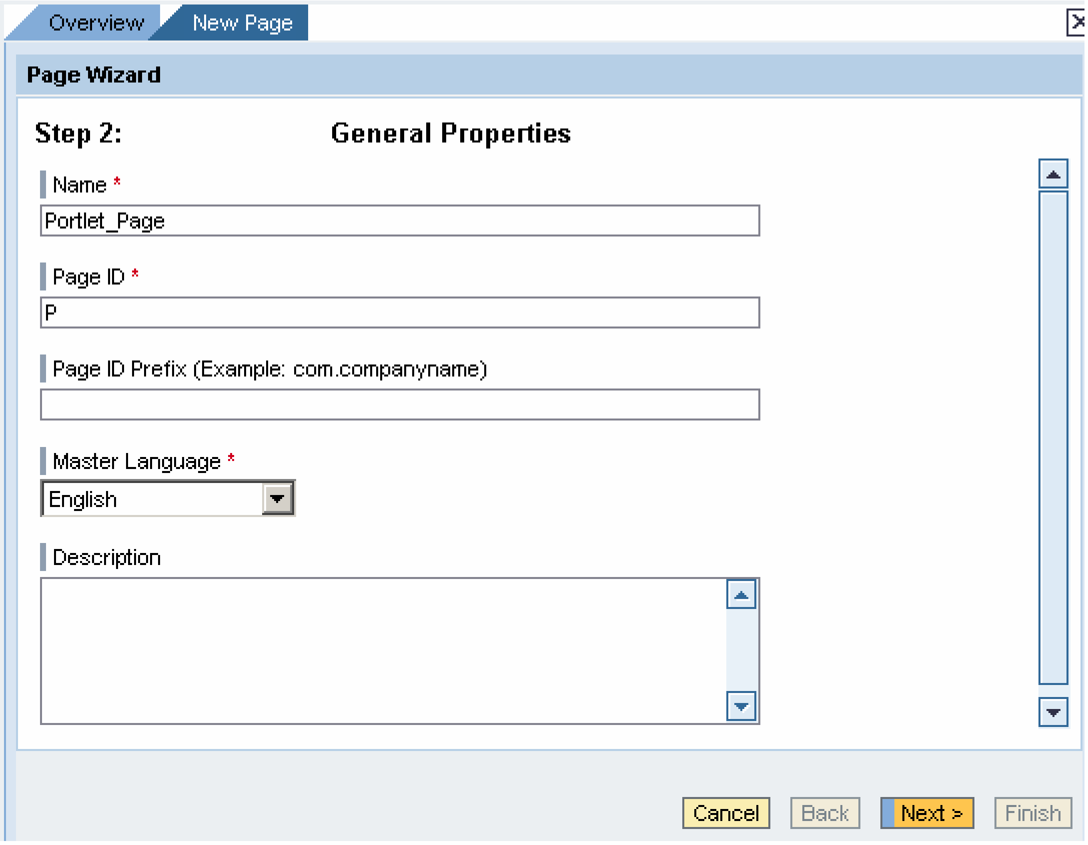
Setting Up Pages for SAP Portals

You must set up a page before portlet users can log on to SAP portal and begin using portlets on the page.

➤ To set up a page:

1 Create the page in the folder that you created in "Adding Portal Content" on page 26.





Page Wizard

Step 2: General Properties

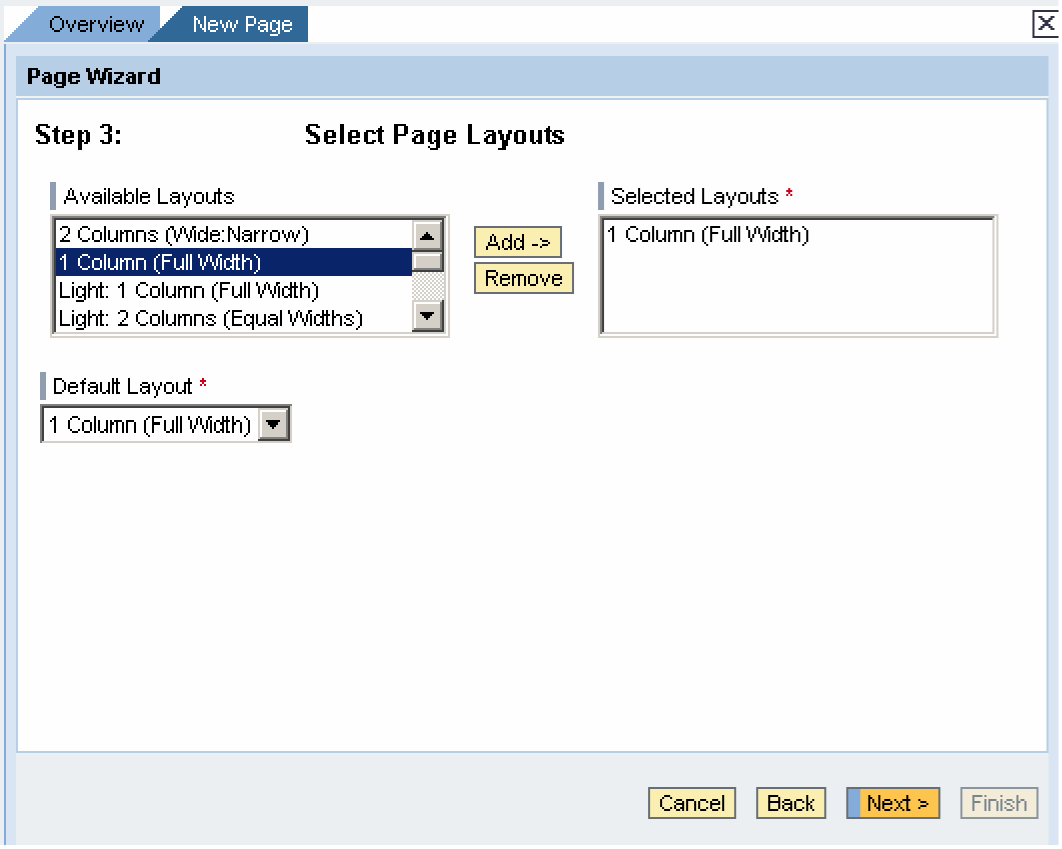
Name *
Portlet_Page

Page ID *
P

Page ID Prefix (Example: com.companyname)

Master Language *
English

Description



Page Wizard

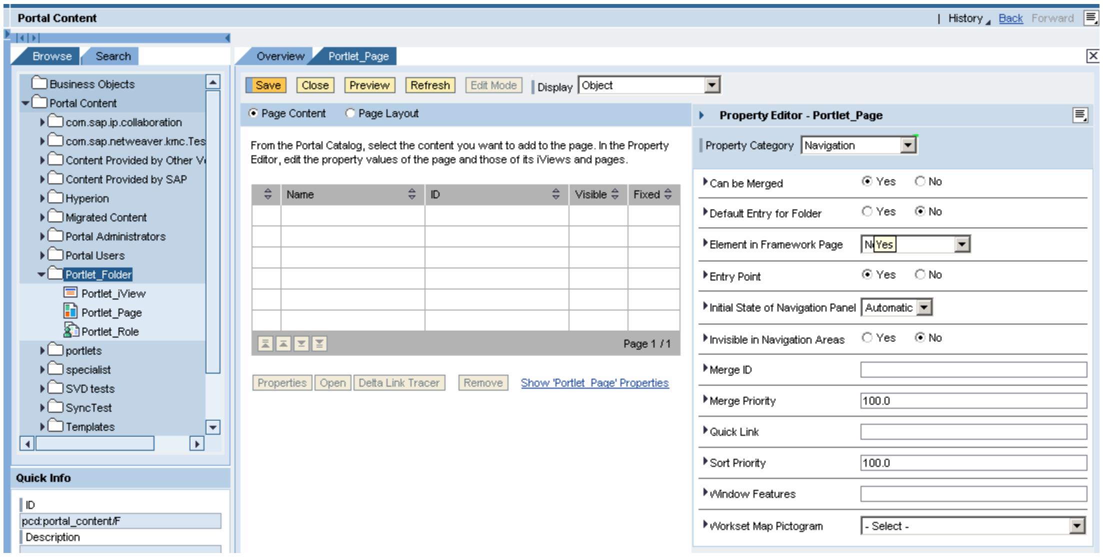
Step 3: Select Page Layouts

Available Layouts
2 Columns (Wide:Narrow)
1 Column (Full Width)
Light: 1 Column (Full Width)
Light: 2 Columns (Equal Widths)

Selected Layouts *
1 Column (Full Width)

Default Layout *
1 Column (Full Width)

2 Select **Yes** for the **Entry Point** property, which is under **Navigation** in the **Property Category** list.



Display: Object

● Page Content ○ Page Layout

From the Portal Catalog, select the content you want to add to the page. In the Property Editor, edit the property values of the page and those of its iViews and pages.

Name	ID	Visible	Fixed

Page 1 / 1

ID: pcd:portal_content/F

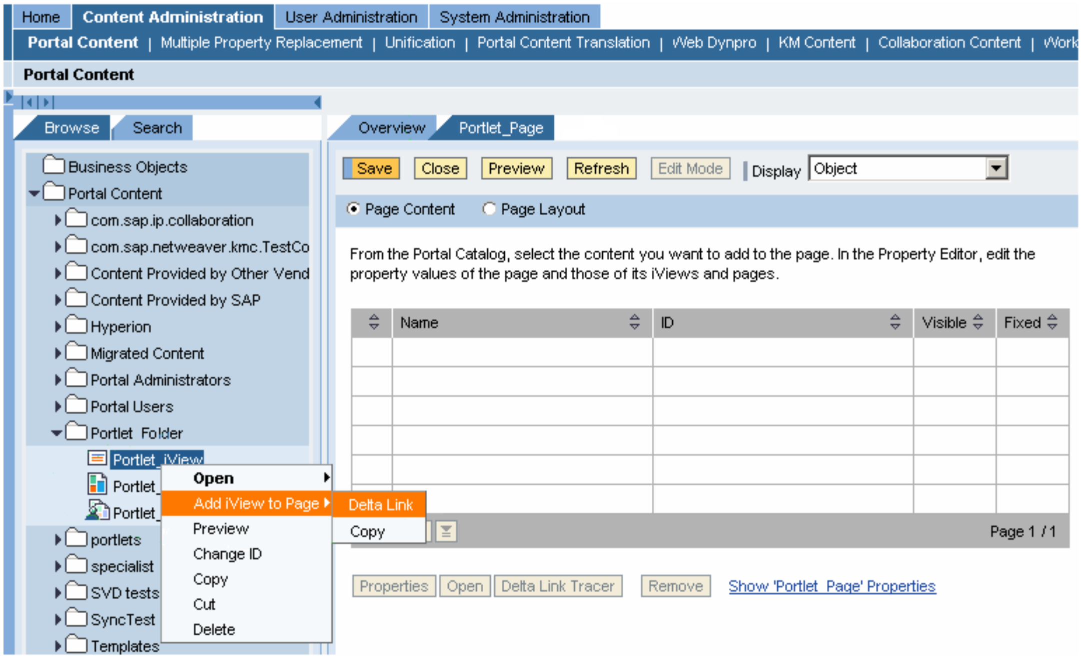
Description

Property Editor - Portlet_Page

Property Category: Navigation

Can be Merged	● Yes ○ No
Default Entry for Folder	○ Yes ● No
Element in Framework Page	N Yes
Entry Point	● Yes ○ No
Initial State of Navigation Panel	Automatic
Invisible in Navigation Areas	○ Yes ● No
Merge ID	
Merge Priority	100.0
Quick Link	
Sort Priority	100.0
Window Features	
Workset Map Pictogram	- Select -

3 Open the new page for editing and select **Add iView to Page as Delta Link.**



Display: Object

● Page Content ○ Page Layout

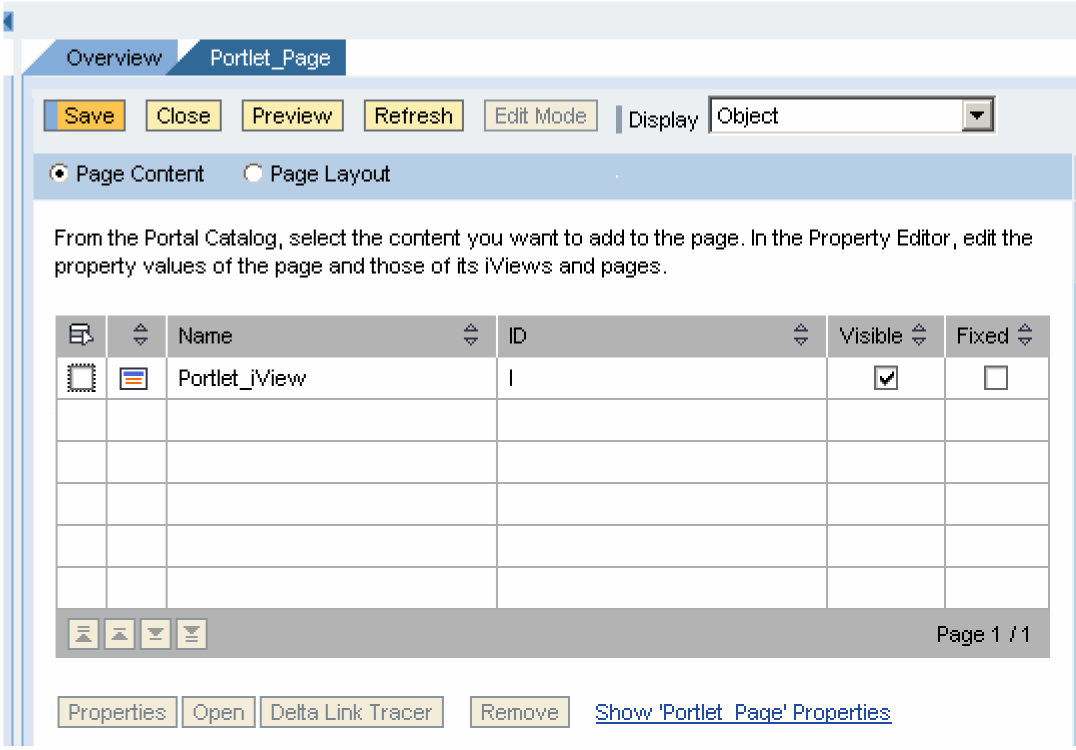
From the Portal Catalog, select the content you want to add to the page. In the Property Editor, edit the property values of the page and those of its iViews and pages.

Name	ID	Visible	Fixed

Page 1 / 1

Tip: You can add several iViews to a page so that a multicolumn layout can be used for displaying several portlets and reports on the page.

4 Click **Save.**



Display: Object

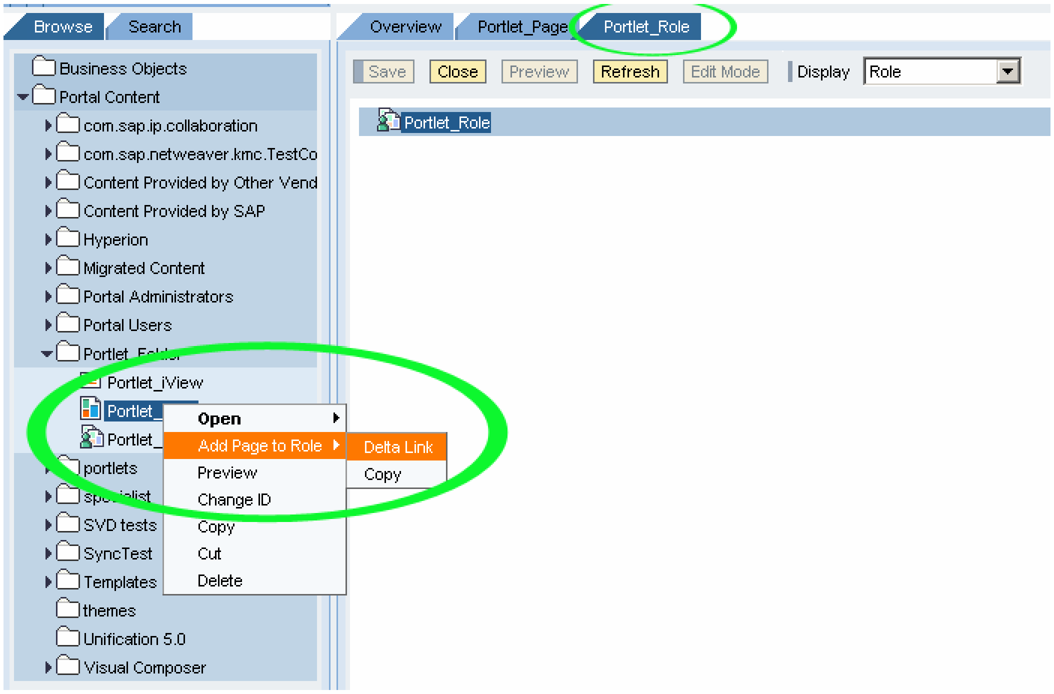
● Page Content ○ Page Layout

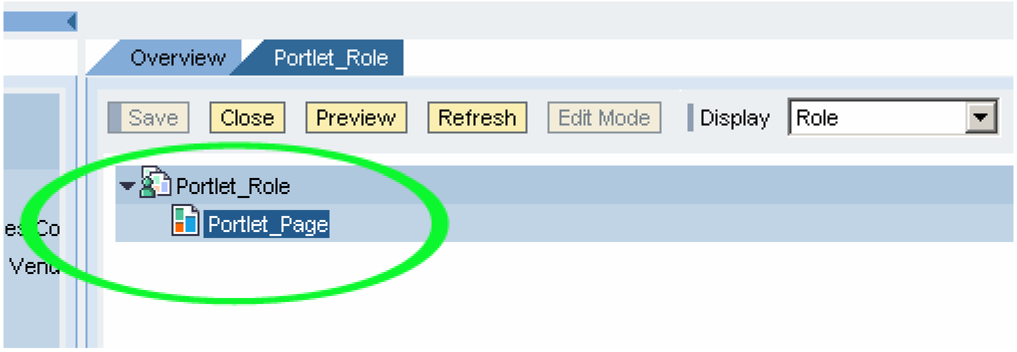
From the Portal Catalog, select the content you want to add to the page. In the Property Editor, edit the property values of the page and those of its iViews and pages.

		Name	ID	Visible	Fixed
□		Portlet_iView	I	☑	□

Page 1 / 1

5 Open for editing the role that you created in "Adding Portal Content" on page 26, and select **Add Page to Role**, then**Delta Link.**

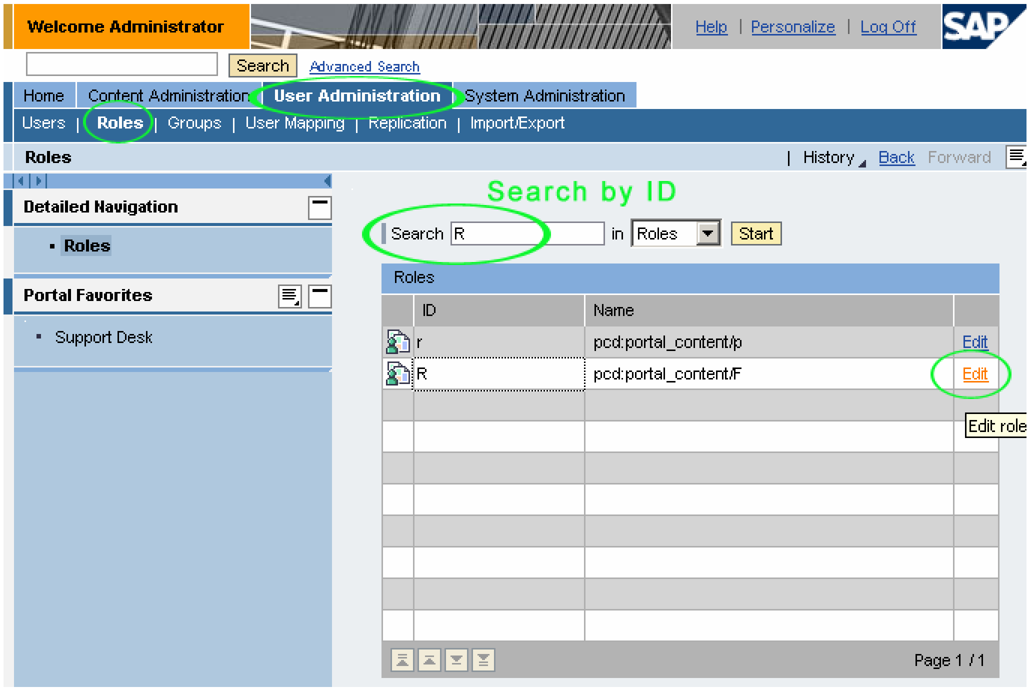




6 **Save your changes.**

7 **Add portlet users to Role.**

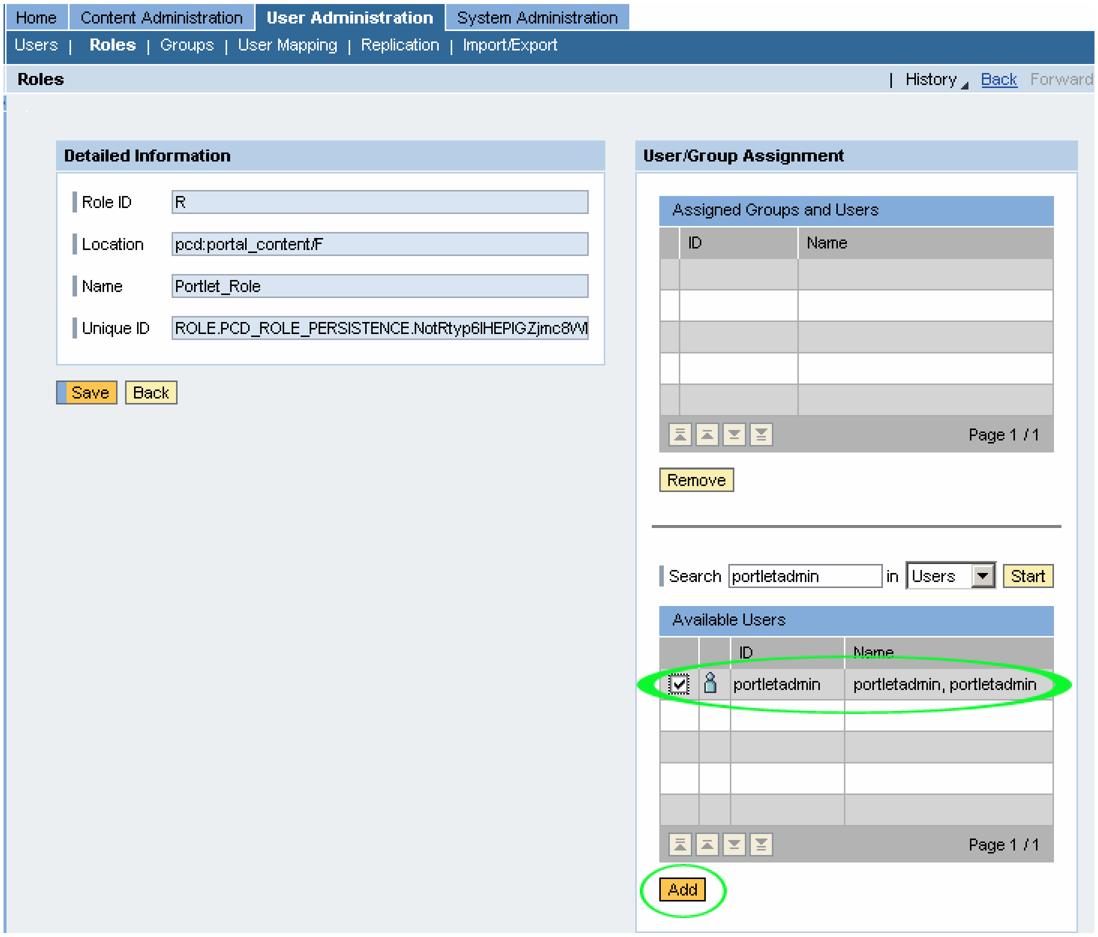
Note: The EPM System portlet uses SSO for ABAP users. Only ABAP users can display content for the EPM System portlet.



Search R in Roles

Roles

ID	Name	
r	pcd:portal_content/p	Edit
R	pcd:portal_content/F	Edit



Detailed Information

Role ID	R
Location	pcd:portal_content/F
Name	Portlet_Role
Unique ID	ROLE.PCD_ROLE_PERSISTENCE.NotRtyp6IHEPIGZjmc8VVl

User/Group Assignment

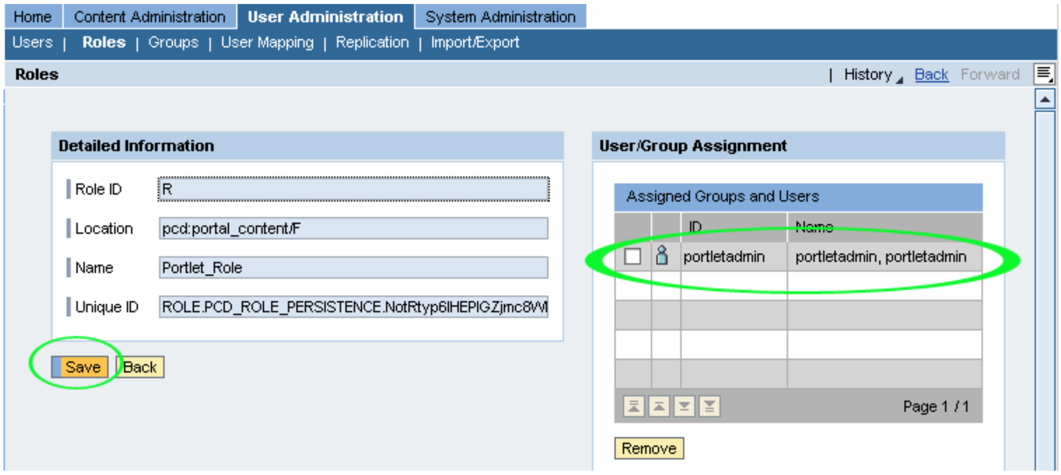
Assigned Groups and Users

ID	Name

Search portletadmin in Users

Available Users

		ID	Name
☑		portletadmin	portletadmin, portletadmin



Detailed Information

Role ID	R
Location	pcd:portal_content/F
Name	Portlet_Role
Unique ID	ROLE.PCD_ROLE_PERSISTENCE.NotRtyp6IHEPIGZjmc8VVl

User/Group Assignment

Assigned Groups and Users

		ID	Name
□		portletadmin	portletadmin, portletadmin

4

SharePoint Portal 2003 Setup

In This Chapter

Hyperion WebPart and SharePoint Portal 2003 39
Installing the EPM System WebPart Application for SharePoint Portal 2003 41
Updating the Hyperion WebPart Application (SharePoint Portal 2003) 62
Uninstalling the Hyperion WebPart Application (SharePoint Portal 2003) 63
SSL Support (SharePoint Portal 2003) 66
Support Activities (SharePoint Portal 2003) 67
Tips and Troubleshooting: SharePoint Portal 2003 68

Hyperion WebPart and SharePoint Portal 2003

Hyperion WebPart is a Web-based solution for working with EPM System content in a Microsoft SharePoint portal. This chapter provides information about application installation, administration, and troubleshooting for SharePoint Portal 2003.

SharePoint Portal 2003 Installation Prerequisites

Before you can install Hyperion WebPart, the following software must be installed on your computer:

- Microsoft Windows Server 2003 or later
- Microsoft Internet Information Services (IIS) 5.0 or later
- Microsoft .NET Framework 1.1
- Microsoft .NET Framework 2.0
- Microsoft SQL Server 2000 Standard Edition SP3 or later
- Microsoft Windows SharePoint Services 2.0
- Microsoft SharePoint Portal 2003

You must complete these tasks before Hyperion WebPart is installed:

- Create a proxy page. Oracle recommends that Hyperion WebPart be installed by the SharePoint Portal 2003 Server administrator. For more information about installation, see the SharePoint Portal Server documentation.
- Create a new Web site outside the default Web site

- Enable ASP.Net to run on the SharePoint virtual server

SharePoint Portal 2003 Installation Package Contents

The Hyperion WebPart installation package is delivered as single archive file, `HyperionWebPart.zip`. The file contains these folders and files:

- `HyperionWebPart` folder
  - `HyperionWebPartDeployment.CAB`—Hyperion WebPart
  - `HyperionWebPartCredentialsManagerDeployment.CAB`—-Microsoft SharePoint deployment file for Hyperion WebPart Credentials Manager
  - `HyperionWebPartWebPart_DB_Create.sql`—Script for creating database
  - `HyperionWebPartWebPart_DB_Update.sql`—Script for updating database
  - `HyperionWebPartPWebPart_DB_Delete.sql`—Script for removing database
  - `AddWebPart.bat`—Utility that automates WebPart deployment
  - `RemoveWebPart.bat`—Utility that automates WebPart removal
  - `UpdateWebPart.bat`—Utility that automates WebPart updates
- `HyperionWebPartProxyPage` folder
  - `Web.config`—`Hyperion WebPart ProxyPage` Web application configuration file
  - `ProxyManager.asmx`—Web service for internal data processing
  - `Global.asax`—`Hyperion WebPart ProxyPage` Web application file pointing to application logic implementation
  - `ErrorList.xml`—Error definitions for logging
  - `WarningsList.xml`—Warning definitions for logging
  - `HyperionWebPartProxyPage_deploy.dll`—`HyperionWebPartProxyPage` Web application assembly file containing the logic and code for Hyperion WebPart, to be installed on a site server
- `HyperionWebPartLogInstaller`: `WebPartLogInstaller.dll`—Assembly file containing the logic and code of Hyperion WebPart log, to be installed on a site server
- `HyperionWebPartResourceHttpHandler` folder
  - Global.asax— Hyperion WebPart ResourceHttpHandler Web application file pointing to application logic implementation
  - Web.config—Hyperion WebPart ResourceHttpHandler configuration file
  - HyperionWebPartResourceHttpHandler_deploy.dll WebPart ResourceHttpHandler assembly file containing the logic and code of Hyperion WebPart, to be installed on a site server
- HyperionWebPartEncryptor folder
  - Global.asax—HyperionWebPartEncryptor Web application file pointing to application logic implementation

- Web.config— HyperionWebPartEncryptor configuration file
- HyperionWebPartEncryptor.aspx — HyperionWebPartEncryptor Web form used to encrypt data
- HyperionWebPartEncryptor.dll— HyperionWebPartEncryptor assembly file containing the logic and code of Hyperion WebPart, to be installed on a site server

Installing the EPM System WebPart Application for SharePoint Portal 2003

To install the Hyperion WebPart application, you must extract the `HyperionWebPart.zip` file to a location on your SharePoint Portal server instance and ensure that SQL Server and Windows Authentication mode are enabled on the SQL server hosting the HyperionWebPart_Cache database.

You must also complete these tasks, which this section describes:

- Configuring single sign-on (SSO)
- Installing Hyperion WebPart ProxyPage
- Installing Hyperion WebPart ResourceHttpHandler
- Creating key container for Hyperion WebPart Encryptor
- Installing Hyperion WebPart Encryptor
- Updating `Web.config`
- Customizing the database creation script
- Installing Hyperion WebPart for the SharePoint portal
- Customizing Hyperion Web Part `app.config` (optional)
- Configuring default permissions for Hyperion WebPart

Configuring Single Sign-On (SharePoint Portal 2003)

You can configure Hyperion WebPart for Microsoft SSO or SiteMinder SSO.

Configuring Hyperion WebPart for Microsoft SSO (SharePoint Portal 2003)

Before configuring Hyperion WebPart for Microsoft SSO, you must configure the Microsoft Single Sign-On service. See the Microsoft Online Reference for instructions.

Note: See "Tips and Troubleshooting: SharePoint Portal 2003" on page 68 if you encounter error messages during SSO configuration.

The Hyperion WebPart stores two types of credentials:

- Persistent credentials are stored in the SSO database and used every time user accesses the portal page, so there is no need to reenter them.

  Note: You can use Hyperion WebPart Credentials Manager or SharePoint Portal Server Single Sign-On Administration to change user credentials.

- Nonpersistent credentials are used when user clears the “Remember me” check box in Hyperion WebPart Credentials Manager. The credentials expire at the end of the current session.

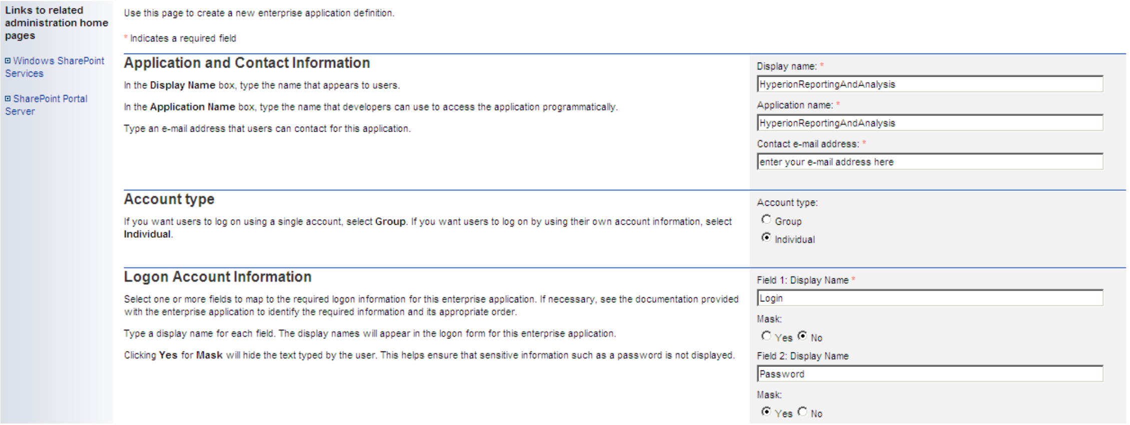
You can customize these parameters in Hyperion WebPart:

- Application name used for storing persistent credentials (Default: HyperionReportingAndAnalysis)
- Application name used for storing nonpersistent credentials (Default: HyperionReportingAndAnalysisTemp)

Note: If you customize parameters, you must modify the `Web.config` file in the `HyperionWebPartProxyPage` folder accordingly.

➤ To customize parameters in Hyperion WebPart:

1. Define an application name to store persistent credentials. (Default: HyperionReportingAndAnalysis
2. In the **Component Configuration** section of **SharePoint Portal Server Central Administration**, click **Manage settings for single sign-on.**
3. In the **Enterprise Application Definition Settings** section, click **Manage settings for enterprise application definitions**, and then click **New Item.**
4. Using the following figure as a guide, add the new enterprise application definition for persistent credentials. See the “Enterprise Application Manager Account” section of Microsoft Online Reference.


Links to related administration home pages
Windows SharePoint Services
SharePoint Portal Server

Use this page to create a new enterprise application definition.

* Indicates a required field

Application and Contact Information

In the **Display Name** box, type the name that appears to users.

In the **Application Name** box, type the name that developers can use to access the application programmatically.

Type an e-mail address that users can contact for this application.

Display name: *
HyperionReportingAndAnalysis

Application name: *
HyperionReportingAndAnalysis

Contact e-mail address: *
enter your e-mail address here

Account type

If you want users to log on using a single account, select **Group**. If you want users to log on by using their own account information, select **Individual**.

