Hyperion® Performance Suite™

Release 8.3

Hyperion® Foundation Administrator's Guide

Hyperion®

Hyperion Solutions Corporation

P/N: D830483000

Copyright © 1999–2004 Hyperion Solutions Corporation.
All rights reserved.

“Hyperion” and Hyperion's product names are trademarks of Hyperion. References to other companies and their products use trademarks owned by the respective companies and are for reference purpose only.

No portion of this manual may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, without the express written permission of Hyperion.

The information contained in this manual is subject to change without notice. Hyperion shall not be liable for errors contained herein or consequential damages in connection with the furnishing, performance, or use of this material.

This software described in this manual is licensed exclusively subject to the conditions set forth in the Hyperion license agreement. Please read and agree to all terms before using this software.

GOVERNMENT RIGHTS LEGEND: Use, duplication or disclosure by the U.S. Government is subject to restrictions set forth in the applicable Hyperion license agreement and as provided in DFARS 227.7202-1(a) and 227.7202-3(a) (1995), DFARS 252.227-7013(c)(1)(ii) (Oct 1988), FAR 12.212(a) (1995), FAR 52.227-19, or FAR 52.227-14, as applicable.

Hyperion Solutions Corporation
1344 Crossman Avenue
Sunnyvale, California 94089

Printed in the U.S.A.

Contents in Brief

Preface

PART I Overview

CHAPTER 1 The Foundation

CHAPTER 2 Administration Tools and Tasks

PART II Security

CHAPTER 3 Role-Based Access Control

CHAPTER 4 Managing Users, Groups, and Roles

CHAPTER 5 Authentication and Login

CHAPTER 6 Integrating Hyperion Applications

PART III Content

CHAPTER 7 Administering Content

CHAPTER 8 Administering Jobs

PART IV Configuration and Maintenance

CHAPTER 9 Configuring the RSC Services

CHAPTER 10 Configuring the LSC Services and Other System Configuration

CHAPTER 11 Configuring the Servlets

CHAPTER 12 Backing Up

PART V System Management

CHAPTER 13 Usage Tracking

CHAPTER 14 Troubleshooting

PART VI Appendices, Glossary, and Index

APPENDIX A Row-Level Security in BQY Documents

APPENDIX B Process Monitor Implementation

Glossary

Index

Contents

Preface

Purpose xv
Audience xvi
Document Structure xvi
Related Documents xvi
Where to Find Documentation xx
Conventions xxi
Additional Support xxii
Documentation Feedback xxiii

PART I Overview

CHAPTER 1 The Foundation

Licensed Packages 1-3
Integration with Hyperion Analyzer and Hyperion Reports 1-3
Architecture 1-4
- Characteristics 1-4
- The Big Picture 1-5
- Note About Security 1-9
- LSC Services and RSC Services 1-10
- Per-Solution Architectures 1-11

Suite Components 1-20
- Core Services 1-20
- Management Services 1-24
- Functional Services 1-25
- Client Components 1-27

Software Development Kit and Web Services 1-28
The Architecture at Work 1-29
Authenticating a User (User Login) 1-30
Displaying a Folder Listing 1-32
Opening an Item 1-33
Publishing a File 1-34
Publishing a BQY File 1-35
Publishing a BQY Job 1-37
Publishing an SQR Job 1-38
Running a BQY Job *Ad Hoc* *1-40*
Running an SQR Job (or Generic Job) *Ad Hoc* *1-43*
Executing a Scheduled BQY Job 1-46
Subscriptions and Notifications 1-47

CHAPTER 2 Administration Tools and Tasks

Administration Tools 2-2
Administration Module 2-2
Remote Service Configurator 2-3
Local Service Configurator 2-4
What Does *Install_Home* Mean? 2-4
Servlet Configurator 2-4
Starting and Stopping the Services 2-5
Before Starting Any Services 2-6
Starting All Services 2-7
Starting a Subset of Services 2-10
Starting Services Individually 2-12
Starting Services in Order 2-15
Stopping Services 2-17
Example of How a Service Starts 2-18
Starting the Servlets 2-19
Quick Guide to Common Administrative Tasks 2-19
Summary 2-21

PART II Security

CHAPTER 3 Role-Based Access Control

About Role-Based Access Control 3-2
Roles 3-2
Groups 3-3

Access Control 3-4
RBAC Implementation 3-5
Access Privileges on Objects 3-8
Printer and Output Directory 3-8
Public Events 3-9
Personal Events 3-9
Jobs and Job Output 3-9
Shortcuts and Other Items 3-10
User 3-10
Group and Role 3-11
Standard RBAC Configuration 3-12
Global Administrator, Administrator, and Content Administrator . . . 3-12
Pre-Configured Roles 3-13
Pre-Configured Users and Groups 3-16
Pre-configured Access Control Settings for Users 3-16
Checking Access Privileges 3-18
Access Privilege Checking for Items 3-18
Access Privilege Checking on Services 3-20
Denying Access 3-21
Additional Access Privilege Checking Examples 3-22
Adaptive States for Intelligence Roles 3-25
Recommendations about Assigning Intelligence Roles 3-26
Summary 3-28

CHAPTER 4 Managing Users, Groups, and Roles

About Managing Users, Groups, and Roles 4-2
Authentication Systems 4-2
Active and Inactive Users and Groups 4-3
Access Control on Users, Groups, and Roles 4-3
Modifying Users, Groups, and Roles 4-4
General Modifying Tasks 4-5
General Properties 4-7
Modifying Associations Between Users, Groups, and Roles 4-9
Modifying Access Privileges 4-11
Adding Users, Groups, and Roles 4-12
Adding a User 4-12
Adding a Group 4-14
Adding a Role 4-14

Creating a Mini-Administrator 4-15
Setting Access Privileges for Publishing 4-16
Summary 4-16

CHAPTER 5 Authentication and Login

Authentication Service Function 5-2
What an Authentication Service Manages 5-2
Types of Authentication 5-3
Native Authentication 5-3
External Authentication 5-3
Synchronization with External Systems 5-5
User Synchronization 5-5
Group Synchronization 5-5
Pass-Through for Jobs and BQY Files 5-6
Configuring Login 5-8
Logging in Directly 5-8
Transparent Login 5-10
Prerequisites for Transparent Login 5-10
Configuring Transparent Login 5-12
Sources for Login Information 5-13
Automatic Login with URLs 5-13
Custom Policies and Macros 5-16
Configuring a Trusted Password 5-19
Summary 5-19

CHAPTER 6 Integrating Hyperion Applications

About Single Sign-On 6-2
Support for SiteMinder 6-3
Prerequisites 6-4
Setting Up the Environment for NT LAN Manager Support 6-5
Setting Up User Rights for NT LAN Manager 6-5
Setting Up User Rights on Windows NT 6-6
Setting Up User Rights on Windows 2000 6-7
UNIX Application Support for NT LAN Manager 6-8
Configuring the Security Platform Driver 6-9
Configuring the Preferred Logging Priority 6-9
Configuring the Provider Search Order 6-10
Configuring Token Timeout 6-11
Configuring an LDAP or Active Directory Provider 6-12

Configuring an NTLM Provider 6-19
Configuring for SiteMinder Single Sign-On 6-21
Sample Deployment Scenarios 6-22
Scenario 1: Single LDAP Directory 6-23
Scenario 2: Single Microsoft Active Directory 6-24
Scenario 3: UNIX Application and Single NTLM Domain 6-25
Scenario 4: Windows Application and Single NTLM Domain 6-26
Scenario 5: UNIX Application Against LDAP, Microsoft Active Directory, and NTLM 6-27
Scenario 6: Windows Application Against LDAP, Microsoft Active Directory, and NTLM 6-28
Scenario 7: Multiple Microsoft Active Directory Instances 6-30
Scenario 8: Multiple LDAP Directory Instances 6-31
Scenario 9: Multiple NTLM Domains 6-32
Scenario 10: Multiple NTLM Domains Connected with Hyperion Remote Authentication Module 6-32
Scenario 11: Single Sign-on with SiteMinder 6-34
Deployment References from LDAP Product Vendors 6-35
About Related Content and Hyperion Hub 6-37
Administrating Related Content 6-37
Using a Property File as a Local Registry 6-38
Set Other Related Content Properties 6-38
Summary 6-39

PART III Content

CHAPTER 7 Administering Content

Organizing Items and Folders 7-2
Working with MIME Types 7-2
Creating a MIME Type 7-3
Modifying a MIME Type 7-3
Inactivating or Re-activating a MIME Type 7-4
Deleting a MIME Type 7-5
Administrating Pushed Content 7-5
Administering Personal Pages 7-6
Setting Up the Generated Personal Page 7-6
Understanding Broadcast Messages 7-9
Providing Optional Personal Page Content to Users 7-10
Displaying an HTML File as a File Content Window 7-10
Setting Up Graphics for Bookmarks 7-11

Configuring Exceptions 7-11
Example of Setting Up Content for Personal Pages 7-12
Viewing the New Users' Personal Page 7-15
Publishing Personal Pages 7-15
Configuring Other Personal Pages Properties 7-16
Summary 7-16

CHAPTER 8 Administering Jobs

Managing Calendars 8-2
Creating a New Calendar 8-4
Deleting Calendars 8-4
Modifying Calendars 8-5
Calendar Manager Properties 8-6
Viewing the Job Log 8-9
Managing Job Elements 8-12
Managing Time Events 8-12
Administering Public Job Parameters 8-16
Managing OCE Files 8-16
Managing Pass-Through for Jobs and BQY Files 8-17
Managing Scheduled Jobs 8-17
Administering Physical Resources 8-18
Adding a Physical Resource 8-18
Modifying a Physical Resource 8-18
Deleting a Physical Resource 8-19
Access Privileges 8-19
Properties of Printers 8-20
Properties of Output Directories 8-21
Summary 8-22

PART IV Configuration and Maintenance

CHAPTER 9 Configuring the RSC Services

Using the Remote Service Configurator (RSC) 9-2
Starting the Remote Service Configurator 9-2
Changing the Authentication System 9-4
The RSC Toolbar 9-5
Deleting a Service 9-6
Pinging a Service 9-6
Defining Hosts 9-7

Changing the Database Password 9-12
Changing the Database Driver or JDBC URL 9-14
Defining Database Servers 9-16
Adding Services 9-22
Modifying Service Properties 9-22
Common Properties 9-24
General Properties 9-24
Advanced Properties 9-26
Storage Properties 9-27
Job Service-Specific Properties 9-29
Database Properties 9-30
SQR Properties 9-32
Application Properties 9-33
Executable Properties 9-38
Job Service Overview 9-40
About Job Services 9-40
Example: Configuring a Job Service for SAP 9-44
Using the ConfigFile Utility 9-49
config.dat 9-49
Modifying the Config.dat File 9-51
Explicit OCE Access to Process BQY Documents/Job Output 9-52
Summary 9-54

CHAPTER 10 Configuring the LSC Services and Other System Configuration

The Local Service Configurator (LSC) 10-2
Starting the Local Service Configurator 10-3
The LSC Toolbar 10-4
Modifying Properties of LSC Services 10-5
Services with Only the Standard Properties 10-6
Authentication Service 10-7
Authentication System: Definition and Default Properties 10-9
Intelligence Service 10-20
Data Access Service 10-23
Modifying the Host Properties 10-29
General Properties 10-30
Database Properties 10-32
Modifying the System Properties 10-34
General Properties 10-34
Notification Properties 10-35

SmartCut Properties 10-37
User Interface 10-39
Registering Hyperion Performance Suite to Hyperion Hub 10-40
Managing Row-Level Security 10-41
The portal.properties File 10-42
Summary 10-43

CHAPTER 11 Configuring the Servlets

Using the Servlet Configurator 11-2
The Properties 11-5
User Interface Properties 11-5
Personal Pages Properties 11-14
Internal Properties 11-17
Cache Properties 11-19
Diagnostics Properties 11-22
Applications Properties 11-23
Changing Application Context 11-25
Zero Administration and the Hyperion Intelligence Client 11-27
Server Processing 11-27
Client Processing 11-28
Load Testing Hyperion Intelligence Clients 11-29
Data Access Servlet 11-29
Data Access Service 11-30
Intelligence Service 11-30
Summary 11-30

CHAPTER 12 Backing Up

What to Backup 12-2
General Backup Procedure 12-2
Backing Up the Hyperion Performance Suite File System 12-3
Complete Backup 12-4
Post-Installation 12-4
Weekly Full and Daily Incremental 12-5

As Needed 12-5
Reference Table for All File Backups 12-6
Sample Backup Script 12-7
Backing Up the Repository Database 12-8
Backing Up the Clients 12-8
Summary 12-8

PART V System Management

CHAPTER 13 Usage Tracking

About Usage Tracking 13-2
How Does Usage Tracking Work 13-2
What Events Can Be Tracked 13-3
Server Time 13-3
Managing Usage Tracking 13-4
Usage Tracking Properties 13-4
Sample Usage Tracking Reports 13-7
Summary 13-8

CHAPTER 14 Troubleshooting

Logging Architecture 14-2
Log4j 14-2
The Logging Service 14-3
Log Management Helper 14-3
Server Synchronization 14-3
Log File Basics 14-4
Location of Log Files 14-4
Log File Naming Convention 14-6
File Format of Log Messages 14-8
Configuring Log Files for Troubleshooting 14-9
Configuration Files 14-9
Configuring Log Levels 14-11
Configuring Appenders 14-13
Configuring Log Rotation 14-15

Analyzing Log Files 14-17
Viewing Log Files 14-17
Standard Console Log File 14-17
Analyzing Specific Log Files 14-18
What to Send to Customer Support 14-24
Summary 14-24

PART VI Appendices, Glossary, and Index

APPENDIX A Row-Level Security in BQY Documents

About Row-Level Security A-2
The Row-Level Security Paradigm A-2
Hyperion Performance Suite and Row-Level Security A-3
Row-Level Security Tables A-6
Creating the Row-Level Security Tables A-6
The BRIOSECG Table A-7
The BRIOSECR Table A-9
Row-Level Security Examples A-12
Defining the Users and Groups A-14
Dealing with “The Rest of the Users” A-15
Overriding Constraints A-16
Cascading Restrictions A-17
Other Important Facts A-19
Custom SQL A-19
Limits A-20
Naming A-22

APPENDIX B Process Monitor Implementation

About Process Monitors B-2
Using Process Monitors B-3
Configuring a Process Monitor B-4
Starting a Service Using a Process Monitor B-6

Glossary

Index

Preface

Welcome to the *Hyperion Performance Suite Foundation Administrator's Guide*. This preface discusses the following topics:

- "Purpose" on page xv
- "Audience" on page xvi
- "Document Structure" on page xvi
- "Related Documents" on page xvi
- "Where to Find Documentation" on page xx
- "Conventions" on page xxi
- "Additional Support" on page xxii
- "Documentation Feedback" on page xxiii

Purpose

This guide provides information that you need to administrator the entire Hyperion Performance Suite system of services, applications, and tools. Most of the information, however, concerns the Hyperion Foundation components, rather than the intelligence or reporting components.

This book does not cover end-user tasks. It assumes that you have read the *Foundation User's Guide*.

Note This book covers the entire Hyperion Performance Suite system, while you may have installed only a subset of it. Therefore, components and features that your system does not include are discussed in this book. For more information, see "Licensed Packages" on page 1-3.

Audience

This guide is written for all levels of administrators, from those who administer only a group of users, to those who oversee the entire system. In addition, some information is intended for developers of SQR programs or system customizations, or for Designer users of BQY files.

Document Structure

This document contains the following information:

- Part I, "Overview," introduces the system architecture, administrative tools, and administrative tasks.
- Part II, "Security," explains the concepts and administration of user authentication and role-based access control.
- Part III, "Content," covers administration related to documents and jobs.
- Part IV, "Configuration and Maintenance," explains how to configure and maintain the system services, applications, and tools, and how to reconfigure or expand, back up, and optimize your system.
- Part V, "System Management," explains how the Management Services work to help you troubleshoot and analyze your system usage.
- Part VI, "Appendices, Glossary, and Index," specifies detailed information about process monitors and row-level security and provides definitions and easy access to information contained in the book.

The Glossary contains a list of key terms and their definitions.

The Index contains a list of Hyperion Performance Suite terms and their page references.

Related Documents

Hyperion Performance Suite's comprehensive documentation set offers detailed technical information, troubleshooting advice, and best practices guidelines that help you maximize your Hyperion Solutions experience. In addition to the manuals listed, Hyperion Performance Suite products include substantial online help systems and release notes.

Note The documents listed in this section are located on the Document CD that ships with Hyperion Performance Suite.

General Documentation

What's New in Hyperion Performance Suite describes the new functionality of the Hyperion Performance Suite system.

The *Hyperion Performance Suite Installation Guide* provides the information you need to successfully install the Hyperion Performance Suite software on both Microsoft Windows and UNIX systems. It includes operating system and third-party software requirements; installation instructions and prerequisite information; installation details including directory structure and contents, registry entries, and sample INI, config, log, and startup files; configuration information for those administration tasks necessary to complete installation; and troubleshooting information including error messages.

The *Hyperion Performance Suite Migration Guide* provides guidelines and recommendations for migrating from Brio Portal 7. 0.x to Hyperion Performance Suite, and for migrating from Brio Intelligence 6.5 to Hyperion Performance Suite.

The *Hyperion Performance Suite Accessibility Guide* describes the accessibility features of all Hyperion Performance Suite products.

Hyperion Foundation Documentation

The *Hyperion Foundation User's Guide* explains how to use Hyperion Performance Suite to find the information you need, make often-used information readily accessible, share information with others, and generate reports. The *Hyperion Foundation User's Guide* is written for all levels of Hyperion Performance Suite users, from those who need to simply find and view documents, to those who need to publish many kinds of files or schedule jobs and distribute the output around the globe.

The *Hyperion Foundation Developer's Guide* provides information on how to customize and extend Hyperion Performance Suite using Foundation APIs, JSP pages, HTML templates, and other provided developer resources. This book is written for Java developers who need to customize the user interface and extend their system.

Hyperion Intelligence Documentation

The *Hyperion Intelligence Getting Started Guide* provides an overview of the Hyperion Intelligence client components and explains the user interface and basic commands. It includes information on how to retrieve data, how to query new data and change existing queries, and how to query a single database as well as multiple databases. It also covers how to work with query results. It is written for all levels of Hyperion Intelligence users.

The *Hyperion Intelligence Data Analysis and Reporting Guide* introduces the types of reports available in the Hyperion Intelligence client components and provides an overview of reporting concepts. It is written for all levels of Hyperion Intelligence users, from those who need to simply retrieve and view data in a report format, to those who need to build queries and reports as well as analyze data.

The *Hyperion Intelligence Object Model and Dashboard Design Guide* provides an understanding of Dashboard sections, and of the JavaScript syntax and object framework, specifically as they apply to interacting with BQY document elements. This book is written for developers who create documents using Hyperion Explorer or Hyperion Designer and who need to create front-ends using the Dashboard functionality provided by Hyperion Intelligence.

The *Hyperion Intelligence Administrator's Guide* helps administrators manage Hyperion Intelligence. The book is written for Hyperion Explorer and Hyperion Designer users who have access to more advanced features (such as connectivity and data modeling) and who may have responsibility for implementing Hyperion Intelligence in an enterprise environment.

Hyperion SQR Documentation

The *Hyperion SQR Getting Started Guide* provides procedures and code example to help develop SQR reports. This book is written for programmers who have a working knowledge of SQL and experience in writing software programs and who are developing reports for relational databases.

The *Hyperion SQR Language Reference* describes the structure, command set, and syntax of the SQR language. It also provides a directory to the library of sample SQR programs, an overview of the SQR initialization file, and a listing of SQR messages. This reference is intended for Hyperion SQR and SQL developers who must report on data from a wide range of enterprise datasources.

Designing Reports with Hyperion SQR Developer explains how to create SQR reports on Windows systems using Hyperion SQR Developer, Hyperion Solutions's GUI report design and layout tool. This book is written for anyone who wishes to create reports using the SQR Developer graphical user interface. To use this book effectively, you should be familiar with general report creation and your particular database and operating system. If you wish to create more complex reports using Hyperion SQR, you should be familiar with the SQR syntax and commands.

Accessing Data with Hyperion SQR for DDO provides an abstraction layer for heterogeneous data sources. This book describes DDO, its architecture and interfaces. It provides examples and instructions for accessing data from a DDO application and for writing a DDO driver. The book also discusses programming considerations and DDO common utilities. This book is written for developers who want to write DDO drivers that implement the DDO interfaces, as well as application developers who want to use the DDO interfaces for data access in their applications.

Using Hyperion SQR Activator explains how to integrate Hyperion SQR into a business application using an application development environment (such as Visual Basic) that supports Microsoft ActiveX Controls to satisfy production

and enterprise reporting needs. This book is written for application developers familiar with ActiveX controls who want to give their users the ability to run, view, and print SQR reports as part of their applications.

Where to Find Documentation

All Hyperion Performance Suite documentation is accessible from the following locations:

- Online help is accessible from the product that it documents. Start the product and click the Help button or menu command.
- The Hyperion Solutions Web site is located at `http://www.hyperion.com`.
- Access to the Hyperion Download Center is through `http://hyperion.subscribenet.com`.

To access documentation from the Hyperion Solutions Web site:

1. **Log on to** `http://www.hyperion.com`.
2. **Select the Support link and type your username and password to log on.**

Note New users must register to receive a username and password.

3. **Follow the on-screen instructions.**

To access documentation from the Hyperion Download Center:

1. **Log on to** `http://hyperion.subscribenet.com`.
2. **In the Login ID and Password text boxes, enter your assigned login ID name and password. Then click Login.**
3. **If you are a member on multiple Hyperion Download Center accounts, select the account that you want to use for the current session.**
4. **Follow the on-screen instructions.**

To order printed documentation:

1. **Visit the Hyperion Solutions Web site at** `http://www.hyperion.com`.
2. **In the United States, call Hyperion Solutions Customer Support at 877-901-4975.**
3. **From outside the United States, including Canada, call Hyperion Solutions Customer Support at 203-703-3600. Clients who are not serviced by support from North America should call their local support centers.**

Conventions

The following table shows the conventions that are used in this document:

Table 1 Conventions Used in This Document

Item	Meaning
➤	Arrows indicate one-step procedures.
Bold	Bold highlights options, buttons, or tabs that you need to choose and text that you need to type.
CAPITAL LETTERS	Capital letters denote commands and various IDs. For example: CLEARBLOCK command
[Ctrl + O]	Keystroke combinations shown with the plus sign (+) indicate that you should press the first key and hold it while you press the next key. Do not type the plus sign.
`Example text`	Courier font indicates that the example text is code or syntax. Courier font is also used for file names, directory/folder names, and path names. For example: `Sample1.bqy` is located in the `\HYPERION_HOME\Samples` directory.

Table 1 Conventions Used in This Document *(Continued)*

Item	Meaning
Courier italics	Courier italic text indicates a variable field in command syntax. Substitute a value in place of the variable shown in Courier italics.
Mouse orientation	This document provides examples and procedures using a right-handed mouse. If you use a left-handed mouse, adjust the procedures accordingly.
Menu options	Options in menus are shown in the following format. Substitute the appropriate option names in the placeholders, as indicated. ***Menu name→Menu command→Extended menu command*** For example: **1.** Select **File→Desktop→Accounts**.

Additional Support

In addition to providing documentation and online help, Hyperion offers the following product information and support. For details on education, consulting, or support options, visit Hyperion's Web site at `http://www.hyperion.com`.

Education Services

Hyperion offers instructor-led training, custom training, and eTraining covering all Hyperion applications and technologies. Training is geared to administrators, end users, and information systems (IS) professionals.

Consulting Services

Experienced Hyperion consultants and partners implement software solutions tailored to clients' particular reporting, analysis, modeling, and planning requirements. Hyperion also offers specialized consulting packages, technical assessments, and integration solutions.

Technical Support

Hyperion provides enhanced electronic-based and telephone support to clients to resolve product issues quickly and accurately. This support is available for all Hyperion products at no additional cost to clients with current maintenance agreements.

Documentation Feedback

Hyperion strives to provide complete and accurate documentation. We value your opinions on this documentation and want to hear from you. Give us your comments by going to `http://www.hyperion.com/services/support_programs/doc_survey/index.cfm`.

PART I

Overview

1 The Foundation

Hyperion Performance Suite stores, protects, and delivers information for your extended enterprise (employees, customers, suppliers and partners). It enables users to analyze, transform, and report data; share, search for, retrieve, and use documents; run queries, execute and schedule jobs, and distribute job output. This functionality can be accessed from the application programs or from a web browser.

The Hyperion Foundation supports the entire Suite and is composed of an extensible set of security platform that underlie the end-user applications of the Suite, plus the various administrative and configuration tools. The Foundation offers role-based access control to secure all of the resources of the system, which include documents, jobs, users, groups, and so on. Hyperion Performance Suite's access control determines, for example, which documents a user can access, and which operations the user can perform on them. So any document can be published in the Repository without compromising its confidentiality.

This chapter describes the product packages of Hyperion Performance Suite, its overall system architecture, Hyperion Foundation services, and the process flows of several basic operations. After reading this chapter, you should understand the services and the system architecture sufficiently to configure, maintain, and troubleshoot your Hyperion Foundation.

Not all of the information in this chapter is necessary for all administrators, especially when starting to work with Hyperion Performance Suite. You can skim this chapter for an overview of the Suite and the Foundation services. Later, you can use this chapter for reference.

In This Chapter

Licensed Packages 1-3

Architecture 1-4
Suite Components 1-20
The Architecture at Work 1-29

Licensed Packages

Hyperion Performance Suite consists of the following product packages:

- Hyperion Intelligence Designer
- Hyperion Intelligence Explorer
- Hyperion Intelligence Server
- Hyperion Intelligence iServer
- Hyperion SQR Developer
- Hyperion SQR iServer
- Hyperion SQR Server

Note If you are an existing Hyperion customer and would like to trial a new Hyperion product or extend an installed trial license, see the *Hyperion Performance Suite Installation Guide* for instructions.

Integration with Hyperion Analyzer and Hyperion Reports

Hyperion Performance Suite has been integrated with Hyperion Analyzer and Hyperion Reports. You can access Hyperion Analyzer and Hyperion Reports content through the Browse module of Hyperion Performance Suite. You can also access Hyperion Performance Suite content through Hyperion Analyzer and Hyperion Reports.

Hyperion Hub integrates the applications. External authentication using the security platform driver is required to use Hyperion Hub.

Architecture

This section outlines the architecture of Hyperion Performance Suite, with a focus on the Hyperion Foundation. The Foundation is a set of common services, servlets, and administrative tools that support the Suite as a whole.

Characteristics

The Hyperion Performance Suite system architecture has the following characteristics:

- **Modular –** If you have not installed all of the Hyperion Performance Suite components, you can add components in the future.
- **Distributed –** The Hyperion Performance Suite components can be distributed across a network, even on heterogeneous hosts (servers). They communicate with each other using either Hyperion's proprietary protocol or an industry-standard framework.
- **Scalable –** As your organization grows, replicated services can be added to handle the increase in users and information.
- **Secure –** Information is protected against unauthorized users at several levels, so every action on every Repository item is available only to users authorized for that action on that item. A full discussion of the security system is found in Chapter 3, "Role-Based Access Control."
- **Accessible –** Using the web-based application modules, end-users can access the system from anywhere, on any browser-capable device.

The Big Picture

Hyperion Performance Suite consists of a server, Java servlets that provide end-user and administrative applications across the web, and desktop tools for administrators and advanced end-users.

The Hyperion Performance Suite server infrastructure consists of collaborative services running on one or more heterogeneous servers in a network. The services can be grouped into *core services, management services*, and *functional services.* The core services are required in every system, providing essential services such as authorization, authentication, session management, and publication of documents. The functional services perform more specialized work and may not be part of every system. The management services provide a way to collect system messages and events for overall troubleshooting and usage pattern assessments.

The security in the system is maintained at three levels: authentication, service-based access, and object-based access. For more information, see Part II, "Security".

Figure 1-1 illustrates the server components and web applications of the system.

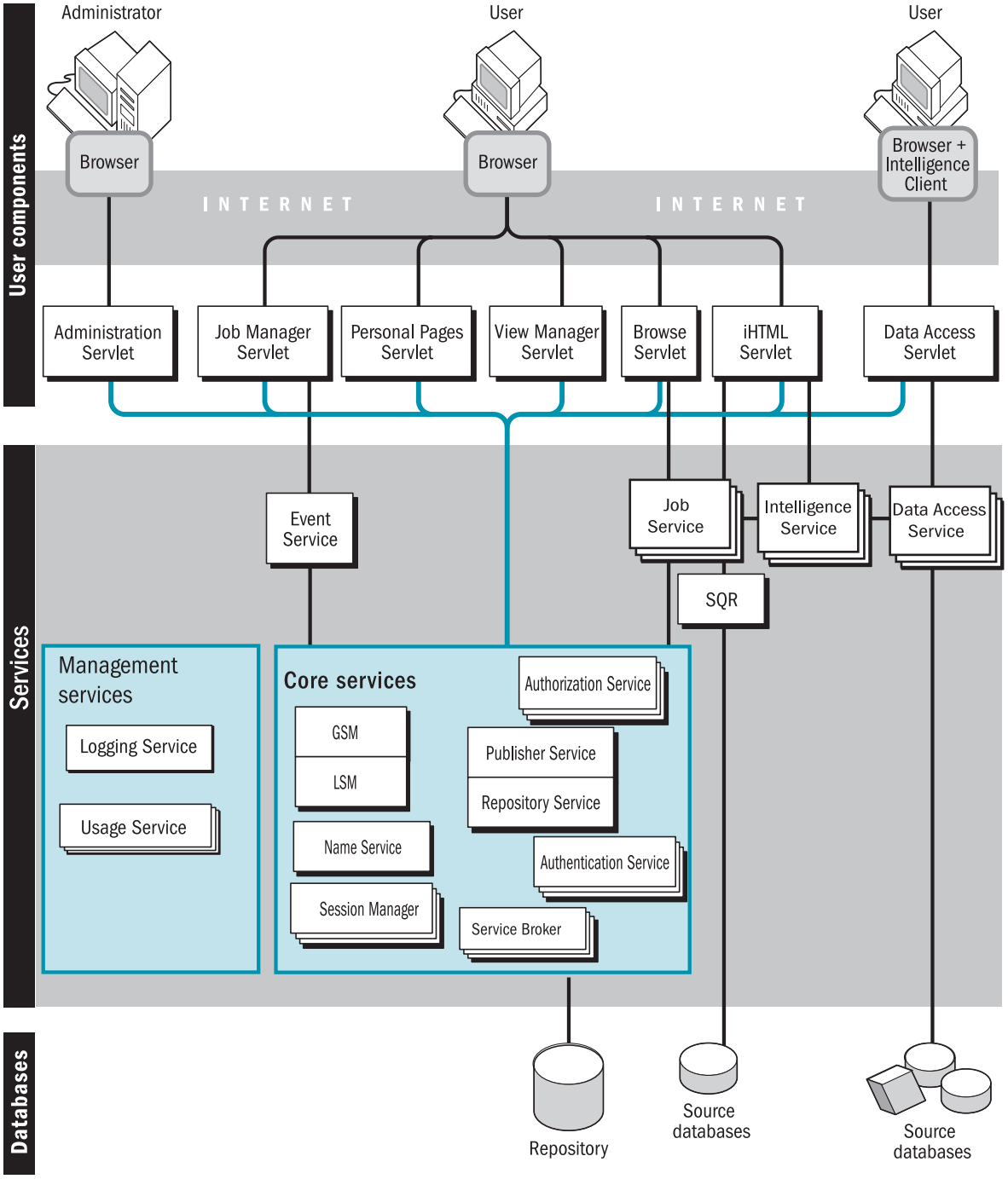


Figure 1-1 Hyperion Performance Suite

More than one service of the same type can exist in the system. You can replicate the following services:

- Service Broker
- Session Manager
- Authentication Service
- Authorization Service
- Job Service
- Usage Service
- Intelligence Service
- Data Access Service

(In addition, the system replicates the Local Service Manager (LSM) automatically for each new server process.)

Replicated services can provide expanded capacity as your user base grows, or be configured differently to perform different functions. Replicated services may use an event mechanism to communicate between themselves and maintain consistency when they cache information.

Users employ the services through web browsers, by accessing the Java servlets. There are also several desktop applications that provide configuration and other functionality, as shown in Figure 1-2. This book covers the Administration web module and the system configuration tools, which are for administrators. For information about the end-user components, see the *Hyperion Foundation User's Guide*.

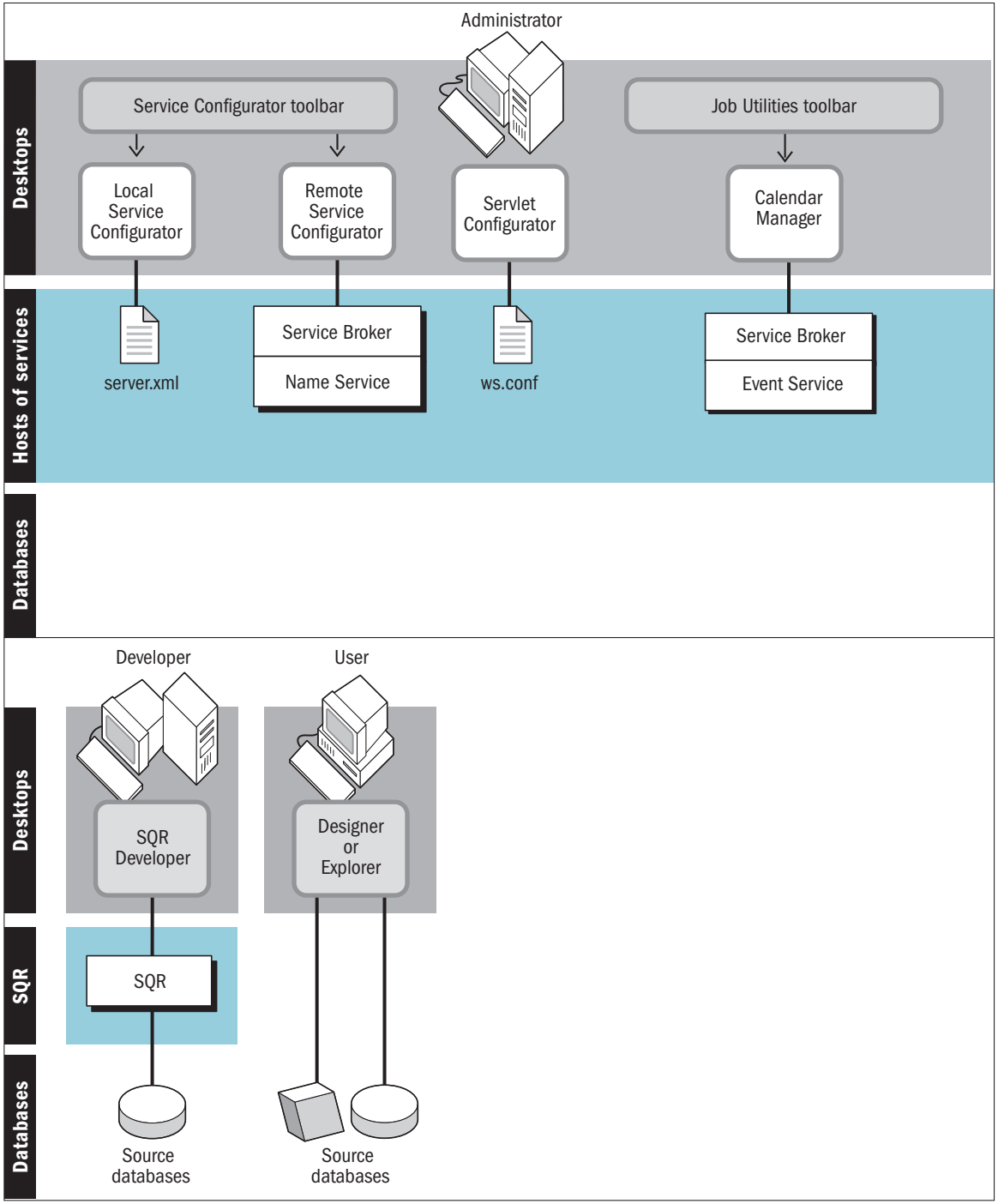


Figure 1-2 Desktop Applications and Tools

Note About Security

User authentication prevents access by unauthorized users.

Role-based access control determines what each authorized user can do with particular content items. You, the administrator, and users who own content items or have administrative privileges over users or groups, define who can perform which actions on each object (*resource*) in the system. The system enforces your restrictions: each time a user tries to access any resource in the system, access control checks whether that user is authorized to access that resource in the attempted manner. You can set up your authorization scheme based on either roles or groups. The Hyperion Performance Suite supports role-based authorization for ease of use and to reflect how authority is actually distributed in enterprises.

Caution! Users can browse all directories below the Hyperion Performance Suite deployment directory, regardless of the role assigned to them. To prevent users from browsing, you must block access through your Web server.

Caution! You should change the default passwords for the items in the following table for security reasons.

Table 1-1 Default Passwords

Password for:	Default Password	Location of instructions for changing the password
Global Administrator user	globaladministrator	See “General Properties” on page 4-7
Administrator user	administrator	See “General Properties” on page 4-7
Config.file	administrator	See “Modifying the Config.dat File” on page 9-51
ServletUser	administrator	See “ServletUser Password” on page 9-53

LSC Services and RSC Services

The Hyperion Foundation services fall into two groups, according to the communication protocol they use to interact with other services. One group uses a Hyperion proprietary communication protocol, while the other uses an industry-standard framework. This framework handles inter-service and service-to-servlet communications, as well as communication among the servlets.

You need to know which group a service belongs to in order to choose the correct tool to configure it. Accordingly, the services configured using the Local Service Configurator (LSC) are called LSC services, while those configured using the Remote Service Configurator (RSC) are called RSC services. Table 1-2 enumerates the services in each group.

Table 1-2 LSC Services and RSC Services

LSC Services	RSC Services
Global Service Manager	Name Service
Local Service Manager	Repository Service
Authentication Service	Service Broker
Session Manager	Job Service
Publisher Service	Event Service
Authorization Service	
(Super Service)	
Intelligence Service	
Logging Service	
Data Access Service	
Usage Service	

Per-Solution Architectures

This section divides the overall architecture, shown in Figure 1-1, into the sub-architectures of specific solutions. Diagrams show the components used by each.

Though most of the solutions are named after products, a given solution's component list may differ from that of the corresponding product, or from the set of components you have for a similar solution.

The sub-architectures depicted in this section are:

- Hyperion Intelligence iServer Solution
- Hyperion Intelligence Server Solution
- Content-Browsing Solution
- Hyperion SQR iServer Solution
- Hyperion SQR Developer Solution
- System Configuration Solution

Hyperion Intelligence iServer Solution

The Intelligence iServer solution as shown in Figure 1-3 employs the following Hyperion Performance Suite components: a web browser, the iHTML Servlet, the Job Service, the Intelligence Service, the Data Access Service, the core services, and the Repository.

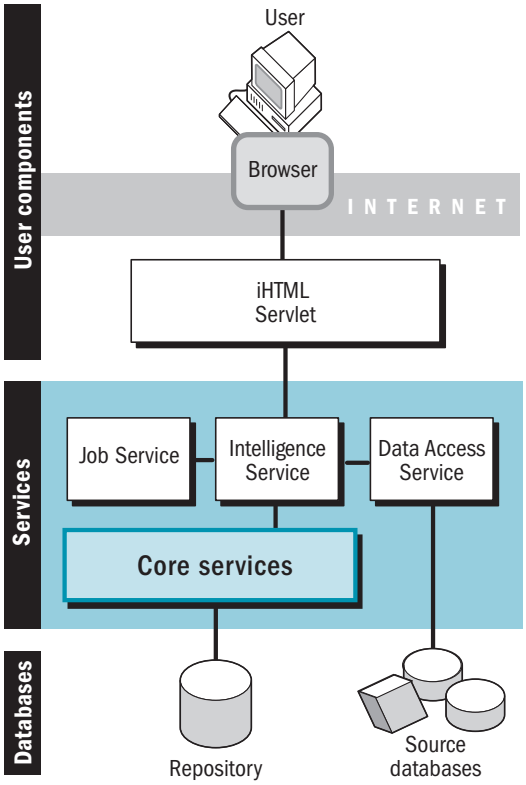


Figure 1-3 Intelligence iServer Solution

Hyperion Intelligence Server Solution

The Hyperion Intelligence Server as shown in Figure 1-4employs the following Hyperion Performance Suite components: a web browser with the Intelligence iServer plugin, the Data Access Servlet, the Job Service, the Data Access Service, the core services, and the Repository.