Account type:
○ Group
● Individual

Logon Account Information

Select one or more fields to map to the required logon information for this enterprise application. If necessary, see the documentation provided with the enterprise application to identify the required information and its appropriate order.

Type a display name for each field. The display names will appear in the logon form for this enterprise application.

Clicking **Yes** for **Mask** will hide the text typed by the user. This helps ensure that sensitive information such as a password is not displayed.

Field 1: Display Name *
Login

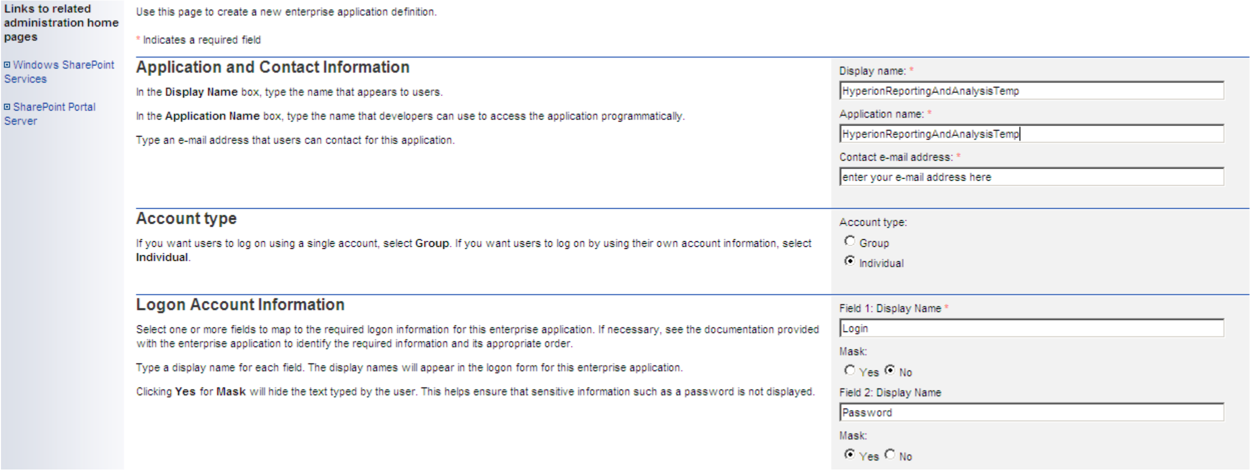
Mask:
○ Yes ● No

Field 2: Display Name
Password

Mask:
● Yes ○ No

5. Define an application name to store nonpersistent credentials. (Default: HyperionReportingAndAnalysisTemp)
6. Repeat step 2 and step 3.

7 **Using the following figure as a guide, add the new enterprise application definitions for nonpersistent credentials. See the “Enterprise Application Manager Account” section of Microsoft Online Reference.**


Links to related administration home pages
⊞ Windows SharePoint Services
⊞ SharePoint Portal Server

Use this page to create a new enterprise application definition.

* Indicates a required field

Application and Contact Information

In the **Display Name** box, type the name that appears to users.

In the **Application Name** box, type the name that developers can use to access the application programmatically.

Type an e-mail address that users can contact for this application.

Display name: *
HyperionReportingAndAnalysisTemp

Application name: *
HyperionReportingAndAnalysisTemp

Contact e-mail address: *
enter your e-mail address here

Account type

If you want users to log on using a single account, select **Group**. If you want users to log on by using their own account information, select **Individual**.

Account type:
○ Group
● Individual

Logon Account Information

Select one or more fields to map to the required logon information for this enterprise application. If necessary, see the documentation provided with the enterprise application to identify the required information and its appropriate order.

Type a display name for each field. The display names will appear in the logon form for this enterprise application.

Clicking **Yes** for **Mask** will hide the text typed by the user. This helps ensure that sensitive information such as a password is not displayed.

Field 1: Display Name *
Login

Mask:
○ Yes ● No

Field 2: Display Name
Password

Mask:
● Yes ○ No

Configuring Hyperion WebPart for SiteMinder SSO (SharePoint Portal 2003)

Hyperion WebPart can use SiteMinder for external authentication. It must pass specific HTTP headers received from the Web server to the Hyperion application server. To prevent sensitive data interception, use either or both of these approaches:

- Producer and consumer should be within the same secure LAN, which is inaccessible to external insecure clients.
- Both producer and consumer should use SSL/HTTPS.

For more information on configuring SiteMinder on IIS, see the SiteMinder installation documentation.

Installing the Hyperion WebPart ProxyPage Web Application (SharePoint Portal 2003)

This section describes how to deploy the Hyperion WebPart Proxy Page Web application to IIS. Hyperion WebPartProxyPage Web Application and Hyperion WebPart ResourceHttpHandler should be installed on the same server as your instance of Microsoft SharePoint portal.

➤ To install the HyperionWebPart ProxyPage Web application:

1 **Open the SharePoint Portal** `web.config` **file in a text editor.**

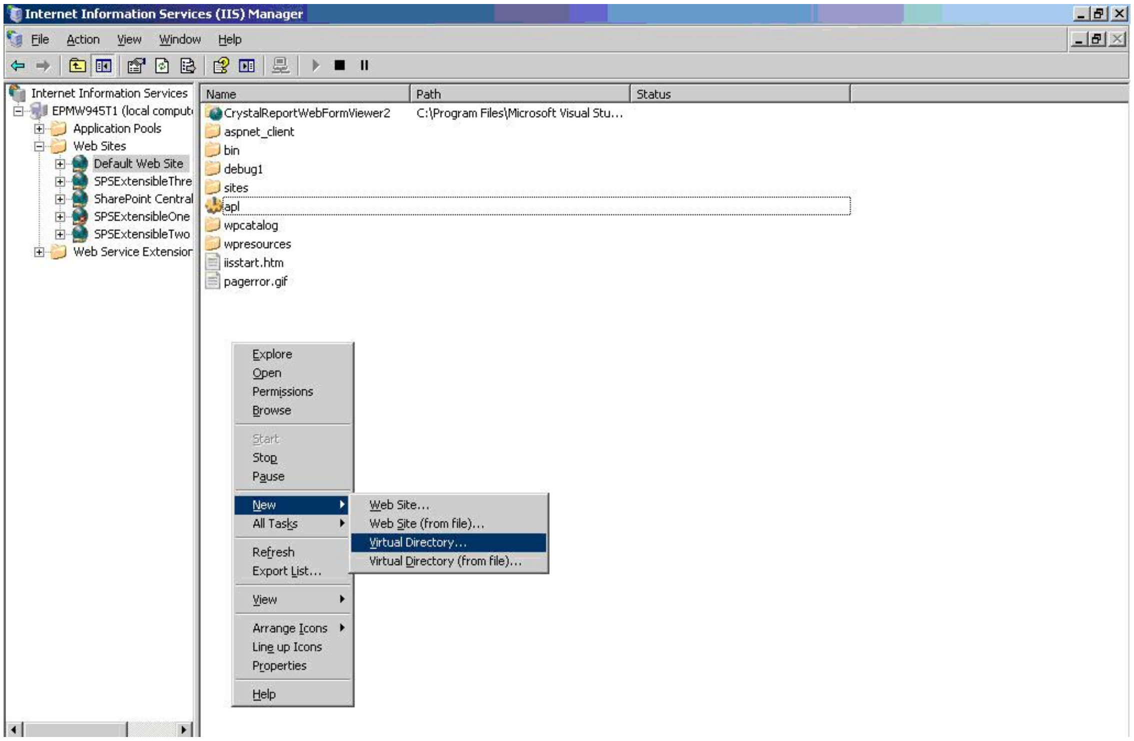
2 **In the** `<system.web>` **section, set** `<trust level="Full" originUrl="" />`**, and then save the modified file.**

3 **Define a folder to store the Hyperion WebPart application, and extract the contents of the** `HyperionWebPart2007.zip` **file into that folder.** `HyperionWebPartProxyPage` **and** `HyperionWebPartResourceHttpHandler` **subfolders store physical contents of respective web applications.**

4 Run to Internet Information Services Manager.

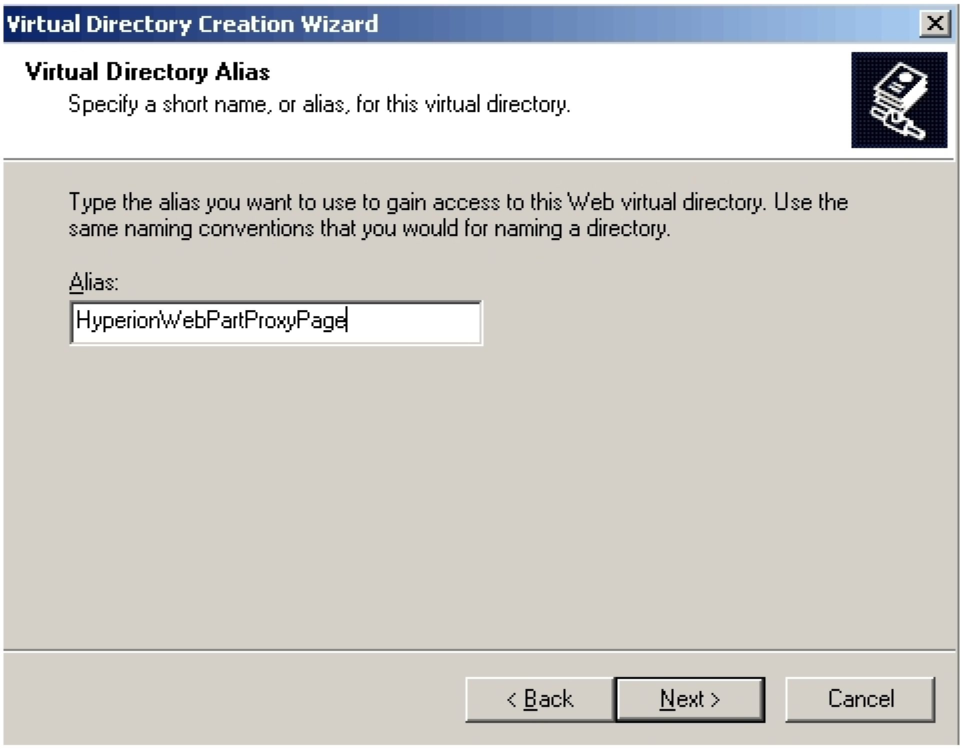
5 Choose **Default Web Site.**

6 Create a virtual folder to work with HyperionWebPartProxyPage physical folder that you created in step 2.



Name	Path	Status
CrystalReportWebFormViewer2	C:\Program Files\Microsoft Visual Stu...	
aspnet_client		
bin		
debug1		
sites		
apl		
wpcatalog		
wpresources		
iisstart.htm		
pagerror.gif		

7 Define a virtual folder alias using the following figure as a guide, and then click **Next.**



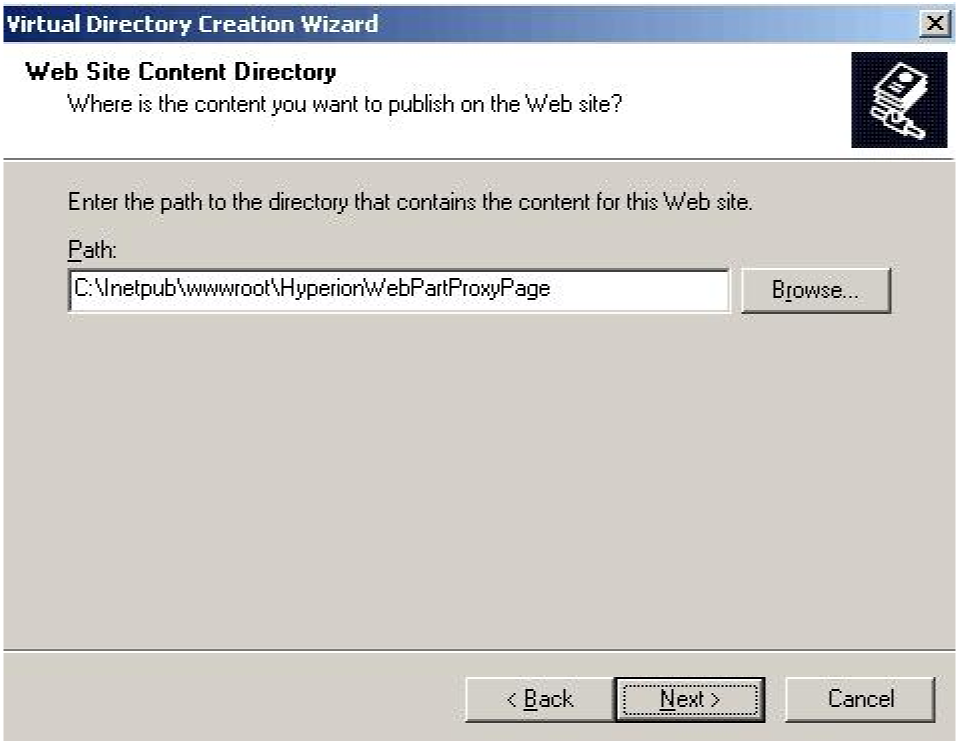
Virtual Directory Alias

Specify a short name, or alias, for this virtual directory.

Type the alias you want to use to gain access to this Web virtual directory. Use the same naming conventions that you would for naming a directory.

Alias: HyperionWebPartProxyPage

8 Specify the path for the application folder that matches the folder name you defined in step 2, and then click **Next.**



Web Site Content Directory

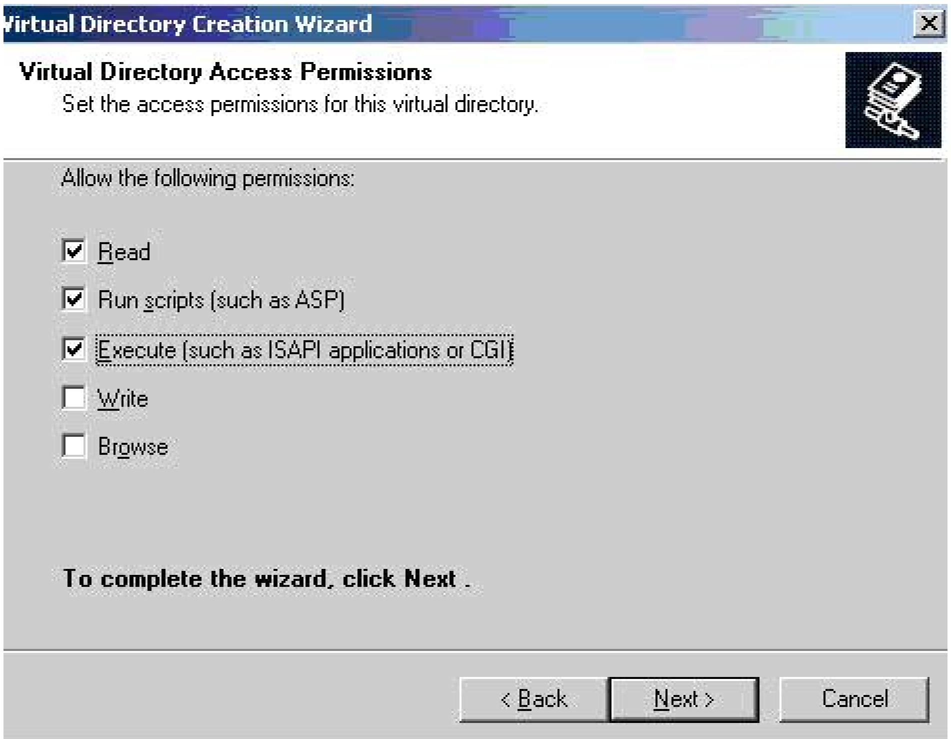
Where is the content you want to publish on the Web site?

Enter the path to the directory that contains the content for this Web site.

Path:

C:\Inetpub\wwwroot\HyperionWebPartProxyPage

9 Set access permissions, as shown in the following figure, and then click **Next.**



Virtual Directory Access Permissions

Set the access permissions for this virtual directory.

Allow the following permissions:

☑ Read

☑ Run scripts (such as ASP)

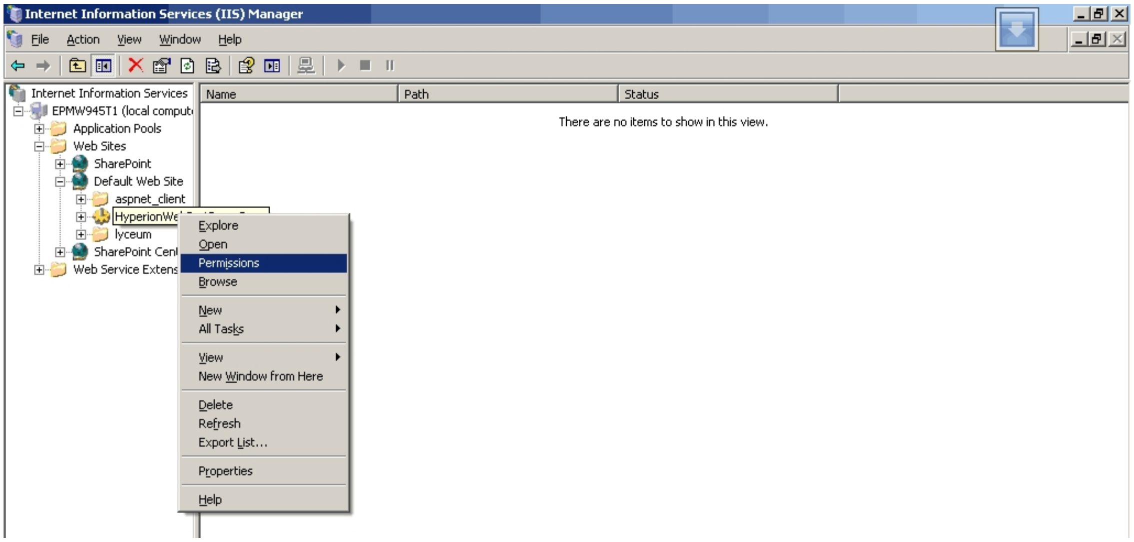
☑ Execute (such as ISAPI applications or CGI)

□ Write

□ Browse

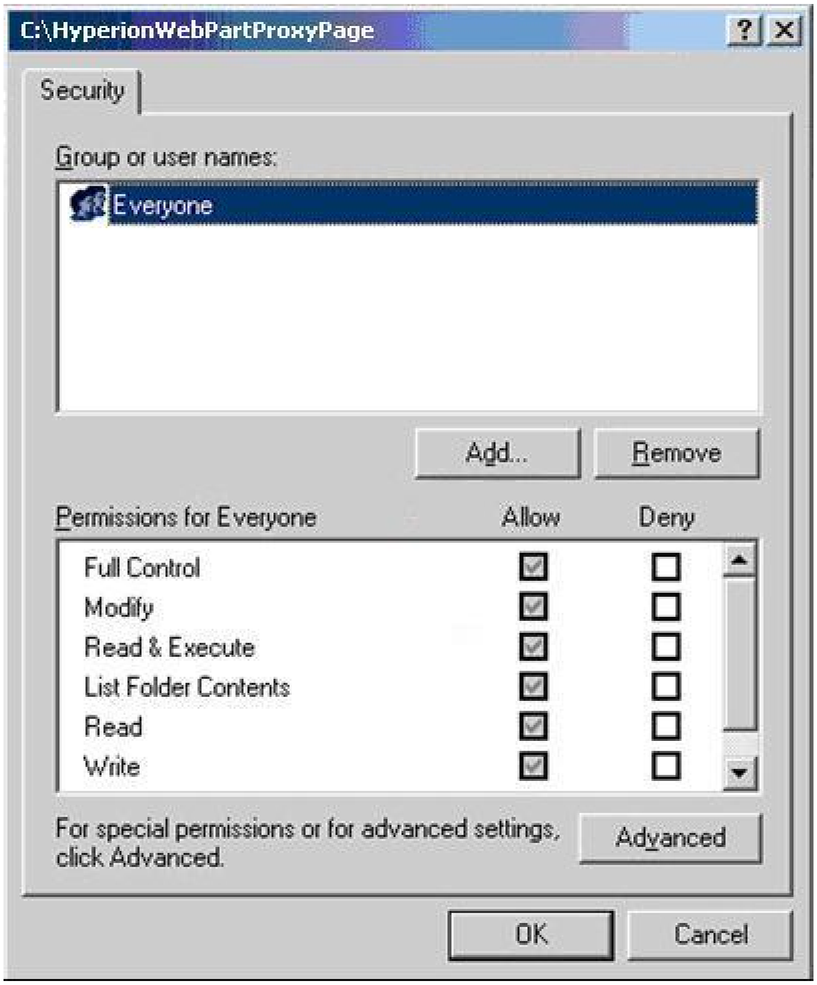
To complete the wizard, click Next .

10 Right-click **HyperionWebPartProxyPage**, and select **Permissions.**



There are no items to show in this view.

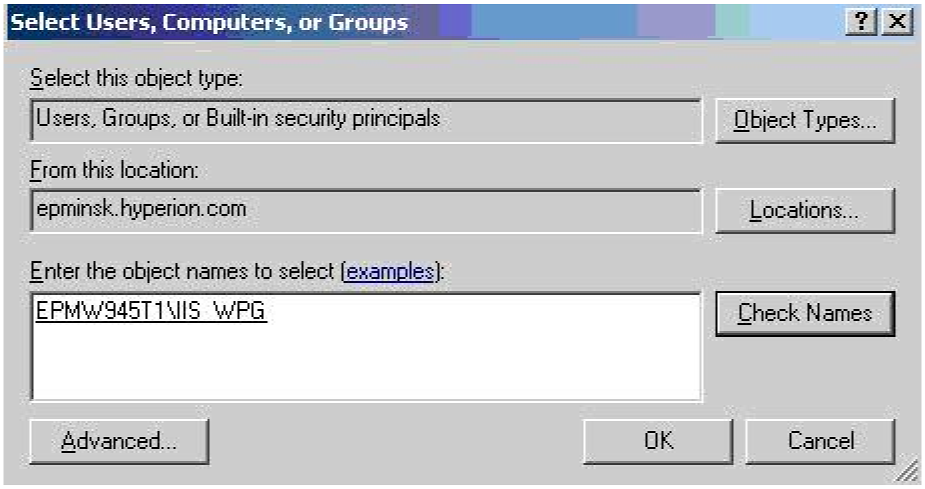
11 Click **Add.**



Permissions for Everyone	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□

For special permissions or for advanced settings, click Advanced.

12 Enter **SHAREPOINT_PORTAL_HOSTNAME\IIS_WPG**, click **OK**, and change **SHAREPOINT_PORTAL_HOSTNAME** to the name of the host where SharePoint is installed.



Select Users, Computers, or Groups

Select this object type:

Users, Groups, or Built-in security principals

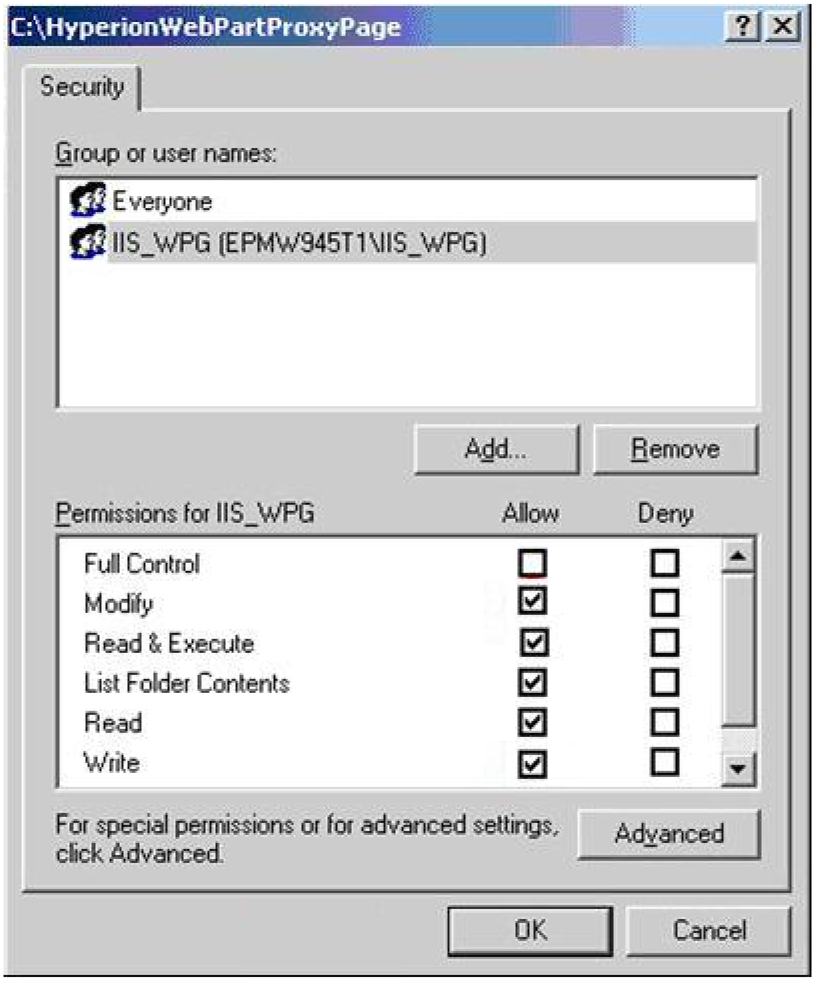
From this location:

epminsk.hyperion.com

Enter the object names to select (examples):

EPMW945T1\IIS_WPG

13 Set permissions for the user as shown in the following figure, and click **OK**.



C:\HyperionWebPartProxyPage

Security

Group or user names:

- Everyone
- IIS_WPG (EPMW945T1\IIS_WPG)

Permissions for IIS_WPG	Allow	Deny
Full Control	☐	☐
Modify	☑	☐
Read & Execute	☑	☐
List Folder Contents	☑	☐
Read	☑	☐
Write	☑	☐

For special permissions or for advanced settings, click Advanced.

14 Open a Command Prompt, and use it to change to the directory that contains the `Adsutil.vbs` file. By default, the file is in `C:\Inetpub\Adminscripts`.

15 Type the following command, and then press **Enter**: `cscript adsutil.vbs set w3svc/NTAuthenticationProviders "NTLM"`

16 Select **Run** from the **Start** menu, type **regedit**, and then click **OK**.

17. In Registry Editor, click this registry key: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0**

18. Right-click **MSV1_0**, select **New**, and then click **Multi-String Value.**

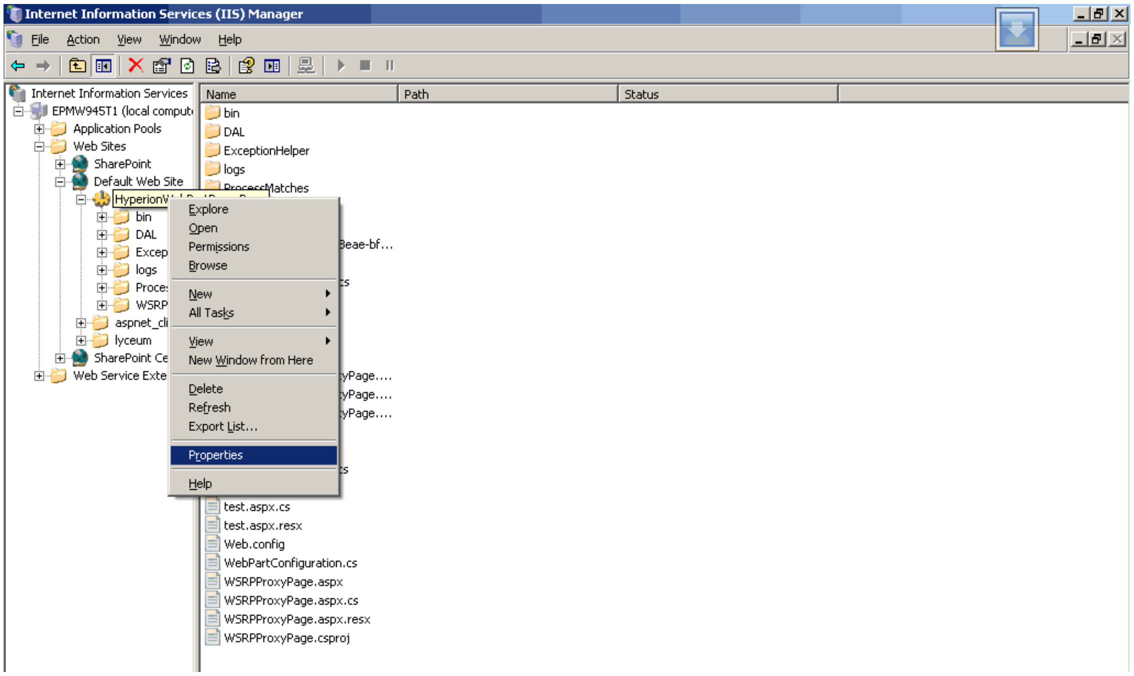
19. Type **BackConnectionHostNames**, and then press **Enter.**

20. Right-click **BackConnectionHostNames**, and then click **Modify.**

21. In the **Value** box, type the full host name of the server where SharePoint Portal is installed, and then click **OK.**

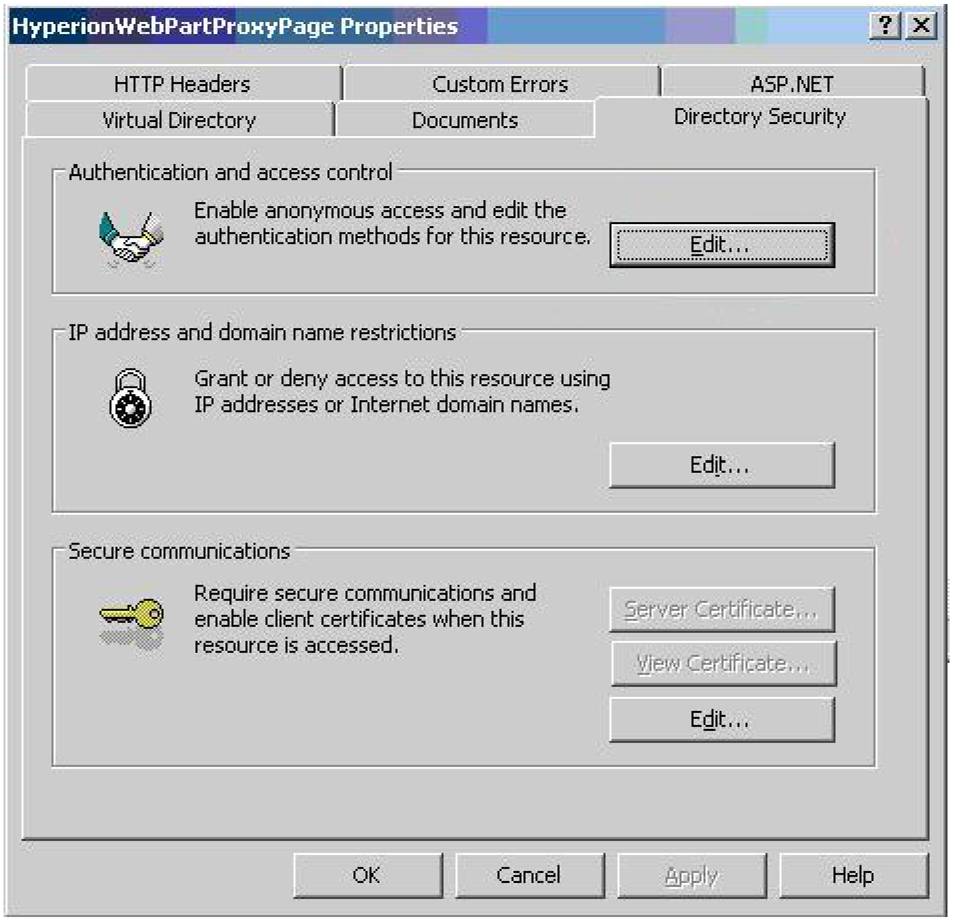
22. Quit Registry Editor, and then restart the IISAdmin service.

23. Navigate to HyperionWebPartProxyPage properties, as shown on the following figure.



24. Click the **Virtual Directory** tab,

25. Click **Edit** in the **Authentication and access control** section on the **Directory Security** tab.



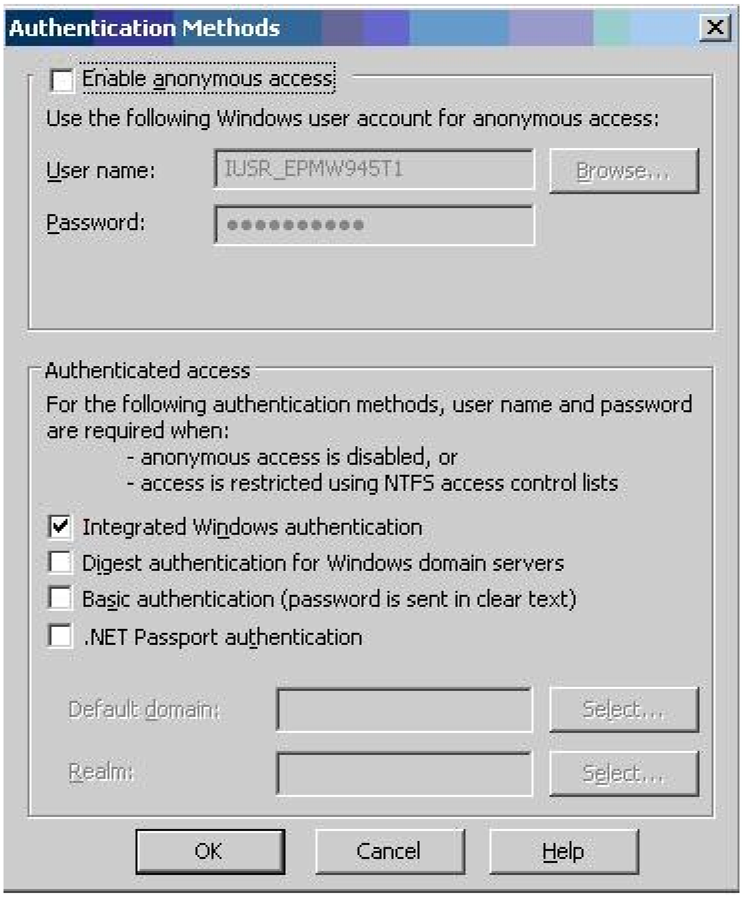
Enable anonymous access and edit the authentication methods for this resource.

Grant or deny access to this resource using IP addresses or Internet domain names.

Require secure communications and enable client certificates when this resource is accessed.

26 In Authentication Methods, select an access option:**Enable anonymous access** is not selected, and if you are using Hyperion WebPart Microsoft SSO, ensure that **Integrated Windows authentication** is selected . Alternatively, ensure that anonymous access is enabled (upper check box must be selected) and Integrated Windows authentication enabled if are using SiteMinder SSO.

- For HyperionEPM System WebPart Microsoft SSO, clear Enable anonymous access and select Integrated Windows authentication.



Authentication Methods

□ Enable anonymous access

Use the following Windows user account for anonymous access:

User name: IUSR_EPMW945T1

Password: ••••••••••

Authenticated access

For the following authentication methods, user name and password are required when:
- anonymous access is disabled, or
- access is restricted using NTFS access control lists

☑ Integrated Windows authentication

□ Digest authentication for Windows domain servers

□ Basic authentication (password is sent in clear text)

□ .NET Passport authentication

Default domain:

Realm:

- For SiteMinder SSO, select **Enable anonymous access** and **Integrated Windows authentication**.

27 Add the URL of the server where HyperionWebPartProxyPage is installed to Local Intranet zone in your client browser.

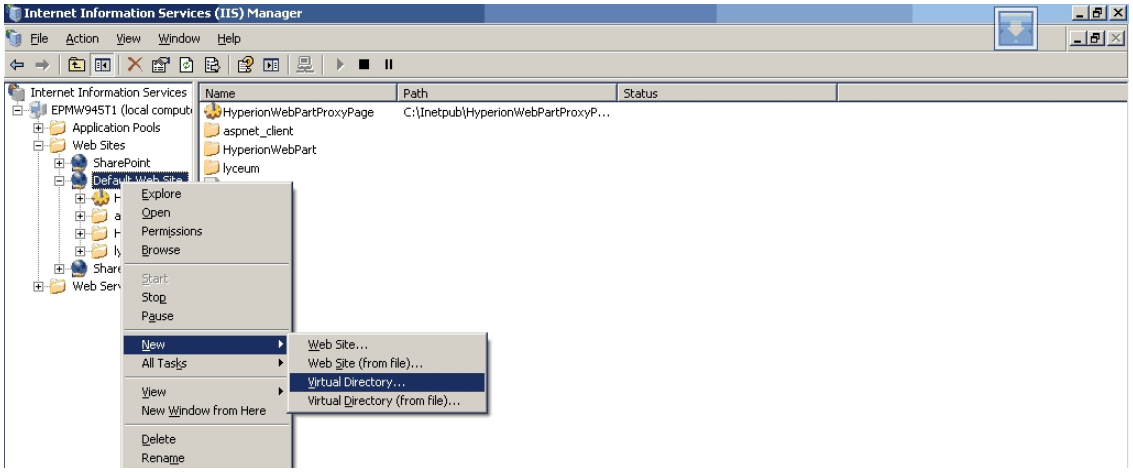
Installing Hyperion WebPart ResourceHttpHandler (SharePoint Portal 2003)

➤ To install Hyperion WebPart ResourceHttpHandler:

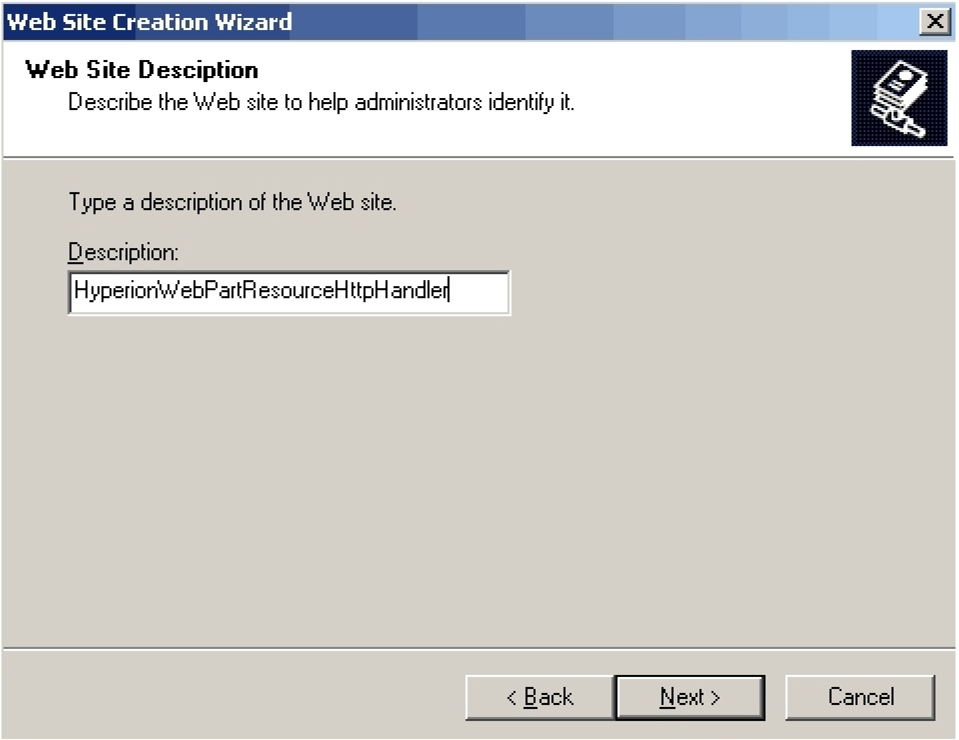
1 Run to Internet Information Services Manager.

2 Select **Default Web Site.**

3 Create a virtual folder to work with the `Hyperion WebPart ResourceHttpHandler` physical folder that you created in step 3 on page 43.



4 Define a virtual folder alias using the following figure as a guide, and click **Next.**



Web Site Creation Wizard

Web Site Desciption

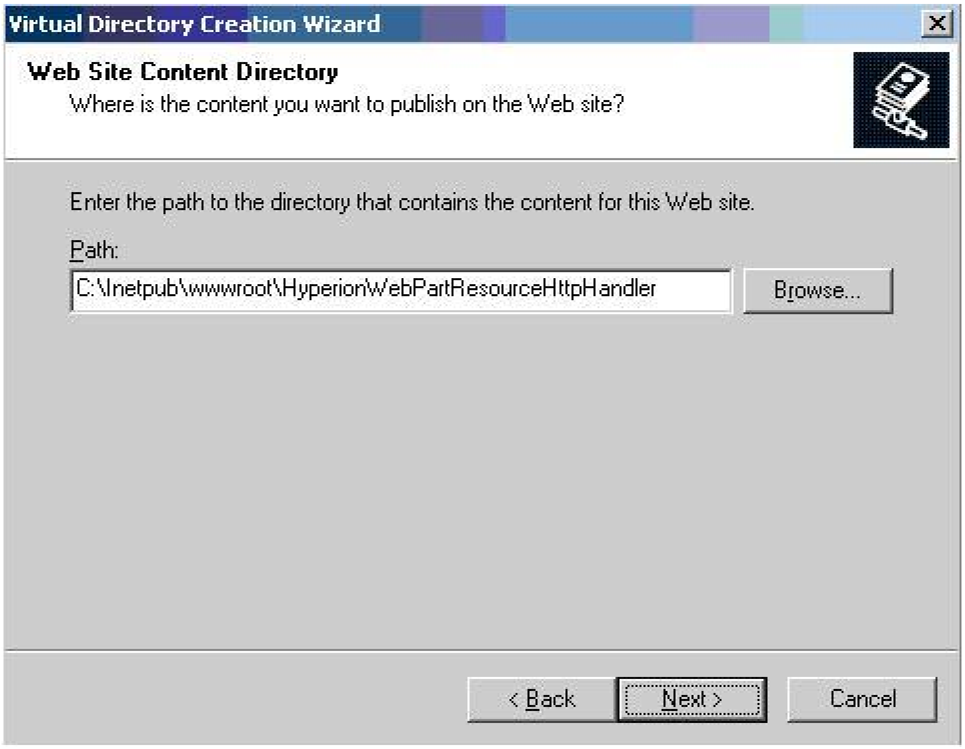
Describe the Web site to help administrators identify it.

Type a description of the Web site.

Description:

HyperionWebPartResourceHttpHandler

5 Point to the application folder that you defined in step 3 on page 43, and click **Next.**



Virtual Directory Creation Wizard

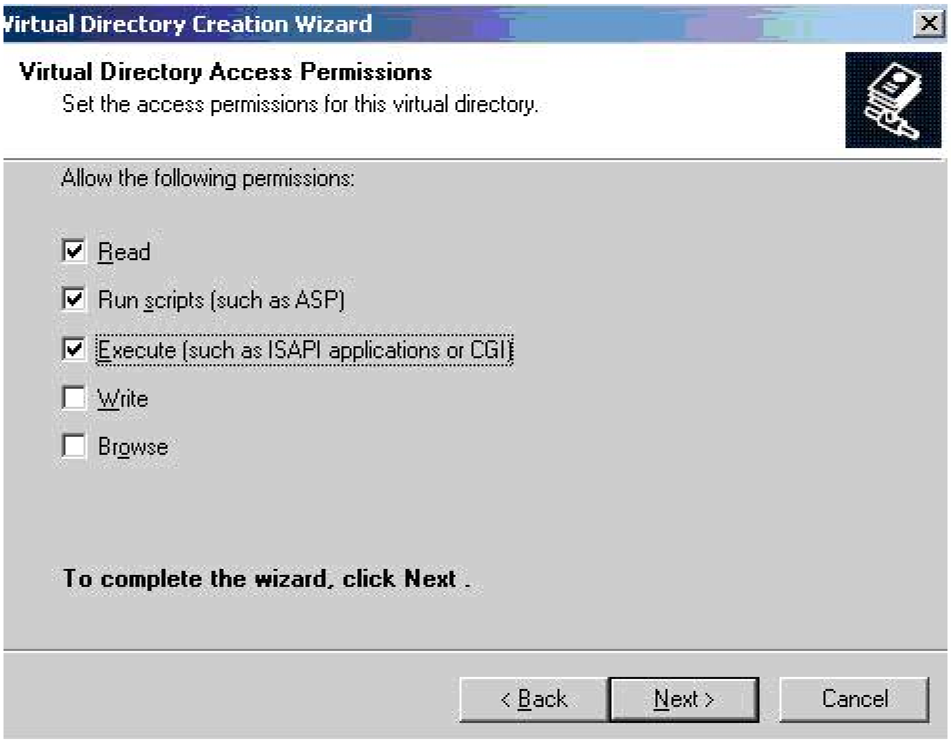
Web Site Content Directory

Where is the content you want to publish on the Web site?

Enter the path to the directory that contains the content for this Web site.

Path: C:\Inetpub\wwwroot\HyperionWebPartResourceHttpHandler

6 Set access permissions as shown in the following figure.



Virtual Directory Creation Wizard

Virtual Directory Access Permissions

Set the access permissions for this virtual directory.

Allow the following permissions:

☑ Read

☑ Run scripts (such as ASP)

☑ Execute (such as ISAPI applications or CGI)

□ Write

□ Browse

To complete the wizard, click Next .

Creating key container for Hyperion WebPart Encryptor

➤ To create key container for Hyperion WebPart Encryptor:

1 **Start command line.**

2 **Navigate to Microsoft .Net 2.0 directory (by default:** `C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727`**)**

3 **Run** `aspnet_regiis -pc HyperionWebPartKeyContainer`**. You can customize your key container name. In this case run** `aspnet_regiis -pc Your_Key_Container_Name`**.**

Installing Hyperion WebPart Encryptor

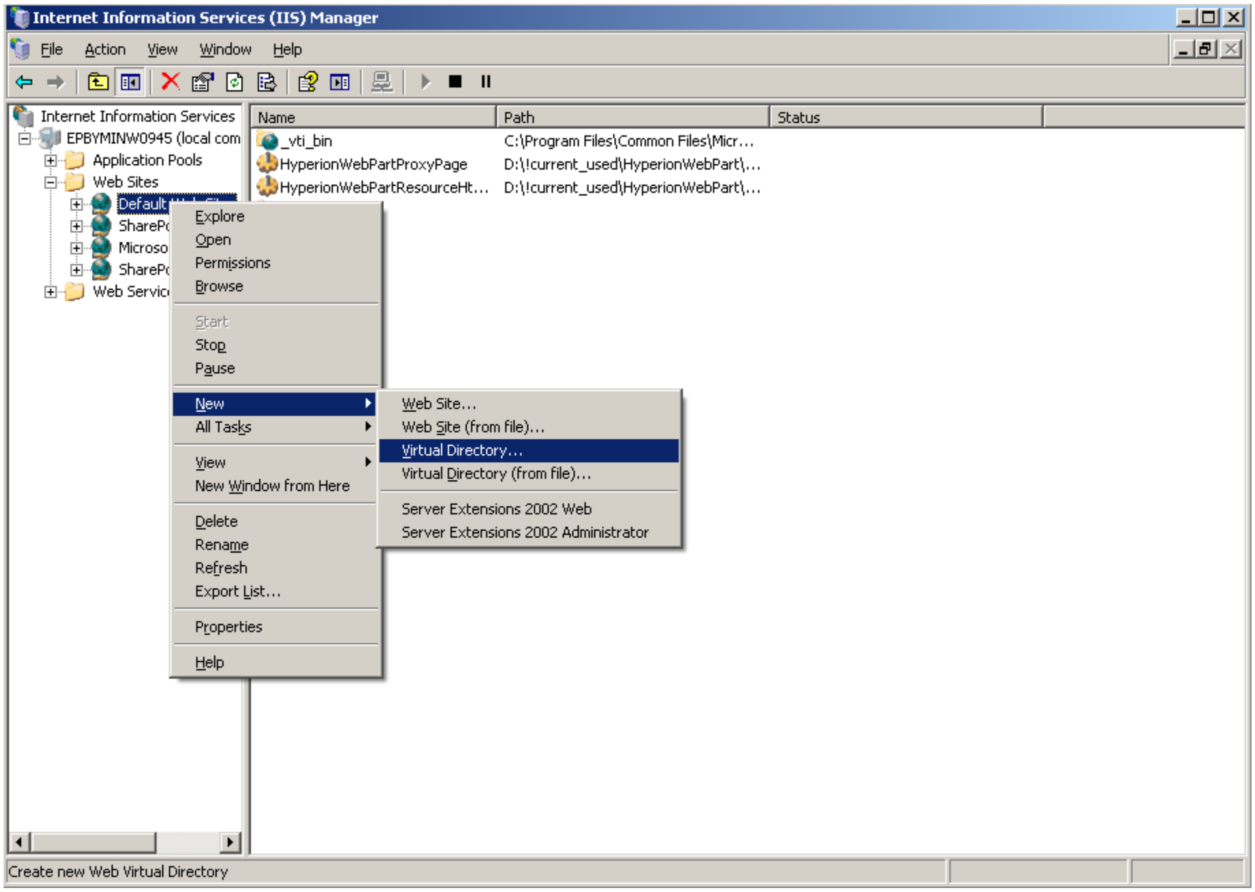
Hyperion WebPart Encryptor is web application used to encrypt connection strings to SQL server used in HyperionWebPartProxyPage and HyperionWebPartResourceHttpHandler web applications.

➤ To install Hyperion WebPart Encryptor:

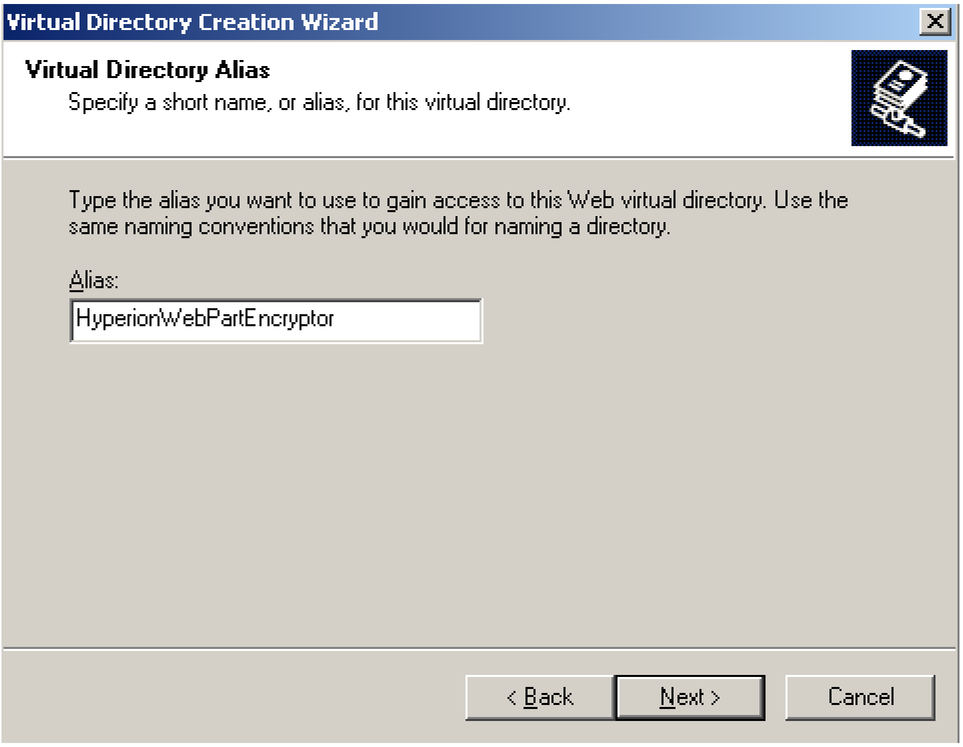
1 **Run to Internet Information Service manager.**

2 **Select Default Web Site.**

3 **Create virtual folder to work with Hyperion WebPart Encryptor physical folder that you created in step 3 on page 43.**


Internet Information Services (IIS) Manager
File Action View Window Help
Internet Information Services
EPBYMINW0945 (local com
Application Pools
Web Sites
Default
ShareP
Microso
ShareP
Web Servic
Name
Path
Status
_vti_bin
C:\Program Files\Common Files\Micr...
HyperionWebPartProxyPage
D:\!current_used\HyperionWebPart\...
HyperionWebPartResourceHt...
D:\!current_used\HyperionWebPart\...
Explore
Open
Permissions
Browse
Start
Stop
Pause
New
All Tasks
View
New Window from Here
Delete
Rename
Refresh
Export List...
Properties
Help
Web Site...
Web Site (from file)...
Virtual Directory...
Virtual Directory (from file)...
Server Extensions 2002 Web
Server Extensions 2002 Administrator
Create new Web Virtual Directory

4 Define a virtual folder alias using the following figure as a guide, and click **Next**.



Virtual Directory Alias

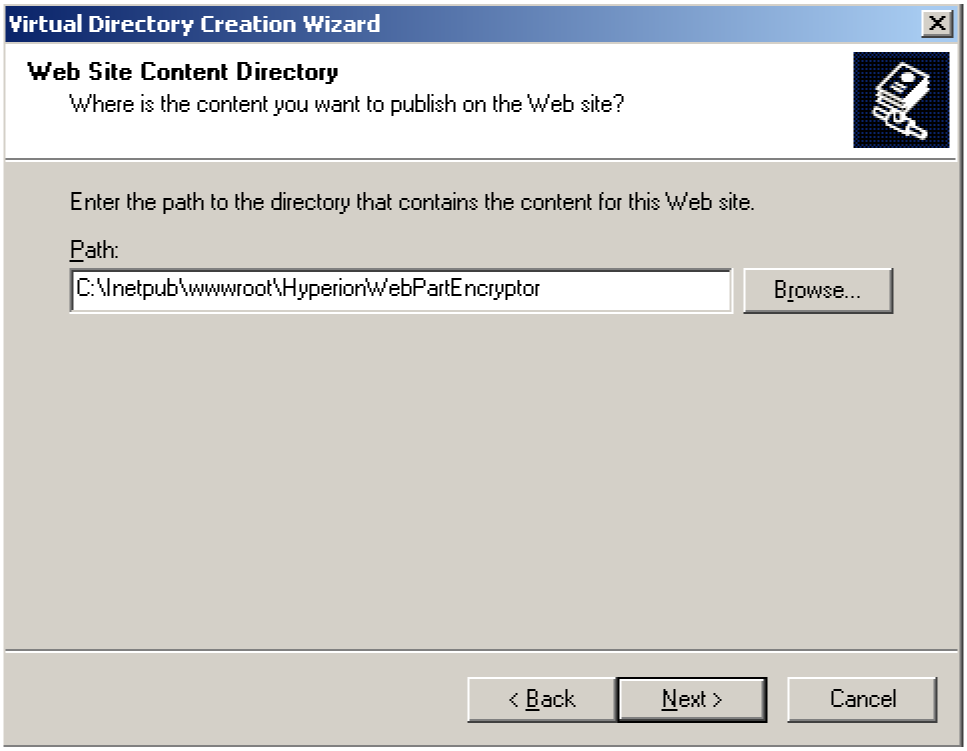
Specify a short name, or alias, for this virtual directory.

Type the alias you want to use to gain access to this Web virtual directory. Use the same naming conventions that you would for naming a directory.

Alias:

HyperionWebPartEncryptor

5 Point to the application folder that you defined in step 3 on page 43, and click **Next**.



Virtual Directory Creation Wizard

Web Site Content Directory

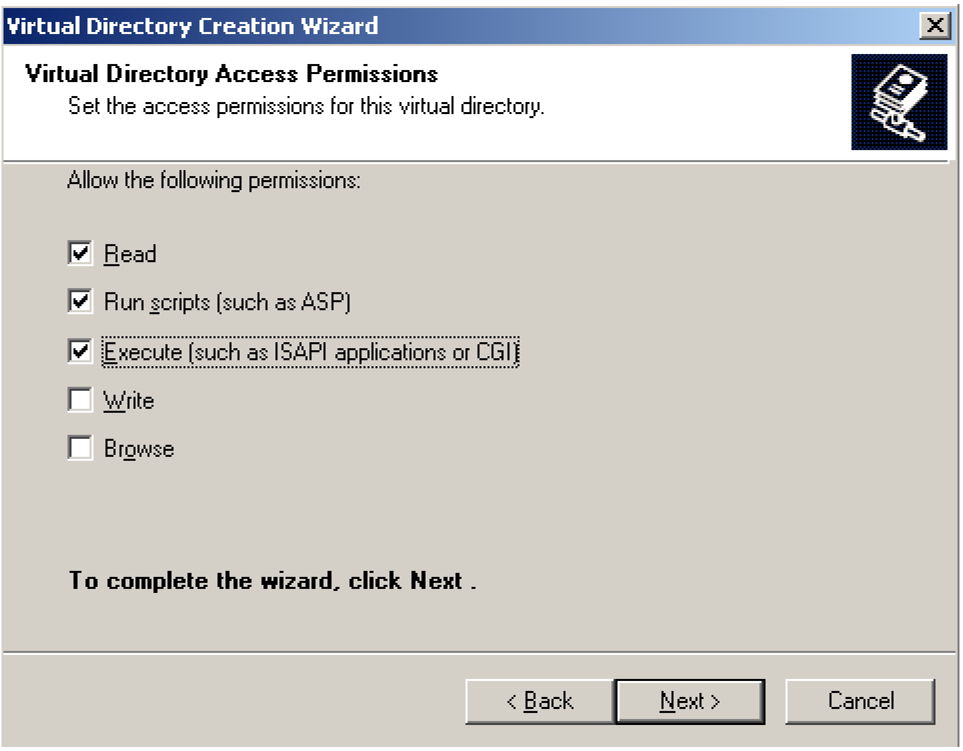
Where is the content you want to publish on the Web site?

Enter the path to the directory that contains the content for this Web site.

Path:

C:\Inetpub\wwwroot\HyperionWebPartEncryptor

6 Set access permissions as shown in the following figure.



Virtual Directory Creation Wizard

Virtual Directory Access Permissions

Set the access permissions for this virtual directory.

Allow the following permissions:

☑ Read

☑ Run scripts (such as ASP)

☑ Execute (such as ISAPI applications or CGI)

□ Write

□ Browse

To complete the wizard, click Next .

7 If you used custom key container name see step 3 in “Creating key container for Hyperion WebPart Encryptor” on page 53. Using a text editor, open Web.config in the HyperionWebPartProxyPage, HyperionWebPartEncyptor and HyperionWebPartResourceHttpHandler folders and make these changes:

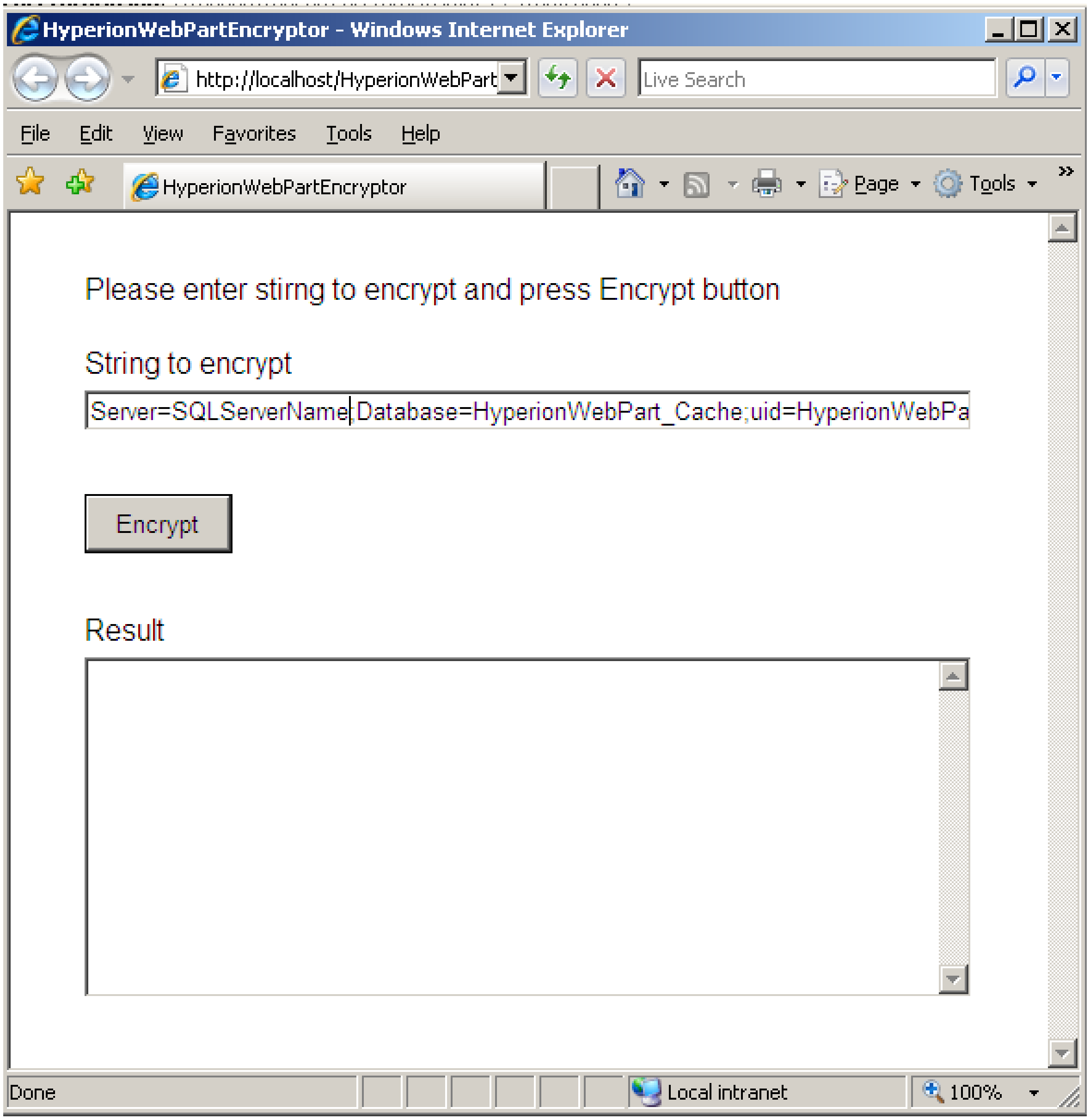
- In each file change `<add key ="KeyContainerName" value="HyperionWebPartKeyContainer " />`

to

- `<add key="KeyContainerName" value=" Your_Key_Container_Name " />`
- Save and close opened `web.config` files.

8 **Using a text editor, open `Web.config` in the HyperionWebPartProxyPage HyperionWebPartResourceHttpHandler folders and make these changes:**

- Run to Internet Information Service manager
- Select Default Web Site
- Select Hyperion WebPart Encryptor virtual directory
- Browse `HyperionWebPartEncryptor.aspx`
- Copy `connectionString` value from `web.config` file to text box



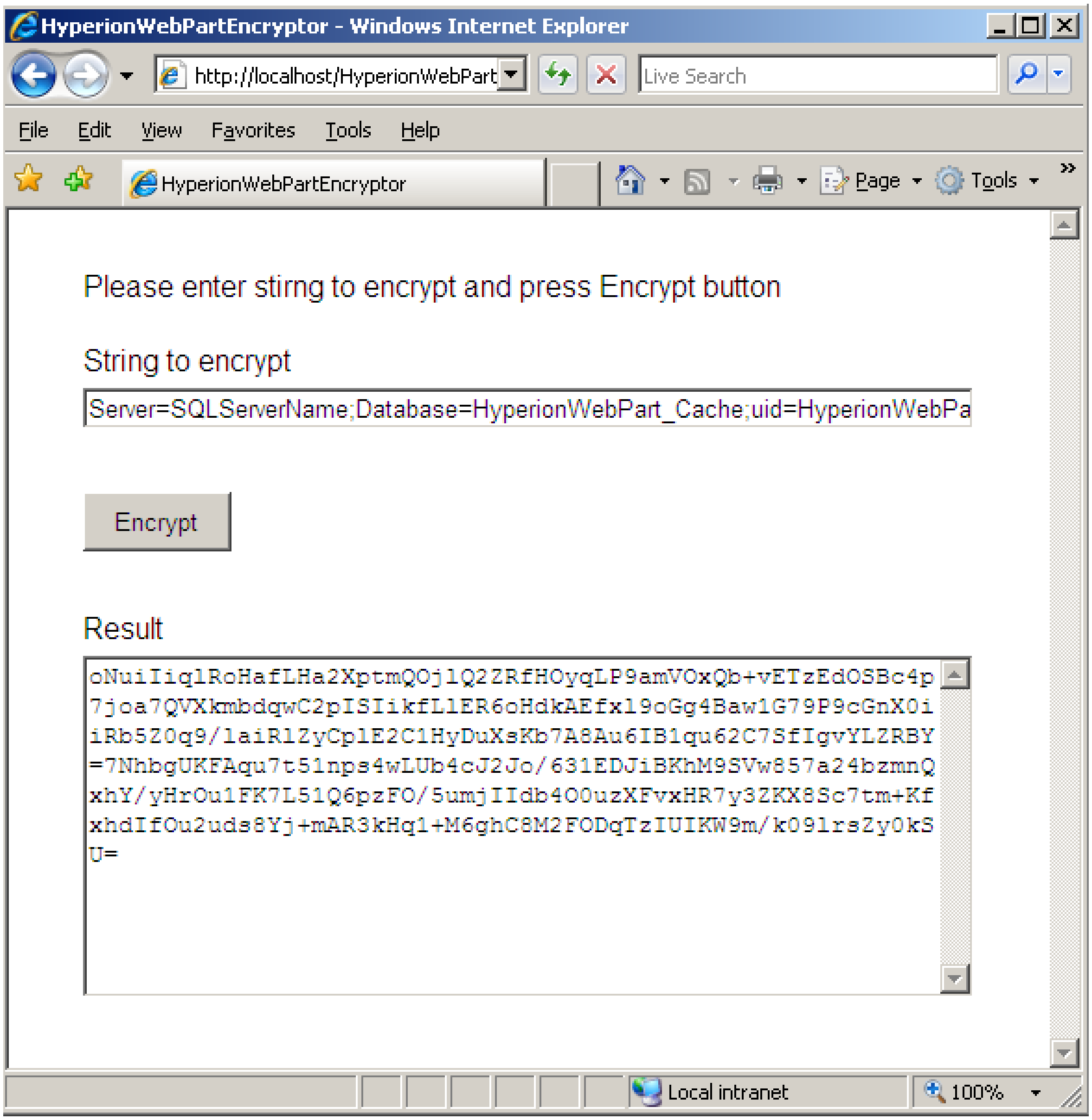
Please enter stirng to encrypt and press Encrypt button

String to encrypt

Server=SQLServerName;Database=HyperionWebPart_Cache;uid=HyperionWebPa

Result

9 Press **Encrypt** button.


HyperionWebPartEncryptor - Windows Internet Explorer
http://localhost/HyperionWebPart
Live Search
File Edit View Favorites Tools Help
HyperionWebPartEncryptor
Page
Tools
Local intranet
100%

Please enter stirng to encrypt and press Encrypt button

String to encrypt

Server=SQLServerName;Database=HyperionWebPart_Cache;uid=HyperionWebPa

Encrypt

Result

```
oNuiIiqlRoHafLHa2XptmQOjlQ2ZRfHOyqLP9amVOxQb+vETzEdOSBc4p
7joa7QVXkmbdqwC2pISIikfLlER6oHdkAEfxl9oGg4Baw1G79P9cGnX0i
iRb5Z0q9/laiRlZyCplE2C1HyDuXsKb7A8Au6IB1qu62C7SfIgvYLZRBY
=7NhbgUKFAqu7t51nps4wLUb4cJ2Jo/631EDJiBKhM9SVw857a24bzmnQ
xhY/yHrOu1FK7L51Q6pzFO/5umjIIdb4O0uzXFvxHR7y3ZKX8Sc7tm+Kf
xhdIfOu2uds8Yj+mAR3kHq1+M6ghC8M2FODqTzIUIKW9m/k09lrsZy0kS
U=
```

10 Copy encrypted connection string to connectionString value in web.config files of Hyperion WebPart ProxyPage and Hyperion WebPart ResourceHttpHandler.

11 **Save** and **Close** opened `web.config` files.

12 Remove Hyperion WebPart Encryptor virtual folder. See“Removing Hyperion WebPart Encryptor” on page 64.

Customizing the Database Creation Script for SharePoint Portal 2003

You can customize these parameters in the HyperionWebPart database creation script:

- Database name (Default: HyperionWebPart_Cache)

If you use custom parameters, you must modify the `Web.config` file in the `HyperionWebPartProxyPage` folder accordingly.

➤ To customize database script parameters:

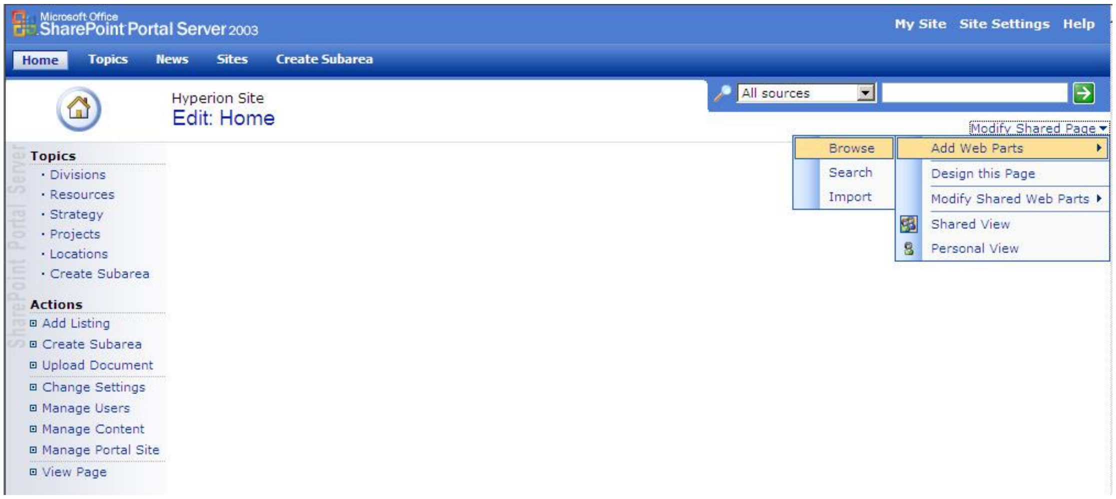
1. **Open `HyperionWebPart_DB_Create.sql` in a text editor.**
2. **Replace all occurrences of `HyperionWebPart_Cache` with a custom name.**

Installing WebPart for SharePoint Portal 2003

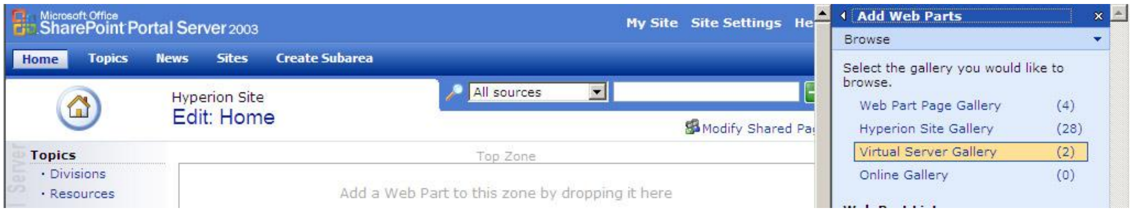
Note: Update the Web.config file before beginning this procedure. See "Updating Web.config (SharePoint Portal 2003)" on page 60.