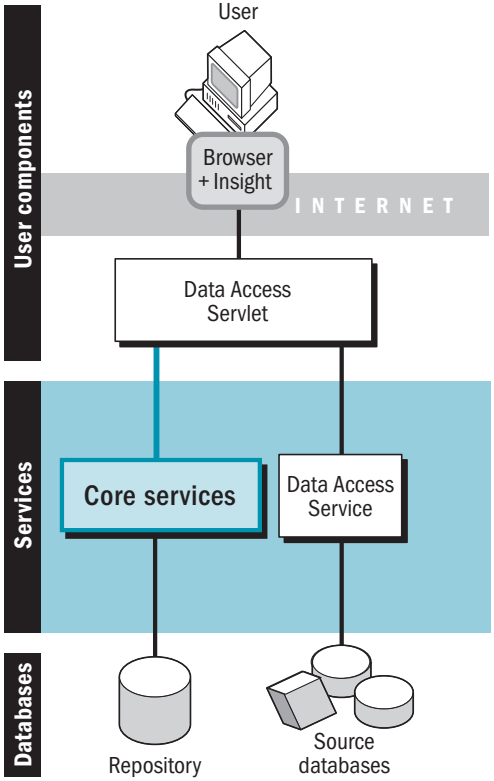


Figure 1-4 Intelligence Server Solution

Content-Browsing Solution

The Content-Browsing Solution as shown in Figure 1-5 refers to the functionality of the Foundation's Browse, View Manager, and Personal Pages servlets. These servlets enable users to browse or search for system content, open documents, and organize frequently used items for fast access. This solution utilizes the following components: web browser, the Browse Servlet, the View Manager Servlet, the Personal Pages Servlet, the core services, and the Repository.

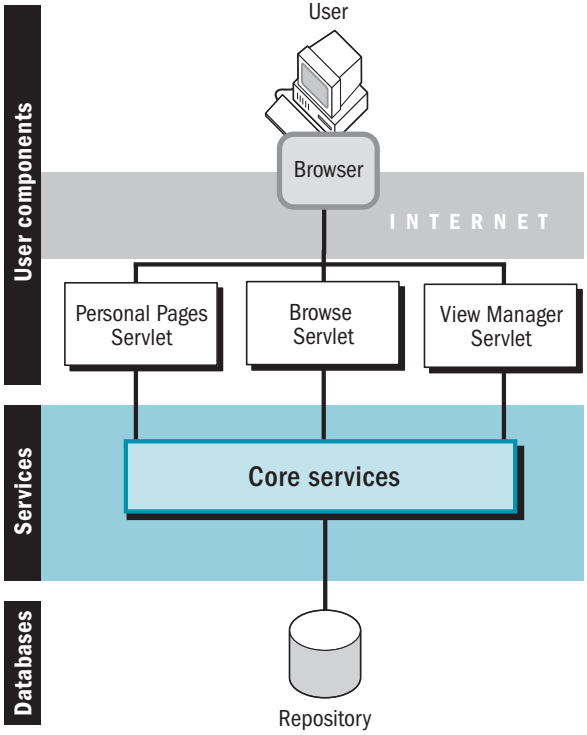


Figure 1-5 Content-Browsing Solution

Hyperion SQR iServer Solution

The SQR iServer solution as shown in Figure 1-6 includes running SQR jobs and viewing their output from the Browse servlet. This solution employs the following components: a web browser, the Browse Servlet, the Job Service, the SQR engine, the core services, and the Repository.

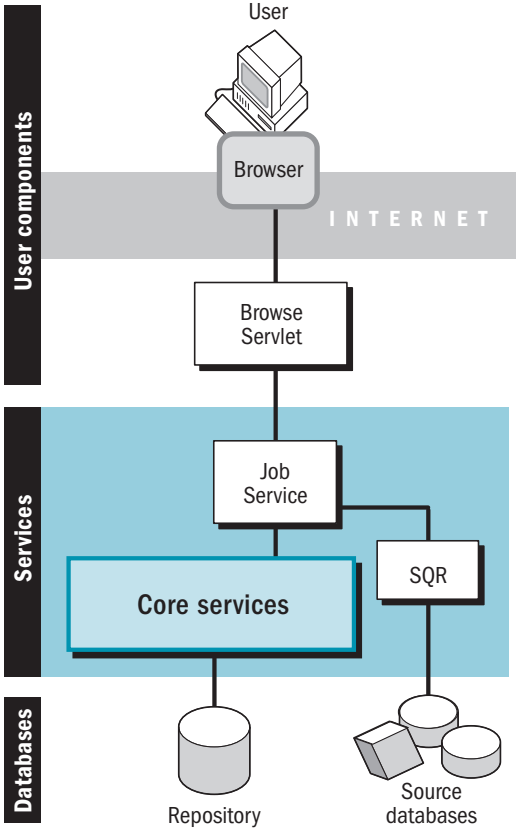


Figure 1-6 Hyperion SQR iServer Solution

Hyperion SQR Developer Solution

The Hyperion SQR Developer solution as shown in Figure 1-7 and Figure 1-8, for developing SQR programs, employs the Hyperion SQR Developer and the Hyperion SQR Server. Publishing SQR programs involves the Browse Servlet, the core services, and the Repository.

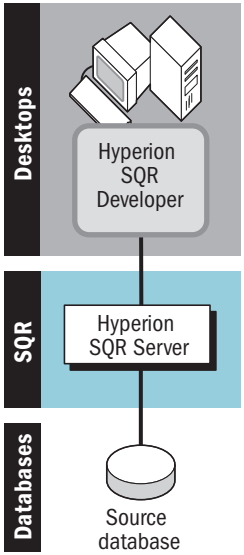


Figure 1-7 Hyperion SQR Developer Solution and Publishing SQR Jobs

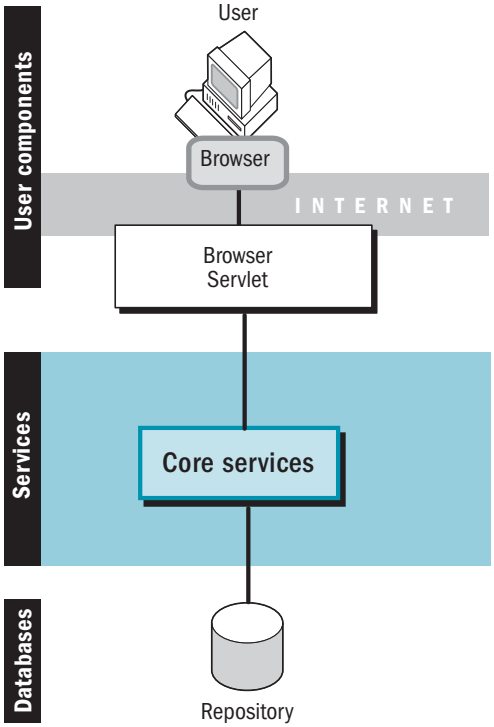


Figure 1-8 Publishing SQR Files

System Configuration Solution

The System Configuration solution as shown in Figure 1-9,Figure , and Figure 1-11 involves the following components:

- **When configuring the LSC services** – the Local Service Configurator and the XML file `server.xml`. You run the Local Service Configurator on the host of the Hyperion Performance Suite services to be configured.

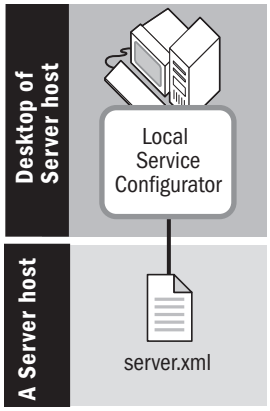


Figure 1-9 Configuration Solution—LSC Services

- **When configuring the RSC services** – the Remote Service Configurator and the Name Service. You can install and run the Remote Service Configurator on any desktop, and from there configure RSC services on any host.

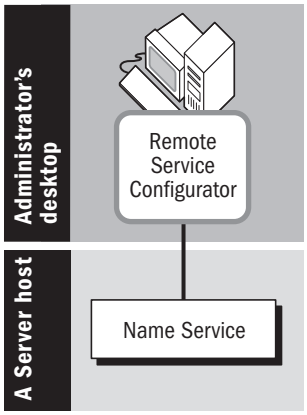


Figure 1-10 Configuration Solution—RSC Services

- **When configuring the servlets** – the Servlet Configurator and all of the servlets. You run the Servlet Configurator on the host of the Hyperion Performance Suite servlets to be configured.

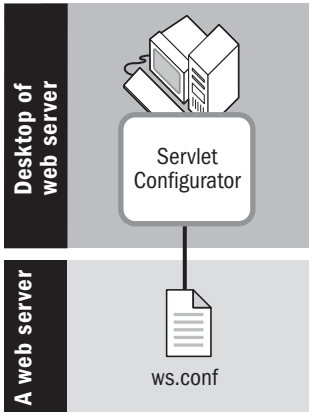


Figure 1-11 Configuration Solution—Servlets

Suite Components

This section describes the components that make up Hyperion Performance Suite. The components are:

- Core Services
- Management Services
- Functional Services
- Client Components
- Web Services
- Software Development Kit and Web Services

Core Services

The core services are:

- Repository Service
- Publisher Service
- Global Service Manager and Local Service Manager
- Authentication Service
- Authorization Service
- Session Manager
- Service Broker
- Name Service

Repository Service

The Repository Service adds, stores, modifies, removes, retrieves, searches, and lists the content of the system, namely: folders, files, jobs, URLs, and shortcuts, and their metadata (properties). The content resides in the Repository, which consists of files in the native file system and metadata for each object in a database in a Relational Database Management System (RDBMS).

The system can have only one Repository Service.

Publisher Service

The Publisher Service handles communications with the Repository Service for the LSC services. (See Table 1-2 for a listing of these services.) When any of these services needs to publish to or retrieve content from the Repository, the service sends its request to the Publisher Service. The Publisher Service forwards the request to the Repository Service and passes the reply back to the initiating service.

The system can have only one Publisher Service.

Global Service Manager and Local Service Manager

The Global Service Manager (GSM) and Local Service Managers (LSMs) act as the service dispatchers. They track all the services of the system and, when a client makes a request, they provide it with a suitable service. They perform load-balancing when dispatching services to clients.

The GSM, in addition to this, holds the system configuration information, and periodically checks all registered services to see if they are running. The system can have only one GSM.

An LSM is part of all LSC and RSC services. An LSM is automatically created when one of those services are started. The GSM also has its own LSM.

When the system's servers start up, they register their services and configuration information with the GSM. Each LSM obtains from the GSM a set of references to all services on other servers, and periodically updates these references. Each LSM handles requests received by its server.

Authentication Service

The Authentication Service checks the user's credentials at login time, and allows or disallows the user to connect. In addition, it determines the user's group membership, which, along with the user's roles, affects what content and other system objects (*resources*) the user can view and modify.

Hyperion Performance Suite can use either native or external authentication, or both. The Authentication Service can be replicated.

An Authentication Service does not have to be co-located on the same server as other services.

Authorization Service

The Authorization Service provides security at the level of resources and actions. Authorization is enforced through access privileges, which are associated with actions and resources, and then bestowed on users. (Resources include folders and items, physical resources, users and groups, and services.) A user can perform a given operation on a given resource only if the user has the access privileges that permit it.

Your access control schema can be structured around roles, groups, or both. Roles organize access according to users' functions in your organization, and groups do so according to departments and other "org chart" groupings.

The Authorization Service manages roles and their associations with operations, users, groups, and other roles. The system must have at least one Authorization Service.

Session Manager

The Session Manager maintains a continuous session across all applications a user uses in their work session, without requiring the user to log in multiple times. The Session Manager can terminate a session after a configured idle time has passed.

The Session Manager can be replicated. Each one manages a set of sessions.

Service Broker

The Service Broker supports the Global Service Manager and the Local Service Managers by dispatching client requests to any of the RSC services, and load-balancing those services. The Service Broker collaborates with the Name Service. (See Table 1-2 for a listing of the RSC services.)

A system can have one or more Service Brokers.

Name Service

The Name Service keeps track of where the RSC services are installed, and provides them with their configuration data. (They may have additional configuration settings obtained from the `server.xml` file.)

The Name Service and Service Broker assist the GSM and LSMs by routing client requests for RSC services. (See Table 1-2 for a listing of the RSC services.)

A system can have only one Name Service.

Management Services

The management services, Logging Service and the Usage Service, help the administrator troubleshoot and determine system usage.

Logging Service

The Logging Service writes log messages from Hyperion Performance Suite components to one or more log files.

A system can have only one Logging Service.

Usage Service

The Usage Service gathers historical information about system activities. It covers usage of the Hyperion Foundation as well as reporting and analytic activities. This service keeps records on logins, opening documents, closing documents for select MIME types, running jobs, viewing job output, and queries processed by the Intelligence iServer.

The system can have multiple Usage Services.

Functional Services

The functional services provide user-oriented functionality to the Foundation. These can be modified or replaced by custom services using the APIs. The functional services are:

- Job Service
- Event Service
- Intelligence Service
- Data Access Service

Job Service

The Job Service executes reports, such as BQY, SQR, and generic jobs. It "listens" for a job request, initiated either by a user or the Event Service, and manages execution of the job. The Job Service publishes the job output to the Repository, and returns the resulting output to the requester.

Every Job Service can process BQY jobs. In addition, you can configure any Job Service to run additional report programs. A Job Service can be configured for any executable, including the Reports iServer engine and generic enterprise reporting programs.

The system can have multiple Job Services.

Event Service

The Event Service manages users' subscriptions and sends notifications of events involving subscriptions, jobs, and exceptions. It also manages the parameter lists for jobs, and dispatches scheduled jobs to be executed by Job Services. In support of subscriptions and scheduled jobs, the Event Service distributes new or modified content via email and FTP. For more information, see "Subscriptions and Notifications" on page 1-47.

The system can have only one Event Service.

Intelligence Service

The Intelligence Service runs BQY jobs and delivers interactive HTML content for BQY files via the iHTML Servlet. When the iHTML servlet requests an action involving a BQY document, the Intelligence Service fulfills that request. Specifically, this service gets the BQY document, processes it, and delivers HTML to the servlet, for display in the user's browser.

Among the capabilities of the Intelligence Service are: opening a BQY document, obtaining its section list, processing the document, rendering sections in HTML, drill-down, pivoting, sorting, modifying Dashboard sections, exporting the document, returning a modified document, and closing the document.

The Intelligence Service communicates with the Repository Service (via the Publishing Service), which stores BQY documents and any pre-generated HTML created for them, and the Data Access Service, which handles database operations.

Data Access Service

The Data Access Service (DAS) provides access to relational and multidimensional databases. It carries out database queries for the plug-in, the Intelligence Service, and BQY jobs. Each DAS typically supports connectivity to multiple data sources, using the connection information in one or more OCE files, so that a single DAS can process a document whose sections require various data sources. The Data Access Service maintains a connection pool for database connections.

Client Components

The client components complete the architecture. They connect end-users and administrators to the functionality provided by the core and functional services. Some client components are servlets running on web servers and accessed through a standard browser. A few are desktop-based, running on the user's machine.

The client components include:

- The Foundation's five common Java servlets (called "the web modules" in the *Hyperion Foundation User's Guide*)
  - **Browse** – End-user web module for browsing the Repository, finding and viewing items, and publishing content to the Repository.
  - **Personal Pages** – End-user web module for user-customizable views of repository content and links to favorite information. Both the content and presentation are customizable.
  - **Job Manager** – End-user web module for scheduling jobs.
  - **View Manager** – End-user web module for viewing subscribed and pushed items.
  - **Administration** – Administrative web module for managing users, groups, and roles, MIME types, physical resources, and SmartCut, notification, and row-level security properties.
- Intelligence and Data Access servlets
  - **Data Access** – Servlet that works with the Hyperion Intelligence Client, enabling users to use queries and reports over the web.
  - **iHTML** – Servlet that enables users to access BQY documents using only a web browser.
- Desktop applications (for various licensed products)
- Job Utilities
  - **Calendar Manager** – Application for managing calendars and scheduled job logs.
- Configuration tools (for various licensed products)
  - **Remote Service Configurator** – Administrative application for managing the RSC services. (Table 1-2 lists the RSC services.)
  - **Local Service Configurator** – Administrative application for managing the LSC services. (Table 1-2 lists the LSC services.)

- **Servlet Configurator** – Administrative application for configuring the servlets.

Note The servlets and the Job Utilities communicate with the services using APIs, and with browsers using HTTP.

Software Development Kit and Web Services

The Software Development Kit (SDK) and the Web Services support extension of the system. They include the following:

- APIs to the services
- JPython APIs to the services
- SOAP/Web Service APIs to the services

For more information about these, see the SDK directory or the Web Services directory, which is installed as part of a server installation of Hyperion Performance Suite.

The Architecture at Work

This section explains how the services collaborate to perform common operations. It presents a set of process flows, which are meant to provide examples of how the services perform their functions. *The process flows do not detail everything happening in the system.* They simplify processes to improve understandability. Also, for clarity and readability some operations, after being introduced, are omitted from subsequent process flows.

If you read this section in its entirety, you will have a clear understanding of the main workings of the server. The following operations are described:

- Authenticating a User (User Login)
- Displaying a Folder Listing
- Opening an Item
- Publishing a File
- Publishing a BQY File
- Publishing a BQY Job
- Publishing an SQR Job
- Running a BQY Job Ad Hoc
- Running an SQR Job (or Generic Job) Ad Hoc
- Executing a Scheduled BQY Job
- Subscriptions and Notifications

Authenticating a User (User Login)

A user "launches" one of the web application modules by entering its URL in a browser. The following sequence of actions as shown in Figure 1-12 ensues:

1. The servlet redirects the user to the login page. The user enters login information and the browser sends it to the servlet.
2. The servlet needs two things from the server: authentication of the user, and a new Session object. First, the servlet sends its hostname and port number to the server to create a Client object. The Client is created and the Global Service Manager, using a load-balancing algorithm, assigns it a Local Service Manager (LSM) for use in locating services. The Client will henceforth be an intermediary between the services and the servlet.
3. Next, the servlet passes login information to the Client, requesting authentication of the user. The Client obtains the location of a Session Manager from its LSM, which load-balances the Session Managers between Clients. The Client then asks the Session Manager to authenticate the user and create a new Session. The Session Manager forwards the information and request to the Authentication Service, and adds a request for lists of the user's groups and roles.
4. The Authentication Service validates this user's credentials. If authentication succeeds, the Authentication Service (a) looks up the user's groups, (b) obtains the user's roles from the Authorization Service, and (c) sends both lists to the Session Manager, along with confirmation that authentication was successful.
5. Using the group and role information, the Session Manager sets up the user's access privileges and creates a new Session containing the access information. The Session Manager returns the session information to the Client. The Client initializes itself with the session and access information and returns successfully to the servlet.

6. The servlet sends its main page to the browser. The user is now logged in and begins the session. The user can enter any of the other web applications without needing to log in again.

Note From here forward, the process flows assume that a Client object exists for the user, and that an LSM is dispatching requests from the Client to (LSC) services. The process flows therefore omit mention of the Client and the LSM, except for particular emphasis.

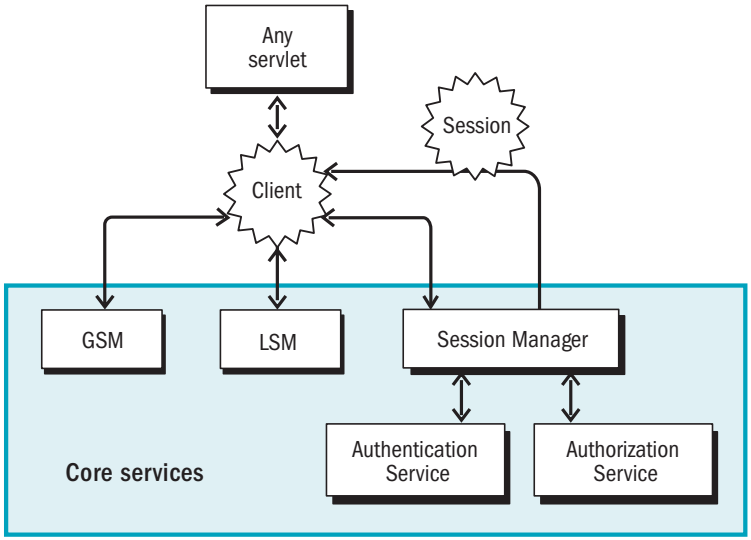


Figure 1-12 Process Flow: Authenticating a User

Displaying a Folder Listing

At the beginning of a Browse session, or whenever the user selects a folder, the contents of a folder are displayed. The following sequence of operations as shown in Figure 1-13 ensues:

1. The Browse module sends a request for a listing of the folder's contents to the Repository Service. The user's Session, which contains the user's access privileges, is passed along with the request.

   Throughout the system, the user's Session is passed with every request and inter-service communication. *From here forward, the process flows will assume, rather than explicitly state, the passing of the Session.*

2. The Repository Service finds all of the items stored in the folder and, for each one, retrieves the basic metadata (properties). The Repository Service obtains access information for the items from the Authorization Service, in order to filter out any that the user does not have access to. In checking access, the Repository Service examines the user's groups and roles, and the items' access settings, and determines what operations are permitted.

3. For each object the user is allowed to view, the basic metadata is returned, along with the user's permissions on that object. This information is passed back to the Browse module by the Repository Service.

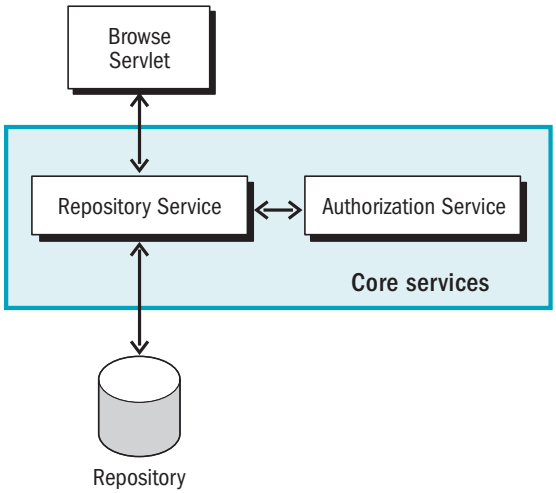


Figure 1-13 Process Flow: Displaying a Folder Listing

Note The diagrams of process flows often *assume,* rather than depict, core services, in order to focus on the principal actors; the core services are involved in almost every system task.

Opening an Item

When a user chooses an item name in the Browse module to view the item, the following sequence of actions as shown in Figure 1-14 occurs:

1. The Browse module requests the item content (file). The Repository Service checks with the Authorization Service to verify that the user has sufficient access privileges to view the content. If so, the Repository Service retrieves the content and returns it to Browse.
2. Browse ascertains the item's MIME type, which it looks up in the browser's MIME type table to find out how to open the item. Depending on the MIME type and its configuration in the browser, Browse may display the content in the browser—either in the current window or in a new window—or launch another application to open the item.

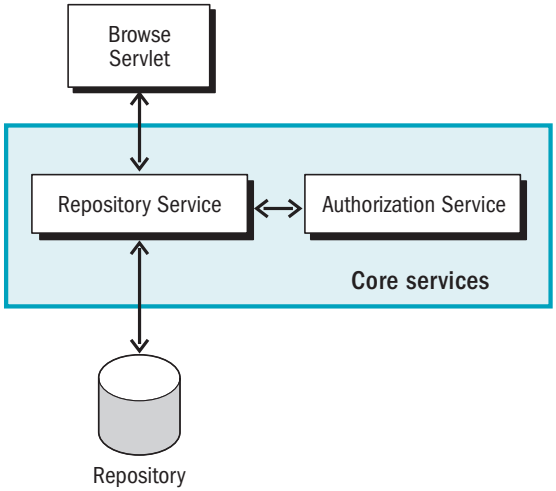


Figure 1-14 Process Flow: Opening an Item

Note From here forward, the process flows assume that the Repository checks a user's access privileges with the Authorization Service before returning an item for that user.

Note Each of these process-flow sections builds on previous ones. For full understanding, read from the beginning of "The Architecture at Work" on page 1-29.

Publishing a File

A user chooses Publish File in the Browse module. The following as shown in Figure 1-15 is the general sequence of actions that ensue:

1. The Browse module displays the first page of the Publish File wizard. The user completes the fields, uploading the file to be published and specifying basic properties.
2. The user proceeds through the wizard, specifying other properties.
3. At the end, when the user chooses Finish, the Browse module attaches the file and its metadata to a request for publication in the Repository. The Repository Service publishes the item and adds it to a list of recently published items, which it keeps for subscriptions.

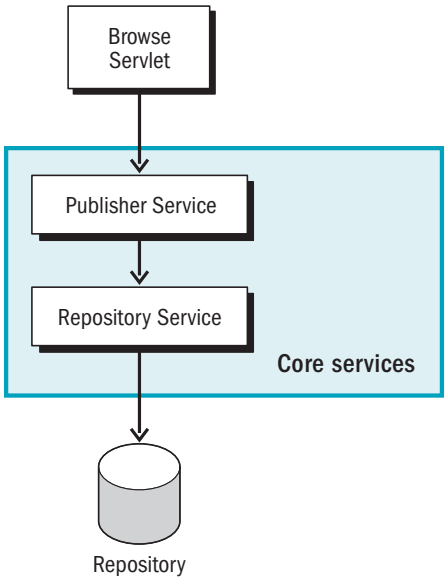


Figure 1-15 Process Flow: Publishing a File

Publishing a BQY File

This sequence applies to publishing any type of file. In the case of a BQY document published as a file, though, the sequence assumes that the user does not choose to pre-generate HTML.

To start publishing a BQY document *as a file*, a user chooses Publish File in the Browse module, and then uploads the BQY document. The following actions as shown in Figure 1-16 ensue:

1. After the user completes the Advanced Properties page, the Browse module displays the first page of the Publish BQY File wizard and sends the file and the already specified properties to the Publisher Service to be pre-published into the Repository. In order to display the *Connecting to Data Sources* and *View in Intelligence iServer properties sections*, Browse asks the Intelligence Service for the BQY file's section names, queries, published OCE files, and so on.
2. The Intelligence Service gets the just published file from the Repository via the Publisher Service, extracts the requested information, and returns the information to the Browse module. Browse displays the *Connecting to Data Sources* and *View in Intelligence iServer* properties sections. Any published OCEs that the user has access to are listed in the menus.
3. When the user completes the wizard and chooses *Finish*, the Browse module sends a request to the Publisher Service to update the item with the complete metadata. The Repository Service updates the metadata in the Repository and lists the item as recently modified.

The Publisher Service handles communications between the Repository Service and the LSC services. *From here forward, the process flows will assume, rather than explicitly state, that the Publisher Service always uses the Repository Service to access the Repository.*

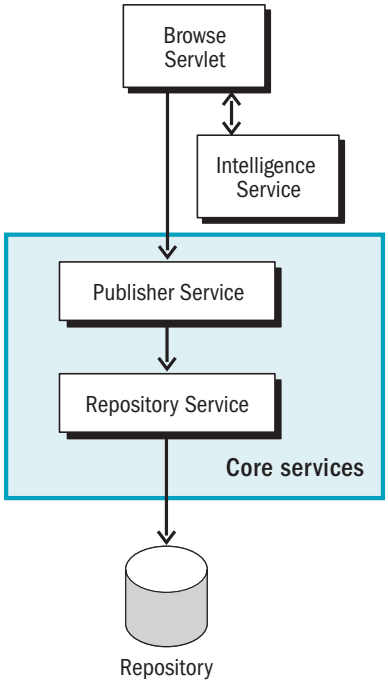


Figure 1-16 Process Flow: Publishing a BQY File

Note Each of these process-flow sections builds on previous ones. For full understanding, read from the beginning of "The Architecture at Work" on page 1-29.

Publishing a BQY Job

To start publishing a BQY document *as a job*, a user chooses *Publish Job* in the Browse module, and then uploads a BQY document. The ensuing actions as shown in Figure 1-17 are generally the same as for publishing a BQY file, with a few exceptions, as follows:

- The Publish BQY Job wizard starts. Many of the properties in this wizard are different from those in the Publish File wizard. The Browse module asks the Intelligence Service for the BQY file's section names, queries, OCE files, and so on, in order to display the *Query* page. The Intelligence Service returns the requested information, just as in publishing of a BQY file. Browse displays the *Query* page.
- In order to display the *BQY Job Properties* page, Browse asks the Intelligence Service for limits, if any. The Intelligence Service extracts the requested information from the document and returns it to Browse.

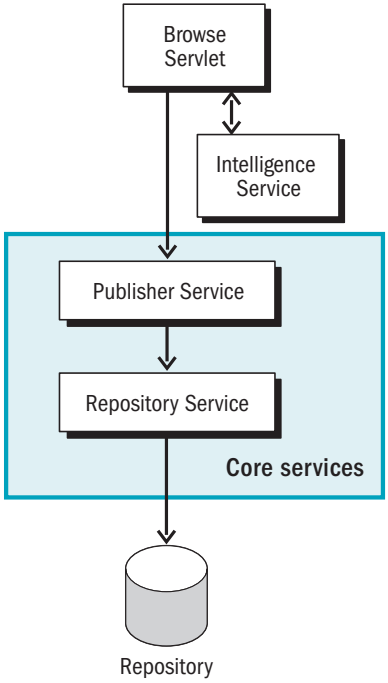


Figure 1-17 Process Flow: Publishing a BQY Job

Publishing an SQR Job

To start publishing an SQR job, a user chooses *Publish Job* in the Browse module. Figure 1-18 graphically shows the following actions:

- The Publish SQR Job wizard starts. The Browse module displays the first page of the Publish SQR Job wizard. The user completes the fields and the file is uploaded. During the publishing process, the Browse servlet communicates with services through the Service Broker and Name Service. *The involvement of the Service Broker and Name Service is assumed for the rest of this process flow.* The wizard leads the user through the job properties and options.
- When the user completes the wizard and chooses *Finish*, the Browse module sends a request to the Publisher Service to update the item with the complete metadata. The Repository Service updates the metadata in the Repository and lists the item as recently modified.
- If the user requests compiling of the program during publishing, a Job Service configured for Reports iServer executes the job (by sending it to the SQR engine).

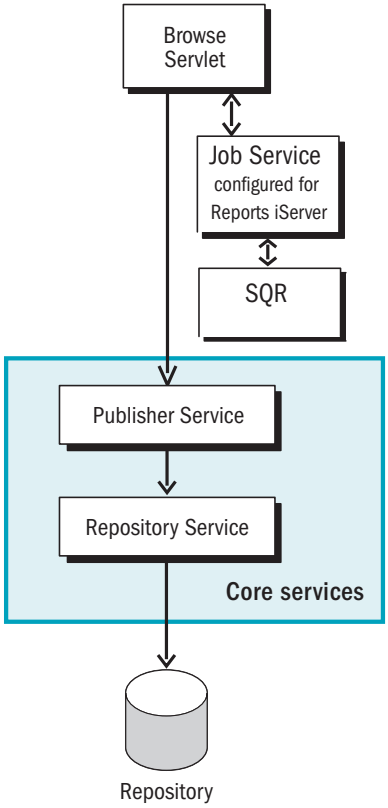


Figure 1-18 Process Flow: Publishing an SQR Job

Note Each of these process-flow sections builds on previous ones. For full understanding, read from the beginning of "The Architecture at Work" on page 1-29.

Running a BQY Job *Ad Hoc*

A job can run in either of the following ways:

- Scheduled – The job has already been scheduled. Job execution starts when the scheduled time is reached.
- *Ad hoc* – Job execution starts when a user, in the Browse module, chooses the job's Run Job icon (or the job's name).

When a user runs a BQY job *ad hoc* from the Browse module, the following sequence of services activity as shown in Figure 1-19 begins.

1. The Browse module communicates with the Publisher Service to obtain the job's metadata from the Repository Service. (If Browse was not already assigned to a Publisher service, it gets one through its LSM.)

   Browse uses the parameter form and other metadata to determine whether and how to prompt the user for additional information needed for the job.

2. When the metadata is complete, the Browse module sends it, with a request for execution of the job, through its Service Broker to a Job Service. (The Service Broker is used instead of the LSM because the LSM, an LSC service, cannot dispatch requests to a Job Service, an RSC service.)

   The Service Broker chooses a Job Service and passes the metadata and execution request to it. The Job Service forms a script for the Intelligence Service to run and forwards the script, the metadata, and the request to an Intelligence Service. The script is only provided when the Intelligence Service is requested to run the job.

3. Through the Publisher Service, the Intelligence Service obtains the BQY file, its metadata, and its OCE file from the Repository Service. The Intelligence Service executes the BQY job, utilizing the Data Access Service for retrieval of data. After creating the output files, the Intelligence Service

returns the output to the Job Service. If the job's metadata specified output to email addresses, ftp directories, or printers, the Intelligence Service also sends the output to these destinations.

4. *What happens next depends on whether the job was configured to run in the foreground or in the background. Notification is briefly described, but is not included in Figure 1-19 because it is not really part of running a job.*

   If the job ran in the foreground:

   The Job Service:

   a. Sends the files and metadata for the new output items to the Repository Service to be published.

   b. Returns the output's metadata to the Service Broker, which sends it on to the servlet.

   The Event Service will learn of the new output when it polls the Repository Service. For more information, see "Subscriptions and Notifications" on page 1-47. The Event Service will then notify:

   - Every subscriber to this job, by email
   - Every subscriber to the folder into which the job output was published, by email

   If the job ran in the background:

   The Job Service:

   a. Sends the files and metadata for the new output items to the Repository Service to be published.

   b. Sends a message to the Event Service that job execution has finished.

   The Event Service notifies:

   - The user who ran the job, by posting the notification on the *View Job Status* page of the Job Manager web module.
   - Every subscriber to this job, by email
   - Every subscriber to the folder into which the job output was published, by email

5. Upon receiving the metadata for the new output, Browse displays a message that the execution of the job finished successfully.

6. The next time the user selects the folder containing the job, the Browse module obtains fresh data from the Repository and redisplays the folder's contents, which include the new job output items. The user can view the output by choosing one of the output formats.

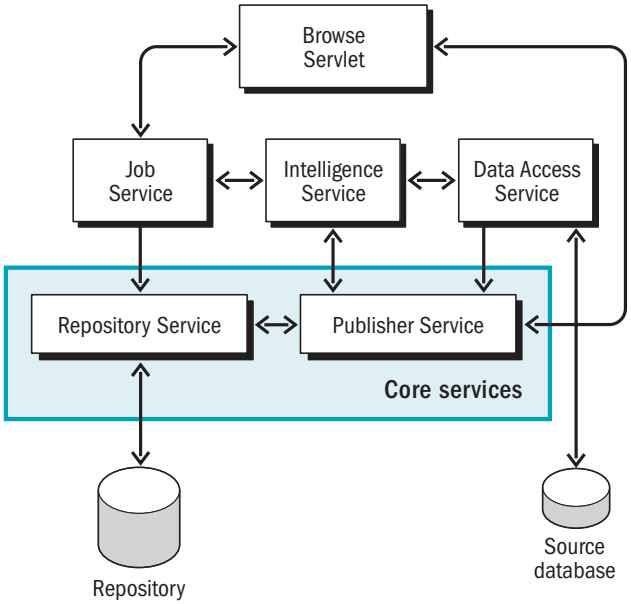


Figure 1-19 Process Flow: Running a BQY Job Ad Hoc (in Foreground)

Running an SQR Job (or Generic Job) *Ad Hoc*

When a user runs an SQR or generic job from the Browse module, by choosing it in an item list, the ensuing activity as shown in Figure 1-20 is similar to that in "Running a BQY Job Ad Hoc" on page 1-40, but with the following differences. The step numbers correspond:

1. The Browse module communicates with the Publisher Service to obtain the job's metadata from the Repository Service. (If Browse was not already assigned to a Publisher service, it gets one through its LSM.)

   Browse uses the parameter form and other metadata to determine whether and how to prompt the user for additional information needed for the job.

2. When the metadata is complete, the Browse module sends it, with a request for execution of the job, through its Service Broker to a Job Service. (The Service Broker is used instead of the LSM because the LSM, an LSC service, cannot dispatch requests to a Job Service, an RSC service.)

   The Service Broker chooses a Job Service that is configured for SQR and passes the metadata and execution request to it.

3. The Job Service obtains the report program file from the Repository Service. It passes the file to SQR (or the generic software), which executes the program and creates the output, returning the results to the Job Service.

Step 4 through Step 6 are the same as in "Running a BQY Job Ad Hoc" on page 1-40.

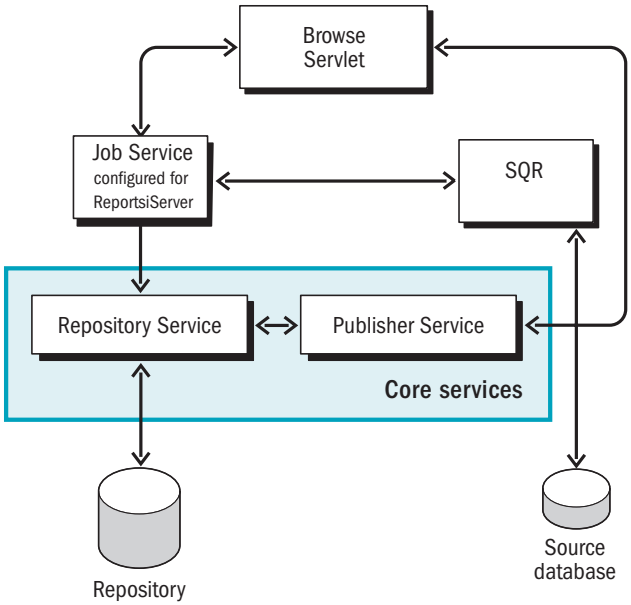


Figure 1-20 Process Flow: Running an SQR or Generic Job Ad Hoc

When an Exception Occurs

If report execution produced an exception, the following additional actions take place:

1. The report program writes the exception text to a file named `output.properties`. The Job Service reads this file and publishes the output with the following metadata: the property *Flag as an exception* is turned on, and *Message* is set to the exception text from `output.properties`. The Repository Service logs the publishing of the new output.

2. When the Event Service next checks the Repository and learns that new job output has been published, it checks whether any users have subscribed to exceptions on that job. If so, the Event Service looks at the output's metadata to see there is an exception. Finding *Flag as an exception* turned on, the Event Service reads the value of the *Message* property.

3. The Event Service sends notifications including the *Message* text to all subscribers to this job's exception.
4. *If the job ran in the foreground:* Upon receiving the metadata of the new output, the Browse module displays a message that the execution of the job was completed successfully.

   The next time the user views the folder's contents, the new job output items are listed, marked with the exception icon, shown in the margin. The user can view the output by choosing the desired output format.

For information about programming exceptions, see the *Hyperion Foundation User's Guide*.

Note Each of these process-flow sections builds on previous ones. For full understanding, read from the beginning of "The Architecture at Work" on page 1-29.

Executing a Scheduled BQY Job

When a scheduled BQY job's time or external trigger occurs, the following sequence of actions as shown in Figure 1-21 ensues:

1. The Event Service, which maintains a list of events, is triggered by the time event or externally triggered event. The Event Service sends a request for background job execution to its Service Broker. The Service Broker dispatches the request to a Job Service.
2. The Job Service forms a script and forwards the script and the job to the Intelligence Service, which obtains BQY file, its metadata, and its OCE file through the Publisher Service. The script is only provided when the Intelligence Service is requested to run the job. The Intelligence Service executes the job, utilizing the Data Access Service for retrieval of data. Upon job completion, the Intelligence Service returns the output to the Repository Service for publication, and also notifies the Event Service.
3. The Event Service sends notifications. For more information on Event Service notifications, see Step 4 of "Running a BQY Job Ad Hoc" on page 1-40, and the section "Subscriptions and Notifications" on page 1-47.

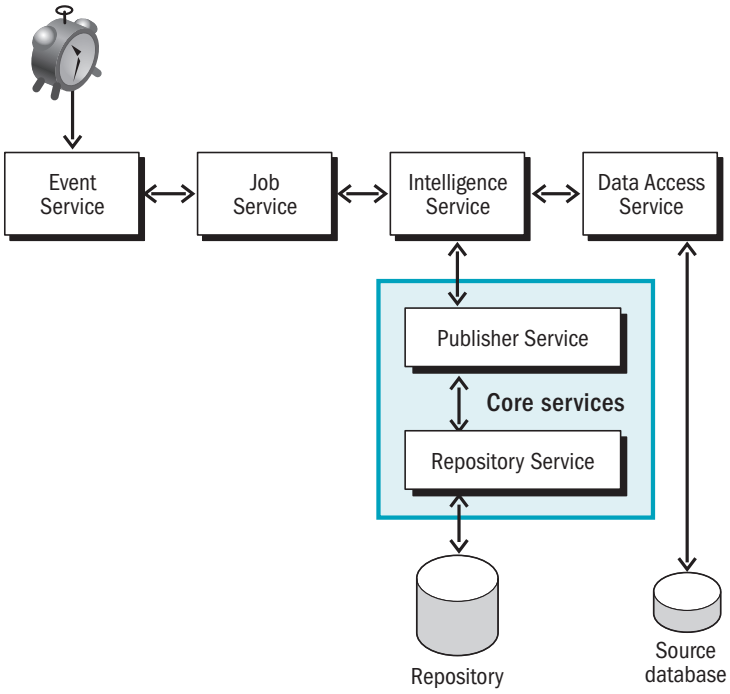


Figure 1-21 Process Flow: Executing a Scheduled BQY Job

Subscriptions and Notifications

To complete your understanding of subscriptions and notifications, this section describes the various kinds of subscriptions and other notification triggers, the Event Service's sources of information, and the various means of notification.