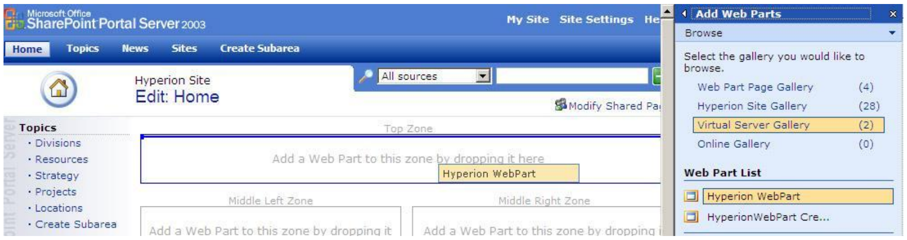
➤ To install WebPart for the SharePoint portal:

1. **Add the path to your version of Microsoft .NET framework to the system PATH variable.**
2. **Run `AddWebPart.bat`.**
3. **Copy full contents of WebPartResources directory to bin directories of each SharePoint Web Site where Hyperion WebPart installed.**
4. **Open the SharePoint Portal site.**
5. **Click Modify Shared Page.**
6. **Select AddWebParts, thenBrowse.**



7. **Drag Virtual Server Gallery from the Browse list to one of your Web Part Zones, or click Add button at the bottom of the column.**


Microsoft Office
SharePoint Portal Server 2003
My Site
Site Settings
He
Home
Topics
News
Sites
Create Subarea
Hyperion Site
Edit: Home
All sources
Modify Shared Pa
Topics
Divisions
Resources
Top Zone
Add a Web Part to this zone by dropping it here
Add Web Parts
Browse
Select the gallery you would like to browse.
Web Part Page Gallery (4)
Hyperion Site Gallery (28)
Virtual Server Gallery (2)
Online Gallery (0)



8 For a more secure configuration, the use of SSL connection between your instance of SharePoint Portal 2003 and your EPM System producer is recommended. See "SSL Support (SharePoint Portal 2003)" on page 66.

Updating Web.config (SharePoint Portal 2003)

➤ To update `Web.config`:

1 Using a text editor, open `Web.config` in the `HyperionWebPartProxyPage` folder and make these changes:

- Replace all occurrences of `$GET(appServerProps.workspaceHost)` with hostname:port where your instance of Hyperion WebPart ResourceHttpHandler is installed.

  Note: `$GET(appServerProps.workspaceHost)` and `$GET(appServerProps.workspacePort)` entries appear in the `web.config` file only if the WepPart 2007 package was not configured during the Reporting and Analysis build installation. The default producer is set when EPM System Configurator installs the EPM System portlet.

- Replace all occurrences of `$GET(appServerProps.workspacePort)` with the number of port used for the EPM System WSRPProducer.
- Replace all occurrences of `SharepointHostName` with the full host name of the server where your instance of Microsoft SharePoint Portal is installed.
- Replace all occurrences of `SQLServerName` with the full host name of the MS SQL server hosting the Hyperion WebPart database. This should be the same SQLServerName that is set during Hyperion WebPart installation.

2 Make these changes to reflect the custom parameters set during Hyperion Hyperion WebPart installation:

- Change `HyperionWebPart_user` to the SQL Server login to use with HyperionWebPart set during Hyperion WebPart installation.
- Change `1#Password` to SQL Server password to use with HyperionWebPart set during Hyperion WebPart installation.

3 If you customized parameters when you configured Hyperion WebPart for Microsoft SSO, make one or more of these changes to reflect the custom parameters:

- Change `HyperionReportingAndAnalysis` to the custom name for the application.

- Change HyperionReportingAndAnalysisTemp to the application name that you specified for storing nonpersistent credentials.

4 **If you customized parameters when you configured Hyperion WebPart for SiteMinder SSO, replace all occurrences of** HyperionReportingAndAnalysisSiteMinderHeader **with the name of the header used for SiteMinder authentication in your instance of EPM System.**

5 **Using a text editor, open** Web.config **in the** HyperionWebPartResourceHttpHandler **folder and make these changes:**

- Change HyperionWebPart_user to the custom user name.
- Replace all occurrences of SQLServerName with the full host name of the MS SQL server hosting the Hyperion WebPart database. This should be the same SQLServerName that is specified in setEnv.bat.
- If you customized parameters when you created the Hyperion WebPart database, make one or more of these changes to reflect the custom parameters:
    - Change HyperionWebPart_Cache to the custom name of the Hyperion WebPart database.
    - Change HyperionWebPart_user to the SQL Server login to use with HyperionWebPart set during Hyperion WebPart installation.
    - Change 1#Password to SQL Server password to use with HyperionWebPart set during Hyperion WebPart installation.

Customizing Hyperion WebPart app.config (SharePoint Portal 2003)

You can customize two parameters in the Hyperion WebPart app.config file:

- Hyperion WebPart ProxyPage host port

The app.config files are stored in the /wpresources/ HyperionWebPart/ and /wpresources/HyperionWebPartCredentialsManager subfolders of your SharePoint portal instance. If you edit one app.config file, you must also edit the other.

➤ To customize parameters in app.config:

1 **Open** app.config **in a text editor.**

2 **To customize port, which Hyperion WebPart should use to communicate with HyperionWebPartProxyPage web application replace 8080 with number of port used for running your instance of HyperionWebPartProxyPage the following line: .**<add key="Port" value="8080"/>

Configuring Default Permissions for EPM System WebPart (SharePoint Portal 2003)

The portal home page is shared by all portal users. If one user adds a Hyperion WebPart to the home page, other users cannot access the home page, and a warning message is displayed when they try to display it. You can prevent this by configuring default permissions for Hyperion WebPart so that users cannot add it to the home page.

➤ To configure default permissions for EPM System WebPart:

1 In your browser, open the Web Parts Maintenance Page on the Microsoft SharePoint site.

2 Enter these settings for the EPM System WSRP WebPart:

   - Open on Page?: Yes
   - Personalized?: No

Updating the Hyperion WebPart Application (SharePoint Portal 2003)

Updating the Hyperion WebPart application involves modifying these items:

- Hyperion WebPart ProxyPage and Hyperion WebPart ResourceHttpHandler Web applications

  See "Updating Hyperion WebPart ProxyPage Web Application and Hyperion WebPart ResourceHttpHandler (SharePoint Portal 2003)" on page 62.

- Web part installation

  See "Updating the Web Part Installation (SharePoint Portal 2003)" on page 63.

- Hyperion WebPart `app.config`

  See "Customizing Hyperion WebPart app.config (SharePoint Portal 2003)" on page 61.

- Updating `Web.config`

  See "Updating Web.config (SharePoint Portal 2003)" on page 60.

Updating Hyperion WebPart ProxyPage Web Application and Hyperion WebPart ResourceHttpHandler (SharePoint Portal 2003)

➤ To update Hyperion WebPart ProxyPage and Hyperion WebPart ResourceHttpHandler Web Application:

1 Replace the contents of the `HyperionWebPartProxyPage` folder (defined when you installed the Hyperion WebPart ProxyPage Web application) with the folder contents included in the update package.

2 Replace the contents of the `HyperionWebPartResourceHandler` folder (defined when you installed Hyperion WebPart ResourceHttpHandler) with the folder contents included in the update package.

Note: Back up your working copy of `Web.config` for `Hyperion WebPart` if you are uncertain about your parameter changes.

Updating the Web Part Installation (SharePoint Portal 2003)

➤ To update the Web part installation for the SharePoint portal, run `UpdateWebPart.bat`.

Uninstalling the Hyperion WebPart Application (SharePoint Portal 2003)

You must update the `setEnv.bat` file to uninstall the Hyperion WebPart application.

You must also remove these items:

- The Web part

  See "Removing the Hyperion Web Part (SharePoint Portal 2003)" on page 63.

- SSO data

  See "Removing SSO Data (SharePoint Portal 2003)" on page 64.

- Hyperion WebPart Encryptor See "Removing Hyperion WebPart Encryptor" on page 64.

- Hyperion WebPart Key Container See "Removing key container for Hyperion WebPart Encryptor" on page 65.

- Hyperion WebPart ResourceHttpHandler

  See "Removing Hyperion WebPart ResourceHttpHandler (SharePoint Portal 2003)" on page 65.

- Hyperion WebPart ProxyPage

  See "Removing Hyperion WebPart ProxyPage (SharePoint Portal 2003)" on page 65.

Removing the Hyperion Web Part (SharePoint Portal 2003)

Be sure to close all instances of Hyperion WebPart in the portal before removing the Web part. Otherwise, users see an error message rather than the Hyperion WebPart contents.

➤ To remove the Web part, run `RemoveWebPart.bat`.

Removing SSO Data (SharePoint Portal 2003)

➤ To remove SSO data:

1 Navigate to the **SharePoint Portal Server Single Sign-On Administration** page.

2 Remove all application definitions.

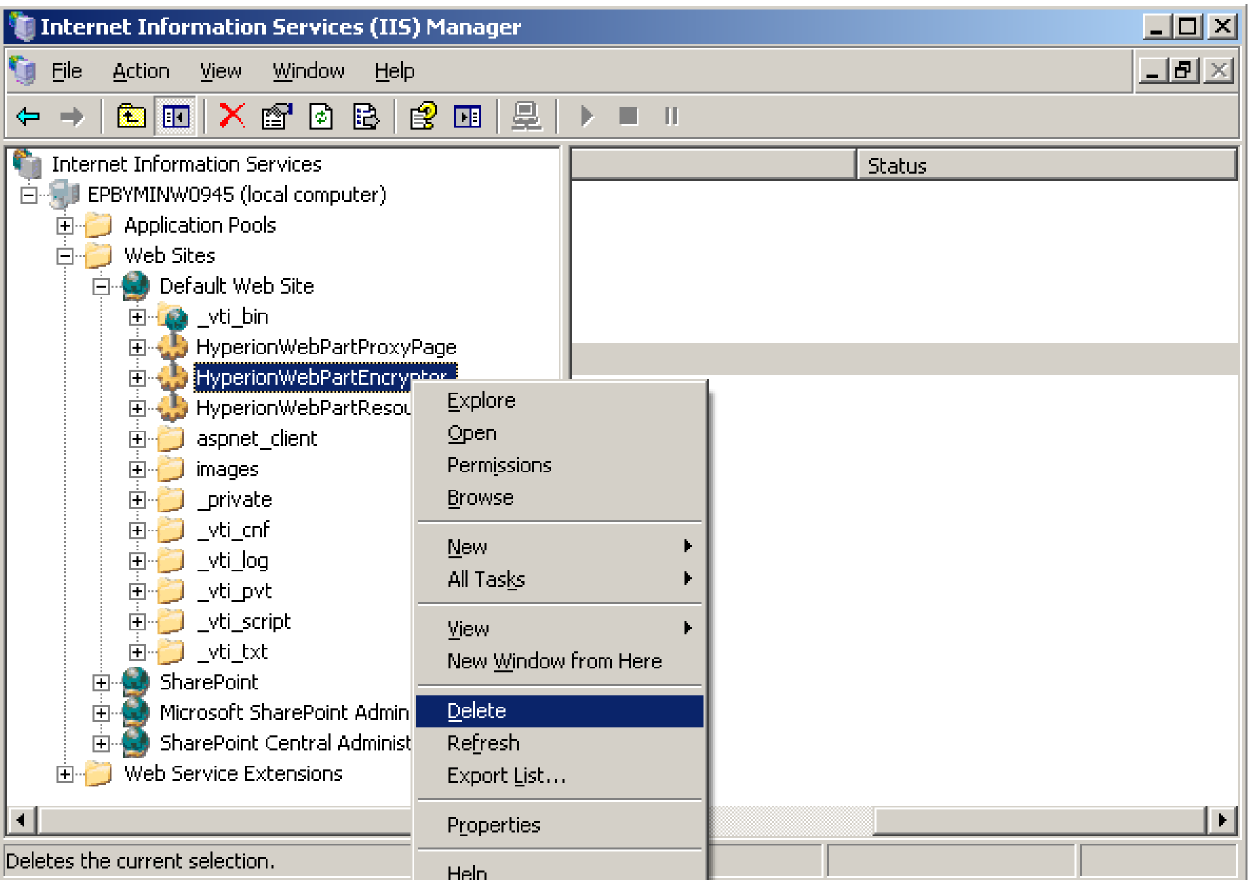
Removing Hyperion WebPart Encryptor

➤ To remove Hyperion WebPart Encryptor:

1 Go to Internet Information Services Manager.

2 Select **Default Web Site.**

3 Remove the Hyperion WebPart Encryptor virtual folder.



4 Delete the Hyperion WebPart Encryptor folder from your hard disk.

Removing key container for Hyperion WebPart Encryptor

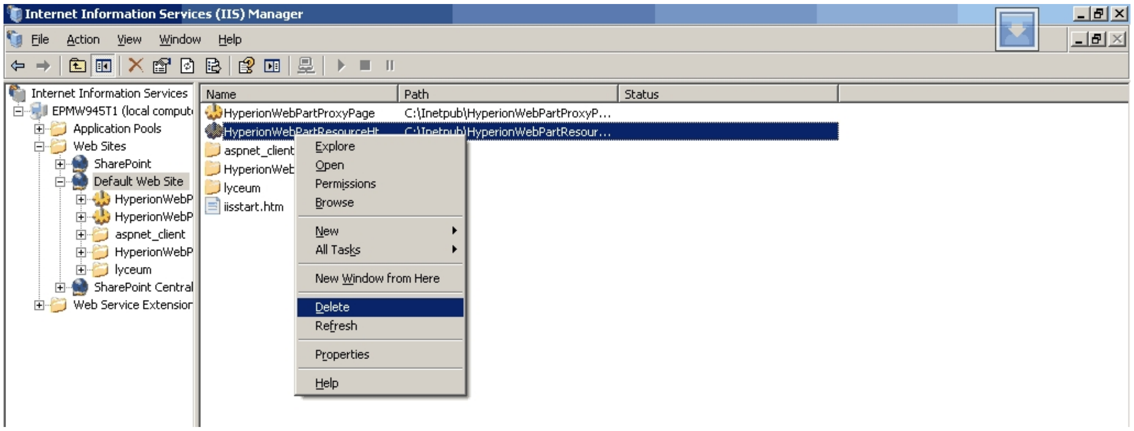
➤ To remove key container for Hyperion WebPart Encryptor:

1. Start command line.
2. Navigate to Microsoft .Net 2.0 directory (by default: C:\WINDOWS\Microsoft.NET\Framework \v2.0.50727).
3. Run `aspnet_regiis -pz HyperionWebPartKeyContainer` . You can customize your key container name. In this case run `aspnet_regiis -pz Your_Key_Container_Name`.
4.

Removing Hyperion WebPart ResourceHttpHandler (SharePoint Portal 2003)

➤ To remove Hyperion WebPart ResourceHttpHandler:

1. Run Internet Information Services Manager.
2. Select **Default Web Site.**
3. Remove the **Hyperion WebPart ResourceHttpHandler** virtual folder.



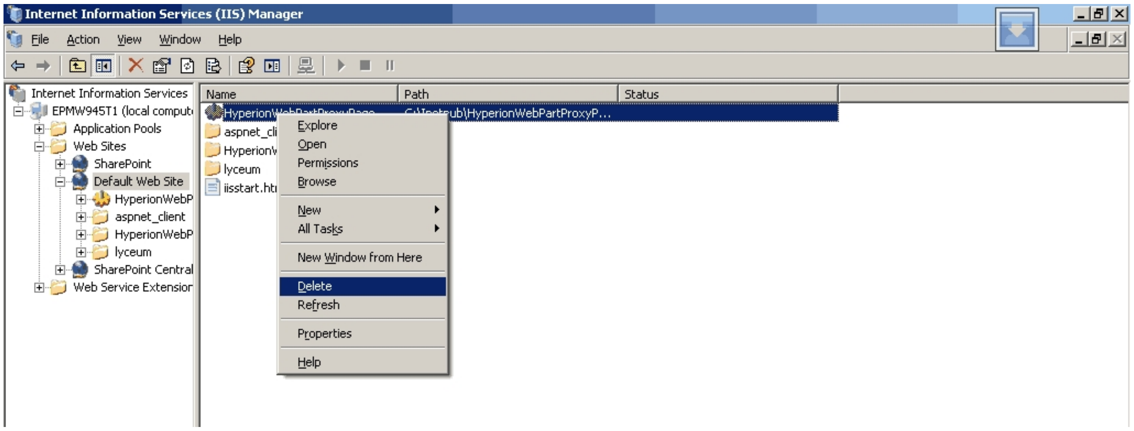
Name	Path	Status
HyperionWebPartProxyPage	C:\Inetpub\HyperionWebPartProxyP…	
HyperionWebPartResourceHt	C:\Inetpub\HyperionWebPartResour…	
aspnet_client		
HyperionWeb		
lyceum		
iisstart.htm		

4. Delete the `HyperionWebPartResourceHttpHandler` folder from your hard disk.

Removing Hyperion WebPart ProxyPage (SharePoint Portal 2003)

➤ To remove Hyperion WebPart ProxyPage:

1. Run Internet Information Services Manager.
2. Select **Default Web Site.**
3. Remove the **HyperionWebPartProxyPage** virtual folder.



4 **Delete the folder containing Hyperion WebPart ProxyPage from your hard disk.**

SSL Support (SharePoint Portal 2003)

Using an SSL channel between your instance of SharePoint Portal 2003 and your EPM System producer requires these actions:

1. Get certificate from EPM System producer.
2. Install the producer certificate on the server where your instance of Microsoft SharePoint Portal is installed.
3. Change the EPM System producer URLs in `Web.config` to work over https.

   For example, change these settings:

   ```
   add key="MarkUpURL" value="http://epmsd111.epminsk.hyperion.com:
   45000/raframework/wsrp4j/WSRPBaseService" />

   <add key=PortletManagementURL”

   value="http://epmsd111.epminsk.hyperion.com:45000/raframework/
   wsrp4j/WSRPPortletManagementService" />

   <add key=RegistrationURL”

   value="http://epmsd111.epminsk.hyperion.com:45000/raframework/
   wsrp4j/WSRPRegistrationService" />

   <add key=ServiceDescription”

   value="http://epmsd111.epminsk.hyperion.com:45000/raframework/
   wsrp4j/WSRPServiceDescriptionService" />
   ```

   to these settings:

   ```
   add key="MarkUpURL" value="https://epmsd111.epminsk.hyperion.com:
   45000/raframework/wsrp4j/WSRPBaseService" />

   <add key=PortletManagementURL”

   value="https://epmsd111.epminsk.hyperion.com:45000/raframework/
   wsrp4j/WSRPPortletManagementService" />
   ```

```
<add key=RegistrationURL"

value="https://epmsd111.epminsk.hyperion.com:45000/raframework/
wsrp4j/WSRPRegistrationService" />

<add key=ServiceDescription"

value="https://epmsd111.epminsk.hyperion.com:45000/raframework/
wsrp4j/WSRPServiceDescriptionService" />
```

Note: In the changed settings, the values begin with "https" rather than "http".

SSO Implementation

Reporting and Analysis user credentials are mapped to SharePoint user account. Hyperion WebPart uses Microsoft Single Sign-On service functionality to store and retrieve user credentials. When you display Hyperion WebPart for the first time, the system prompts for EPM System user credentials. On subsequent calls, the EPM system user credentials are used to authenticate requests from the particular portal user.

Support Activities (SharePoint Portal 2003)

The application is designed run unattended. However, you should perform these tasks to maintain the application:

- Database backup—The database files should be backed up regularly in accordance with the schedule described in the IT department policies. Oracle recommends full daily backup at night and several incremental backups during the day. Regular transaction log backups are also recommended.
- Disk space monitoring—As the Hyperion WebPart database grows, you must constantly monitor disk space availability on both the hard drive where system data file is located and the one where its transaction log file resides. While both files should be allowed unrestricted growth, Oracle recommends truncating the transaction log from time to time to improve performance and save the disk space. Please refer to the SQL Books Online for the detailed instructions on how to truncate the log.
- Configuration files archive—After each change in the system configuration files they should be backed up and stored in a safe location with the Hyperion WebPart version to which this configuration files belong and they should be clearly marked.

Tips and Troubleshooting: SharePoint Portal 2003

Configuring Log Storage (SharePoint Portal 2003)

You can log all errors raised in Hyperion WebPart. You can configure log storage to store logs in these locations:

- The Microsoft Windows Event Log
- Plain text `.log` file
- The Microsoft Windows Event Log and in a `.log` file

Note: If you select neither the Microsoft Windows Event Log option nor the `.log` file option, users get error messages with error codes but no additional details.

➤ To configure log storage:

1. **Using a text editor, open `Web.config` in the `HyperionWebPartProxyPage` folder.**
2. **Change the `EnableWindowsLogging` value to `true` to enable storing logs to Microsoft Windows Event Log or to `false` to disable it.**
3. **Change the `EnableFileLogging` value to `true` to enable storing logs to the `.log` file or to `false` to disable it.**
4. **To customize the `.log` file name, change the `LogFileNamePrefix` value. Default prefix: HyperionWebPart.**

   If you use the default `LogFileNamePrefix`value, log file names are in this format:

   ```
   HyperionWebPart-mm-dd-yyyyy.log
   ```

Customizing Hyperion WebPart app.config (SharePoint Portal 2003)

Additionally you can customize two parameters in the Hyperion WebPart app.config file:

- Hyperion WebPart ProxyPage hostname
- Hyperion WebPart ProxyPage virtual directory

The app.config files are stored in the /wpresources/ HyperionWebPart/ and / wpresources/ HyperionWebPartCredentialsManager subfolders of your SharePoint portal instance. If you edit one app.config file, you must also edit the other.

➤ To customize parameters in app.config:

1. **Open app.config in a text editor.**

2 **To customize hostname, which Hyperion WebPart should use to communicate with HyperionWebPartProxyPage web application, add the following line to appSettings section:** `<add key=”Host” value=”SomeHostName”/>`**, where SomeHostName is hostname you want to use.**

3 **To customize virtual directory, which Hyperion WebPart should use to communicate with HyperionWebPartProxyPage web application add the following line to appSettings section:** `<add key=="RemoteDirectory" value="SomeVirtualDirectoryName" />`**, where SomeVirtualDirectoryName is virtual directory you want to use. Default value is HyperionWebPartProxyPage.**

Error Messages (SharePoint Portal 2003)

Depending on your log storage configuration, all handled exceptions are stored into Microsoft Windows Event Log or in a text file in HyperionWebPartProxyPage directory.

The following sections describe errors that are beyond the scope of Hyperion WebPart.

Hyperion WebPart Errors (SharePoint Portal 2003)

The following table lists Hyperion WebPart errors with possible causes and solutions. The possible cause and suggested solution for each error are written to the system log.

Table 3

Message Displayed	Possible Cause	Suggested Solution
Error #100: Unknown error occurred. Please contact your portal administrator.	The access credentials that you entered are incorrect, or the database does not exist.	Ensure that the database exists and that the access credentials you entered are valid.
Error #101: WebPart is not configured properly. Please contact your portal administrator.	The access credentials that you entered are invalid, or the database does not exist.	Ensure that the database exists and that the access credentials you entered are valid.
Error #102: The credentials provided are invalid. Please enter valid credentials using WebPart Credentials Manager.	The credentials that you entered are invalid.	Enter valid credentials using WebPart Credentials Manager.
Error #103: WebPart is not configured properly. Please, contact your portal administrator.	The `proxymanager.asmx` file does not exist or has incorrect access permissions.	● Ensure that `proxymanager.asmx` exists. ● Set correct access permissions.

Message Displayed	Possible Cause	Suggested Solution
Error #104: The portlet service is unavailable. Please contact your portal administrator.	WebPart settings are invalid, or producer services are stopped.	Check your producer connection settings.
Error #105: No credentials found. Please enter credentials using WebPart Credentials Manager, or contact your portal administrator.	Single Sign-On service is stopped or is not configured, or credentials for the current user were not found.	● Restart Microsoft Single Sign-On service. ● Configure SSO in SharePoint Portal Server Central Administration. ● Check the current user's credentials.
Error #106: WebPart is not configured properly. Please contact your portal administrator.	WebPart or the database is out of date.	Reinstall all Hyperion WebPart components.
Error #107: WebPart doesn't work properly. Please, contact your portal administrator.	The portlet handle is invalid.	Ensure that the portlet handle is valid.
Error #108: WebPart is not configured properly. Please contact your portal administrator.	SSO system is not configured.	● Disable anonymous access to the `HyperionProxyPage` folder to use Microsoft Single Sign-On. ● Ensure that SiteMinder SSO system is configured properly.
Error #109: WebPart is not configured properly. Please contact your portal administrator.	The SSL certificate on the consumer side is not installed.	Install a valid SSL certificate.
Error #110: WebPart does not work as expected. Please contact your portal administrator.	User has not enough permission to write to Windows Event Log, or Event Log does not exist.	Check User permissions and Event Log existence.
Error #111: WebPart does not work as expected. Please contact your portal administrator.	User does not have permission to write to `logs` subfolder of HyperionWebPartProxyPage, or the `logs` subfolder does not exist.	Check User permissions and existence of the `logs` folder.
Error #112: WebPart does not work as expected. Please contact your portal administrator.	Database size exceeded the limit.	Remove Hyperion WebPart and reinstall.

Message Displayed	Possible Cause	Suggested Solution
Error #113: WebPart cannot be removed from this page.	User does not have enough permission to remove WebPart from the page.	Please contact your portal administrator to check your permissions.
Error#114: Could not load LoginForm.ascx.	LoginForm.ascx file not found.	Check LoginForm.ascx availability. Refer to the Administration Guide for more information.
Error #115: Validation of one or more parameters failed.	Parameters used are not correct.	Check if producer works correctly.

Other Error Messages (SharePoint Portal 2003)

The following errors are beyond the scope of Hyperion WebPart.

Writing to Event Log Error

Symptoms — When you trying to use HyperionWebPart, you get error message: " Error #110: WebPart does not work as expected. Please contact your portal administrator."

Cause — User does not have permissions or Event Log is full.

➤ To resolve this error:

1. **Check whether Event Log is full. If full, clear Event Log.**
2. **If not, run** `regedit`**.**
3. **Find the** `CustomSD` **registry entry at this location:** `HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Services\Eventlog\WSRPWebPart`
4. **Add** `(A;;0x3;;;AU)` **to the end of** `CustomSD` **value data.**

System.Security.SecurityException: Request for the permission of type System.Net.WebPermission failed.

Symptoms—When you try to render Hyperion WebPart, you receive the following exception:

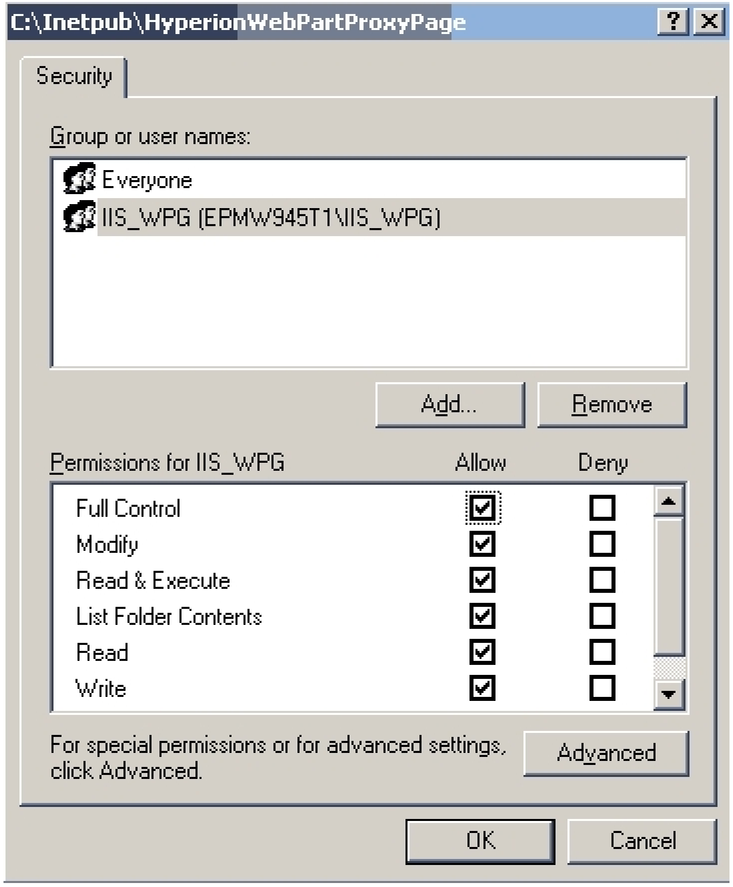
```
System.Security.SecurityException: Request for the permission of type
System.Net.WebPermission, System, Version=1.0.5000.0, Culture=neutral,
PublicKeyToken=b77a5c561934e089 failed.
```

Cause—Hyperion WebPart does not have permission to create Hyperion WebPart ProxyPage.

Resolution

- Open the SharePoint Portal `web.config` file for editing. Go to section `<system.web>`. Set `<trust level="Full" originUrl="" />`. Save your changes.

- Navigate to the `Hyperion WebPart ProxyPage` folder. Set IIS_WPG user permissions for the `Hyperion WebPart ProxyPage` folder as shown on the following figure.



C:\Inetpub\HyperionWebPartProxyPage

Security

Group or user names:

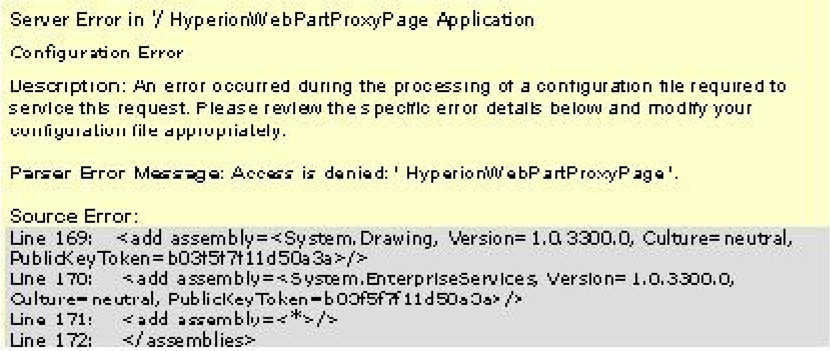
Everyone
IIS_WPG (EPMW945T1\IIS_WPG)

Permissions for IIS_WPG	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□

For special permissions or for advanced settings, click Advanced.

Server Error in '/HyperionWebPartProxyPage' Application. Parser Error Message: Access is denied: ' WSRPProxyPage '

Symptoms—When you access a page after an AppDomain load—for example, when you modify the `Bin` directory or the `Web.config` file on computers running Microsoft Index Services—this error message is displayed:



```
Server Error in '/ HyperionWebPartProxyPage Application

Configuration Error

Description: An error occurred during the processing of a configuration file required to
service this request. Please review the specific error details below and modify your
configuration file appropriately.

Parser Error Message: Access is denied: ' HyperionWebPartProxyPage'.

Source Error:
Line 169:   <add assembly=<System.Drawing, Version= 1.0.3300.0, Culture=neutral,
PublicKeyToken=b03f5f7f11d50a3a>/>
Line 170:   <add assembly=<System.EnterpriseServices, Version= 1.0.3300.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a>/>
Line 171:   <add assembly=<*>/>
Line 172:   </assemblies>
```

Cause—If you run Index Server (`Cisvc.exe`), then Index Server may rescan the `Temporary ASP.NET Files` directory while it requests a Microsoft ASP.NET page. `Cisvc.exe` then holds a lock on the `Temporary ASP.NET Files` directory for 1 to 5 minutes, depending on the size of the directory that causes the `Aspnet_wp.exe` process (or `W3wp.exe` process for applications that run on IIS 6.0) not to load the particular DLL.

Resolution—If you do not use Index Server on the server, you can disable it.

➤ To disable Index Server:

1 Click **Start**, and then click **Services.**

2 Locate **Indexing Service** in the list of services, and then click **Indexing Service Properties** from the subform.

3 On the **General** tab of the **Indexing Service Properties** dialog box, in the **Startup type** drop-down list, click **Disabled.**

4 Click **OK.**

If you use Index Server, you can exclude the `Temporary ASP.NET Files` directory from the folders that the Index Server scans.

➤ To exclude the `Temporary ASP.NET Files` directory Index Server scanning

1 Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Computer Management.**

2 Expand the **Services and Applications** node, expand the **Indexing Service** node, and then expand the **System** node.

3 Right-click the **Directories** folder, point to **New**, and then click **Directory** from the subform to open the Add Directory dialog box.

4 Click **Browse**, and then locate the Temporary ASP.NET Files directory. You typically find the Temporary ASP.NET files in the following path:

```
c:\<WINDIR>\Microsoft.NET\Framework\<Version Number>\Temporary
ASP.NET Files
```

Note: <Version Number> is the version of .NET Framework installed on your computer.

5 Click **No** under the **Include in Index?**

6 Click **OK.**

7 Close the **Computer Management** dialog box.

8 Restart the Indexing Services service.

SharePoint Single Sign-On Error on Windows Server 2003 SP1

Symptoms—When you trying to configure Server Settings for SSO, this error message is displayed:

"Failed to connect to the database server. Verify connectivity and rights for the configuration account and try again."

Cause—This problem occurs because Windows Installer 3.1 is installed when you apply Windows Server 2003 SP1.

Resolution

➤ To resolve this error:

1 **Run** `regedit`**.**

2 **Find the ImagePath registry entry at this location:**

```
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\ssosrv
```

3 **Remove the quotation strings from around the ImagePath value.**

4 **Restart Microsoft Single Sign-On service.**

5 SharePoint Portal 2007 Setup

In This Chapter

Hyperion WebPart and Microsoft SharePoint Portal 2007 75
Installing the EPM System WebPart Application (SharePoint Portal 2007) 77
Updating the Hyperion WebPart Application (SharePoint Portal 2007) 90
Removing Hyperion WebPart....91
SSL Support: SharePoint Portal 2007 93
Support Activities (SharePoint Portal 2007) 94
Tips and Troubleshooting: SharePoint Portal 2007....94

Hyperion WebPart and Microsoft SharePoint Portal 2007

Hyperion WebPart is a Web-based solution for working with EPM System content in a Microsoft SharePoint portal. This chapter provides information about application installation, administration, and troubleshooting.