Types of Subscriptions

The Event Service enables users to subscribe to the following:

- **New or updated versions of items –** By subscribing to an item, a user requests to be notified whenever a new version of an item is published or its properties are modified.
- **Changed content in a folder –** By subscribing to a folder, a user requests to be notified when the folder's contents (or content of any of its subfolders) change. When any item within the folder changes, or when a new item is added, the Event Service notifies the subscriber.
- **Job completion –** By subscribing to a job, a user requests to be notified when the job finishes execution.
- **Job exceptions –** By subscribing to a job's exceptions, a user requests to be notified when execution of the job has produced an exception.

Beyond Subscriptions

Independent of subscriptions, the Event Service sends notifications to the following users:

- The owner of a scheduled job, when execution finishes
- The user who ran a background job, when execution finishes

How the Event Service Obtains Information

When a user subscribes to an item or folder, the Browse module sends the subscription information through the LSM to the Event Service, which adds the new subscription to its subscriptions list.

The Repository Service maintains a list of objects that have been published or updated. Publishing or updating includes all of the following:

- Publishing a new item
- Modifying an item's properties
- Adding or replacing a version
- Publishing new job output
- Creating a folder
- Modifying an object's metadata

The Repository Service includes in its list both the published or modified item or folder, and the folder that contains it.

Every 60 seconds, the Event Service obtains the Repository Service's list of new or modified items, and compares them to the subscription list. Then the Event Service sends the appropriate kind of notifications to each subscribing user.

The Repository Service discards its list after giving it to the Event Service. The Event Service in turn discards the list after it has notified subscribers of the changes.

Other services notify the Event Service when they complete actions that may trigger subscriptions, such as the successful execution of a job. The Event Service checks these events against the subscription list and sends the appropriate kind of notification to each subscriber.

Notification Mechanism

There are several ways the Event Service can notify a user:

- Send an email with embedded SmartCuts to notify the user about changes to an object or folder, new output of a report, completion of a job, or occurrence of an exception.

  Optionally, the Event Service may also send file attachments. The user chooses how to be notified on the Subscribe page.

- Display notification of completion of a scheduled job or a background job in the Job Manager web module.

- Display notification of job completion in the Browse web module after a job runs in the foreground.

- Display a "red light" icon on the Exceptions Dashboard when `output.properties` indicates that an exception occurred. When an exception occurs, the publisher of the file sets the file's properties to indicate the presence of an exception and to specify the exception message. The publisher is usually a Job Service, and the file is usually job output.

  SQR code can flag exceptions. Exceptions can also be flagged either manually by the user who publishes a file or job output, or by use of APIs to set the exception properties on the file or output. The Intelligence Service does not support exceptions, but you can set exceptions on BQY documents by using the API or manual methods.

  Individual users choose whether to include the Exceptions Dashboard on a Personal Page. They also choose, on the Subscribe page, whether to include a particular job on their Exceptions Dashboard.

2 Administration Tools and Tasks

This chapter introduces the administrative tools which allow you to configure and administer your Hyperion Performance Suite system. It also contains how to start and stop the services and a quick reference to the most common administrative tasks.

In This Chapter

Administration Tools 2-2

Starting and Stopping the Services 2-5

Starting the Servlets 2-19

Quick Guide to Common Administrative Tasks 2-19

Administration Tools

For the various tasks of administering a Hyperion Performance Suite system, there are several software tools. This chapter introduces the major tools:

- Administration (web module)
- Local Service Configurator (desktop application)
- Remote Service Configurator (desktop application)
- Servlet Configurator (desktop application)

Administration Module

For most administrative tasks, you use the web module named Administration. Specifically, with the Administration module you can configure system properties and add or modify users, groups, roles, MIME types, printers, and FTP directories.

The user interface of the Administration module is similar to that of the end-user web modules (Browse, Job Manager, Personal Pages), which are discussed in the *Foundation User's Guide*. For information about common user-interface features among the web modules, see the *Hyperion Foundation User's Guide*.

Setting Preferences for the Administration Module

Preference options enable you to customize the Administration module. Your Preference settings apply to you personally, that is, to the user you are currently logged in as. To view or change Preference settings, choose the Preferences tab.

The Preferences options for the Administration module are in two groups, *General* and *Items Display*. The options in each of these folders are listed in the following two tables.

Table 2-1 General Preferences of the Administration Module

Show advanced administration options	If this option is turned off, Advanced options do not appear at all in the Administration module. Advanced options include the MIME type properties *Icon* and *MIME type name*.

Table 2-2 Items Display Preferences of the Administration Module

Never list users/groups/roles until Update List button is clicked	Enabling this option prevents delay in displaying a list page when the list is very long. Your default setting for this option should be *on*. Also, turn this option *on* if list displays are slow or if you usually filter lists.
Display all users/groups/roles in the system	Enable this option to display all specified items in the system either right away or after the Update List button is chosen.
List up to ___ users/groups/roles	To maintain good performance, you can limit the number of items listed. If the list spans pages, this number is the total for all pages. If this option is set to a number less than the number of users in your system, you will not be able to list all users; you must use filtering to show a smaller number of users.
Display users/groups/roles ___ per page	This option sets the default value for the setting that determines how much scrolling you need to do to see one page's worth of a list.

Remote Service Configurator

The Remote Service Configurator (RSC) provides a graphical interface to manage a subset of the Hyperion Performance Suite service types referred to as the "RSC services". For explanation and a list of the RSC services, see "LSC Services and RSC Services" on page 1-10.

The RSC can configure services on any host in the system. Using the RSC, you can:

- Modify or view properties of the RSC services
- Ping a Service
- Add, modify, or delete hosts
- Add, modify, or delete database servers in the system
- Delete a service
- View online help

Local Service Configurator

The Local Service Configurator (LSC) enables you to configure the LSC services, a subset of the Hyperion Performance Suite services. You also use the LSC to create or modify authentication systems. For explanation and a list of the LSC services, see "LSC Services and RSC Services" on page 1-10.

The LSC configures only the services on the local host. Using the LSC, you can do the following:

- View or modify properties of LSC services.
- View or modify properties of the local Install_Home (see the following section).
- Create or modify authentication systems.

What Does *Install_Home* Mean?

The *Install_Home* directory is the directory that contains Hyperion Performance Suite products. Its subdirectories include `BrioPlatform` and `servlets`. You specified the name and path of *Install_Home* during installation.

It is possible to have more than one *Install_Home* directory on a single physical host. All the Hyperion Foundation services in a particular *Install_Home* directory run in a single process space and share a GSM (not necessarily on the same host). If there are multiple *Install_Home* directories on a host, each *Install_Home* requires its own separate services process space and is managed by its own GSM. The services in a particular *Install_Home* directory are referred to as a Install_Home.

Servlet Configurator

The Servlet Configurator enables you to customize the Browse, Personal Pages, Scheduler, and Administration servlets for your organization. The many settings include the length of time to cache various types of data on the servlets, colors of various user interface elements, the locale and language.

Starting and Stopping the Services

To start the Hyperion Performance Suite system, you start the services in each Install_Home, and start each installation of the servlets (usually on a web server).

This section focuses on how to start the services of a particular Install_Home, except for a discussion at the end about starting the various Install_Homes and hosts of a distributed system.

On a particular Install_Home, you can start all of the installed Foundation services, a subset of them, or an individual service. The Intelligence Service and the Data Access Service are Intelligence Products services and always need to be started individually.

How you start services depends on your operating system, Hyperion Performance Suite system configuration, and objectives. How you stop services depends on how you started them.

This section explains the prerequisites for starting services and the methods for starting and stopping the services. It is divided into the following subsections:

- Before Starting Any Services
- Starting All Services
- Starting a Subset of Services
- Starting Services Individually
- Starting Services in Order
- Stopping Services
- Example of How a Service Starts

Before Starting Any Services

Before starting any services, ensure that all required network resources are available to the service. For example, the Intelligence Service needs to create job output on a printer or file directory belonging to a different host on the network than where the server is running. These connections must be established before the Intelligence Service can start.

For Windows, a service may need to log on as a specific user account rather than as the local system account to establish these connections to shared resources on the network. ODBC data sources must be set up as "system" data sources rather than user data sources. Consult with the site's network administrator(s) to set up the correct environment.

For UNIX platforms, all necessary environmental settings should be made prior to starting the services. Consult with the site's network administrator(s) to set up the necessary software configuration.

Regardless of your method for starting Hyperion Performance Suite, you must first start the database for the Repository.

Starting All Services

This section explains how to start all of the Foundation services of a given Install_Home together. Regardless whether you installed the complete set of services in the Install_Home, a few services, or only a single service, the methods presented in this section can be used.

For a usable system, all of the core services must be started. For a list of the core services, see "Core Services" on page 1-20.

Note The Intelligence Service and Data Access Service, which belong to Hyperion Intelligence products rather than the Foundation, must be started separately. For details, see "Intelligence Service and Data Access Service" on page 2-12.

Note It is recommended that you restart your web server after restarting the Hyperion Performance Suite services. If you do not restart the web server, there will be a delay of several minutes before users can login.

The startCommonServices Method

The startCommonServices method of startup is the preferred method for UNIX, and an alternative method for Windows.

To start all the Foundation services, run the `startCommonServices` script. This script, installed in *`Install_Home`*`/BrioPlatform/bin`, is named `startCommonServices.sh` (UNIX) or `startCommonServices.bat` (Windows).

`startCommonServices` starts all of the Foundation services in the Install_Home, except any you have inactivated. Inactivating services is discussed in "Starting a Subset of Services" on page 2-10.

The following table lists the commonly used flags in the startCommonServices startup script.

Table 2-3 Flags in startCommonServices Script

`-Dminimum_password_length`	Specifies the length of database passwords. Default=5.
`-Ddisable_htmlemail`	Specifies whether emails will be in HTML format or text file format. Default=false which means HTML formatted email notifications are used.
`-DPerformance.MaxSTWorkers`	Specifies the number of job worker threads.This determines the speed at which jobs are built and sent to the job factory. This should be configured based on the number of job factories, schedules, and events; and the size of the connection pool for the repository. Default=2.
`-DPerformance.SchedulerBatchSize`	Specifies how many schedules are processed at a time by the scheduler worker thread. Default=15.
`-DPerformance.SchedulerDelay`	Specifies the number of seconds job execution is delayed when the job factories are busy. Default=300.
`-Djob_limit`	Specifies the number of concurrent jobs per each job factory. There is no default limit.

The BrioPlatform Server Method (Windows Only)

On Windows, the preferred method for starting all of the Foundation services is by running the BrioPlatform Server from Windows Services (the Services tool of the Control Panel).

To run the BrioPlatform Server:

1. **Open the Windows Services tool from the Control Panel.**
2. **Start the BrioPlatform Server by choosing the Start Service button or double-clicking on the service name.**

   The BrioPlatform Server is named, by default:

   `BrioPlatform_`*`LocalHost_GSMHost_GSMPort`*

   where:

   - *LocalHost* is the name of the machine hosting the services you are starting
   - *GSMHost* is the name of the machine where the Global Service Manager for these services is installed
   - *GSMPort* is the port number for the GSM (the default port is 8100)

Example

If the BrioPlatform Server resides on a machine named *zeus*, and its GSM resides on *apollo* and listens on port 21800, then the default name of the BrioPlatform Server is:

```
BrioPlatform_zeus_apollo_21800
```

Starting a Subset of Services

You can start a subset of the services by inactivating those you do not want to start. You can inactivate LSC services, RSC services, or both.

To start a subset of an Install_Home's services:

1. Inactivate the service or services you want to prevent from starting.
   - **LSC services** – Using the LSC, set the Runtype property to *Hold* for each service.
   - **RSC services** – Edit the `BrioPlatform....dat` file, deleting the names of the services you want to inactivate. Before modifying this file the first time, it is prudent to save a backup of the original.

     Details about `BrioPlatform....dat` are provided in the next section, "Services Startup and the BrioPlatform....dat File" on page 2-10.
2. **Run the *`start_CommonServices`* script or start the BrioPlatform server in Windows Services.**

   For detailed instructions, see "Starting All Services" on page 2-7.

Services Startup and the BrioPlatform....dat File

When the Hyperion Performance Suite server is started, either by the `startCommonServices` script or the Hyperion Performance Suite Windows service, it determines which RSC services to start by reading a file located in the *`BrioHome`*`/BrioPlatform/etc` directory. Only the RSC services listed in this file are started. This file is named:

`BrioPlatform#_`*`LocalHost_GSMHost_GSMPort`*`.dat`

where:

- # is a unique identifying number for the BrioHome.
- *LocalHost* is the name of the host of the services.
- *GSMHost* is the name of the machine where the Global Service Manager is installed.
- *GSMPort* is the port number for the GSM.

Example

If this DAT file (a) is installed on a machine named *zeus*, (b) is managed by a GSM on port 1800 (the default) of the host *apollo*, and (c) was assigned the number 2 by the installer, then its name is:

`BrioPlatform2_zeus_apollo_1800.dat`

Example If (a) the Install_Home for this DAT file resides on the same host as the GSM, (b) the host is named *zeus*, (c) the GSM listens on port 10123, and (d) the GSM was assigned the number 5 by the installer, then the name of the DAT file is:

```
BrioPlatform5_zeus_zeus_10123.dat
```

Each line in the `BrioPlatform....dat` file is formatted as:

`serviceType``:`*`serviceName`*

The *serviceType* must be one of the strings shown in the first column of Table 2-4.

Table 2-4 Service types

Service type field in the server.dat file	Official Service Type Name
com.sqribe.transformer.NameServerImpl	Name Service
com.sqribe.transformer.RepositoryAgentImpl	Repository Service
com.sqribe.transformer.MultiTypeServerAgentImpl	Event Service
com.sqribe.transformer.SQRJobFactoryImpl	Job Service
com.sqribe.transformer.ServiceBrokerImpl	Service Broker

The *serviceName* is the name of the particular service, which has the form

`serviceAbbrev#_localHost`

where:

- *`serviceAbbrev`* is one of the abbreviations in Table 2-5 on page 14
- `#` is a number uniquely identifying the service
- *`localHost`* is the name of the machine where the service is installed

For example, to inactivate only the Service Broker and the Event Service located on the host apollo, you would remove the following lines of `BrioPlatform#_apollo_`*`GSMHost_GSMPort`*`.dat`:

```
com.sqribe.transformer.ServiceBrokerImpl:SB1_apollo
com.sqribe.transformer.MultiTypeServerAgentImpl:ES1_apollo
```

Starting Services Individually

Some services have their own startup scripts. These single-service startup scripts make it possible to start a service in a separate process from the other services in the same Install_Home, but this is desirable only for specific services and situations. This section explains whether and when you should start a service using its startup scripts, and how to start services individually.

Intelligence Service and Data Access Service

You must start Intelligence Service and Data Access Service (DAS) individually. This is true whether the service is installed in the same Install_Home as the Foundation services or alone in its own Install_Home.

Note When you connect to a machine to start the BI Service on Windows, make sure the color property setting for the display is 16-bits or higher. If the color property setting is less than 16-bits, users may encounter extremely long response times when opening Chart sections of BQY documents with the Intelligence iServer. This is an important pre-startup step, especially when starting the services remotely (for example using VNC, Terminal Services, Remote Administrator or Timbuktu, etc.), because many remote administration clients connect with only 8-bit colors by default.

To start the Intelligence Service (or DAS):

1. **In the Local Service Configurator, verify that the Intelligence Service's (or Data Access Service's) *Run Type* property is set to *Start*.**
2. **Start the common services.**
3. **Start the Intelligence Service (or DAS) in its own process using a process monitor.**

   It is recommended that you use a process monitor to start the Intelligence Service and the Data Access Service. For details on using the process monitor for starting and stopping the BI and DAS services, see Appendix B, "Process Monitor Implementation."

   For Windows, to start the service without a process monitor:

Run its startup script – For the syntax of script names, see "The Individual Startup Scripts," just ahead. Typical startup script names are, for example, `BI1_apollo_start.bat` (Intelligence Service) and `DAS1_apollo_start.bat` (DAS).

For UNIX, see "Starting a Service Using a Process Monitor" on page B-6.

The RSC Services

All of the RSC services have individual startup scripts. These can be useful for debugging or isolating issues. However, due to complex dependencies between the Hyperion Performance Suite services, the order in which the services are started is critical. You should use these scripts only (a) if you have a firm understanding of the system's interdependencies, or (b) with the guidance of Hyperion Customer Support.

For information about some of the sequential requirements, see "Starting Services in Order" on page 2-15.

The Individual Startup Scripts

Each startup script is either an executable Bourne shell script file with the extension `.sh` (UNIX), or a batch file with the extension `.bat` (Windows). All of the scripts are stored in the *`Install_Home`*`/BrioPlatform/bin` directory.

Each startup script name is composed of an abbreviation for the service type, a number uniquely identifying the particular service, an underscore, and the string *start*, followed by the extension `.sh` or `.bat`.

The service-name abbreviations used in startup scripts are listed in Table 2-5.

Table 2-5 Abbreviations for Service Names

Service Type	Abbreviation
Data Access Service	DAS
Event Service	ES
Intelligence Service	BI
Job Service	JF

Table 2-5 Abbreviations for Service Names *(Continued)*

Service Type	Abbreviation
Name Service	NS
Repository Service	RM
Service Broker	SB

Example The startup script for the first Name Service installed on a UNIX host named apollo is:

```
NS1_apollo_start.sh
```

Example The startup script for the third Job Service installed on a Windows host named zeus is:

```
JF3_zeus_start.bat
```

Starting Services in Order

When you start all services in a single process, the startup script or service controls the startup sequence and timing to assure that all dependencies are met. For example, if service A's startup depends on services B and C being available, then B and C must start successfully before A tries to start.

When you start services in separate processes, the proper timing and sequence is your responsibility. So, when using individual start scripts, proceed as follows:

1. **Start the LSC services using `startCommonServices` or the BrioPlatform Server.**
2. **Make certain that the GSM and Session Manager have started.**

   To find out whether they are running, view `stdout_console.log`, which is located in *`Install_Home`*`/BrioPlatform/log`.
3. **Start the Name Service.**

   Verify that it is running by viewing `stdout_console.log` before proceeding.
4. **Start the Service Broker.**

Verify that it is running by viewing `stdout_console.log` before proceeding.

5 **Start the other RSC services, in any order.**

Stopping Services

You stop all the Hyperion Performance Suite services, or services started individually, by stopping their processes. Do so at each service's host machine. In all cases, stopping the services constitutes a hard shutdown and causes the service(s) to stop immediately. In the event of a hard shutdown, all work in progress stops.

The method for stopping a service must match how it was started:

- **To stop an individual RSC service started with its startup script**, run its stop script. The name of a service's stop script is identical to that of its startup script except for the substitution of *stop* for *start*. For example, if a Job Service's startup script is `JF1_apollo__start.bat` (or `.sh`), the stop script will be `JF1_apollo__stop.bat` (or `.sh`). The stop scripts are found in the `Install_Home/BrioPlatform/bin` directory.

Caution! Use a service's stop script *only* if the service was started with its start script. A stop script cannot be used to terminate a single service within a multi-service process. The stop script stops *all* of the services running in that process.

- **Process running in a console window** – Use a shutdown command, such as `shutdown` or [Ctrl+C] on Windows. Using an operating system *kill* command (such as `kill` on UNIX) to stop the Hyperion Performance Suite services does not cause damage to the system. However, do not use `kill -9`.
- **A Windows service** – Use the Stop command in the Services tool.

If you are running services as different servers (that is, as separate processes), you will need to stop the Repository Service last.

Note Do *not* terminate the Job Service when it is executing a job. If you do so, you will not be able to restart the Job Service until the job exits (or until you terminate it).

If a job exists that never terminates, you can restart the Job Service by terminating the process. On Windows systems, use the Task Manager to terminate the process. On UNIX systems, use the *kill* command. You can also reboot the machine on which the Job Service resides, but of course this method is a last resort.

Example of How a Service Starts

At startup time, all of the services go through similar startup procedures. For example, the Job Service does the following:

1. Locates its local `config.dat` file.

   The `config.dat` file contains information for connecting with the Name Service that has this Job Service's configuration data. For more information about `config.dat`, see the section “config.dat” on page 9-49.

2. Reads from the `config.dat` file.

3. Establishes a connection with the Name Service to download its (the Job Service’s) configuration information.

Since a service looks up its configuration information only when it starts, it does not learn about changes made to the environment later. Therefore, if you make changes to a service’s configuration and want them to take effect immediately, restart the service.