Installation Prerequisites (SharePoint Portal 2007)

Before you can install Hyperion WebPart, the following software must be installed on your computer:

- Microsoft Windows Server 2003 or later
- Microsoft Internet Information Services (IIS) 5.0 or later
- Microsoft .NET Framework 2.0
- Microsoft SQL Server 2000 Standard Edition SP3 or later
- Microsoft Windows SharePoint Services 3.0
- Microsoft SharePoint Portal 2007

A proxy page must also be created before Hyperion WebPart is installed. Oracle recommends that Hyperion WebPart be installed by the SharePoint Portal Server administrator. For more information about installation, see the SharePoint Portal Server documentation.

Installation Package Contents (SharePoint Portal 2007)

The Hyperion WebPart installation package is delivered as single archive file, HyperionWebPart2007.zip. The file contains these folders and files:

- HyperionWebPart folder
  - HyperionWebPartDeployment.CAB—Microsoft SharePoint deployment file for Hyperion WebPart
  - HyperionWebPartCredentialsManagerDeployment.CAB—-Microsoft SharePoint deployment file for Hyperion WebPart Credentials Manager
  - HyperionWebPartWebPart_DB_Create.sql—Script for creating database
  - HyperionWebPartWebPart_DB_Update.sql—Script for updating database
  - HyperionWebPartPWebPart_DB_Delete.sql—Script for removing database
  - AddWebPart.bat—Utility that automates WebPart deployment
  - RemoveWebPart.bat—Utility that automates WebPart removal
  - UpdateWebPart.bat—Utility that automates WebPart updates
- HyperionWebPartProxyPage folder
  - Web.config—Hyperion WebPart ProxyPage Web application configuration file
  - ProxyManager.asmx—Web service for internal data processing
  - Global.asax—Hyperion WebPart ProxyPage Web application file pointing to application logic implementation
  - ErrorList.xml—Error definitions for logging
  - WarningsList.xml—Warning definitions for logging
  - HyperionWebPartProxyPage_deploy.dll—HyperionWebPartProxyPage Web application assembly file containing the logic and code for Hyperion WebPart, to be installed on a site server
- HyperionWebPartLogInstaller: WebPartLogInstaller.dll—Assembly file containing the logic and code of Hyperion WebPart log, to be installed on a site server
- HyperionWebPartResourceHttpHandler
  - Global.asax— Hyperion WebPart ResourceHttpHandler Web application file pointing to application logic implementation
  - Web.config—Hyperion WebPart ResourceHttpHandler configuration file
  - HyperionWebPartResourceHttpHandler_deploy.dll—Hyperion WebPart ResourceHttpHandler assembly file containing the logic and code of Hyperion WebPart, to be installed on a site server

Installing the EPM System WebPart Application (SharePoint Portal 2007)

To install the Hyperion WebPart application, you must extract the `HyperionWebPart2007.zip` file to a location on your SharePoint Portal server instance. You must also Ensure that SQL Server and Windows Authentication mode is enabled on the SQL server hosting the HyperionWebPart_Cache database.

These additional installation tasks must be completed:

- Add the server hosting SharePoint Portal 2007 to the Local Intranet in the Internet Explorer security settings. (Otherwise, you might encounter an “Invalid index” message while browsing the repository in Internet Explorer).
- Uninstall the Enhanced Security Configuration from Windows 2003 clients (to prevent double-logon issues).

You must also complete these tasks, which this section describes:

- Configuring single sign-on (SSO)
- Installing Hyperion WebPart ProxyPage
- Installing Hyperion WebPart ResourceHttpHandler
- Customizing the database creation script
- Updating `Web.config`
- Installing Hyperion WebPart for the SharePoint portal
- Customizing Hyperion Web Part `app.config` (optional)
- Configuring default permissions for Hyperion WebPart

Configuring Single Sign-On (SharePoint Portal 2007)

You can configure Hyperion WebPart for Microsoft SSO or SiteMinder SSO.

Configuring Hyperion WebPart for Microsoft SSO (SharePoint Portal 2007)

Before configuring Hyperion WebPart for Microsoft SSO, you must configure the Microsoft Single Sign-On service. See the Microsoft Online Reference for instructions.

Note: See “Tips and Troubleshooting: SharePoint Portal 2003” on page 68 if you encounter error messages during SSO configuration.

The Hyperion WebPart stores two types of credentials:

- Persistent credentials are stored in the SSO database and used every time user accesses the portal page, so there is no need to reenter them.

Note: You can use Hyperion WebPart Credentials Manager or SharePoint Portal Server Single Sign-On Administration to change user credentials.

- Nonpersistent credentials are used when user clears the “Remember me” check box in Hyperion WebPart Credentials Manager. The credentials expire at the end of the current session.

You can customize these parameters in Hyperion WebPart:

- Application name used for storing persistent credentials (Default: HyperionReportingAndAnalysis
- Application name used for storing nonpersistent credentials (Default: HyperionReportingAndAnalysisTemp

Note: If you customize parameters, you must modify the `Web.config` file in the `HyperionWebPartProxyPage` folder accordingly.

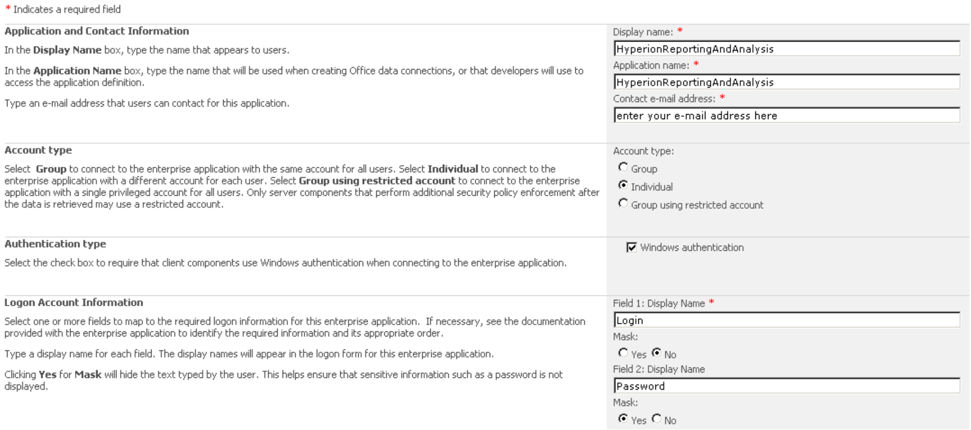
➤ To customize parameters in Hyperion WebPart:

1 Define an application name to store persistent credentials. (Default: HyperionReportingAndAnalysis

2 In the **Component Configuration** section of **SharePoint Portal Server Central Administration**, click **Manage settings for single sign-on.**

3 In the **Enterprise Application Definition Settings** section, click **Manage settings for enterprise application definitions**, and then click **New Item.**

4 Using the following figure as a guide, add the new enterprise application definition for persistent credentials. See the “Enterprise Application Manager Account” section of Microsoft Online Reference.



* Indicates a required field

Application and Contact Information

In the **Display Name** box, type the name that appears to users.

In the **Application Name** box, type the name that will be used when creating Office data connections, or that developers will use to access the application definition.

Type an e-mail address that users can contact for this application.

Display name: *
HyperionReportingAndAnalysis

Application name: *
HyperionReportingAndAnalysis

Contact e-mail address: *
enter your e-mail address here

Account type

Select **Group** to connect to the enterprise application with the same account for all users. Select **Individual** to connect to the enterprise application with a different account for each user. Select **Group using restricted account** to connect to the enterprise application with a single privileged account for all users. Only server components that perform additional security policy enforcement after the data is retrieved may use a restricted account.

Account type:
○ Group
● Individual
○ Group using restricted account

Authentication type

Select the check box to require that client components use Windows authentication when connecting to the enterprise application.

☑ Windows authentication

Logon Account Information

Select one or more fields to map to the required logon information for this enterprise application. If necessary, see the documentation provided with the enterprise application to identify the required information and its appropriate order.

Type a display name for each field. The display names will appear in the logon form for this enterprise application.

Clicking **Yes** for **Mask** will hide the text typed by the user. This helps ensure that sensitive information such as a password is not displayed.

Field 1: Display Name *
Login

Mask:
○ Yes ● No

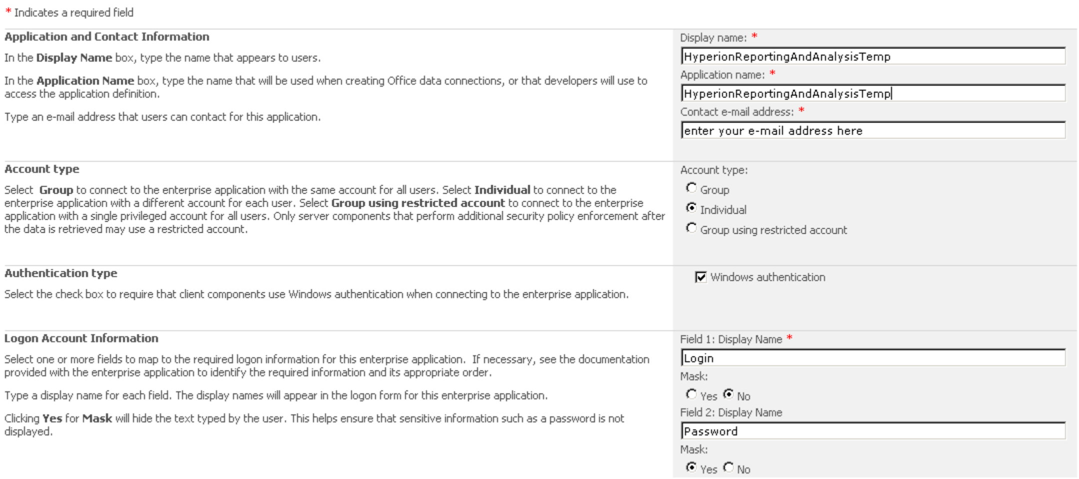
Field 2: Display Name
Password

Mask:
● Yes ○ No

5 Define an application name to store nonpersistent credentials. (Default: HyperionReportingAndAnalysisTemp

6 Repeat step 2 and step 3.

7 Using the following figure as a guide, add the new enterprise application definitions for nonpersistent credentials. See the “Enterprise Application Manager Account” section of Microsoft Online Reference.



* Indicates a required field

Application and Contact Information

In the **Display Name** box, type the name that appears to users.

In the **Application Name** box, type the name that will be used when creating Office data connections, or that developers will use to access the application definition.

Type an e-mail address that users can contact for this application.

Display name: *
HyperionReportingAndAnalysisTemp

Application name: *
HyperionReportingAndAnalysisTemp

Contact e-mail address: *
enter your e-mail address here

Account type

Select **Group** to connect to the enterprise application with the same account for all users. Select **Individual** to connect to the enterprise application with a different account for each user. Select **Group using restricted account** to connect to the enterprise application with a single privileged account for all users. Only server components that perform additional security policy enforcement after the data is retrieved may use a restricted account.

Account type:
○ Group
● Individual
○ Group using restricted account

Authentication type

Select the check box to require that client components use Windows authentication when connecting to the enterprise application.

☑ Windows authentication

Logon Account Information

Select one or more fields to map to the required logon information for this enterprise application. If necessary, see the documentation provided with the enterprise application to identify the required information and its appropriate order.

Type a display name for each field. The display names will appear in the logon form for this enterprise application.

Clicking **Yes** for **Mask** will hide the text typed by the user. This helps ensure that sensitive information such as a password is not displayed.

Field 1: Display Name *
Login
Mask:
○ Yes ● No

Field 2: Display Name
Password
Mask:
● Yes ○ No

Configuring Hyperion WebPart for SiteMinder SSO (SharePoint Portal 2007)

Hyperion WebPart can use SiteMinder for external authentication. It must pass specific HTTP headers received from the Web server to the Hyperion application server. To prevent sensitive data interception, use either or both of these approaches:

- Producer and consumer should be within the same secure LAN, which is inaccessible to external insecure clients.
- Both producer and consumer should use SSL/HTTPS.

For more information on configuring SiteMinder on IIS, see the SiteMinder installation documentation.

Installing the Hyperion WebPart ProxyPage Web Application (SharePoint Portal 2007)

This section describes how to deploy the Hyperion WebPart Proxy Page Web application to IIS. Hyperion WebPartProxyPage Web Application and Hyperion WebPart ResourceHttpHandler should be installed on the same server as your instance of Microsoft SharePoint portal.

➤ To install the HyperionWebPart ProxyPage Web application:

1 **Open the SharePoint Portal `web.config` file in a text editor, make these changes, and then save the modified file:**

   - In the `<system.web>` section, set `<trust level="Full" originUrl="" />`.
   - Replace this section:

     ```
     <sessionState mode="SQLServer" timeout="60"

     allowCustomSqlDatabase="true"

     partitionResolverType="Microsoft.Office.Server.Administration.
     SqlSes
     ```

```
sionStateResolver, Microsoft.Office.Server, Version=12.0.0.0,

Culture=neutral, PublicKeyToken=71e9bce111e9429c" />
```

with this section:

```
sessionState mode="InProc"

stateConnectionString="tcpip=127.0.0.1:42424"

sqlConnectionString="data source=127.0.0.1;

Trusted_Connection=yes"

cookieless="false"

timeout="15"
```

- Comment the following line in the <httpModules> section:

```
<!-- <add name="PublishingHttpModules"

type="Microsoft.SharePoint.Publishing.PublishingHttpModules,

Microsoft.SharePoint.Publishing, Version=12.0.0.0,
Culture=neutral,

PublicKeyToken=71e9bce111e9429c" /> -->
```

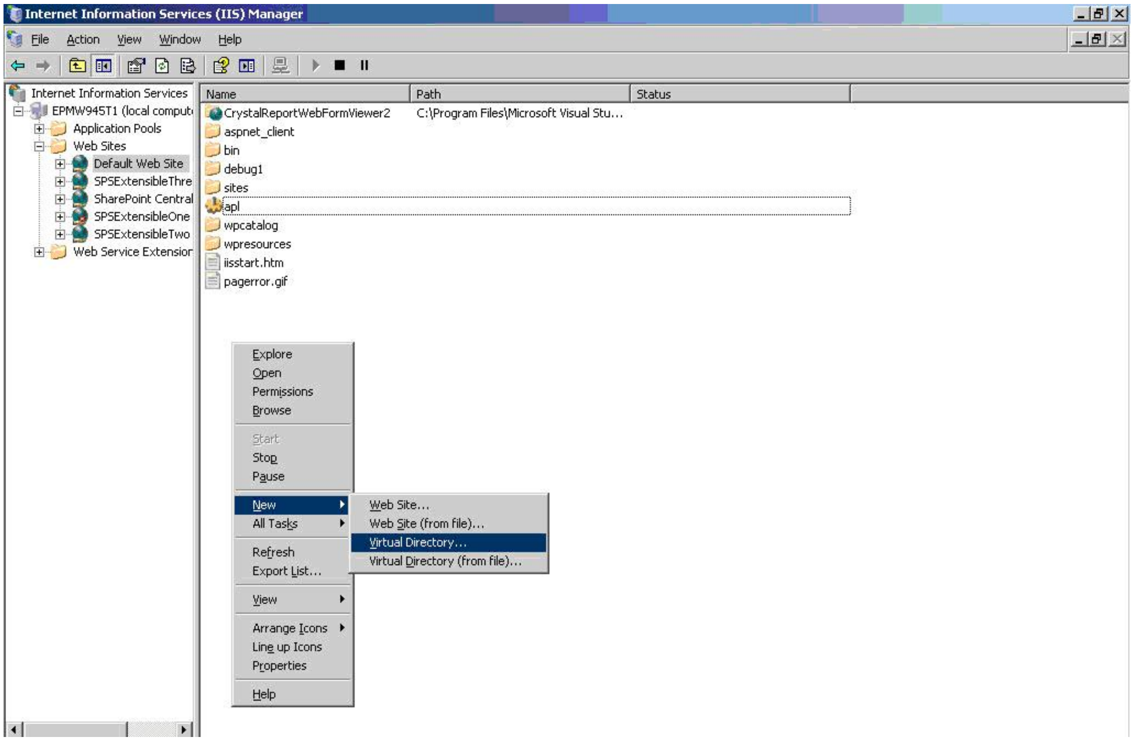
2 **Define a folder to store the Hyperion WebPart application, and extract the contents of the** `HyperionWebPart2007.zip` **file into that folder.** `HyperionWebPartProxyPage` **and** `HyperionWebPartResourceHttpHandler` **subfolders store physical contents of respective web applications.**

3 **Run to Internet Information Services Manager.**

4 **Choose the site used to run your instance of SharePoint Portal 2007.**

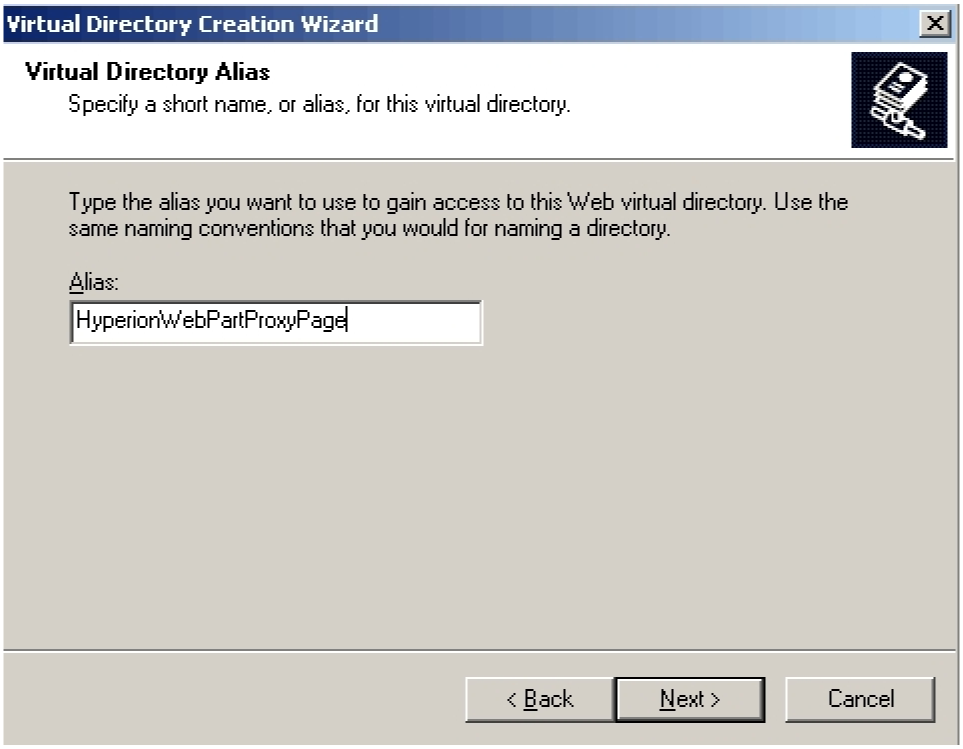
Note: if you have more than SharePoint Portal 2007 instance, repeat step 1, step 3-step 12, and step 22–step 26 of this procedure for each instance.

5 **Create a virtual folder to work with the** `HyperionWebPartProxyPage` **physical folder that you created in step 2.**



Name	Path	Status
CrystalReportWebFormViewer2	C:\Program Files\Microsoft Visual Stu...	
aspnet_client		
bin		
debug1		
sites		
apl		
wpcatalog		
wpresources		
iisstart.htm		
pagerror.gif		

6 Define a virtual folder alias using the following figure as a guide, and then click **Next.**



Virtual Directory Alias

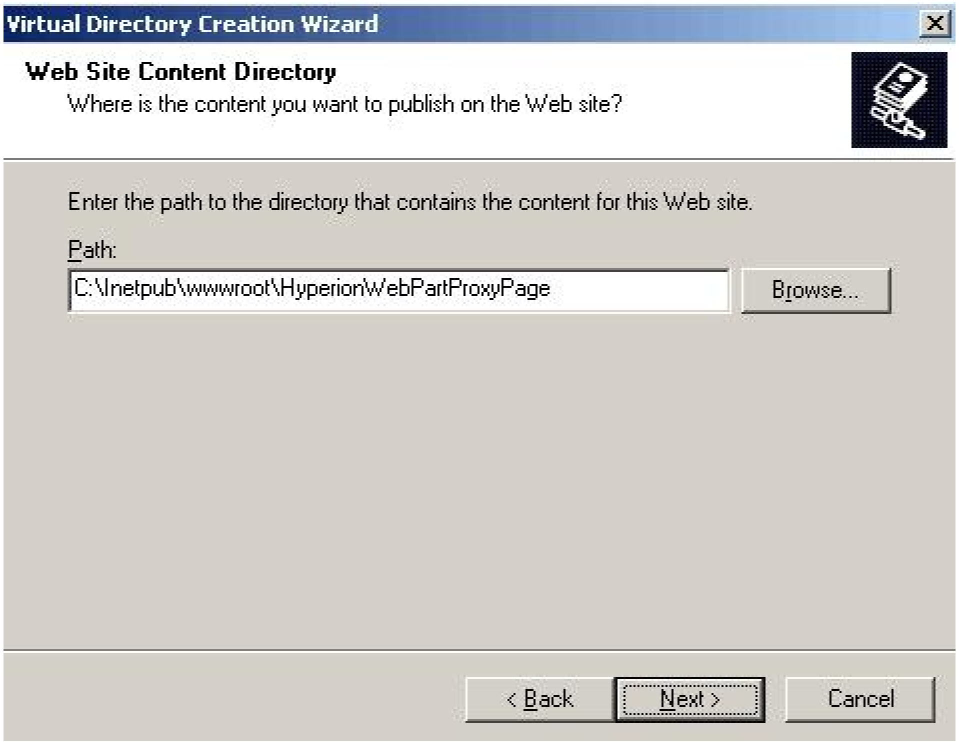
Specify a short name, or alias, for this virtual directory.

Type the alias you want to use to gain access to this Web virtual directory. Use the same naming conventions that you would for naming a directory.

Alias:

HyperionWebPartProxyPage

7 Specify the path for the application folder that matches the folder name you defined in step 2 on page 80, and then click **Next.**



Virtual Directory Creation Wizard

Web Site Content Directory

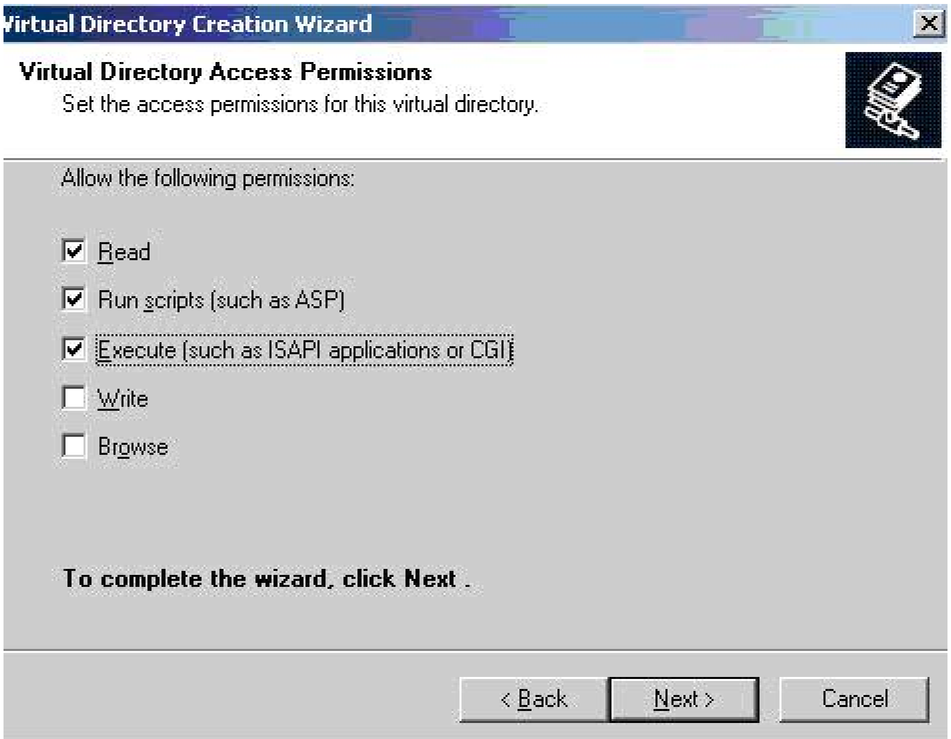
Where is the content you want to publish on the Web site?

Enter the path to the directory that contains the content for this Web site.

Path:

C:\Inetpub\wwwroot\HyperionWebPartProxyPage

8 Set access permissions, as shown in the following figure, and then click **Next.**



Virtual Directory Creation Wizard

Virtual Directory Access Permissions

Set the access permissions for this virtual directory.

Allow the following permissions:

☑ Read

☑ Run scripts (such as ASP)

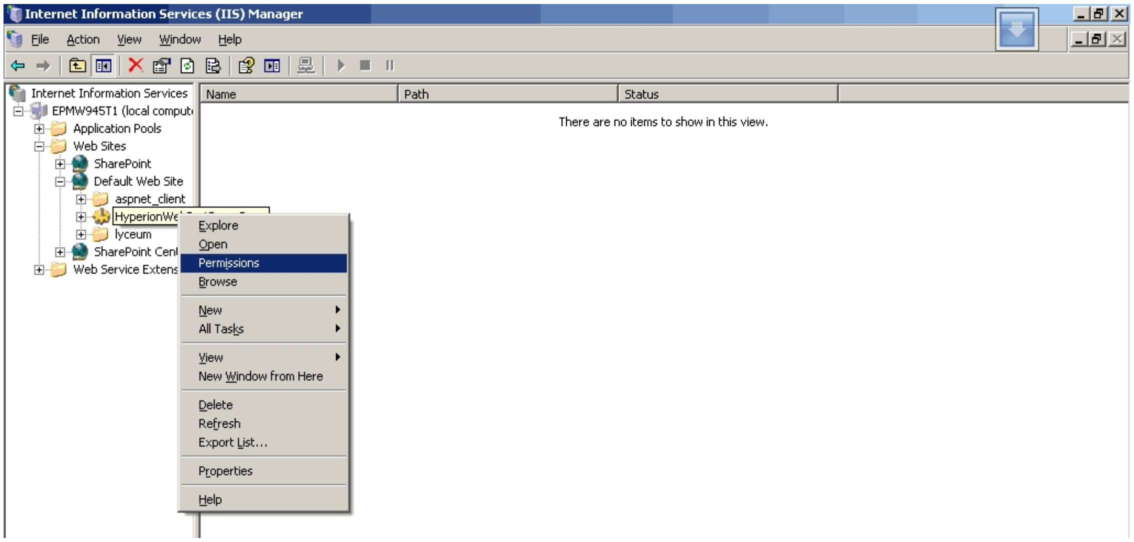
☑ Execute (such as ISAPI applications or CGI)

☐ Write

☐ Browse

To complete the wizard, click Next .

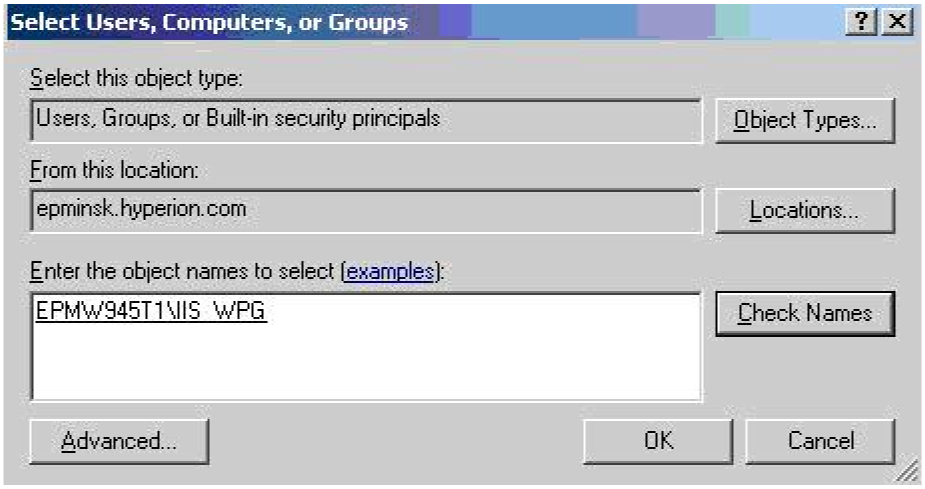
9 Right-click **HyperionWebPartProxyPage**, and select **Permissions.**



There are no items to show in this view.

10 Click **Add.**

11 Enter **SHAREPOINT_PORTAL_HOSTNAME\IIS_WPG**, click **OK**, and change **SHAREPOINT_PORTAL_HOSTNAME** to the name of the host where SharePoint is installed.

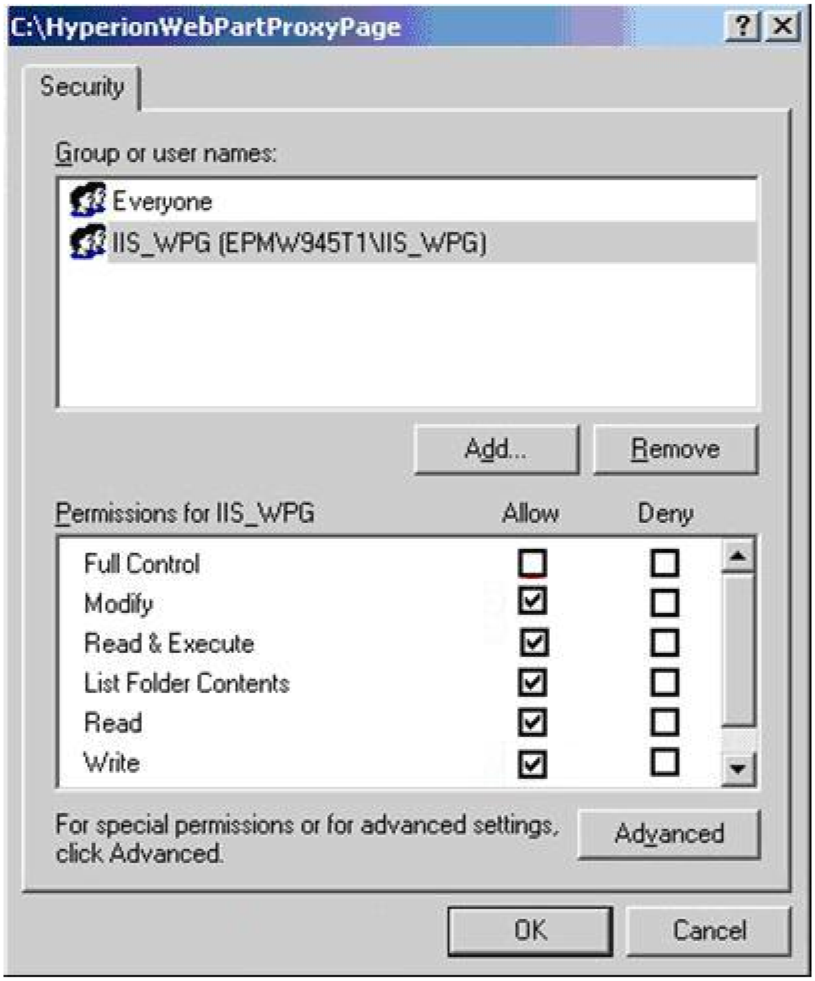


Select this object type:
Users, Groups, or Built-in security principals

From this location:
epminsk.hyperion.com

Enter the object names to select (examples):
EPMW945T1\IIS_WPG

12 Set permissions for the user as shown in the following figure, and click **OK.**



Group or user names:

- Everyone
- IIS_WPG (EPMW945T1\IIS_WPG)

Permissions for IIS_WPG	Allow	Deny
Full Control	□	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□

For special permissions or for advanced settings, click Advanced.

13 Open a Command Prompt, and use it to change to the directory that contains the `Adsutil.vbs` file. By default, the file is in `C:\Inetpub\Adminscripts`.

14 Type the following command, and then press **Enter**: `cscript adsutil.vbs set w3svc/NTAuthenticationProviders "NTLM"`

15 Select **Run** from the **Start** menu, type **regedit**, and then click **OK**.

16 In Registry Editor, click this registry key: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0**

17 Right-click **MSV1_0**, select **New**, and then click **Multi-String Value**.

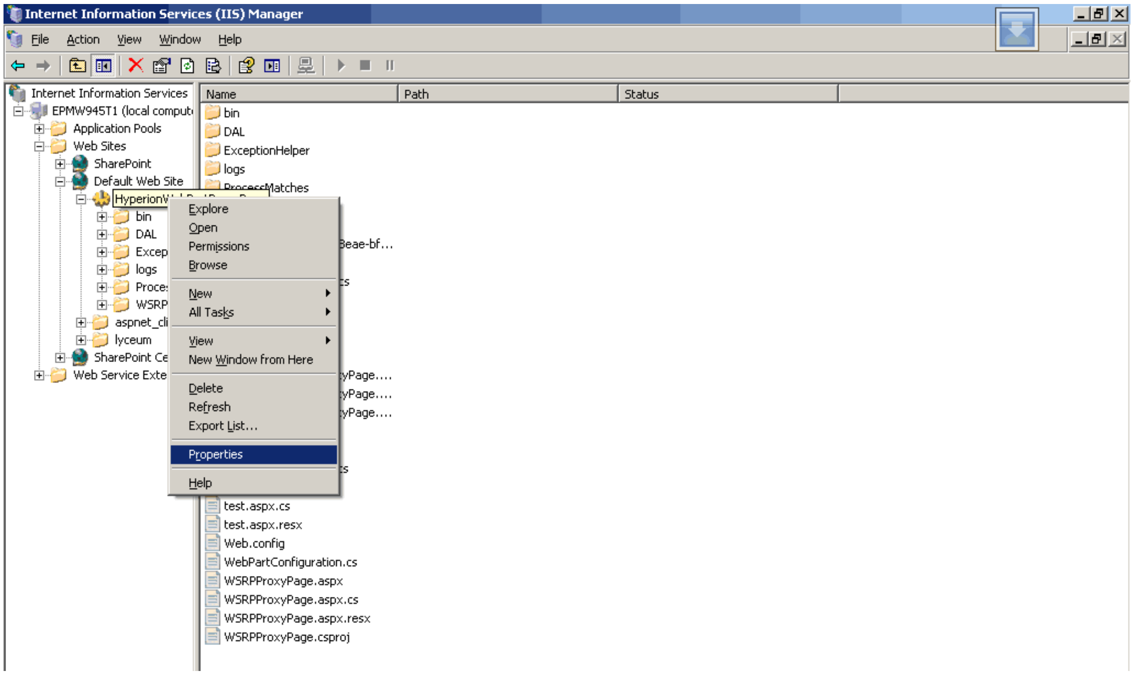
18 Type **BackConnectionHostNames**, and then press **Enter**.

19 Right-click **BackConnectionHostNames**, and then click **Modify**.

20 In the **Value** box, type the full host name of the server where SharePoint Portal is installed, and then click **OK**.

21 Quit Registry Editor, and then restart the IISAdmin service.

22 Navigate to HyperionWebPartProxyPage properties, as shown on the following figure.



23 Click the **Virtual Directory** tab,

24 Click **Edit** in the **Authentication and access control** section on the **Directory Security** tab.

25 In Authentication Methods, select an access option:**Enable anonymous access** is not selected, and if you are using Hyperion WebPart Microsoft SSO, ensure that **Integrated Windows authentication** is selected . Alternatively, ensure that anonymous access is enabled (upper check box must be selected) and Integrated Windows authentication enabled if are using SiteMinder SSO.

- For HyperionEPM System WebPart Microsoft SSO, clear Enable anonymous access and select Integrated Windows authentication.
- For SiteMinder SSO, select **Enable anonymous access** and **Integrated Windows authentication**.

26 Add the URL of the server where HyperionWebPartProxyPage is installed to Local Intranet zone in your client browser.

Installing Hyperion WebPart ResourceHttpHandler (SharePoint Portal 2007)

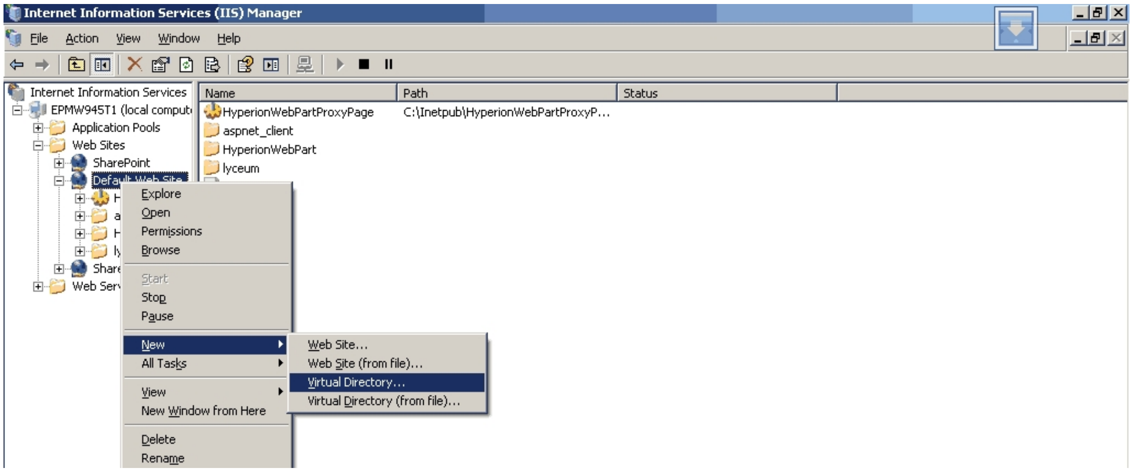
Complete the following procedure for each instance of SharePoint Portal 2007.

➤ To install Hyperion WebPart ResourceHttpHandler:

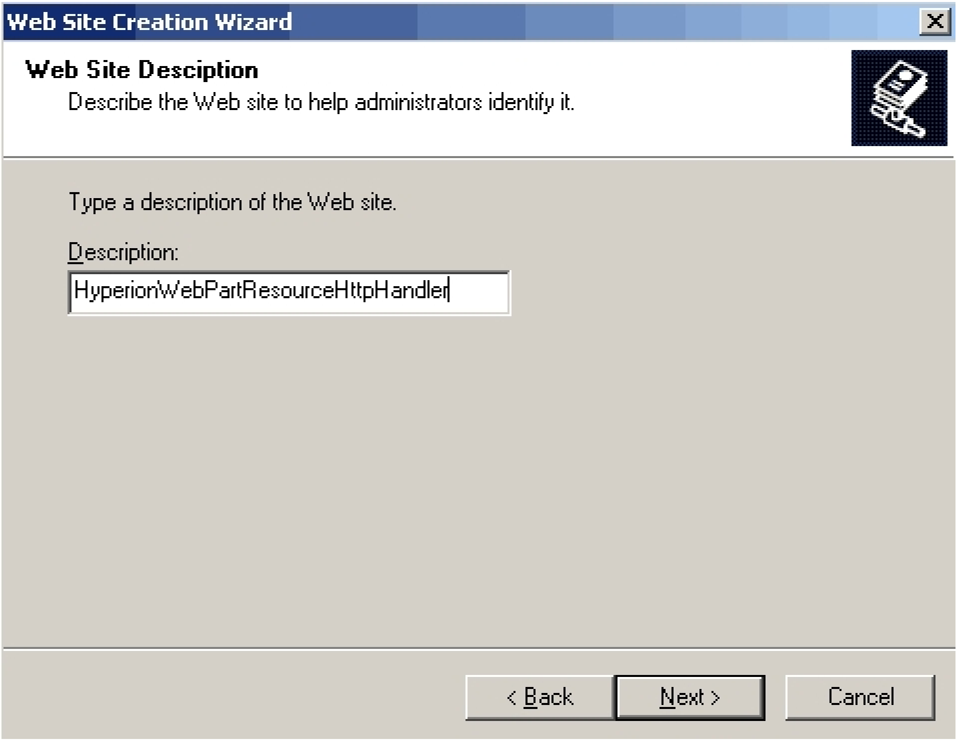
1 Run to Internet Information Services Manager.

2 Select the site that is used to run your instance of SharePoint Portal 2007.

3 Create a virtual folder to work with the `Hyperion WebPart ResourceHttpHandler` physical folder that you created in step 2 on page 80.



4 Define a virtual folder alias using the following figure as a guide, and click **Next.**



Web Site Creation Wizard

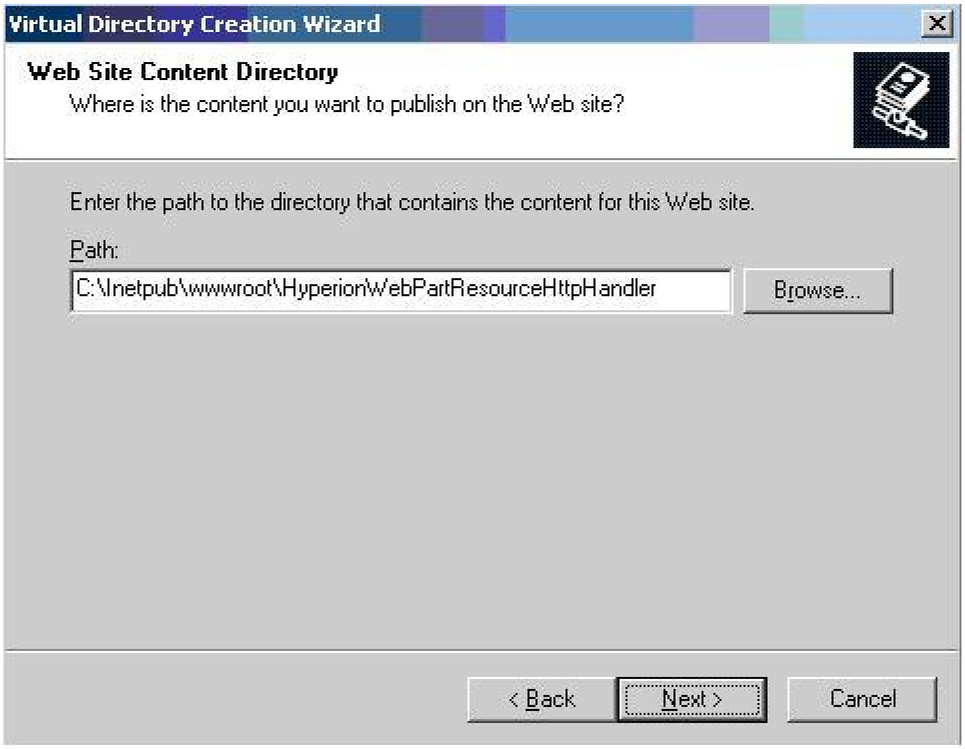
Web Site Desciption

Describe the Web site to help administrators identify it.

Type a description of the Web site.

Description: HyperionWebPartResourceHttpHandler

5 Point to the application folder that you defined in step 2 on page 80, and click **Next.**



Virtual Directory Creation Wizard

Web Site Content Directory

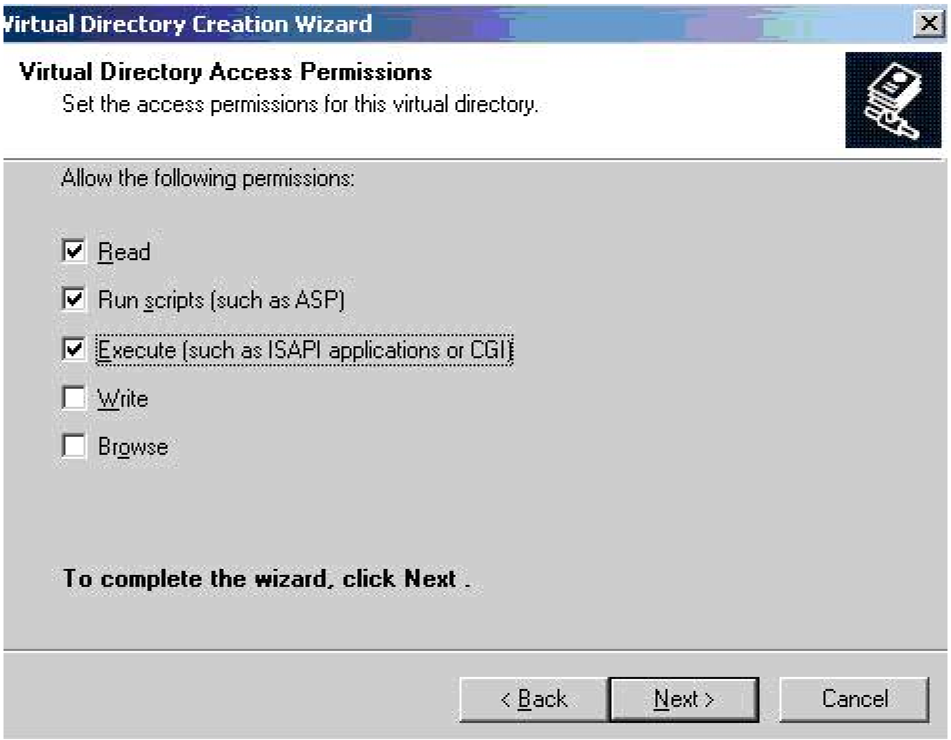
Where is the content you want to publish on the Web site?

Enter the path to the directory that contains the content for this Web site.

Path:

C:\Inetpub\wwwroot\HyperionWebPartResourceHttpHandler

6 Set access permissions as shown in the following figure.



Virtual Directory Creation Wizard

Virtual Directory Access Permissions

Set the access permissions for this virtual directory.

Allow the following permissions:

☑ Read

☑ Run scripts (such as ASP)

☑ Execute (such as ISAPI applications or CGI)

☐ Write

☐ Browse

To complete the wizard, click Next .

Customizing the Database Creation Script (SharePoint Portal 2007)

You can customize these parameters in the HyperionWebPart database creation script:

- Database name (Default: HyperionWebPart_Cache)

If you use custom parameters, you must modify the `Web.config` file in the `HyperionWebPartProxyPage` folder accordingly.

➤ To customize database script parameters:

1 Open `HyperionWebPart_DB_Create.sql` in a text editor.

2 Replace all occurrences of `HyperionWebPart_Cache` with a custom name.

Installing WebPart for SharePoint Portal 2007

Note: Update the Web.config file before beginning this procedure. See "Updating Web.config (SharePoint Portal 2007)" on page 88.

➤ To install WebPart for the SharePoint portal:

1 Add the path to your version of Microsoft .NET framework to the system PATH variable.

2 Run `AddWebPart.bat`. You need to specify SQL Server host name, SQL Server administrator name and password, custom user name and password to use for Hyperion WebPart database (they should match ones you provided in Web.config files)..

3 Open the SharePoint Portal site.

4 Click **Site Actions**.

5 Select **Edit Page** on the right side.

6 Click **Add WebPart** on the right side.

7 Select Hyperion WebPart and Hyperion WebPart Credentials Manager and click **Add**.

8 Click **Exit Edit Mode**.

Updating Web.config (SharePoint Portal 2007)

For a more secure configuration, the use of use SSL connection between your instance of SharePoint Portal 2007 and your EPM System producer is recommended. See "SSL Support: SharePoint Portal 2007" on page 93.

➤ To update `Web.config`:

1 Run `decrypt.bat` if `web.config` file was encrypted previously.

2 **Using a text editor, open `Web.config` in the `HyperionWebPartProxyPage` folder and make these changes:**

- Replace all occurrences of `$GET(appServerProps.workspaceHost)` with the full host name of the EPM System WSRPProducer server.

  Note: `$GET(appServerProps.workspaceHost)` and `$GET(appServerProps.workspacePort)` entries appear in web.config file only if the WepPart 2007 package was not configured during the Reporting and Analysis build installation. (The default producer is set when EPM System Configurator installs the EPM System portlet).

- Replace all occurrences of `$GET(appServerProps.workspacePort)` with the number of port used for the EPM System WSRPProducer.
- Replace all occurrences of `SharepointHostName` with hostname:port where you instance of Hyperion WebPart ResourceHttpHandler is installed.
- Replace all occurrences of `SQLServerName` with the full host name of the MS SQL server hosting the Hyperion WebPart database. This should be the same SQL Server Name that is set during Hyperion WebPart installation.
- Change HyperionWebPart_user to the custom user name.
- Change 1#Password to the custom password.
- If you customized database creation script, change HyperionWebPart_Cache to the custom name of Hyperion WebPart database.

3 **If you customized parameters when you configured Hyperion WebPart for Microsoft SSO, make one or more of these changes to reflect the custom parameters:**

- Change `HyperionReportingAndAnalysis` to the custom name for the application.
- Change `HyperionReportingAndAnalysisTemp` to the application name that you specified for storing nonpersistent credentials.

4 **If you customized parameters when you configured Hyperion WebPart for SiteMinder SSO, replace all occurrences of `HyperionReportingAndAnalysisSiteMinderHeader` with the name of the header used for SiteMinder authentication in your instance of EPM System.**

5 **Using a text editor, open `Web.config` in the `HyperionWebPartResourceHttpHandler` folder and make these changes:**

- Replace all occurrences of `SQLServerName` with the full host name of the MS SQL server hosting the Hyperion WebPart database.
- Change `HyperionWebPart_user` to the custom user name.
- Change 1#Password to the custom password.
- If you customized database creation script, change HyperionWebPart_Cache to the custom name of Hyperion WebPart database.

6 **If you want to encrypt connection strings in `Web.Config` files, edit `Encrypt.bat` and `Decrypt.bat` by specifying actual path to `Hyperion Web Part ProxyPage` and `Hyperion Web Part ResourseHttpHandler` folders , then run `Encrypt.bat`.**

Configuring Default Permissions for EPM System WebPart (SharePoint Portal 2007)

The portal home page is shared by all portal users. If one user adds a Hyperion WebPart to the home page, other users cannot access the home page, and a warning message is displayed when they try to display it. You can prevent this by configuring default permissions for Hyperion WebPart so that users cannot add it to the home page.

➤ To configure default permissions for EPM System WebPart:

1. In your browser, open the Web Parts Maintenance Page on the Microsoft SharePoint site.
2. Enter these settings for the EPM System WSRP WebPart:
   - Open on Page?: Yes
   - Personalized?: No

Updating the Hyperion WebPart Application (SharePoint Portal 2007)

Updating the Hyperion WebPart application involves these tasks:

- Backing up your working copy of Web.config for Hyperion Web Part ProxyPage and Hyperion Web Part ResourseHttpHandler if you are uncertain about parameter changes.
- Updating physical folders of Hyperion Web Part ProxyPage and Hyperion Web Part ResourseHttpHandler
- Customizing database update script
- Updating Web.config
- Running UpdateWebPart.bat
- Updating app.config (optional)

Updating physical folders of Hyperion Web Part ProxyPage and Hyperion Web Part ResourseHttpHandler

➤ To update physical folders of Hyperion Web Part ProxyPage and Hyperion Web Part ResourseHttpHandler:

1. Replace the contents of the HyperionWebPartProxyPage folder (defined when you installed the Hyperion WebPart ProxyPage Web application) with the folder contents included in the update package.
2. Replace the contents of the HyperionWebPartResourceHandler folder (defined when you installed Hyperion WebPart ResourceHttpHandler) with the folder contents included in the update package.

Note: Back up your working copy of `Web.config` for `Hyperion WebPart` if you are uncertain about your parameter changes.

Customizing Database Update Script

➤ To customize the HyperionWebPartWebPart database update script, open HyperionWebPart_DB_Update.sql in a text editor and make these changes:

- Replace all occurrences of HyperionWebPartWebPart_Cache with your custom name.

Updating Web.config

➤ Please refer to "Updating Web.config (SharePoint Portal 2007)" on page 88. Alternatively, you can copy parameter values from your backup `Web.config` files.

Running UpdateWebPart.bat

Run `UpdateWebPart.bat`. You need to specify SQL Server host name, SQL Server administrator name and password, custom user name and password to use for `Hyperion WebPart` database (they should match ones you provided in `Web.config` files).

Updating app.config

Please refer to "Customizing Hyperion WebPart app.config (SharePoint Portal 2007)" on page 95.

Removing Hyperion WebPart

To remove Hyperion WebPart, you need to specify SQL Server host name, SQL Server administrator name and password, custom user name and password to use for Hyperion WebPart database (they should match ones you provided in `Web.config` files).

You must also remove these items:

- The Web part

  See "Removing the Hyperion Web Part (SharePoint Portal 2003)" on page 63.

- SSO data

  See "Removing SSO Data (SharePoint Portal 2003)" on page 64.

- Hyperion WebPart ResourceHttpHandler

  See "Removing Hyperion WebPart ResourceHttpHandler (SharePoint Portal 2003)" on page 65.

- Hyperion WebPart ProxyPage

  See "Removing Hyperion WebPart ProxyPage (SharePoint Portal 2003)" on page 65.

Removing the Web Part (SharePoint Portal 2007)

Be sure to close all instances of Hyperion WebPart in the portal before removing the Web part. Otherwise, users see an error message rather than the Hyperion WebPart contents.

➤ To remove the Web part, run `RemoveWebPart.bat`.

Removing SSO Data (SharePoint Portal 2007)

➤ To remove SSO data:

1 Navigate to the **SharePoint Portal Server Single Sign-On Administration** page.

2 Remove all application definitions.

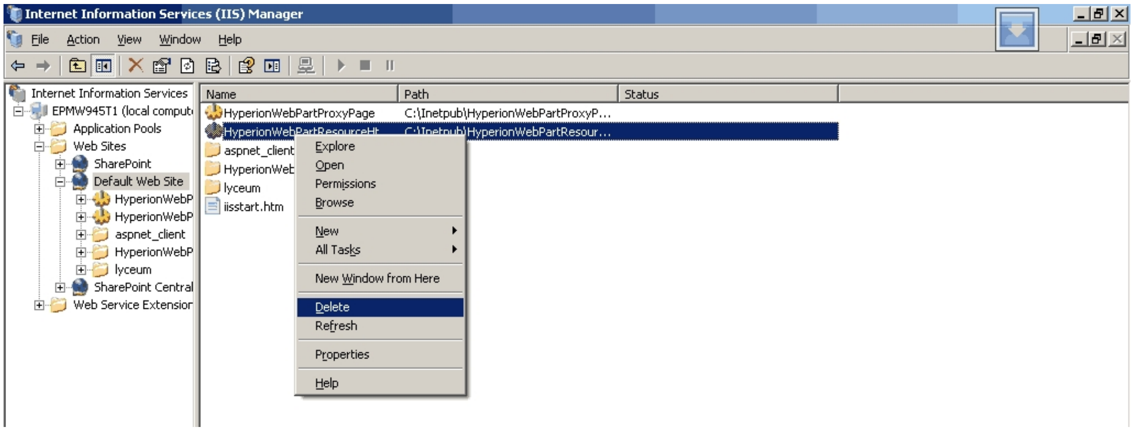
Removing Hyperion WebPart ResourceHttpHandler (SharePoint Portal 2007)

➤ To remove Hyperion WebPart ResourceHttpHandler:

1 Run Internet Information Services Manager.

2 Select **Default Web Site.**

3 Remove the **Hyperion WebPart ResourceHttpHandler** virtual folder.



4 Delete the `HyperionWebPartResourceHttpHandler` folder from your hard disk.

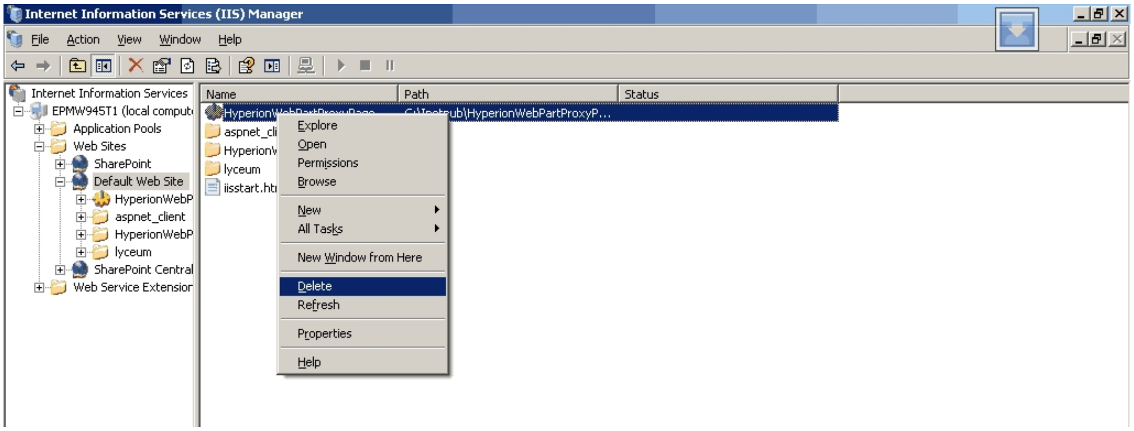
Removing Hyperion WebPart ProxyPage (SharePoint Portal 2007)

➤ To remove Hyperion WebPart ProxyPage:

1 Run Internet Information Services Manager.

2 Select **Default Web Site**.

3 Remove the **HyperionWebPartProxyPage** virtual folder.



4 **Delete the folder containing Hyperion WebPart ProxyPage from your hard disk.**

SSL Support: SharePoint Portal 2007

Using an SSL channel between your instance of SharePoint Portal 2007 and your EPM System producer requires these actions:

1. Get certificate from EPM System producer.
2. Install the certificate on the server where your instance of Microsoft SharePoint Portal is installed.
3. Change the EPM System producer URLs in `Web.config` to work over https.

   For example, change these settings:

   ```
   add key="MarkUpURL" value="http://epmsd111.epminsk.hyperion.com:
   45000/raframework/wsrp4j/WSRPBaseService" />

   <add key=PortletManagementURL”

   value="http://epmsd111.epminsk.hyperion.com:45000/raframework/
   wsrp4j/WSRPPortletManagementService" />

   <add key=RegistrationURL”

   value="http://epmsd111.epminsk.hyperion.com:45000/raframework/
   wsrp4j/WSRPRegistrationService" />

   <add key=ServiceDescription”

   value="http://epmsd111.epminsk.hyperion.com:45000/raframework/
   wsrp4j/WSRPServiceDescriptionService" />
   ```

   to these settings:

   ```
   add key="MarkUpURL" value="https://epmsd111.epminsk.hyperion.com:
   45000/raframework/wsrp4j/WSRPBaseService" />

   <add key=PortletManagementURL”
   ```

```
value="https://epmsd111.epminsk.hyperion.com:45000/raframework/
wsrp4j/WSRPPortletManagementService" />

<add key=RegistrationURL"

value="https://epmsd111.epminsk.hyperion.com:45000/raframework/
wsrp4j/WSRPRegistrationService" />

<add key=ServiceDescription"

value="https://epmsd111.epminsk.hyperion.com:45000/raframework/
wsrp4j/WSRPServiceDescriptionService" />
```

Note: In the changed settings, the values begin with “https” rather than “http.”

Support Activities (SharePoint Portal 2007)

The application is designed run unattended. However, you should perform these tasks to maintain the application:

- Database backup—The database files should be backed up regularly in accordance with the schedule described in the IT department policies. Oracle recommends full daily backup at night and several incremental backups during the day. Regular transaction log backups are also recommended.
- Disk space monitoring—As the Hyperion WebPart database grows, you must constantly monitor disk space availability on both the hard drive where system data file is located and the one where its transaction log file resides. While both files should be allowed unrestricted growth, Oracle recommends truncating the transaction log from time to time to improve performance and save the disk space. Please refer to the SQL Books Online for the detailed instructions on how to truncate the log.
- Configuration files archive—After each change in the system configuration files they should be backed up and stored in a safe location with the Hyperion WebPart version to which this configuration files belong and they should be clearly marked.

Tips and Troubleshooting: SharePoint Portal 2007

Configuring Log Storage (SharePoint Portal 2007)

You can log all errors raised in Hyperion WebPart. You can configure log storage to store logs in these locations:

- The Microsoft Windows Event Log
- Plain text `.log` file
- The Microsoft Windows Event Log and in a `.log` file

Note: If you select neither the Microsoft Windows Event Log option nor the `.log` file option, users get error messages with error codes but no additional details.

➤ To configure log storage:

1. **Using a text editor, open `Web.config` in the `HyperionWebPartProxyPage` folder.**
2. **Change the `EnableWindowsLogging` value to `true` to enable storing logs to Microsoft Windows Event Log or to `false` to disable it.**
3. **Change the `EnableFileLogging` value to `true` to enable storing logs to the `.log` file or to `false` to disable it.**
4. **To customize the `.log` file name, change the `LogFileNamePrefix` value. Default prefix: HyperionWebPart.**

   If you use the default `LogFileNamePrefix`value, log file names are in this format:

   `HyperionWebPart-mm-dd-yyyyy.log`

Customizing Hyperion WebPart app.config (SharePoint Portal 2007)

Additionally you can customize three parameters in the Hyperion WebPart app.config file:

- Hyperion WebPart ProxyPage hostname
- Hyperion WebPart ProxyPage port
- Hyperion WebPart ProxyPage virtual directory

The app.config files are stored in the /wpresources/ HyperionWebPart20/ and / wpresources/ HyperionWebPartCredentialsManager subfolders of your SharePoint portal instance. If you edit one app.config file, you must also edit the other.

➤ To customize parameters in app.config:

1. **Open app.config in a text editor.**
2. **To customize hostname, which Hyperion WebPart should use to communicate with HyperionWebPartProxyPage web application, add the following line to appSettings section: `<add key="Host" value="SomeHostName" />`, Where SomeHostName is hostname you want to use.**
3. **3. To customize port, which Hyperion WebPart should use to communicate with HyperionWebPartProxyPage web application, add the following line to appSettings section: `<add key="Port" value="SomePort" />`, Where SomePort is number of port you want to use.**
4. **4. To customize virtual directory, which Hyperion WebPart should use to communicate with HyperionWebPartProxyPage web application, add the following line to appSettings section: `<add key="RemoteDirectory" value="SomeVirtualDirectoryName" />`, Where SomeVirtualDirectoryName is virtual directory you want to use. Default value is HyperionWebPartProxyPage.**

Error Messages (SharePoint Portal 2007)

Depending on your log storage configuration, all handled exceptions are stored into Microsoft Windows Event Log or in a text file in HyperionWebPartProxyPage directory.

The following sections describe errors that are beyond the scope of Hyperion WebPart.

Hyperion WebPart Errors (SharePoint Portal 2007)

The following table lists Hyperion WebPart errors with possible causes and solutions. The possible cause and suggested solution for each error are written to the system log.

Table 4

Message Displayed	Possible Cause	Suggested Solution
Error #100: Unknown error occurred. Please contact your portal administrator.	The access credentials that you entered are incorrect, or the database does not exist.	Ensure that the database exists and that the access credentials you entered are valid.
Error #101: WebPart is not configured properly. Please contact your portal administrator.	The access credentials that you entered are invalid, or the database does not exist.	Ensure that the database exists and that the access credentials you entered are valid.
Error #102: The credentials provided are invalid. Please enter valid credentials using WebPart Credentials Manager.	The credentials that you entered are invalid.	Enter valid credentials using WebPart Credentials Manager.
Error #103: WebPart is not configured properly. Please contact your portal administrator.	The `proxymanager.asmx` file does not exist or has incorrect access permissions.	● Ensure that `proxymanager.asmx` exists. ● Set correct access permissions.
Error #104: The portlet service is unavailable. Please contact your portal administrator.	WebPart settings are invalid, or producer services are stopped.	Check your producer connection settings.
Error #105: No credentials found. Please enter credentials using WebPart Credentials Manager, or contact your portal administrator.	Single Sign-On service is stopped or is not configured, or credentials for the current user were not found.	● Restart Microsoft Single Sign-On service. ● Configure SSO in SharePoint Portal Server Central Administration. ● Check the current user's credentials.

Message Displayed	Possible Cause	Suggested Solution
Error #106: WebPart is not configured properly. Please contact your portal administrator.	WebPart or the database is out of date.	Reinstall all Hyperion WebPart components.
Error #107: WebPart doesn't work properly. Please, contact your portal administrator.	The portlet handle is invalid.	Ensure that the portlet handle is valid.
Error #108: WebPart is not configured properly. Please contact your portal administrator.	SSO system is not configured.	● Disable anonymous access to the `HyperionProxyPage` folder to use Microsoft Single Sign-On. ● Ensure that SiteMinder SSO system is configured properly.
Error #109: WebPart is not configured properly. Please contact your portal administrator.	The SSL certificate on the consumer side is not installed.	Install a valid SSL certificate.
Error #110: WebPart does not work as expected. Please contact your portal administrator.	User has not enough permission to write to Windows Event Log, or Event Log does not exist.	Check User permissions and Event Log existence.
Error #111: WebPart does not work as expected. Please contact your portal administrator.	User does not have permission to write to `logs` subfolder of HyperionWebPartProxyPage, or the `logs` subfolder does not exist.	Check User permissions and existence of the `logs` folder.
Error #112: WebPart does not work as expected. Please contact your portal administrator.	Database size exceeded the limit.	Uninstall and reinstall Hyperion WebPart.
Error #113: WebPart cannot be removed from this page.	User does not have enough permission.	Contact your portal administrator.
Error #114: Could not load LoginForm.ascx.	LoginForm.ascx file not found.	Check LoginForm.ascx availability. Refer to Administration Guide for more details.
Error #115: Validation of one or more parameters failed.	Parameters used are not correct.	Check if producer works.

Other Error Messages (SharePoint Portal 2007)

The following errors are beyond the scope of Hyperion WebPart.

Writing to Event Log Error

Symptoms — When you trying to use HyperionWebPart, you get error message: " Error #110: WebPart does not work as expected. Please contact your portal administrator."

Cause — User does not have permissions or Event Log is full.

➤ To resolve this error:

1. **Check whether Event Log is full. If full, clear Event Log.**
2. **If not, run** `regedit`**.**
3. **Find the** `CustomSD` **registry entry at this location:** `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\WSRPWebPart`
4. **Add** `(A;;0x3;;;AU)` **to the end of** `CustomSD` **value data.**

System.Security.SecurityException: Request for the permission of type System.Net.WebPermission failed.

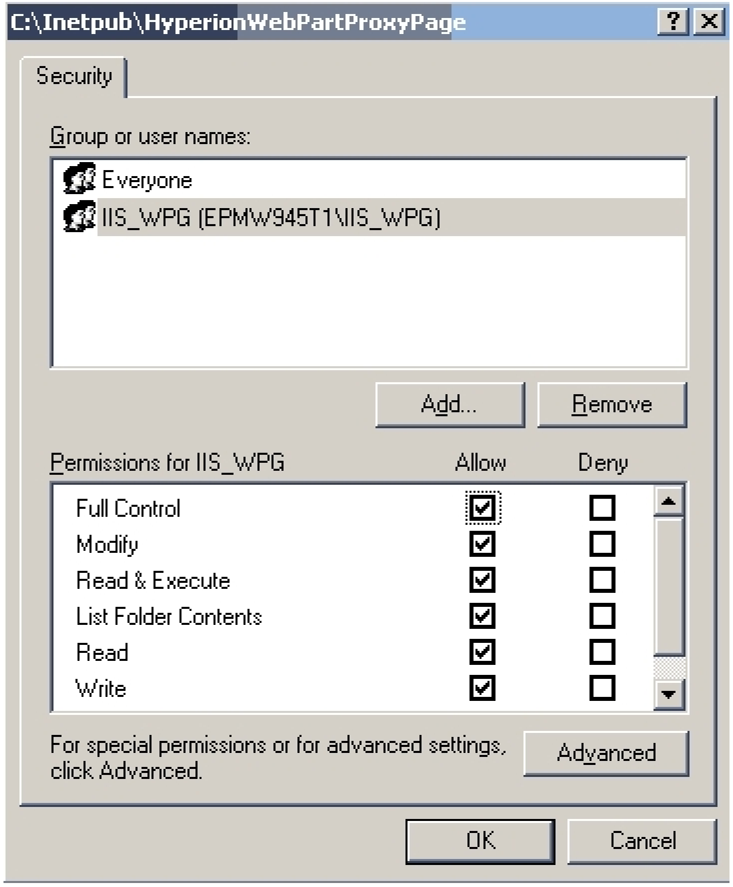
Symptoms—When you try to render Hyperion WebPart, you receive the following exception:

```
System.Security.SecurityException: Request for the permission of type
System.Net.WebPermission, System, Version=1.0.5000.0, Culture=neutral,
PublicKeyToken=b77a5c561934e089 failed.
```

Cause—Hyperion WebPart does not have permission to create Hyperion WebPart ProxyPage.

Resolution

- Open the SharePoint Portal `web.config` file for editing. Go to section `<system.web>`. Set `<trust level="Full" originUrl="" />`. Save your changes.
- Navigate to the `Hyperion WebPart ProxyPage` folder. Set IIS_WPG user permissions for the `Hyperion WebPart ProxyPage` folder as shown on the following figure.



Group or user names:

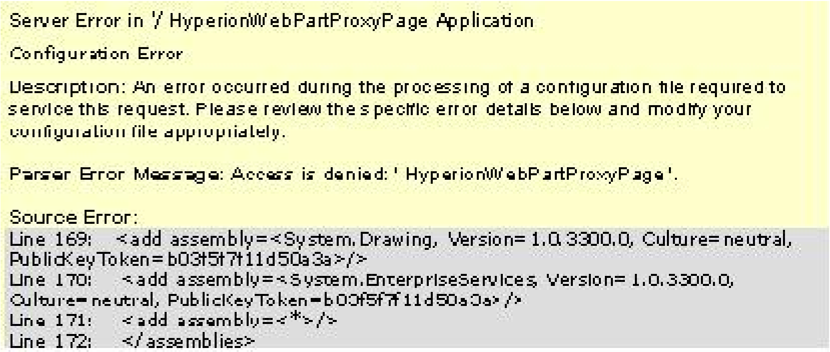
- Everyone
- IIS_WPG (EPMW945T1\IIS_WPG)

Permissions for IIS_WPG	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□

For special permissions or for advanced settings, click Advanced.