Starting the Servlets

Start the servlets (web modules) according to the instructions given in your web server documentation.

Make the URLs available to your system's end-users. The URLs have the form:

`http://host/Hyperion/servlet/login`

where:

- *host* is the server on which the servlets are installed
- *Hyperion* is the "web application" name, as configured in your web server software. The default name is the literal *Hyperion.*
- *servlet* is the name of the servlet, which is one of the following:
  - browse
  - personalpages
  - jobmanager

For example, to start the Browse module, the URL would be similar to the following:

`http://apollo.acme.com/Hyperion/browse/login`

Quick Guide to Common Administrative Tasks

This section can help you quickly locate instructions for some of the common tasks of an administrator. Table 2-6 lists tasks involved in initially setting up and populating your system, and the system component used for each task. Table 2-7 gives the same information for tasks involved in maintaining a system. These tables do *not* include all tasks covered in this *Administrator's Guide*.

Table 2-6 Tasks of Setting Up a New System

If you need to...	Use this component...	See...
Start or stop a server		"Starting and Stopping the Services" on page 2-5 "Stopping Services" on page 2-17
Set up access control for roles, groups, and users	Administration	"Modifying Access Privileges" on page 4-11

Table 2-6 Tasks of Setting Up a New System *(Continued)*

If you need to...	Use this component...	See...
Assign roles to users	Administration	"Modifying Associations Between Users, Groups, and Roles" on page 4-9
Create a user account	Administration	"Adding a User" on page 4-12
Create a group	Administration	"Adding a Group" on page 4-14
Create a role	Administration	"Adding a Role" on page 4-14
Give a user administrative access on a particular group only	Administration	"Global Administrator, Administrator, and Content Administrator" on page 3-12
Set up the generated Personal Page	Browse	"Setting Up the Generated Personal Page" on page 7-6
Set up Broadcast Messages	Browse	"Understanding Broadcast Messages" on page 7-9
Provide optional Personal Page content	Browse	"Providing Optional Personal Page Content to Users" on page 7-10
Provide graphics for bookmarks	Browse	"Setting Up Graphics for Bookmarks" on page 7-11
Create custom calendars for scheduling jobs	Calendar Manager	"Creating a New Calendar" on page 8-4
Create public job parameters		"Administering Public Job Parameters" on page 8-16
Create or modify printers or directories for job output	Administration	"Administering Physical Resources" on page 8-18
Define database servers	Remote Service Configurator	"Adding a Database Server" on page 9-16
Configure services	Remote Service Configurator	Chapter 9, "Configuring the RSC Services"
	Local Service Configurator	Chapter 10, "Configuring the LSC Services and Other System Configuration"
Set system properties	Administration module	"Modifying the System Properties" on page 10-34
Configure the Browse, Personal Pages, Scheduler, and Administration servlets	Servlet Configurator	Chapter 11, "Configuring the Servlets"

Table 2-7 Tasks of Maintaining a System

If you need to...	Go to this module...	See...
Change which services run in a server		"Starting Services Individually" on page 2-12 or "Services Startup and the BrioPlatform....dat File" on page 2-10
Modify a service	Remote Service Configurator	Chapter 9, "Configuring the RSC Services"
	Local Service Configurator	Chapter 10, "Configuring the LSC Services and Other System Configuration"
Modify a Job Service	Remote Service Configurator	"Job Service Overview" on page 9-40
Modify system properties	Administration module	"Modifying the System Properties" on page 10-34
Delete a service	Remote Service Configurator or the Installation program	Chapter 9, "Configuring the RSC Services" or the *Hyperion Performance Suite Installation Guide*
Modify a group a user, group, or role	Administration	"Modifying Users, Groups, and Roles" on page 4-4
Inactivate obsolete users, groups, or roles	Administration	"Inactivating or Activating an Item" on page 4-6
Create a MIME type	Administration	"Creating a MIME Type" on page 7-3
Modify a MIME type	Administration	"Modifying a MIME Type" on page 7-3
Inactivate an obsolete MIME type	Administration	"Inactivating or Re-activating a MIME Type" on page 7-4
Add hosts	Remote Service Configurator	"Adding a New Host" on page 9-7
Add a service	installation program	*Hyperion Performance Suite Installation Guide*
Configure common Metadata Services	Administration	*"Hyperion Hub Properties" on page 10-41*

Summary

This chapter provides an overview of all Hyperion Performance Suite administration tasks. It also details how to start and stop the Hyperion Performance Suite services.

PART II

Security

3 Role-Based Access Control

Role-Based Access Control (RBAC) and the Authentication system provides the basis for security in the Hyperion Performance Suite system. This chapter explains how RBAC works. It also contains descriptions of the preconfigured system roles and users in your Hyperion Performance Suite system and of the access privileges for each item.

For more information on the Authentication system, see Chapter 5, “Authentication and Login”.

In This Chapter

About Role-Based Access Control 3-2

Access Privileges on Objects 3-8

Standard RBAC Configuration 3-12

Checking Access Privileges 3-18

Adaptive States for Intelligence Roles 3-25

About Role-Based Access Control

Role-Based Access Control (RBAC) determines what each authorized user can do with particular content items. You, the Hyperion Performance Suite administrator, and users who own content items or have administrative privileges over users or groups, define who has access to the operations and the data in the system. The system enforces the restrictions: each time a user tries to perform any activity in the system, access control checks whether that user is authorized to use that service in the attempted manner. For example, a user can run Job A because the user has the Job Runner role and the user has the Modify and Run access privilege on Job A. The role gives the user access to the job runner application or service. The access privilege gives the user permission to run this specific job. The user needs both the role and an access privilege to run the job.

Roles

Roles define what operations in the system a user may perform. Operations include access to Hyperion tools such as the Intelligence Clients and the Intelligence iServer, and services such as running jobs. Roles can be assigned to groups, other roles, and users. Roles can also be created by combining the pre-configured roles. Operations include:

- Viewing items in the browse list
- Publishing content to the Hyperion Performance Suite system
- Running jobs
- Using the Intelligence iServer
- Using Intelligence Clients

The Hyperion Performance Suite system comes with pre-configured roles. See "Pre-Configured Roles" on page 3-13 for a complete list of the pre-configured roles.

Roles—whether pre-configured with the system or administrator-created—can be defined to contain other roles. Thus, it is possible to define roles at a very granular level. If a role is contained within another role, all the access privileges that apply to the contained role are inherited by the container role.

For example, Figure 3-1 shows that the *Enterprise Publisher* role contains the *Job Publisher* role. Because the *Enterprise Publisher* role contains the *Job Publisher* role which grants the privilege of publishing jobs, the *Enterprise Publisher* role also grants the privilege of publishing jobs.

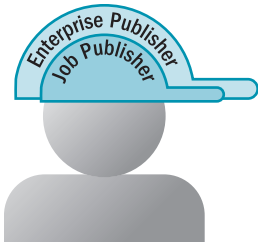


Figure 3-1 Role Containment Example

Groups

Groups are collections of users. Group membership usually follows organizational or functional lines. Groups can be associated with roles, assigned to be members of other groups, or assigned to users. Examples of groups include:

- Everyone in the company
- Everyone at headquarters
- Everyone in marketing
- Marketing administrators
- All testers
- CEO

Like roles, groups can inherit privileges from other groups. For example, if a group is a member of another group, the member group inherits all access privileges granted to the group in which it has membership.

Access Control

Access control determines what information a user can view and use in the system. For any object, an administrator or object owner determines who has access and the level of access (access privilege). If the owner has the View Manager Content Pusher role, the content owner can push content to users' View Manager module. Objects include all content that is published to the repository, printers, outside directories, users, groups, roles, jobs, and job output collections. Access control on specific objects is granted by administrators or object owners to groups and users depending upon their job needs.

The level of access—view, modify, run, full control—that you grant to others on an item you publish is termed access privilege. As the owner or publisher of an item you can change the access privilege level for groups, roles, and users.

The way in which you implement the product controls how access privileges are granted. Hyperion recommends you associate access privileges with groups. (All preconfigured roles are by default hidden from end users, so they cannot assign access to roles).

Assigning access to a mixture of users, groups, and roles will make it difficult to determine the access privileges of users since they are derived from a combination of their group and role membership and explicit access that may have been granted to them at the user level. The ability to assign access at the user level is a powerful feature, but should only be used when a content owner wishes to treat an individual user differently from their group (or role). For example, a content owner may grant the Marketing group VIEW access to a document, but grant User A (a member of the Marketing group) FULL CONTROL access in order to maintain the document. In this case, granting access at the user level is the correct approach."

RBAC Implementation

Role-Based Access Control is very flexible and can be set up to suit the needs of any organization. You can combine roles, groups, and users in a number of ways depending upon your organization. RBAC allows you to give specific users, groups, or roles access to particular operations and objects in the system. For example, the Marketing group has the job runner role and has Modify and Run access to Job A. Seth is a member of the Marketing group, so Seth can run Job A. Frank, from sales, wants Seth to run Job B. Seth is not a member of a group that has access to Job B and Seth does not have direct access to run Job B. Seth could not run Job B because he does not have access to run this particular job. Seth could be given Modify and Run access to Job B either directly or indirectly (via group or role membership).

User's Roles and Access Privileges

A user can be granted a role directly or through membership in a group or through an association with a role that contains that role. Users are also granted access to objects in the system either directly or through membership in a group or through an association with a role.

Mini-Administrators

Through RBAC you can create mini-administrators who have control over limited operations and content. These mini-administrators can have control over administrative functions for a particular group. For example, you may want to delegate administration to two mini-administrators, one for the eastern region and one for the western region. For details on how to create mini-administrators, see "Adding a Role" on page 4-14.

Access to Roles

Your system comes configured such that only the global administrator and the administrator roles have access to roles. As the administrator you can configure your system to allow mini-administrators and users access to roles when publishing. This is not recommended. In most cases mini-administrators and users do not need access to roles. They should assign access privileges on content primarily through groups.

Setting Access Control

As an administrator or as an item owner, you can set up access control to objects in the system either individually or automatically. To individually set access control, each time you add a new object to the system, open the access control section and set up your access control list of users, groups, and roles. (see the *Foundation User's Guide* for details). If the access control settings you use are usually the same, you can set access control automatically.

To automatically set access for objects you add to the system, check the *Make these the default access privileges for all (insert type of object here) I (create or publish)* box. After you check this box, every time you add the same type of object, all of the settings you set as your default settings will apply. You can modify your default access control settings for individual objects if necessary. This provides a quick way to set access privileges.

This principle applies to all objects in which you can add to the Hyperion Performance Suite system.

The preference section of the *Foundation User's Guide* shows another way to set up your access control defaults when publishing different types of content.

For example, Rick manages the Marketing department's user accounts and has the following default access control settings for every user he adds:

- Marketing Admin: Full Control over all users created by Rick. This means that for each user Rick creates, the Marketing Admin role will be able to fully modify all that user's properties, including inactivating them.
- Marketing User: View (a user name on a list). For each user Rick creates, all users that belong to the Marketing Users group will be able to see that user in the system, for example, when they are assigning access to content that they publish

Figure 3-2 illustrates this example.

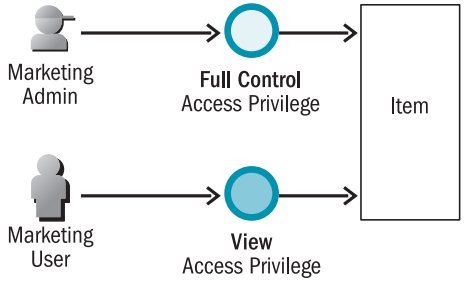


Figure 3-2 Default Access Control for a Departmental Administrator

Note If user accounts in some departments need a unique set of default access control settings, add a different administrator role for each of these departments. For the mini or departmental administrator role that is created, the default access control settings for users created must include view access to all users in the system.

Setting the default access control for items is the same as for users. Once the default access is specified, every item published by a given user will have the same access control settings.Figure 3-3shows that for all documents published by this user, the User Administrator has full control, Group A has modify access, and the World group has view access.

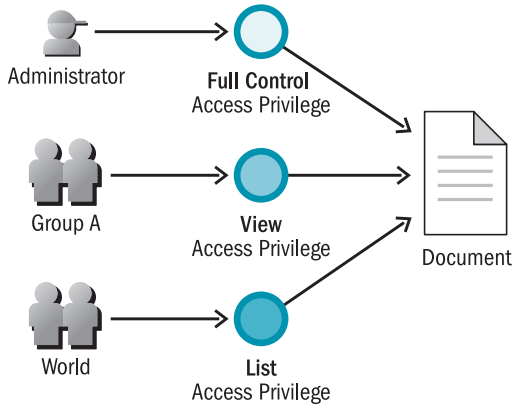


Figure 3-3 Default Access Control on an Item

Access Privileges on Objects

Access privileges are the possible level of access control granted on objects in Hyperion Performance Suite. Table 3-1 lists access privileges for objects in the system. The chart lists the access privileges from most restricted to least restricted. Each level contains all of the checked levels above it. For example, the modify assess privilege for user contains the view and the list access privilege.

Table 3-1 Access Privileges Per Object

Access Privilege	Printer, Output Directory	Public Event	Job	Job Output	Folder, Shortcut, other items	User	Group	Role
List						✓	✓	
View	✓	✓	✓	✓	✓	✓	✓	✓
Assign							✓	✓
Modify				✓	✓	✓	✓	✓
Run			✓					
Modify and Run			✓					
Full Control	✓	✓	✓	✓	✓	✓	✓	✓
No Access	✓	✓	✓	✓	✓	✓	✓	✓

Printer and Output Directory

The access privileges for printers and output directories where users store their jobs outputs are:

- *No access*
- *View* allows viewing of general properties
- *Full control* includes view and allows modification of access control and the ability to delete properties, as well as delete a directory.

Public Events

The access privileges for public events are:

- *No access*
- *View* general properties, days to run, time to run, and valid dates.
- *Full control* provides the ability to modify all properties, including days to run, time to run, valid dates, and access control; also provides the ability to delete public events.

Personal Events

The creator/owner has full control of personal events. Access privileges cannot be given to any other users.

Jobs and Job Output

The access privileges for jobs are:

- *No access*
- *View* general properties
- *Run* job, contains view, also provides access to runtime parameters.
- *Modify and Run* general properties; view and modify advanced properties, except access control. Contains *Run*.
- *Full control* contains modify and run access privileges; also provides ability to specify access control and delete capabilities.
- No entry means "undefined."

The access privileges for jobs outputs are:

- *No access*
- *View* general properties
- *Full control* provides the ability to modify general properties; also provides ability to specify access control and delete capabilities.
- No entry means "undefined."

In addition to access privileges, BQY documents, jobs, and job output also have adaptive states. For more information about setting access privileges on BQY documents, see the *Foundation User's Guide*.

Shortcuts and Other Items

The access privileges for shortcuts and other items are:

- *No access*
- *View* allows viewing of general properties (name and description).
- *Modify* general properties and advanced properties, excluding access control; includes view access privilege.
- *Full control* gives the privilege to modify access control and to delete; includes the modify privilege.

When browsing the Repository, users are denied access to folders for which they have not been granted the view access privilege, so users are restricted to only those items (or a subset of those items) within the folders to which they can navigate.

However, a search will return items that match the search criteria and that are in folders to which the user cannot directly navigate, as long as the user has access to the item and the parent folder of the item.

User

The following access privileges can be applied on a user:

- *No access.*
- *List* gives the ability to view name of users in any listing of users.
- *View* allows viewing of general properties.
- *Modify* general properties and advanced properties, excluding access control; includes view access privilege.
- *Full control* gives the privilege to modify access control and to inactivate.

Group and Role

The following access privileges apply to groups and roles:

- *No access*
- *List* gives the ability to view the name of the group or role.
- *View* allows viewing of general properties
- *Assign* allows adding and removing of users or groups from groups
  - For groups, provides the ability to change the group membership – to add or remove users or groups from membership in the group. Need minimum of list access privilege on the user or assign access privilege on the group being added.
  - For roles, provides the ability to assign users or groups to that role.
- *Modify* general properties and advanced properties, excluding access control; includes assign access privilege. For roles, it means that roles can be associated with other roles.
- *Full control* gives the privilege to modify access control and inactivate. For roles, full control includes an additional feature; the ability to define which users, groups, and roles that role can access and the level of access. This feature should be used when creating mini-administrator roles.

Standard RBAC Configuration

The Role-Based Access Control can be configured in many different ways. This section details the pre-configured roles which cannot be modified and the pre-configured groups, users, and access control settings which can be modified.

Global Administrator, Administrator, and Content Administrator

These three roles have wide ranging access and should not be given to too many people.

Global Administrator Role

The *global administrator* role has unrestricted access to all resources in the system. No access checking is done on the global administrator role. This means that anyone with the global administrator role cannot be denied access to any resources in the system.

Note Since no access checking is done on the global administrator role, it is important to guard against granting this role to many administrative users.

Administrator Role

If you want an administrative user to have full control access to a subset of all departmental or local resources, do not use the global administrator role. Rather, you can grant the administrator role and selectively deny access to other resources. The content administrator role is contained in the administrator role.

Content Administrator Role

A user with the content administrator role has administrative access over all system resources, except when:

- Denied access at the user level.
- The content administrator role is denied access.

Pre-Configured Roles

The following table lists the pre-configured roles.

All roles with asterisks are internal system roles that can only be seen by the global administrator.

Table 3-2 Preconfigured Roles

Role Name	Definition and Containing Roles	Contains
Administrator	Implicit administrative access to all items and services. Only "No Access" can deny the Administrator role access.	All roles in this table except for Global Administrator.
Browser	Access to Browse application. Provides the ability to specify preferences, search and view content, and subscribe to content.	
Content Administrator	Implicit access to all items in the system. Only "No Access" denies the Content Administrator access to an item.	
Content Publisher	Access to publish and modify files, BQY files, URLs, shortcuts and folders. Ability to modify content is based on user's privilege on that content.	
Event Service Administrator*	Internal system role. Grants administrative privileges on the Event Service.	
Global Administrator	Explicit administrative access to all resources. **Note:** Since the globaladministrator has complete access to all items and services, the global administrator role should be judiciously used.	
Group Administrator*	Internal system role. Grants access to operations on Authentication Service for managing and creating groups.	Group Locator*
Group Locator*	Internal system role. Grants access to operations on Authentication Service for accessing Groups.	
IHTML Viewer	Allows access to the Intelligence iServer for viewing BQY content and embedding BQY content in Personal Pages.	
Intelligence Analyzer	Grants access to the Hyperion Intelligence Client application for working with BQY files, with full analytic capabilities available.	

Table 3-2 Preconfigured Roles *(Continued)*

Role Name	Definition and Containing Roles	Contains
Intelligence Dynamic Viewer	Grants access to the Hyperion Intelligence Client application for working with BQY files, with the ability to view, print, and re-process the document.	
Intelligence Viewer	Grants access to the Hyperion Intelligence Client application to work with BQY files, with the ability to only view and print the document.	
Job Administrator	Grants access to create and manage public job parameters, output directories, and output printer locations. Ability to modify the properties of any of these items is based on the user's access privileges on those items.	Job Publisher, Physical Resource Manager, Content Publisher, Job Runner
Job Publisher	Grants access to publish and modify jobs. Ability to modify the properties of any of these items is based on the user's access privileges on those items.	Job Runner, Content Publisher
Job Runner	Grants access to Job Manager application: run jobs, create and manage personal job parameters, view public job parameters, view physical resources.	
Job Scheduler	Grants access to create and maintain scheduled jobs, personal parameters, and personal recurring time events. Grants access to view public recurring time events, externally triggered events, and calendars.	Job Runner
MIME Type Administrator*	Internal system role. Provides administrative capabilities on MIME types.	
Name Service Administrator*	Internal system role. Grants access to all privileged commands on the Name Service.	
OCE Publisher	Grants access to publish and modify OCE files subject to a user's access permissions on the files.	
Organizational Administrator	Grants access to Administration application. Ability to add and modify users, groups, and roles. Ability to modify the properties of any of these items is based on the user's access privileges on those items.	User Administrator*, Group Administrator*, Role Administrator*
Personal Page	Grants access to the Personal Page module.	
Personal Page Publisher	Grants access to publish personal pages	
Physical Resource Administrator*	Internal system role. Grants access to the creation/ modification of Physical Resources.	