Server Error in '/HyperionWebPartProxyPage' Application. Parser Error Message: Access is denied: ' WSRPProxyPage '

Symptoms—When you access a page after an AppDomain load—for example, when you modify the `Bin` directory or the `Web.config` file on computers running Microsoft Index Services—this error message is displayed:



```
Server Error in '/ HyperionWebPartProxyPage Application

Configuration Error

Description: An error occurred during the processing of a configuration file required to
service this request. Please review the specific error details below and modify your
configuration file appropriately.

Parser Error Message: Access is denied: ' HyperionWebPartProxyPage'.

Source Error:
Line 169:   <add assembly=<System.Drawing, Version=1.0.3300.0, Culture=neutral,
PublicKeyToken=b03f5f7f11d50a3a>/>
Line 170:   <add assembly=<System.EnterpriseServices, Version=1.0.3300.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a>/>
Line 171:   <add assembly=<*>/>
Line 172:   </assemblies>
```

Cause—If you run Index Server (`Cisvc.exe`), then Index Server may rescan the `Temporary ASP.NET Files` directory while it requests a Microsoft ASP.NET page. `Cisvc.exe` then holds a lock on the `Temporary ASP.NET Files` directory for 1 to 5 minutes, depending on the size of the directory that causes the `Aspnet_wp.exe` process (or `W3wp.exe` process for applications that run on IIS 6.0) not to load the particular DLL.

Resolution—If you do not use Index Server on the server, you can disable it.

➤ To disable Index Server:

1. Click **Start**, and then click **Services.**
2. Locate **Indexing Service** in the list of services, and then click **Indexing Service Properties** from the subform.
3. On the **General** tab of the **Indexing Service Properties** dialog box, in the **Startup type** drop-down list, click **Disabled.**
4. Click **OK.**

If you use Index Server, you can exclude the `Temporary ASP.NET Files` directory from the folders that the Index Server scans.

➤ To exclude the `Temporary ASP.NET Files` directory Index Server scanning

1. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Computer Management.**
2. Expand the **Services and Applications** node, expand the **Indexing Service** node, and then expand the **System** node.
3. Right-click the **Directories** folder, point to **New**, and then click **Directory** from the subform to open the Add Directory dialog box.
4. Click **Browse**, and then locate the Temporary ASP.NET Files directory. You typically find the Temporary ASP.NET files in the following path:

   ```
   c:\<WINDIR>\Microsoft.NET\Framework\<Version Number>\Temporary
   ASP.NET Files
   ```

   Note: <Version Number> is the version of .NET Framework installed on your computer.
5. Click **No** under the **Include in Index?**
6. Click **OK.**
7. Close the **Computer Management** dialog box.
8. Restart the Indexing Services service.

SharePoint Single Sign-On Error on Windows Server 2003 SP1

Symptoms—When you trying to configure Server Settings for SSO, this error message is displayed:

"Failed to connect to the database server. Verify connectivity and rights for the configuration account and try again."

Cause—This problem occurs because Windows Installer 3.1 is installed when you apply Windows Server 2003 SP1.

Resolution

➤ To resolve this error:

1 **Run** `regedit`**.**

2 **Find the ImagePath registry entry at this location:**

```
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\ssosrv
```

3 **Remove the quotation strings from around the ImagePath value.**

4 **Restart Microsoft Single Sign-On service.**

6 WebLogic Portal Setup

In This Chapter

Deploying the EPM System Portlet for WebLogic 103

Assigning Privileges for WebLogic 105

Resetting the Producer Preference in WebLogic 105

Configuring the EPM System Portlet SSL for WebLogic.....106

Changing the EPM System Portlet Title 106

Choosing Look and Feel.....106

Setting Up Pages for WebLogic Portal 107

Note: All procedures in this chapter assume that you are logged on to WebLogic 9.2 or 10 as a portal administrator and have access to portal file system.

Deploying the EPM System Portlet for WebLogic

You can deploy the EPM System portlet for WebLogic Portal 9.2 and 10.

➤ To deploy the EPM System portlet for WebLogic:

1 **Extract the contents of the `bea-avaproxy.zip` file (which usually it resides in the `\Hyperion\products\biplus\InstallableApps\portlets\unconfigured`) to a temporary folder.**

2 **Merge the contents of the `WEB-INF\portlet.xml` and `WEB-INF\web.xml` files with the corresponding files in your portal Web application (in the `WEB-INF` folder).**

Note: If your application does not have a `WEB-INF\portlet.xml` file, copy the `WEB-INF\portlet.xml` file that is provided in `bea-avaproxy.zip` in its entirety.

Caution! Make sure that when merging `portlet.xml` and `web.xml` you do not change the correct order of XML elements.

Note: Unless the server is running in development mode, you may need to restart the WebLogic server instance after making the changes.

3 **Copy the `portlets`, `util`, `WEB-INF\classes`, and `WEB-INF\lib` folders into corresponding folders of your portal web application.**

For example, copy the contents of `bea-avaproxy.zip` to the WebContent directory of your application. If prompted, do not overwrite `WEB-INF\web.xml` or `WEB-INF \portlet.xml`.

4 **Add security role assignments and run-as role assignments into the `weblogic.xml` file in the `WEB-INF` folder as follows, where *`principal-name`* and *`run-as-principal-name`* are the log-on credentials for an administrative user:**

```
<wls:security-role-assignment>
   <wls:role-name>weblogic</wls:role-name>
    <wls:principal-name>weblogic</wls:principal-name>
 </wls:security-role-assignment>
 <wls:run-as-role-assignment>
    <wls:role-name>weblogic</wls:role-name>
    <wls:run-as-principal-name>weblogic</wls:run-as-principal-name>
  </wls:run-as-role-assignment>
```

5 **If you plan to use Firefox to navigate the EPM System portlet in WebLogic Portal 9.2, ensure that in the `beehive-netui-config.xml` configuration file in the `WEB-INF` folder of you portal Web application, the `html-amp-entity` option set to `false`, as in this extract:**

```
 …

<pageflow-config>

    <module-config-locators>

      <module-config-locator>

        <description>Module locator to support struts applications as portlets.</
description>

        <locator-class>com.bea.struts.adapter.util.ModuleConfigLocator</locator-
class>

     </module-config-locator>

    </module-config-locators>

 </pageflow-config>

<url-config>

     <html-amp-entity>false</html-amp-entity>

</url-config>

<request-interceptors>

    <global>

      <request-interceptor>

        <interceptor-class>org.apache.beehive.netui.tags.tree.TreeCRI</interceptor-
```

```
class>
      </request-interceptor>
       <request-interceptor>
        <interceptor-class>org.apache.beehive.netui.tags.divpanel.DivPanelCRI</
interceptor-class>
      </request-interceptor>
    </global>
</request-interceptors>
```

…

For more information, see the BEA Portal Development Guide at http://edocs.bea.com/wlp/docs92/portals/upgrade_app_from_81_TP.html#wp1006566

6. Restart your portal Web application.

Assigning Privileges for WebLogic

After deploying the EPM System portlet for WebLogic, you assign privileges for the portlet. Only authenticated users can use the portlet.

➤ To assign portlet privileges:

1. Log on to WebLogic Administration Portal.
2. Navigate to the EPM System portlet.
3. Click the **Entitlements** tab.
4. Add the required roles and capabilities for the portlet.

Resetting the Producer Preference in WebLogic

The EPM System portlet contains the wsrp_producer_url setting, which points to the Reporting and Analysis Framework instance, or producer, that contains the other portlets. The default producer is set when EPM System Configurator installs the EPM System portlet. To use a different producer, you must change the preference setting.

➤ To reset the producer preference:

1. Log on to WebLogic Administration Portal.
2. Navigate to the EPM System portlet.
3. Click the **Portlet Preferences** tab.
4. Click **Edit** to the right of the wsrp_producer_url preference value.

5 Enter a new producer URL. (Example: `http://`*`ComputerName`*`:`*`Port`*`/raframework/wsrp4j`)

6 Click **Save Portlet Preference.**

7 If you want all existing portlets to use new producer, click **Propagate to Instances.**

Caution! If you click Propagate to Instances, all user selections and preferences (selected reports, portlet size, and so on) are deleted.

Configuring the EPM System Portlet SSL for WebLogic

Configuring SSL for the EPM System portlet SSL for WebLogic involves these tasks:

- Resetting the producer preference to point to the SSL address of the EPM System server (which usually has the prefix https://).
- Importing the public EPM System server certificate into the trusted certificates list. For example, you can run this command in your WebLogic Server JRE folder:

```
keytool -import -file <CERTIFICATE_FILE> -alias HyperionSystem9 -
keystore lib/security/cacerts -trustcacerts
```

Changing the EPM System Portlet Title

Users with Administrative privileges can change the default title of the EPM System portlet. For example, you can change the title from EPM System to Primary.

Note: Procedures in this guide use the default title for the EPM System portlet.

➤ To change the EPM System portlet title:

1 Log on to WebLogic Administration Portal.

2 Navigate to the EPM System portlet.

3 Click the **Portlet Properties** tab.

4 Click **Add New Locale.**

5 Enter a name for the new locale.

6 Enter the new title and description of EPM System portlet.

7 Click **Save New Locale.**

Choosing Look and Feel

To ensure correct display of the EPM System portlet HTML content, use Look and Feel, which starts the quirks layout mode in the browser. WebLogic Portal uses Legacy Look and Feel. For more details about which document type declaration correspond to the quirks mode, refer to `http://hsivonen.iki.fi/doctype/`.

Setting Up Pages for WebLogic Portal

You can place EPM System portlet on portal pages using either BEA WebLogic Workshop or WebLogic Administration Portal.

➤ To place the EPM System portlet using BEA WebLogic Workshop:

1. Open BEA WebLogic Workshop.
2. Open the `.portal` file that you want to modify, or create a `.portal` file.
3. Drag the EPM System portlet from the **Data Palette** to the placeholder on the page.
4. Save the `.portal` file.

➤ To place EPM System portlet using WebLogic Administration Portal:

1. Log on to WebLogic Administration Portal.
2. Select the page to modify.
3. Click the **Manage Page Contents** tab.
4. Click the **Add to Page** button next to theEPM System portlet.

Caution! When using Hyperion portlet in WebLogic Portal, make sure that portal is rendered in streamed mode. In other case portlet preferences can not be saved and portlet does not work as expected. The easiest way to ensure this is to make sure that the portal desktop URL does not end with `.portal` suffix. For details, see the *WebLogic Portal User Interface Framework Guide*.

SSO Implementation

SSO implementation in WebLogic portal uses embedded WebLogic credentials mapping capabilities to store mapping between portal user and EPM System user in the embedded LDAP server. When the proxy portlet is displayed the first time, the system prompts for the EPM System user credentials. On subsequent calls, the EPM system user credentials are used to authenticate requests.

7 Oracle 10g Portal Setup

In This Chapter

Configuring Server Components for SSO 109
Oracle Portal Security Recommendations 110
Deploying the EPM System Portlet for Oracle 110
Configuring Parallel Page Engine 112
Assigning Privileges for Oracle 112
Changing the Producer Preference Setting for Oracle 113
Configuring the EPM System Portlet SSL for Oracle 113
Setting Up Pages for Oracle 114
Tips and Troubleshooting: Oracle Portal 114

Note: All procedures in this chapter assume that you are logged on to Oracle Application Server Portal 10g Release 2 (10.1.4) as a portal administrator.

Note: Ensure that your Oracle portal has all necessary updates. See Metalink Note 335911.1 on the Oracle MetaLink site for the latest patches.

Configuring Server Components for SSO

To use SSO between the Oracle portal and Reporting and Analysis, you must ensure that Oracle Portal and Hyperion are using same user directory for user authentication. In most cases, the user directory is Oracle Internet Directory.

➤ To configure server components for SSO:

1. Log on to the External Authentication Configuration Console of Hyperion Shared Services and add Oracle Internet Directory as LDAP provider.
2. Ensure that **Provider Trust Setting** is set to true.
3. In the **Security Options** tab, ensure **Support Single Sign-on** and **Oracle Single Sign-on** are selected.
4. Restart Hyperion Shared Services and Hyperion products referencing the Shared Services external authentication configuration. (This includes restarting product services, servlets, and Web applications).
5. Ensure that you can log on to the Hyperion products (for example EPM Workspace) with credentials of user from Oracle Internet Directory.

For more information, see the *Oracle Hyperion Enterprise Performance Management System Security Administration Guide*.

Oracle Portal Security Recommendations

- EPM System Web applications must be on a trusted network or deployed to an Oracle application server configured as a participating entity in the Oracle SSO environment.
- The point-to-point communication between the EPM System Portlet for Oracle Application Server Portal and Reporting and Analysis must be secured by one of these means:
  - The Reporting and Analysis Framework Web application is not exposed to an untrusted network.
  - SSL is being used between the EPM System portlet and the Reporting and Analysis Framework Web application

Deploying the EPM System Portlet for Oracle

When you complete the following procedure, your portlet should be available for adding to pages like any other portlet in the portlet repository. To add your portlet to a page, follow the instructions in the *Oracle Application Server Portal User's Guide*.

➤ To deploy the EPM System portlet for Oracle:

1. **Configure your application server to run JPS-compliant portlets, and verify it is working correctly. For more information, see the *Oracle Application Server Portal Developer's Guide*.**

   Note: To download Oracle Portlet Container, go to download.oracle.com.

2. **Deploy the** `oracle-avaproxy.war` **file (in the** `\Hyperion\products\biplus\InstallableApps\portlets\unconfigured` **folder) to the Oracle application server:**

   a. Log on to the Application Server Control Console for the Oracle Application Server middle tier instance to which you wish to deploy the EPM System portlet.

      The Application Server Control Console usually displays multiple instances that you can manage.

   b. Click the Oracle Application Server middle tier instance to which you are deploying the EPM System portlet.

   c. Click the OC4J container that you created for the JPS- compliant portlets.

   d. Click the **Applications** tab.

   e. Click **Deploy WAR file**.

   f. Enter the following information in the Web Application page:

Setting	Value
Web Application	*Hyperion*\products\biplus\InstallableApps\portlet\unconfiguredoracle-avaproxy.war where *Hyperion* is your Reporting and Analysis installation directory
Application Name	hs9
Map to URL	/hs9

g. Click **Deploy**.

h. Click **OK** to close the confirmation page.

i. Test the WSDL URL of the oracle-avaproxy.war file by entering it into a browser as `http://host:port/hs9/portlets?WSDL`.

   You should see the correct WSDL definition in your browser.

3 **Add the required JVM parameters:**

a. On the **Administration** tab of your portlet container OC4J instance, click **Server Properties**.

b. Add this text in the **Java Options** input field:

```
-Daxis.xml.reuseParsers=false
```

c. Click **Apply**.

d. Restart the OC4J instance.

4 **Register the EPM System producer in the Oracle application server portal:**

a. Open OracleAS Portal and log on.

Note: To register your provider, you need Manage or Edit privileges on providers. If you do not have these privileges, request them from your administrator.

b. Unless you are already on the Portal Builder page, click **Builder** in the upper right corner.

c. Click the **Administer** tab.

d. Click the **Portlets** subtab.

e. In the **Remote Providers** portlet, click **Register a Provider**.

f. On the **Register Provider** page, enter these values:

Setting	Value
Name	HyperionProvider
Display Name	Hyperion Provider
Timeout	150
Timeout Message	The Hyperion Provider has timed out!

Setting	Value
Implementation Style	WSRP*

*If WSRP is not available as a selection, your Oracle application server portal has not been patched to the required version, 10.1.4. See Oracle Metalink for more information.

g. Click **Next**.

h. On the **Define Connection** page, enter the WSDL URL for the Hyperion provider in the WSDL URL field.

   Example: `http://myserver.com:7778/hs9/portlets?WSDL`

i. Click **Finish**.

   The Registration Confirmation page is displayed.

j. Click **OK**.

Configuring Parallel Page Engine

To see images from the EPM System portlet, you must configure the `resourceURLKey`parameter. The Parallel Page Engine uses this key to calculate checksums for URLs that are requested by WSRP and JPDK resource proxying. For WSRP resource proxying to work, the key must be set to an alphanumeric value of 10 characters or more.

➤ To configure WSRP resource proxying:

1. **Open the** `web.xml` **file that is associated with the OC4J_PORTAL instance on the middle tier. The file is in the directory** `MID_TIER_ORACLE_HOME\j2ee\OC4J_Portal\applications\portal\portal\WEB-INF\`**.**
2. **Uncomment the lines that contain the resourceURLKey parameter definition.**
3. **Set the** `resourceURLKey` **parameter to an alphanumeric value of 10 characters or more.**
4. **Save the** `web.xml` **file.**
5. **Run this command to synchronize the manual configuration changes:** `MID_TIER_ORACLE_HOME/dcm/bin/dcmctl updateconfig`**.**
6. **Run this command to restart OC4J_Portal:** `MID_TIER_ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=OC4J_Portal`**.**

Assigning Privileges for Oracle

After deploying the EPM System portlet for Oracle, you can assign privileges for the portlet. Only authenticated users can use the EPM System portlet. EPM System portlet users need View privileges for the item, which contains the EPM System portal. For more information, see the *Oracle Application Server Portal User's Guide.*

Changing the Producer Preference Setting for Oracle

The EPM System portlet contains the wsrp_producer_url setting, which points to the Reporting and Analysis Framework instance, or producer, that contains all the other portlets. The default producer is set when Hyperion Configuration UtilityOracle's Hyperion Enterprise Performance Management System Configurator installs the EPM System portlet. To use a different producer, you must change the preference setting.

Note: To configure SSL for the EPM System portlet, you change the producer preference setting to point to the SSL address of the EPM System server. See "Configuring the EPM System Portlet SSL for Oracle" on page 113

➤ To change the producer preference setting:

1 Log on to the Oracle application server portal.

2 Go to the page that includes the EPM System portlet, which should be configured to use a different producer

3 Click **Edit** at the top of the page to switch to Edit mode.

4 Click the **Actions** icon beside the portlet.

5 Click **Delete.**

You must delete previous instances of the EPM System portlet from the pages to reset per-user personalization, which includes producer preference.

6 On the confirmation page, click **Yes** to delete the portlet and return to the page.

7 Click the **Add Portlet** icon in the region where you are adding a portlet.

8 In the Portlet Repository, enter **Hyperion** in the **Search** field, and then click **Go.**

Tip: You can also click the repository links to drill to the portlet's location.

9 Click the portlet name.

10 Click **OK** to return to the page.

11 Click the **Edit Defaults** icon beside the portlet.

12 Enter new producer URL in the **wsrp_producer_url** field, and then click **OK.**

Configuring the EPM System Portlet SSL for Oracle

Configuring the EPM System portlet SSL for the Oracle application server portal involves these tasks:

- Changing the producer preference setting to point to the SSL address of the EPM System server (which usually has the prefix https://), and changing the port to the SSL port.
- If the public certificate of the EPM System server is not signed with trusted authority and the error message "sun.security.validator.ValidatorException: No trusted certificate found"

is in the log file, you must import the signer certificate into trusted certificates list of your application server. For example, you can run the command `keytool -import -file <CERTIFICATE_FILE> -alias HyperionSystem9 -keystore lib/security/cacerts -trustcacerts` in your Oracle application server portal JRE folder and then pass these parameters to your application server:

```
-Djavax.net.ssl.trustStore=<PATH_TO_TRUSTSTORE> –

Djavax.net.ssl.trustStorePassword=<TRUSTSTORE_PASSWORD>
```

For more information, see the Oracle Application Server 10g Release 2 documentation.

Setting Up Pages for Oracle

➤ To place the EPM System portlet on the page:

1 **Log on to the Oracle application server portal.**

2 **Go to the page where you are adding a portlet.**

3 **Click Edit at the top of the page to switch to Edit mode.**

Note: Oracle recommends adding the EPM System portlet from Edit Page screen rather than from Personalize Page screen so that you retain the ability to change the producer preference setting. The page used for adding the portlet may also affect the availability of the portlet.

4 **Click the Add Portlet icon in the region where you are adding a portlet.**

5 **In the portlet repository, enter EPM System in the Search field and click Go. Alternatively, click the repository links to drill to the portlet's location.**

Tip: You can also click the repository links to drill to the portlet's location.

6 **Click the portlet name.**

7 **Click OK to return to the page.**

Tips and Troubleshooting: Oracle Portal

In Portal 10.1.4 JSR168 /WSRP portlets generate this error message when a user session is idle for more than 30 minutes and the user then attempts to access an item on the page:

Error: Could not get markup. The cookie or session is invalid or there is a runtime exception.

This error message is unavoidable when the provider session times out, and the message cannot be customized. Users can resolve this error by refreshing the portal page. You can also increase the session timeout value so that users do not encounter this message.

➤ To increase the session timeout value for your wsrp providers:

1 **Navigate to the `WEB-INF` directory where the wsrp provider was deployed; for example, `/ORACLE_HOME/j2ee/wsrp/applications/sampleportlets/hs9/WEB-INF`.**

2 **Make a backup copy of the `web.xml` file.**

3 **Edit the `web.xml` file to reset the session-timeout parameter to a value appropriate to your application needs.**

   Example:

```
<session-config>

session-timeout>120</session-timeout>

</session-config>
```

   Note: This parameter is set in minutes, so 120 equals 2 hours.

4 **Save your changes.**

5 **Restart the middle-tier processes (opmnctl stopall and startall).**

SSO Implementation

SSO implementation between EPM System and Oracle Portal is a “trusted” SSO. EPM System portlet transfers Oracle Portal User ID (user logon name) to the EPM System server, where the user is authenticated using this ID. To use “trusted” SSO, server components should be properly configured.

8

Oracle® Web Center 10g (10.1.3.4.0) Setup

In This Chapter

Configuring Server Components for SSO 117
Oracle WebCenter Security Recommendations 118
Deploying the Hyperion Portlet for Oracle WebCenter 118
Changing the Producer Preference Setting in Oracle WebCenter 120
Configuring Hyperion Portlet SSL for Oracle WebCenter 121
Setting Up Pages for Oracle WebCenter 121
SSO Implementation 122
Interactive Reporting Page Parameter Wiring Feature in Oracle Web Center 122

Configuring Server Components for SSO

To use SSO between the Oracle Web Center and Reporting and Analysis, you must ensure that Oracle Web Center and Hyperion are using the same user directory for user authentication. In most cases, the user directory is Oracle Internet Directory.

➤ To configure server components for SSO:

1. Log on to the External Authentication Configuration Console of Shared Services and add **Oracle Internet Directory** as an LDAP provider.
2. Ensure that Provider Trust Setting is set to true.
3. In the Security Options tab, ensure Support Single Sign-on and Oracle Single Sign-on are selected.
4. Restart Shared Services and Hyperion products referencing the Oracle's Hyperion® Shared Services external authentication configuration. (This includes restarting product services, servlets, and Web applications.)
5. Ensure that you can log on to the Hyperion products, for example EPM Workspace with credentials of user from Oracle Internet Directory.

For more information, see the *Oracle Hyperion Enterprise Performance Management System Installation and Configuration Guide.*

Oracle WebCenter Security Recommendations

1. Hyperion Web applications must be on a trusted network or deployed to an Oracle application server configured as a participating entity in the Oracle SSO environment.
2. The point-to-point communication between the Hyperion Portlet for Oracle WebCenter and Reporting and Analysis must be secured by one of these:
   - The Reporting and Analysis Framework Web application is not exposed to an untrusted network.
   - SSL is being used between the Hyperion portlet and the Reporting and Analysis Framework Web application.

Deploying the Hyperion Portlet for Oracle WebCenter

➤ To deploy the Hyperion portlet for Oracle WebCenter:

1 **Prepare `oracle-avaproxy.ear` for deployment:**

   a. Copy the `oracle-avaproxy.ear` file from the `\Hyperion\products\biplus\InstallableApps\portlets\unconfigured` folder to some temporary folder.

   b. Rename `oracle-avaproxy.ear` file in temporary folder to `oracle avaproxy_initial.ear`.

   c. Run WSRP producer predeployment tool on `oracle-avaproxy_initial.ear`. Execute `java -jar <PATH TO wsrp-predeploy.jar> oracle-avaproxy_initial.ear oracle-avaproxy.ear` from the folder with `oracle-avaproxy_initial.ear`, where `<PATH TO wsrp-predeploy.jar> is path to wsrp-predeploy.jar` (for example, `c:\jdeveloper\adfp\lib\wsrp-predeploy.jar`)

   Note: For details about WSRP producer pre-deployment tool, see *Oracle® WebCenter Framework Developer's Guide 10g*.

2 **Deploy `oracle-avaproxy.ear` to application server.**

Note: For detailed information about deploying applications to OC4J, see *Oracle Containers for J2EE Deployment Guide* on the OracleAS Portal Documentation page on Oracle Technology Network (OTN).

3 **To deploy `oracle-avaproxy.ear` using Application Server Control Console, perform the following steps:**

   a. Log in to the Application Server Control Console for the Oracle Application Server instance to which you wish to deploy Hyperion portlet. The Application Server Control Console usually displays multiple instances that you can manage.

   b. Click the Oracle Application Server middle tier instance to which you are deploying the Hyperion portlet.

   c. Click the OC4J container.

Note: Make sure that selected OC4J container includes Oracle Portlet Container. For more information about configuring your application server or standalone OC4J to run portlets, refer to *Oracle® WebCenter Framework Developer's Guide 10g*.

d. Click the Applications tab and click Deploy button.

e. If the `oracle-avaproxy.ear` file is located on the local computer, then select the **Archive is present on local host** option and browse to the location of the `oracle-avaproxy.ear` file, or select the **Archive is already present on the server where Application Server Control is running** option.

f. Click Next.

g. Fill out the Deploy Application Attributes page as described in table below:

Table 5 Deploy Application Attributes

Setting	Value
Application Name	hs9
Context Root	/hs9

h. Click **Next**.

i. Click **Deploy**.

j. Click **Return** to dismiss the confirmation page.

k. You can test your Hyperion portlet and producer to check the configuration and to ensure that the portlet and its producer operate correctly. To test your Hyperion portlet and producer, run the producer URL in your browser in the following syntax: http://<host>:<port>/hs9/info where:

host is the server to which your `oracle-avaproxy.ear` file has been deployed

port is the HTTP Listener port

WSRP Producer Test Page is displayed in your browser.

4 **Register the Hyperion portlet producer:**

a. In the Applications Navigator in JDeveloper, right-click the application under which to create the producer and select **New** from the context menu.

b. In New Gallery under Categories, expand the Web Tier node and select Portlets.

c. In New Gallery under Items, select WSRP Producer Registration.

d. Click **OK**.

e. On the Welcome page, click **Next**.

f. In the Name field, enter a “Hyperion Producer” for the name of producer and click **Next**.

g. In the URL Endpoint field, enter the producer's URL:

http://<host>:<port>:/hs9/portlets/wsrp2?WSDL

For example http://myhost:8888/hs9/portlets/wsrp2?WSDL

Note: Make sure to use WSRP 2.0 URL to register Hyperion portlet producer.

h. If the application uses an HTTP proxy to connect to the producer, enter proxy details.

i. Click **Next**.

j. In the Default Execution Timeout (Seconds) field, enter 240.

k. Click **Next**.

l. Click **Next**.

m. Click **Finish** to complete registration of the Hyperion portlet producer.

n. Hyperion portlet is available for adding to pages similar to other portlets. To add Hyperion portlet to a page, follow the instructions in the *Oracle® WebCenter Framework Developer's Guide 10g*.

Note: The user must be logged in to the application as an authenticated user to access the personalization feature and to be able to select particular report. For details on setting up security for your WebCenter application, see *Oracle® WebCenter Framework Developer's Guide 10g*.

Changing the Producer Preference Setting in Oracle WebCenter

The Hyperion portlet contains the wsrp_producer_url setting, which points to Reporting and Analysis Framework instance, or producer, that contains all the other portlets. The default producer is set when Oracle's Hyperion® Configuration Utility™ installs the Hyperion portlet. To use a different producer, you must change the preference setting.

Note: To configure SSL for the Hyperion portlet, you change the producer preference setting to point to the SSL address of the Hyperion server. See "Configuring Hyperion Portlet SSL for Oracle WebCenter" on page 121.

➤ To change the producer preference setting:

1. Go to the page that includes the Hyperion portlet, which is configured to use different producer.
2. Delete this portlet instance from the page and then add it back to the same page. This is required to reset per-user personalization, which includes producer preference.
3. Run the page and log on to the Oracle WebCenter application.
4. Click the Customize link beside the portlet.
5. Enter new producer URL in the wsrp_producer_url field.
6. Click **OK**.

Configuring Hyperion Portlet SSL for Oracle WebCenter

Configuring SSL for the Hyperion portlet SSL for Oracle WebCenter involves these tasks:

1. Changing the producer preference setting to point to the SSL address of the Hyperion server (which usually has the prefix https://), and changing the port to the SSL port.
2. If the public certificate of the Hyperion server is not signed with trusted authority and the error message “sun.security.validator.ValidatorException: No trusted certificate found” is in the log file, you must import the signer certificate into trusted certificates list of your application server. For example, you can run the command:

   ```
   keytool -import -file <CERTIFICATE_FILE> - alias HyperionSystem9 -
   keystore lib/security/cacerts -trustcacerts
   ```

   in your OC4J JRE folder.

   See *Oracle® Application Server Administrator's Guide 10g* for more information.

Setting Up Pages for Oracle WebCenter

➤ To add a Hyperion portlet to a page, perform the following steps (in Oracle JDeveloper):

1 In the Applications Navigator, right-click the application page (jspx file) to which you want to add the Hyperion portlet, and select **Open** from the context menu.

2 In the Component Palette, select the **Hyperion Producer**.

3 Select a Oracle's Hyperion® Portal Integration Toolkit portlet, and drag it over the `h:form` element in the Oracle JDeveloper Structure pane. Alternatively, drag the Hyperion portlet directly onto the page in the editor.

4 Set IframeDtd attribute value to **none** in the Property Inspector for the portlet to make sure that portlet content renders correctly.

Caution! When using Firefox to browse WebCenter pages with Hyperion portlet, you may have difficulty changing portlet content size using Edit mode. In this case, set portlet width and height explicitly to fit content size in `adfp:portlet` tag on the WebCenter page.

Navigational parameters

Hyperion portlet under Oracle WebCenter supports WSRP 2.0 navigational parameters. For more information about navigational parameters, refer to *Oracle® WebCenter Framework Developer's Guide 10g*.

In current release, “hs9_filter” parameter supported for Web Analysis and Interactive Reporting reports. This parameter can be used to apply additional filtering criteria to reports.

The value of this parameter is semicolon-separated list of name/value pairs, where name can contain more than one value (values are comma-separated) and name and value are separated by equals sign. Names should be unique in the list. For example, “hs9_filter” parameter value:

```
Product=Colas,Beers;Country=USA;
```

where `Product` and `Country` are names, and `Colas`, `Beers`, `USA` are values.

Special characters (“,”, “;”, “=”, “\”) in names and in values should be escaped with backslash character (“\”). For example, if you have name “Dimension;1” and value “Member=3\2”, resulting “hs9_filter” parameter value should look like:

```
Dimension\;1= Member\=3\\2;
```

You can register special managed bean, to handle encoding of “hs9_filter” parameter names and values directly in EL expression. The class for this bean is:

`com.hyperion.portlet.proxy.oracle.util.pov.HS9Bean` and it is located in `portlets-consumer-oracle.jar file` (`portlets-consumer-oracle.jar` file can be found in `oracle-avaproxy.ear` archive). If you register this special managed bean under hs9bean name, then expression like following can be used to handle encoding: `${hs9bean.encoder['Dimension;1']} ${'='}${hs9bean.encoder[' Member=3\2']} ${';'}`. For more details on how `hs9_filter` parameter impacts Web Analysis and Interactive Reporting reports, see “Interactive Reporting Page Parameter Wiring Feature in Oracle Web Center” on page 122 and Chapter 10, “Web Analysis Portlets”.

SSO Implementation

SSO implementation between EPM System and Oracle WebCenter is a “trusted” SSO. EPM System portlet transfers Oracle WebCenter User ID (user logon name) to the EPM System server, where the user is authenticated using this ID. To use “trusted” SSO, server components must be configured properly.

Interactive Reporting Page Parameter Wiring Feature in Oracle Web Center

Interactive Reporting Page Parameter wiring allows the portlets to exchange parameters and their corresponding values among them. The value to any parameter is a list of Name/Value pairs separated by semicolon. The "Name" and the "Value" components of each Name/Value pair are separated by an "=" sign. Also, the "Value" component can have one or multiple values, separated by comma. As mentioned in the previous section, only one parameter, hs9_filter, is implemented in Reporting and Analysis Framework portlet and is consumed in Interactive Reporting Portlet. The following are examples of hs9_filter parameter values:

Region = South,.1 Name and 1 Value

Region = South, Central, North, 1 name and 3 values

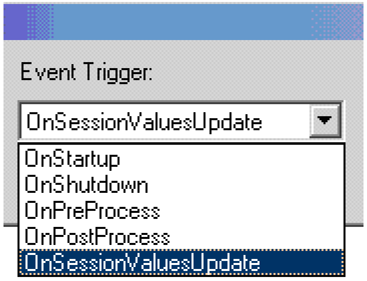
Note: Use Oracle's Hyperion® Interactive Reporting Studio for creating the Interactive Reporting document in the procedure that follows.

➤ Creation of an Interactive Reporting document to consume hs9_filter parameter value equals to Region = South for Oracle Web Center with Parameter Wiring support:

1 Create an Interactive Reporting document with Query, Results, and Table sections you want to apply the Limits or Filters to a column in Query/Results/Table section. In this example we apply a Limit/Filter to column named "Region".

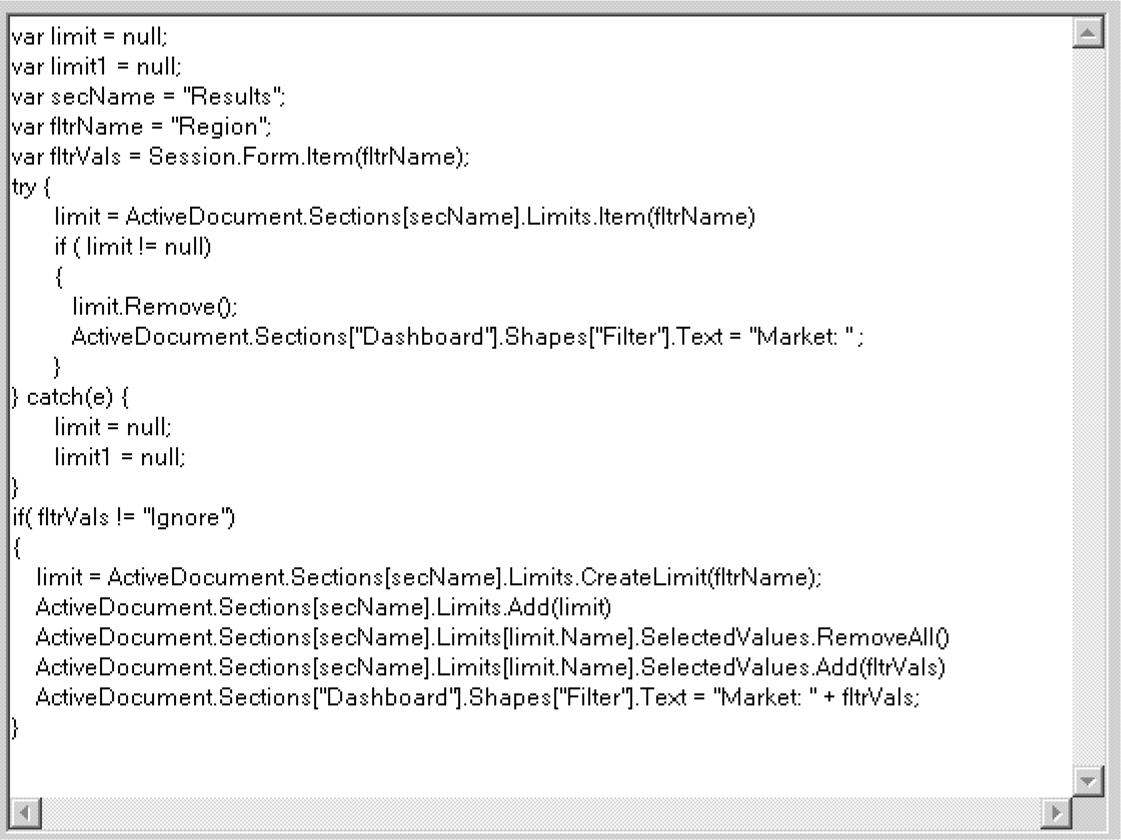
2 Select **File**, then **Document Scripts.**

3 Select **OnSessionValuesUpdate** under **Event Trigger** drop down.



Event Trigger: OnSessionValuesUpdate

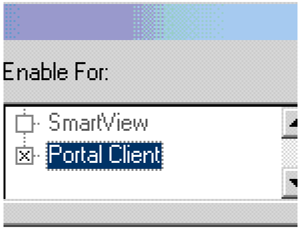
4 In the Script Editor, create a document script for the trigger **OnSessionValuesUpdate.** The following is the sample script to consume the hs9_filter parameter value (Name/Value) Region = West and use it for setting the Limit/Filter in a Results section.



```
var limit = null;
var limit1 = null;
var secName = "Results";
var fltrName = "Region";
var fltrVals = Session.Form.Item(fltrName);
try {
      limit = ActiveDocument.Sections[secName].Limits.Item(fltrName)
      if ( limit != null)
      {
        limit.Remove();
        ActiveDocument.Sections["Dashboard"].Shapes["Filter"].Text = "Market: " ;
      }
} catch(e) {
      limit = null;
      limit1 = null;
}
if( fltrVals != "Ignore")
{
   limit = ActiveDocument.Sections[secName].Limits.CreateLimit(fltrName);
   ActiveDocument.Sections[secName].Limits.Add(limit)
   ActiveDocument.Sections[secName].Limits[limit.Name].SelectedValues.RemoveAll()
   ActiveDocument.Sections[secName].Limits[limit.Name].SelectedValues.Add(fltrVals)
   ActiveDocument.Sections["Dashboard"].Shapes["Filter"].Text = "Market: " + fltrVals;
}
```

It is important that the Name component of Name/Value pair, here "Region", should be the <key> to extract the item value from "Session.Form.Item(<key>)". Which means, all of the Names used in Name/Value pairs should be known while creating the document. If there are multiple values present in the "Value" component of Name/Value pair, say for example "Region = South, Central, North", then the user has to parse the "Value" expression and use accordingly.

5 Enable the **Portal Client** under Enable For. This is needed to execute the script under HTML client.



Enable For:

□ SmartView
☒ Portal Client

➤ To test Interactive Reporting Portlet with Oracle Web Center:

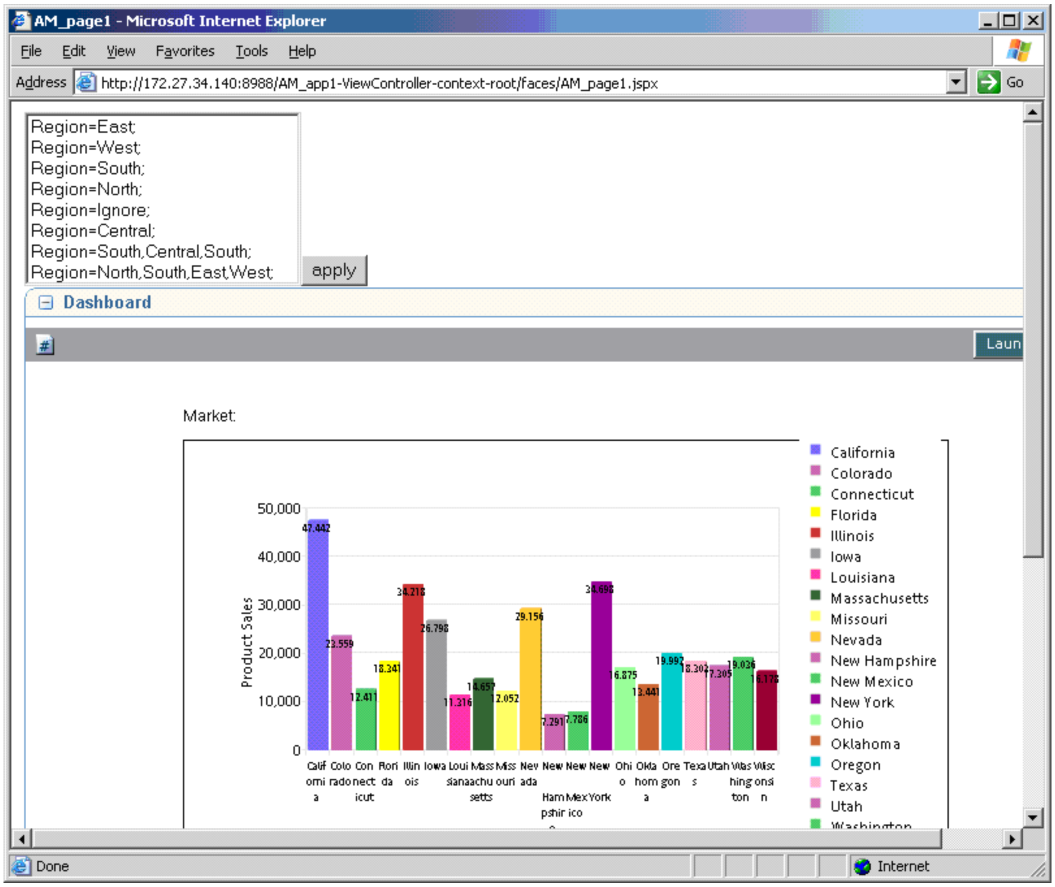
1 Publish the document in the Reporting and Analysis Framework repository.

2 Configure the Oracle Web Center portal to talk to the Producer for Interactive Reporting Portlet.

3 Create Portal page with an Interactive Reporting Portlet instance and a Page Parameters place holder.

4 Configure the Proxy Portlet.

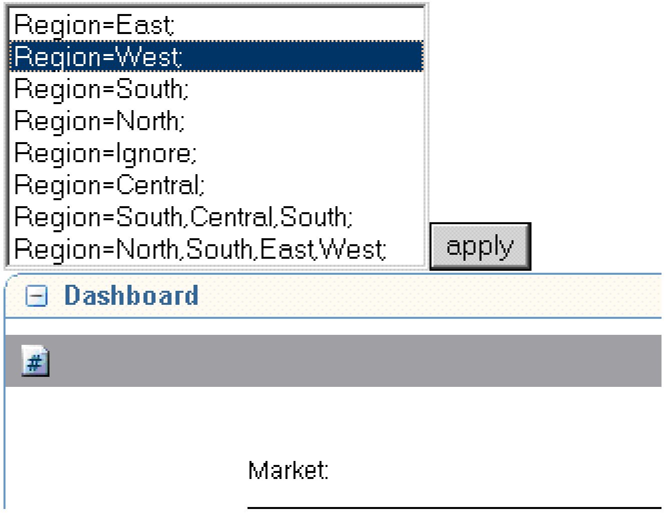
5 Open the Portal page with no Page parameters applied. Here is the sample,



AM_page1 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://172.27.34.140:8988/AM_app1-ViewController-context-root/faces/AM_page1.jspx
Go

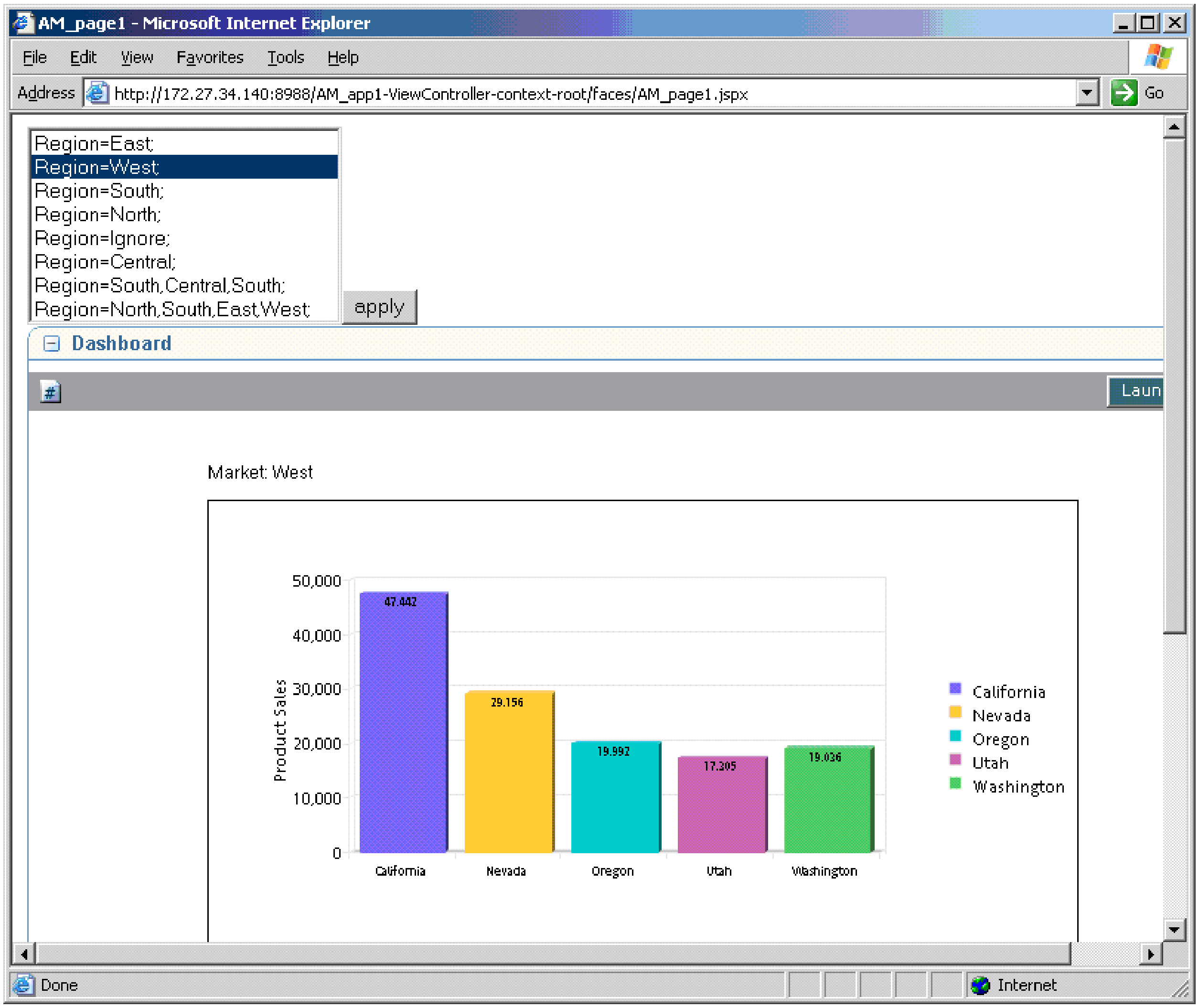
Region=East;
Region=West;
Region=South;
Region=North;
Region=Ignore;
Region=Central;
Region=South,Central,South;
Region=North,South,East,West;

6 Select Region = West and select **Apply** button to apply the hs9_filter parameter value as Region = West, which is further consumed in Interactive Reporting document.



Region=East;
Region=West;
Region=South;
Region=North;
Region=Ignore;
Region=Central;
Region=South,Central,South;
Region=North,South,East,West;

7 Interactive Reporting document content is refreshed by applying the hs9_filter parameter value selected from the Portal Page.



Address: http://172.27.34.140:8988/AM_app1-ViewController-context-root/faces/AM_page1.jspx

Region=East;
Region=West;
Region=South;
Region=North;
Region=Ignore;
Region=Central;
Region=South,Central,South;
Region=North,South,East,West;

Market: West

9

Oracle® Web Center 11g (11.1.1) Setup

In This Chapter

Configuring Server Components for SSO 127

Oracle WebCenter 11 Security Recommendations 127

Deploying the Hyperion Portlet for Oracle WebCenter 11 128

Changing the Producer Preference Setting in Oracle WebCenter 11................................129

Configuring Hyperion Portlet SSL for Oracle WebCenter 11...130

Setting Up Pages for Oracle WebCenter 11 130

Navigational Parameters 131

SSO Implementation..131

Configuring Server Components for SSO

To use SSO between Oracle Web Center and Reporting and Analysis, Oracle Web Center 11 and Hyperion must use the same user directory for user authentication. In most cases, the user directory is Oracle Internet Directory.

➤ To configure server components for SSO:

1. **Log on to the External Authentication Configuration Console of Shared Services and add Oracle Internet Directory as an LDAP provider. Verify that Provider Trust Setting is set to true.**
2. **In the Security Options tab, verify Support Single Sign-on and Oracle Single Sign-on are selected.**
3. **Restart Shared Services and Hyperion products referencing the Oracle's Hyperion® Shared Services external authentication configuration. (This includes restarting product services, servlets, and Web applications).**
4. **Confirm by logging on to the Hyperion products, for example EPM Workspace with credentials of user from Oracle Internet Directory.**

For more information, see the *Oracle Hyperion Enterprise Performance Management System Installation and Configuration Guide.*

Oracle WebCenter 11 Security Recommendations

The following are recommendations that users should review.

1. Hyperion Web applications must be on a trusted network or deployed to an Oracle application server configured as a participating entity in the Oracle SSO environment.
2. The point-to-point communication between the Hyperion Portlet for Oracle WebCenter and Reporting and AnalysisReporting and Analysis must be secured by one of these:
   a. Reporting and Analysis Framework Web application is not exposed to an untrusted network.

   b. SSL is being used between the Hyperion portlet and the Reporting and Analysis Framework Web application.

Deploying the Hyperion Portlet for Oracle WebCenter 11

➤ To deploy the Hyperion portlet for Oracle WebCenter:

1 **Prepare `oracle-avaproxy11.ear` for deployment.**

   a. Copy the `oracle-avaproxy11.ear` file from `EPM_ORACLE_HOME\products\biplus\InstallableApps\portlets\unconfigured\` folder to a temporary folder.

   b. Rename `oracle-avaproxy11.ear` file in temporary folder to `oracle-avaproxy11_initial.ear`.

   c. Run WSRP producer predeployment tool on `oracle-avaproxy11_initial.ear`. Execute `java -jar <PATH TO wsrp-predeploy.jar>oracle-avaproxy11_initial.ear oracle-avaproxy11.ear` from the folder with `oracle-avaproxy11_initial.ear`, where `<PATH TO wsrp-predeploy.jar> is path to wsrp-predeploy.jar` (for example, `MW_HOME/WC_HOME/webcenter/modules/oracle.portlet.server_11.1.1/wsrp-predeploy.jar`).

   Note: For details about WSRP producer pre-deployment tool, see *Oracle® Fusion Middleware Administrator's Guide for Oracle WebCenter 11g Release 1 (11.1.1)*.

2 **Deploy `oracle-avaproxy11.ear` to application server.**

   Note: For detailed information about deploying portlet producer applications, see *Oracle® Fusion Middleware Administrator's Guide for Oracle WebCenter 11g Release 1 (11.1.1)*.

3 **To deploy `oracle-avaproxy11.ear` using WLS Administration Console, perform the following steps:**

   a. Log in to the WLS Administration Console.

   b. In the Domain Structure pane, select **Deployments**.

   c. On the Deployment Summary pane, select **Install**.

   d. Using the Install Application Assistant Path field, locate the `oracle-avaproxy11.ear`. Select the `oracle-avaproxy11.ear` file and select **Next**.

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

f. Select the deployment target to which to deploy the Web application and select **Next.**

g. Review the configuration settings you specified, and select **Finish** to complete the installation.

4 **Register the WSRP Producer:**

a. To register WSRP Producer using Fusion Middleware Control, Login to Fusion Middleware Control and navigate to the home page for your custom WebCenter application (or WebCenter Spaces).

b. Do one of the following:

i. For custom WebCenter applications - From Application Deployment menu, select **WebCenter**, then **Register Producer.**

ii. For WebCenter Spaces - From WebCenter menu, select **Register Producer**.

c. In the Add Portlet Producer Connection section, enter connection details for the WSRP producer:

Table 6 Add Portlet Producer

Setting	Value
Connection Name	Oracle Hyperion Producer
Producer Type	WSRP Producer
WSDL URL	`http://host_name:port_number/hs9/portlets/wsrp2?WSDL` where *host_name* is the server where your producer is deployed, *port_number* is the HTTP listener port number for example: `http://myhost.com:7778/hs9/portlets/wsrp2?WSDL`

If the application uses an HTTP proxy to connect to the producer, enter proxy details.

d. Select **Next.**

e. Select **Next.**

f. Select **Next.**

g. Select **OK** to save WSRP producer details.

h. Hyperion portlet is available for adding to pages similar to other portlets. To add Hyperion portlet to a page, follow the instructions in the *Oracle® Fusion Middleware User's Guide for Oracle WebCenter 11g Release 1 (11.1.1)*.

Changing the Producer Preference Setting in Oracle WebCenter 11

The Hyperion portlet contains the wsrp_producer_url setting, which points to Oracle's Hyperion Reporting and Analysis Framework instance, or producer, that contains all the other portlets. You must change the preference setting to specify which producer server you would like to use.

Note: To configure SSL for the Hyperion portlet, change the producer preference setting to point to the SSL address of the Hyperion server. See "Configuring Hyperion Portlet SSL for Oracle WebCenter 11" on page 130.

➤ To change the producer preference setting:

1 Go to the page that includes the Hyperion portlet, which is configured to use a different producer. Delete this portlet instance from the page and then add it back to the same page. This is required to reset per-user personalization, which includes producer preference

2 Run the page and log on to the Oracle WebCenter application.

3 Select **Customize** from Actions menu beside the portlet.

4 Enter new producer URL in the **wsrp_producer_url** field.

5 Select **OK.**

Configuring Hyperion Portlet SSL for Oracle WebCenter 11

Configuring SSL for the Hyperion portlet SSL for Oracle WebCenter involves these tasks:

1. Changing the producer preference setting to point to the SSL address of the Hyperion server (which usually has the prefix https://), and changing the port to the SSL port.
2. If the public certificate of the Hyperion server is not signed with trusted authority and the error message "sun.security.validator.ValidatorException: No trusted certificate found" is in the log file, you must import the signer certificate into trusted certificates list of your application server. For example, you can run the command: `keytool -import -file <CERTIFICATE_FILE> - alias HyperionSystem9 - keystore lib/security/ cacerts -trustcacerts` in your WebLogic Application Server JRE folder.

Setting Up Pages for Oracle WebCenter 11

➤ To add a Hyperion portlet to a page, perform the following steps:

1 Log in to Oracle WebCenter Spaces. Go to the page where you want to add a portlet.

2 From Page Actions menu, select **Edit Page** to open Oracle Composer.

3 Select **Add Content** button associated with the location where you want to place the portlet.

4 Select **Add link** next to the portlet of interest, or drill to the portlet by clicking the **Open** link next to the folder that contains the portlet.

5 Select **Close** for the Catalog.

6 Select **Save** in Oracle Composer to save your changes

7 Optionally, select **Close** to exit Oracle Composer.

Navigational Parameters

Hyperion portlet under Oracle WebCenter supports WSRP 2.0 navigational parameters. For more information about navigational parameters, refer to *Oracle® Fusion Middleware Administrator's Guide for Oracle WebCenter 11g Release 1 (11.1.1)*.

In current release, hs9_filter parameter is supported for Web Analysis and Interactive Reportingreports. This parameter can be used to apply additional filtering criteria to reports. The value of this parameter is semicolon-separated list of name or value pairs, where name can contain more than one value (values are comma-separated) and name and value are separated by equals sign. Names should be unique in the list. For example, hs9_filter parameter value: Product=Colas,Beers;Country=USA; where Product and Country are names, and Colas,Beers,USA are values. Special characters (“,”, “;”, “=”, “\”) in names and in values should be escaped with backslash character (“\”). For example, if you have name Dimension;1 and value Member=3\2, resulting hs9_filter parameter value should look like: Dimension\; 1= Member\=3\\2;

You can register special managed bean to handle encoding of hs9_filter parameter names and values directly in EL expression. The class for this bean is: com.hyperion.portlet.proxy.oracle.util.pov.HS9Bean and it is located in portlets-consumer-oracle.jar file (portlets-consumer-oracle.jar file can be found in oracle-avaproxy11.ear archive). If you register this special managed bean under hs9bean name, then expression like following can be used to handle encoding: $ {hs9bean.encoder[‘Dimension;1’]} ${‘=’}${hs9bean.encoder[‘ Member=3\2’]} ${‘;’}. For more details on how hs9_filter parameter impacts Web Analysis and Oracle's Hyperion® Interactive Reporting reports, see “Interactive Reporting Page Parameter Wiring Feature in Oracle Web Center” on page 122 and Chapter 10, “Web Analysis Portlets.”

SSO Implementation

SSO implementation between EPM System and Oracle WebCenter 11 is a “trusted” SSO. EPM System portlet transfers Oracle WebCenter User ID (user logon name) to the Oracle Hyperion Enterprise Performance Management System server, where the user is authenticated using this ID. To use “trusted” SSO, server components must be configured properly.

10

Web Analysis Portlets

In This Chapter

Subscription Controls Functional in Portlets 133

Designer Components Not Supported in Portlets 133

Launch Out to EPM Workspace 134

Points of View, Personal Variables, and Subscription Controls 134

Web Analysis Portlet External POV feature from End User Perspective 134

Subscription Controls Functional in Portlets

In Web Analysis portlets, all navigation are performed through the Subscription Controls.

The Subscription Controls working principle is based on JavaScript functions. In VIEW mode, the Web Analysis portlet represents the Web Analysis document selected by administrator in EDIT mode, which contains all data source and design objects as well as Subscription Controls. No right-click functions are available.

Designer Components Not Supported in Portlets

The Web Analysis Portlet does not render these designer components:

- Tab selection controls
- Slider deselection controls
- Splitter panels
- Some service buttons:
  - Assign Edit Data
  - Data Layout
  - Send to Excel
  - Send to Clipboard
  - Toggle Toolbar
  - Toggle Status Bar
  - Toggle Menu
  - Toggle Info Panel

- Logout
- Dimension Browser
- User Preferences
- Launch Executable
- Close Report
- Open Report
- Next Tab
- Previous Tab
- Desktop
- Home
- File Open
- Open Presentation
- Edit Data
- Dimension Browser
- Save
- Save As

Launch Out to EPM Workspace

“Launch Out to Workspace” enables launching a section of the screen in a Oracle Enterprise Performance Management Workspace, Fusion Edition window with fully interactive menus.

Note: Modifications to the launched instance are not applied back to the portlet instance.

Points of View, Personal Variables, and Subscription Controls

Member-selection related points of view and personal variables are passed to the launch out instance, so that the same exact Web Analysis document (dimension layout, member selection, data) is displayed. If points of view or personal variables are used for member selection in the portlet (probably also in the source Web Analysis document overall), they should be selected.

Web Analysis Portlet External POV feature from End User Perspective

From the Oracle's Hyperion Reporting and Analysis end user perspective, the most useful and reasonable interpretation of Oracle Web Center portlet parameters wiring facility would be sharing of common point of view (POV) between all Hyperion portlets on the portal page in Oracle Web Center. The external POV must be defined according to special format and passed as the parameter with name hs9_filter. The external POV format allows user specifying a number of OLAP members to be selected in one or more OLAP dimensions.

Current format is `<Dim1>=<Mem1>[,<Mem2>[,...]]` `[,<Dim2>=<Me3>[,<Mem2[, ...]]]=[,[,…]][;=[,[,…]]]`. For example: “Year=Qtr1,Qtr2,Qtr3;Product=100”.

Note: Comma, semicolon and sign of equality are reserved characters. This format is maintained by Infrastructure layer which is common for all Hyperion portlet implementations.

The following is important to know about external POV support in Web Analysis portlet:

- Passing the external POV to Web Analysis portlets produces effect similar to one user observes when Web Analysis document is opened as Related Content document.
- The same external POV is applied to all data sources within Web Analysis document. In other words, the POV parameters are data source independent.
- If some OLAP dimension is not found in the data source while applying external POV, this dimension is ignored.
- If some OLAP member is not found in corresponding OLAP dimension of the data source while applying external POV, this member is ignored.
- External POV affects all data source views and all axis of the data source view (rows, columns, pages and filters).
- External POV affects the state of Subscription Controls (they are filtered accordingly).
- OLAP dimensions’ and OLAP members’ names are case-sensitive.
- OLAP members must be identified by there names (ID’s). Aliases are not supported.
- External POV does not allow advanced member selections. Only single member selection mode is supported.
- If external POV either appears, changes, or disappears Web Analysis portlet reloads the document in order to apply the changes and set up new context.
- External POV does not affect the state of the document in the repository. It’s used by Oracle's Hyperion® Web Analysis portlet to modify the document at runtime only.

Note: This feature is only supported in Oracle Web Center.

11 Performance Scorecard Portlet Pages

In This Chapter

About Performance Scorecard Portlets 137
Creating Portlet Pages 137

About Performance Scorecard Portlets

Build portlet pages in Edit mode to select the application data to display and the fashion in which to render it. You cannot change data in applications from portlet pages. You can use the following:

- Presentation views containing this scorecard data:
  - All scorecard components
  - Historic trend data
  - Values and performance chart
  - Annotations and initiatives
- Presentation views containing this measure data:
  - Historic trend data
  - Values and performance chart
  - Annotations
- Measure Performance Report
- Scorecard Performance Report content
- Initiative Status Report
- Employee Details Report

Creating Portlet Pages

➤ To create portlet pages:

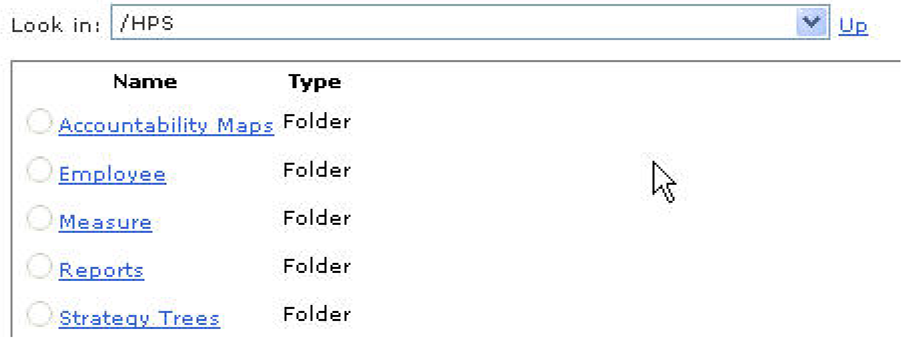
1. **Log in to the portal using the credentials specified during installation and configuration.**
2. **Perform these tasks:**
   - Create a portal and add the **Hyperion** portlet.

- Connect to the Performance Scorecard database.
- Enable **Edit Mode** to add content to the portlet page.

3 **Navigate the application hierarchy shown below in which data is grouped by type.**

For example, to use accountability element data, select **Accountability Maps**, then *map*, and then *element*.

Figure 1 Data Type Selection



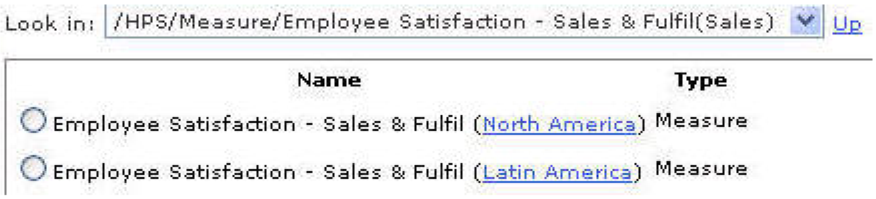
Look in: /HPS Up

	Name	Type
○	Accountability Maps	Folder
○	Employee	Folder
○	Measure	Folder
○	Reports	Folder
○	Strategy Trees	Folder

4 **To select dimensional measures, select Measure, then *measure template*, and then *measure*.**

For example, to select the dimensional measure quantifying Employee Satisfaction for North American offices, select **Measure**, then **Employee Satisfaction**, then **North America**, and then *office*, as shown:

Figure 2 Dimensional Measure Selection



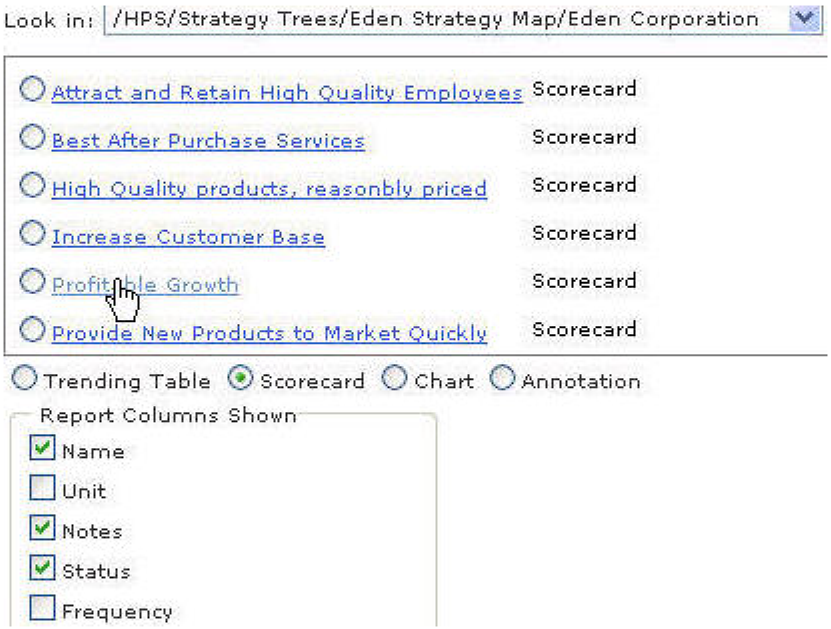
Look in: /HPS/Measure/Employee Satisfaction - Sales & Fulfil(Sales) Up

	Name	Type
○	Employee Satisfaction - Sales & Fulfil (North America)	Measure
○	Employee Satisfaction - Sales & Fulfil (Latin America)	Measure

5 **Select the data to display such as scorecard, and the associated content, such as the status, results, and so on.**

For example, in the following figure the portlet page will contain the name, status, and any notes for all components on the scorecard evaluating the performance of the **Profitable Growth** strategy element.

Figure 3 Content Selection



Look in: /HPS/Strategy Trees/Eden Strategy Map/Eden Corporation

○ Attract and Retain High Quality Employees	Scorecard
○ Best After Purchase Services	Scorecard
○ High Quality products, reasonbly priced	Scorecard
○ Increase Customer Base	Scorecard
○ Profitable Growth	Scorecard
○ Provide New Products to Market Quickly	Scorecard

○ Trending Table ● Scorecard ○ Chart ○ Annotation

Report Columns Shown

☑ Name

☐ Unit

☑ Notes

☑ Status

☐ Frequency

6 **Build presentation views. See:**

- "Measure Trending Table" on page 139
- "Measure Chart" on page 140
- "Annotations " on page 140
- "Scorecard Trending Table " on page 140
- "Scorecard Detail " on page 141
- "Scorecard Chart " on page 141

Measure Trending Table

Click the calendar icon, 📅, in **From** and **To** to specify a date range for which to display measure data. Then select display preferences:

- PTD Result—Results calculated by period-to-date formulas or manually entered
- Result—Results collected during the period of time that you specify
- Target—Target value used during the period of time that you specify
- Score—Previous scores achieved during the time that you specify
- Status—Performance levels during the period of time that you specify
- Status as color—Apply the color corresponding to the performance level, such as green for good performance, to the page
- Trend—If performance has improved, declined, or remained the same
- Shown targets—Calculate the score or performance level of the measure using another target

Measure Chart

Click the calendar icon, 📅, in **From** and **To** to specify a date range for which to graph data. Then select display preferences:

- Display legends—Text describing the measure values graphed
- Chart type—Kind of chart to use. Select combo to display measure data in bars and lines in a single graph.
- Display uncollected results—Display indicators or substitute values for unavailable results
- Score—Graph scores
- Result—Graph result values
- PTD result—Graph calculated period-to-date result values
- Targets—Graph target values
- Targets show—Calculate and graph measure score or performance level using another target.

Annotations

- Reporting period—The period of time, such as a corporate event or financial quarter for which context-specific annotations and notes exists.
- Show attachments—Link to file attachments

Scorecard Trending Table

Click the calendar icon, 📅, in **From** and **To** to specify a date range for which to display scorecard data. Then select display preferences:

- Group by perspective—Display scorecard measures by perspective
- Result—Display results
- Target—Target values used to evaluate performance
- Score—Previous scores
- Status—Previous performance levels
- Status as color—Apply the color corresponding to the performance level, such as yellow for acceptable performance, to the page
- Trend—If the performance of the object that the scorecard evaluates, has improved, declined, or remained the same

Scorecard Detail

Click the calendar icon, , in **From** and **To** to specify a date range for which to display scorecard —related data (one year ago-present). Then select display preferences:

- Notes—Link to associated notes
- PTD Result—Measure results calculated by period-to-date formulas or manually entered
- Result—Measure results
- Data confidence—Indicate as a percent or fraction the extent to which missing results impact overall performance.
- Unit—Units quantifying measures, such as hours
- Frequency—Frequency that determines when measure results are collected
- Owners—Employees who own measures
- Target setters— Employees who enter measure target values
- Data collectors—Employees who enter measure results
- Target—Current value of the measure target
- Targets shown—Calculate and display scorecard performance level or score using another target.
- Target score—Score of target
- Score—Scorecard or measure scores
- Status—Current performance level
- Weight—Percent indicating how much scorecard components are used to evaluate performance
- Show scores—Scores for the perspectives that group measures on the Perspective Chart
- Weighted score—Indicates the extent to which perspective scores impact performance (on Perspective Chart)
- Status as color—Apply the color corresponding to the performance level, such as green for good performance, to the page
- Trend—Indicate if the performance of the object that the scorecard evaluates has improved, declined, or remained the same

Scorecard Chart

Click the calendar icon, , in **From** and **To** to specify a date range for which to graph data. Then select display preferences:

- Legends—Text that identifies each kind of data graphed
- Short perspective name—Use abbreviated perspective names
- Scale x y axis—Automatically adjust axis sizing to accommodate data
- Row\column layout—Specify how to display multiple charts and graphs

- Chart type—The kind of graphs to use
- Scores—Raw scores of perspectives on the Perspective Chart
- Show weighted scores—Scores of perspectives based on the weighting of the measures that they group.
- Result—Graph all measure result values in a Radar Chart
- Normalize results—Display scorecard components as adding to 100% while maintaining their relative individual weights. This scales measures so that they fit on the Radar Chart.
- Target—Graph target values
- Comparator—Calculate and graph values using a different reporting target