Table 3-2 Preconfigured Roles *(Continued)*

Role Name	Definition and Containing Roles	Contains
Related Content Viewer	Grants access to content from other Hyperion applications.	
Role Administrator*	Internal system role. Grants access to create, update, and delete roles in the system.	Role Locator*
Role Locator*	Internal system role. Grants access to search for roles in the system.	
Scheduler Administrator	Grants access to create and manage all schedules, events (public recurring time events and externally triggered events) and calendars, scheduled jobs, parameters, personal recurring time events. Ability to modify the properties of any of these items is based upon user's privileges on those items.	Job Administrator, Event Service Administrator*, Job Scheduler, Job Publisher, Physical Resource Manager*, Job Runner, Content Publisher
Session Administrator*	Internal system role. Grants administrative privileges over Session Manager, including viewing other users' sessions.	
System Crawler	Implicit read-only access for all items in the system. Only "No Access" denies the System Crawler access to an item. Used for crawling the system.	
System Viewer*	Internal system role. Grants access to view items in the system.	Browse, Subject Locator*, Group Locator*, Role Locator*, View Manager, Related Content Viewer
Trusted Application	Provides access to Single Sign-on information to an application.	
User	The user is able to log in to the system. Provides access to Browse.	System Viewer*
User Administrator*	Internal system role. Grants access to methods on Authentication Service for modifying and creating users.	User Locator*
User Locator*	Internal system role. Grants access to operations on Authentication Service for accessing users.	

Table 3-2 Preconfigured Roles *(Continued)*

Role Name	Definition and Containing Roles	Contains
View Manager	Grants access to the View Manager module.	
View Manager Administrator	Grants the same access as the View Manager and the View Manager Content Pusher roles.	View Manager, View Manager Content Pusher
View Manager Content Pusher	Grants access to push content to accessible users/groups/roles.	

Pre-Configured Users and Groups

The product comes with two pre-configured users: Administrator and Global Administrator. The administrator role contains all the other roles except the globaladministrator role. The globaladministrator role has access to the entire system. Explicit *no access* on an object overrides the administrator role, but not the globaladministrator role.

The product comes with two pre-configured groups: World and Root. World contains all users, and Root is contained in world. The World group has the User role which allows users to login and have access to the Browse module.

Pre-configured Access Control Settings for Users

For ease of administration of users, groups, and roles, the following defaults for users are implemented:

- A user is granted the modify access privilege on themselves upon creation. This allows the user to modify his own:
  - Default folder
  - Email address
  - Password
- A user belongs to the root group.
- The system is configured so that every user, group, or non-preconfigured role that is created by the administrator or the global administrator is visible to the World group. Since every user belongs to the World group, every user can see every other user, group, or role that gets created by the

administrator. (Users, groups, and roles created by the organizational administrator are not visible to the World group unless this is set to a default.)

- The system is configured with a User role that gives the minimal access to the system needed for any user. The World group (to which every user belongs) is configured to have the User role. Thus, by default, every user created in the system will automatically have the User role.
- A user is the owner of any job he publishes or any file he adds to the Repository. As owner, this user has full control access privilege over the item. This means that he can perform all the applicable operations on the item, such list, run (job), modify, delete, or change access privileges.

Checking Access Privileges

Users, documents, jobs, and printers are all items within the Hyperion Performance Suite system. When a user logs on to the system, the user's access to these items is determined. The system allows users to access the documents or jobs at specified levels, such as Modify, which allows users to modify the item or Full Control, which allows the user to delete the item. To determine what access privileges the user has to resources and items, the system goes through an access privilege checking routine, which is described in this section. This process occurs at login for each item in the system.

Access Privilege Checking for Items

A user gets access privileges to an item through the set of groups of which the user is a member, or through the set of roles assigned to that user. Access privilege checking for items is implemented in the following order:

1. User has the global administrator role? If the answer is yes, access is granted and checking stops.
2. User is the owner of the item? If the answer is yes, access is granted and checking stops.
3. User is denied access to the item? If the answer is yes, access is denied and checking stops.
4. User is granted specific access to the item? If the answer is yes, access is granted and checking stops.
5. User belongs to a group or role that has been denied access? If the answer is yes, access is denied and checking stops.
6. User belongs to a group or role that has been granted access to the item? If the answer is yes, access is granted and checking stops.
7. User belongs to a group or role that has been granted the content administrator role? If the answer is yes, access is granted and checking stops.

For steps 4 and 6, if the access privilege granted is at the same level or higher than required, then access is granted.

Figure 3-4 illustrates how the system determines a user's level of access for items.

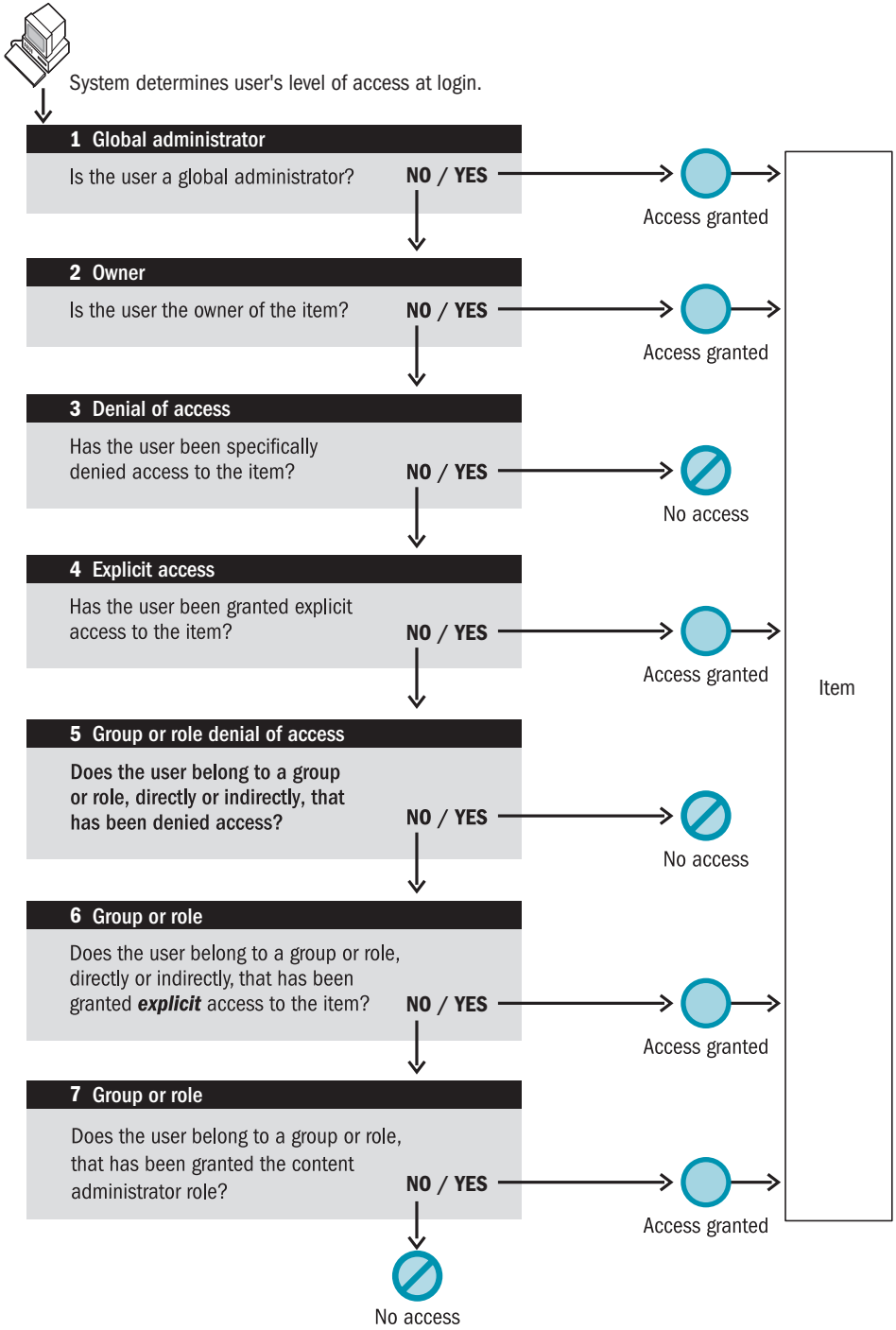


Figure 3-4 Access Privilege Checking for Items

Access Privilege Checking on Services

Access privilege checking for access to services is implemented in the following the order:

1. Has the global administrator role?
2. Access privilege granted directly or indirectly through an assigned role; that is, either the user is directly assigned the role, or a group that the user belongs to either directly or indirectly is assigned that role?

If the response is:

- **Yes**, then *access is granted and checking stops*.
- **No** to the first question, then *checking continues*.
- **No** to the second question, then *access is denied*.

Figure 3-5 illustrates how the system determines a user's access privilege on services.

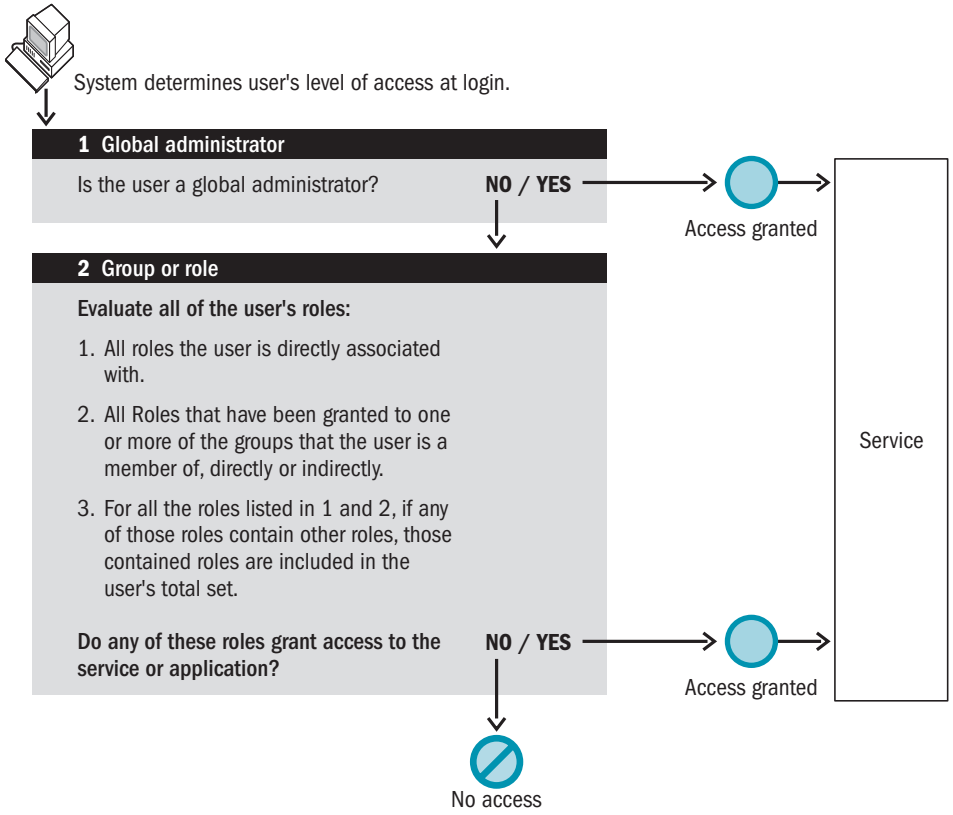


Figure 3-5 Access to Services

Denying Access

The system allows the global administrator, item owner, or a user with full control privileges on an item to deny access to the item by assigning *No Access* to the item. *No Access* applies to users, groups, or roles and works.

For example, Bob needs to publish a document for viewing by the sales group which includes Jane and John. Jane is a contractor and should not be able to view the document. John is the sales group's administrative assistant and may need to modify the item. Bob publishes the document with the following access privileges:

- Sales group gets view access
- Jane gets no access
- John gets modify access

In the example above, if Jane had the global administrator role or was the owner of the document, even though Bob gave her no access, she would still have full control access on the document.

The system determines *no access* using the following rules:

1. If an individual user is denied access, then the user cannot access the item in any way, unless the user is the owner or a global administrator
2. If the *No Access* is assigned to a group or role, a user that is in that group will have access to the item, if either:
   a. The user is the owner of the item.
   b. The user is granted access privileges to the item at the user level.
   c. The user has the global administrator role.

Additional Access Privilege Checking Examples

Look at the following examples to further your understanding of how access privilege checking works.

Example: Role Precedences

Figure 3-6 shows the access privilege that Ann has, considering order of access privilege checking and total of role and group associations.

What access does Ann have to Document A if she has the Developer role and belongs to the Management group?

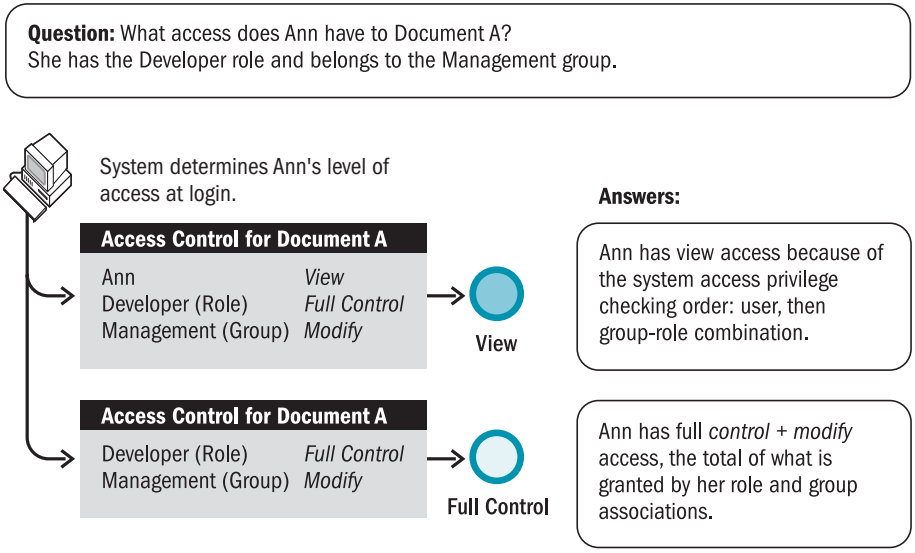


Figure 3-6 Role Precedences Example

Example: Overriding Access-Privileges Granted

Figure 3-7 shows an example of how access-privilege overrides work.

What access does Ann have to Document A if she has the Developer role and belongs to the Management group?

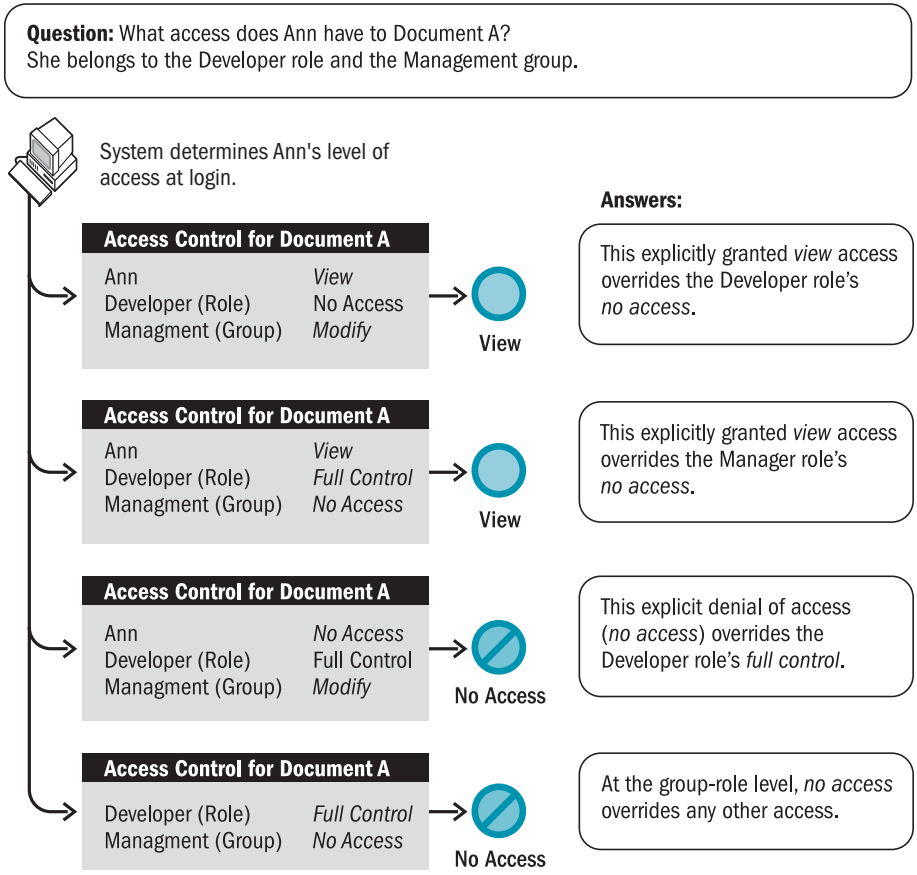


Figure 3-7 Overriding Access Privileges Granted

Example: Full Control and No Access Overrides

Figure 3-8 shows examples of full control access privilege and no access overrides.

What access does Ann have to Document A if she has the Content Administrator Role and belongs to the Management group?

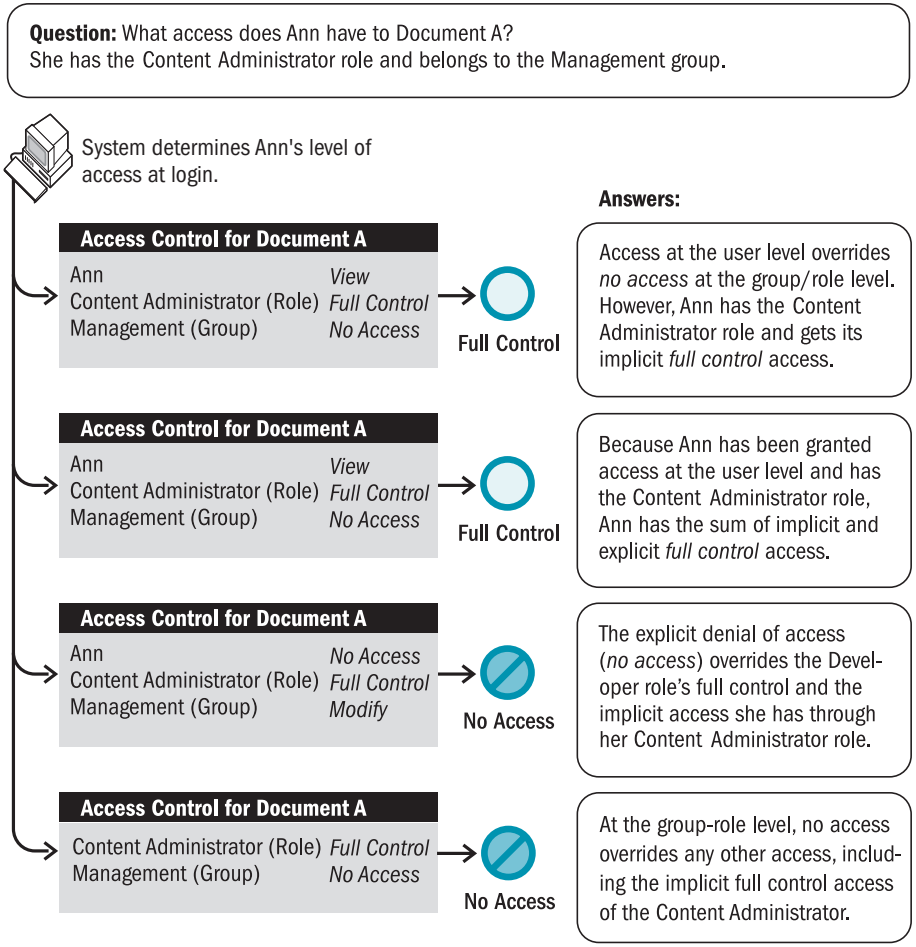


Figure 3-8 Full Control and No Access Overrides

Adaptive States for Intelligence Roles

BQY content also has adaptive states. The adaptive state is the access privilege on the BQY content. Table 3-3 shows which adaptive state permissions are available with the three Intelligence roles.

Table 3-3 BQY Content Adaptive States

	Intelligence Viewer	Intelligence Dynamic Viewer	Intelligence Analyzer
View	✓	✓	✓
View and Process		✓	✓
Analyze			✓
Analyze and Process			✓
Query and Analyze			✓
DataModel and Analyze			✓

A user can have the DataModel and Analyze Adaptive state on a BQY document and get the maximum analytical permission on BQY content. However, if the user has only been granted the Intelligence Viewer role, which is restricted to view and print, he will only be able to view and print the content.

If users are granted access privileges that are more powerful than those they have through their Intelligence role, then the icon next to the BQY content will represent the permission the user was granted (for example, the DataModel and Analyze icon). However, once users open the document, they will only be able to perform the operations allowed by their Intelligence role, which in the case of the Intelligence Dynamic Viewer or Intelligence Viewer role, is less than DataModel.

These examples are consistent with the behavior of role-based administration: a user could be granted full control access privileges on a job, but if the user only has the Job Runner role, he is restricted to running the job.

Recommendations about Assigning Intelligence Roles

Some customers might wish to assign different Intelligence roles at the group and user levels. For example, an administrator might wish to give the Accounting Group the Intelligence Analyzer role, but users John, Kristen, and James do not require the Intelligence Analyzer role.

The recommended practice would be either to assign these roles only at the group level and avoid assigning them individually at the user level, or to assign them all at the user level and not the group level. This means that every time a user is created, one of these roles should be assigned to that user, if the user is intended to have access through Intelligence Client.

Summary

This chapter explains how Hyperion Performance Suite Role-Based Access Control works and how to manage it in a secure and efficient manner.

4 Managing Users, Groups, and Roles

Hyperion Performance Suite maintains information about its users, the groups in which they have membership, and the roles they are assigned. The users of the system change, as do their associations with groups and roles. This chapter discusses managing the interaction between users, groups, and roles.

In This Chapter

About Managing Users, Groups, and Roles 4-2

Modifying Users, Groups, and Roles 4-4

Adding Users, Groups, and Roles 4-12

Setting Access Privileges for Publishing 4-16

About Managing Users, Groups, and Roles

Users, groups, and roles are part of the security system. Users and/or groups can be associated with roles and granted access privileges to specific items. You can grant users access to items individually, or to facilitate user management, you can place users into groups and grant access privileges to the groups. Criteria for creating groups could include geographical location, departments within the organization, or job function. Some groups could include all users. Others would be formed according to some need to share information. Examples of such groups are HQ, QA, Sales.

Predefined users in the system are *administrator* and *globaladministrator*, which are described later in this chapter. Predefined groups in the system are World, which contains all users, and Root, which is contained in world.

Authentication Systems

Users and groups are managed within an authentication system. The authentication system maintains the metadata (properties) about a given set of users and groups. When a user requests entry to the system (login), or use of its resources, such as opening a file or running a job, where a secure data source is being accessed, the system authenticates the user.

Every authentication system is managed by an Authentication Service (See Chapter 5, "Authentication and Login" for more detailed information). When a user makes a request, an Authentication Service verifies with the authentication system that the user request is valid. For a login request, the authentication system checks that user ID and password are valid. For a request to run a job, it verifies that the user has the required access privilege to run the specified job.

Groups can contain users and groups from different authentication systems. A group (with the members it contains) associated with an external authentication system can be added as a member of a group associated with a native authentication system.

The Authentication Service repository (ASR) always contains a "complete" model of users/groups in the external system. For more information on users maintained in an external system, see "Synchronization with External Systems" on page 5-5.

Active and Inactive Users and Groups

Users and groups can be active or inactive. *Active* indicates that the user or group is currently entitled to access the system. *Inactive* indicates that at the present time the user or group cannot access the system. Inactivation characteristics include the following:

- An inactivated user can no longer log in.
- Users who were members of a group that is inactivated are no longer members of the group.
- Access control on a group no longer applies when the group is inactivated.
- Users, groups, and roles that were granted a role that is inactivated no longer have the role.
- Access to items that the user, group, or role had is also inactivated: the inactivated user, group, or role no longer appears on that item's access control screen. However, other users who have access to the item through another group or a role association will still have access.

The information on the inactive user or group remains in the authentication system. Users and groups cannot be deleted from the Hyperion Performance Suite system. Users and groups can be deleted from external authentication systems. On synchronization, any imported internal users or groups not found in the external system becomes inactive.

Access Control on Users, Groups, and Roles

Users, groups, and roles are access-controlled, just like any object. The access control determines both:

- Who can do what to a user/group/role; for example, list, modify, or inactivate
- What a user and members of a group can do. For example, a user can be given a "mini-administrator" role that delegates the administration of users or groups

Modifying Users, Groups, and Roles

Managing users, groups, and roles includes the following tasks:

- Activating and inactivating users/groups/roles
- Modifying the properties of users/groups/roles
- Associating users/groups/roles with other users/groups/roles
- Granting or removing access privileges to users/groups/roles

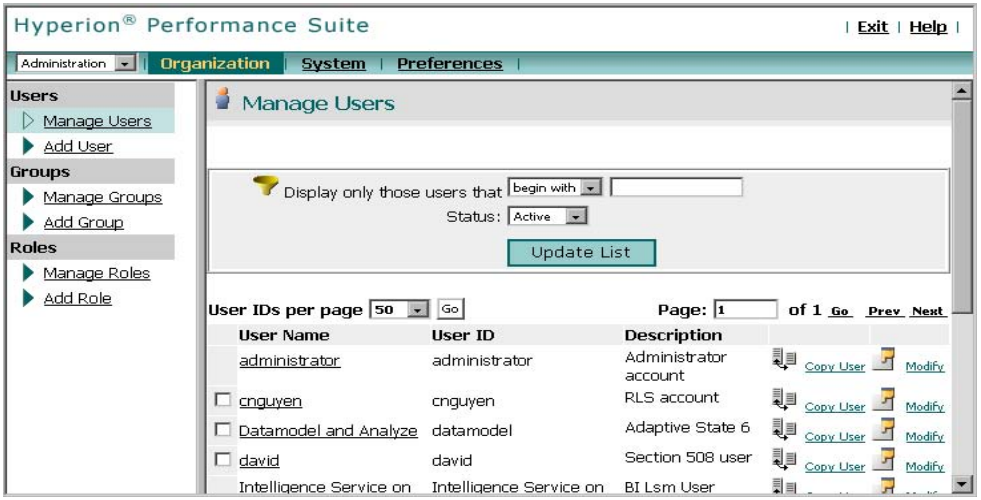
Note Users cannot be deleted from the system. Inactivate users that are no longer necessary.

User, group, and role management is done through the Organization tab of the Administrator module.

To access the Organization tab:

➤ Select **Administration** from the drop-down module list.

The first page displayed is the *Manage Users* page.



Note If you want to view all users, groups, or roles in a single listing, go to the Preferences tab. Choose the check box for List up to _____ users/groups/roles, and enter a number at least as large as the number of users in your system. Be aware that listing a large number of users may be slow.

If your criteria return a listing of multiple pages, you can type a specific page number in the entry box above and to the right of the listing, and then choose **Page**.

General Modifying Tasks

On the first page of the Organization tab, you display the item you want to modify. This is the same page where you inactivate an item or display the item you want to re-activate.

Listing Users, Groups, or Roles

To list or find the desired user, group, or role:

1. **Select the command Manage Users, Manage Groups, or Manage Roles in the navigation pane.**

2. **Choose Update List to display a listing of the specified item.**

   To display the name of an item not in the current list:

   a. Type an appropriate entry for *begin with* or *contain* in the User IDs, Groups, or Roles field, as applicable.

      For example, if you specify *contain* `Jac`, the users with the following User Names would be listed: Jack Jones, Mary Jacobson, Sonya Dejac.

      This field can be left blank. A blank field serves as a wildcard selection.

   b. Select **Active** in the Status field, then choose **Update List**.

3. **Choose the desired user, group, or role.**

Inactivating or Activating an Item

If you want to remove a user, group, or role, you need to *inactivate* the item. To inactivate a user, group, or role:

1. **On the Manage Users/Groups/Roles page, display the item to be inactivated.**
   - If the item is not currently displayed, type an appropriate entry for *begin with* or *contain* in the User IDs, Groups, or Roles field.
   - Ensure that *Active* is selected in the Status field, then choose **Update List**.
2. **Locate the item in the list displayed and select the field to the left of the user name.**
3. **Choose Inactivate Selected.**

   The listing for the item disappears. However, Repository items that the user, group, or role owns continue to be maintained by the system.

   You can verify that the item has been inactivated by displaying IDs in the *Inactive* list.

To re-activate a user/group/role:

1. **Select Inactive in the Status field of the first Manage Users/Groups/Roles page, then choose Update List.**

   If the ID is not currently displayed, type the first letter(s) of the ID in the field provided, then choose **Update List**.
2. **Locate the user/group/or role in the list displayed and choose the associated check box.**
3. **Choose Activate Selected.**

   The listing for the item disappears from the current page. When you display activated items again, the re-activated user/group/role will appear in the Manage Users/Groups/Roles page. Access to any items to which the inactivated users/groups/roles had access will be re-instated, unless the access control on that object was modified after the user/group/role was inactivated.

Modifying General Properties

To modify general properties of a user, group, or role:

1. **Choose Modify (User/Group/Role) in the navigation pane and choose Update List.**
2. **Select the item you want to modify and display or find and list the item according to search criteria you type in the User IDs, Group Names, or Role Names field:**
   - Beginning character(s)
   - Characters contained
   - Group(s) membership
3. **Choose Update List.**
4. **Modify properties, as desired.**

   Table 4-1 on page 4-7 lists general properties for users/groups/roles.
5. **Choose Apply or OK.**

General Properties

The first Modify page for user, group, or role displays the General Properties page. The list of general properties are shown in Table 4-1 and Table 4-2.

Table 4-1 General Properties for Users

Property	Description
User ID	Follows some naming convention in your organization, for example, first name initial followed by last name, as in *jyoung*. The user ID cannot be changed.
Name	Full name of user.
Description	A descriptive string that would assist in determining how user, group, or role might use the system: for example, marketing manager.
Email address	Email address in the organization.

Table 4-1 General Properties for Users *(Continued)*

Property	Description
Password	User password that the user subsequently changes (unless the user is associated with an external authentication system). Password must be between 5 and 64 characters. You can change the minimum password length by adding a java property, `-Dminimum_password_length=n`, to the following files: ■ servlet's java settings (Web server dependent) ■ startCommonServices.bat (located in *Install_Home*\BrioPlatform\bin) ■ ServiceConfig.bat (located in *Install_Home*\admin\bin) ■ settrustpass.bat (located in *Install_Home*\servlets\bin)
Confirm Password	Re-enter password.
Authentication System	Specified when a user is created. If an external authentication system, specified at the time the external users are imported into the system.
Default Folder	User's home folder.

Table 4-2 General Properties for Groups and Roles

Property	Description
Name	Full name of group or role.
Description	A descriptive string that would assist in determining the group's place within the organization or, in the case of a role, access privileges associated with the role, for example, "Content Publisher."
Authentication System (Groups only)	Specified when a group is created. If an external authentication system, specified at the time the external groups are imported into the system.

Modifying Associations Between Users, Groups, and Roles

You can change the following associations among users, groups, and roles:

- Adding users to a group
- Associating a group with groups
- Associating users/groups with a role

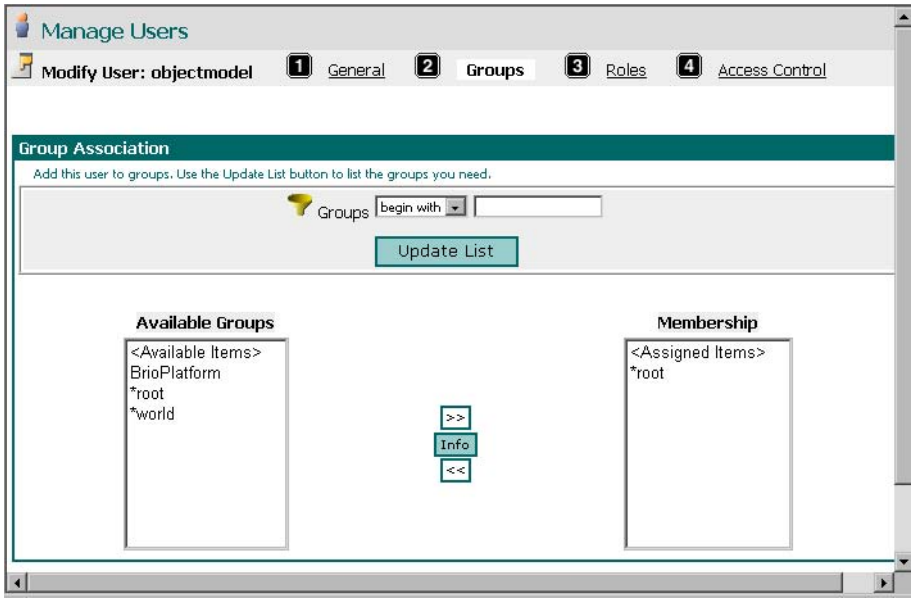
Adding Users to Groups

If you are adding one user to a group or groups, do so from the Group Association page of the *Manage Users* pages.

Note If a group is managed by an external authentication system, and it is configured to use external groups, then you cannot add new users or groups to the group.

To add a user to a group/groups from the Manage Users page:

1 **Display the Group Association page by choosing Manage Users → Modify (selected user name) → Groups.**



Note If a group in the Available Groups list is preceded by an asterisk (*), you cannot add a new member to the group, either because the group is managed by an external authentication system or you do not have the necessary access privilege to assign members to the group.

2 **From the Group Association page, select the groups to add from the Available Groups list.**

When selecting multiple groups, press the CTRL key as you make your selections.

3 **Choose the left facing arrows (>>).**

4 **Choose Apply.**

Associating a Group with Groups

You add a group to another group or to groups from the Group Association page of the *Modify Groups* wizard.

To add a group to group(s):

1 **Display the Group Association page by choosing Manage Groups→Modify (selected group name)→Groups.**

2 **From the Group Association page, select the group to add.**

When selecting multiple groups, press the CTRL key as you make your selections.

3 **Choose the left facing arrows (>>).**

4 **Choose Apply.**

Associating Users/Groups with a Role

Associating a user or group with a role means granting the user or group access to specific system operations or resources. For example, granting a group the Job Publisher role means that every member of the group (including members of subgroups) is granted the ability to publish jobs. For exceptions to this rule, see Figure 3-4 on page 3-19.

To associate users/groups with a role (or to assign a role to a user/group):

1 Choose **Manage Users/Groups** → **Modify** (selected user or group name) → **Roles.**

2 From the Role Association page, select the roles to add from the Available Roles list.

When selecting multiple roles, press the CTRL key as you make your selections.

3 Choose **Apply.**

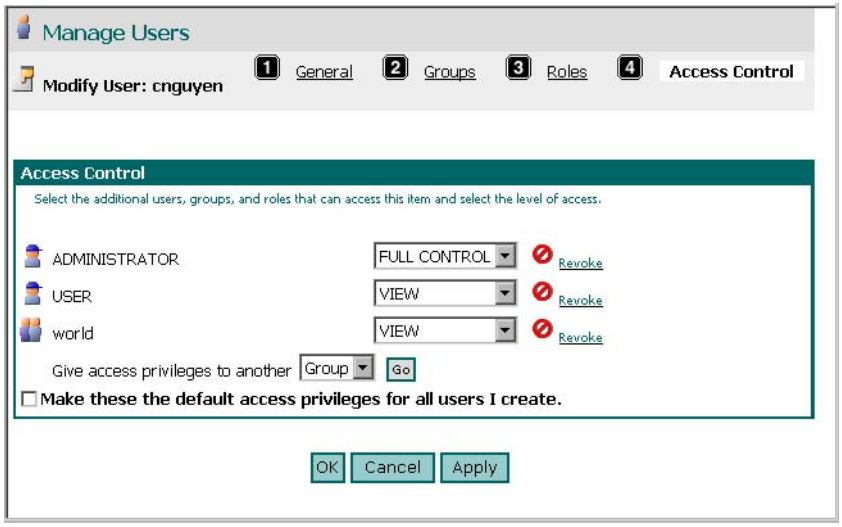
Modifying Access Privileges

To modify access privileges on a user, group, or role, the administrator or user who wants to make a change must have full control access privileges on the user, group, or role.

Note The owner of a user, group, or role automatically has full control access privileges on the item. Anyone who creates or publishes an item is defined as the owner of that item.

To modify access privileges:

1 Display the Access Control page by choosing **Manage Users/Groups/Roles** → **Modify** → **Access Control.**



To use the same access control settings for each user, group, or role you create, choose the check box for *Make these the default access privileges for all roles/groups /users I create*.

2 **Select role, group, or user, then choose Go to display the Give Access Privilege to a User/Group/Role page.**

3 **Select the user/group/role in which you want to modify the access privileges.**

4 **Select the access privilege from the drop-down list.**

To use the same access control settings for each user, group, or role you create, you have one more change to make. Choose the check box for *Make these the default access privileges for all <roles/groups /users> I create*.

Adding Users, Groups, and Roles

To add a user/group/role, choose the appropriate command in the navigation pane of a Manage Organization page.

Note If the authentication system is external and is configured to import users automatically, then new users or groups cannot be created.

Adding a User

To give a person access to the system, you add a *user* account for that person. There are two ways to add a user. You can copy an existing user and then change only the properties that need modification or you can create a new user from scratch.

Copying an Existing User

If your system has an existing user similar to the user you want to create, the easiest way to create the new user is to copy the existing one. When you copy an existing user, you fill in the general properties of the new user. The description, authentication system and default folder of the existing user are copied. Groups, roles, and access control are also copied: make any changes in these after copying the existing user.

To add a new user by copying an existing one:

1 **Locate the user you want to copy.**

For detailed instructions, see "Listing Users, Groups, or Roles" on page 4-5.

2 **Choose Copy User for the desired user.**

A General Properties form displays, with authentication system and default folder copied from the user you indicated.

3 **Type the new User ID and User Name.**

For descriptions of general properties, see Table 4-1 on page 4-7.

4 **Choose Next if you want to modify group membership, role assignments, or access control settings, which have been copied from the user.**

5 **Choose Finish to create the new user.**

Adding a New User

To add a user whose properties are different from those of existing users, fill out a blank General Properties form.

To add a new user:

1 **Choose Add User in the navigation pane.**

2 **Set the General Properties for the new user.**

For descriptions of general properties, see Table 4-1 on page 4-7.

3 **Choose Next if you want to add the user to any groups, assign roles, or change the default access control settings.**

Note To use the same access control settings for all users you create, choose the check box for *Make these the default access privileges for all users I create*.

4 **Choose Finish to create the new user.**

Adding a Group

Adding a group includes defining the general properties, associating users, other groups, and roles with the new group, and defining access to the new group.

To add a group:

1. **Choose Add Group in the navigation pane.**
2. **Set the General Properties for the new group.**

   For descriptions of the properties, see Table 4-2 on page 4-8.
3. Choose **Next** to **add users to the new group, add the new group to existing groups, assign roles to the new group, and change the access control settings.**

Note To use the same access control settings for all groups you create, choose the check box for *Make these the default access privileges for all groups I create*.

4. **Choose Finish to complete creation of the new group.**

Adding a Role

Hyperion Performance Suite provides a large number of preconfigured roles that grant access to operations on items, such as jobs, reports, users, and groups. You can assign these preconfigured roles to users, groups, or other roles and/or combine a number of them into a new role. For example, you can add a role called ProjectX that contains Personal Page Publisher, OCE Publisher, Job Runner, and Content Publisher. You can also create mini-administrators by giving a role access to users, groups, and roles. See "Creating a Mini-Administrator" on page 4-15.

To add a new role:

1. **Choose Add Role in the navigation pane.**
2. **Set the General Properties for the new role, and then choose Next.**

   For descriptions of the properties, see Table 4-2 on page 4-8.

3 Choose **Next** to assign the new role to users, groups, and other roles, and to change the access control settings.

Note To use the same access control settings for all roles you create, choose the check box for *Make these the default access privileges for all roles I create*.

4 Choose **Finish** to complete creation of the new role.

Creating a Mini-Administrator

A mini-administrator is an administrator with limited power. The regular administrator has access to all users, groups, roles, and content unless explicitly denied access. As the administrator you define what each mini-administrator has access to by creating a role for each mini-administrator. For example, you can set up a marketing mini-administrator who only has access to marketing users and groups and the roles marketing uses.

To create a mini-administrator:

1 Create a new role by following the steps above.

Give the new role the organizational administrator role. The organizational administrator role allows the user with this new role to access the organization tab of the administration module. By default this new role has no administration privileges.

2 Assign a user to this new role.

This user will be a mini-administrator.

3 On the Access Control page, open the **Role Has Access to These Users, Groups, and Roles** interface and specify an access privilege for all users, groups, and roles that this mini-administrator will need to access.

You can assign various levels of access such as the following examples:

a. If you want this mini-administrator to assign users and groups to roles, but not modify the roles themselves, grant the ASSIGN access privilege on the roles.

b. If you want this mini-administrator to modify group properties and link users to that group, grant the MODIFY or FULL CONTROL access privilege on the group.

4 **Choose Finish to complete creation of the mini-administrator role.**

The user assigned in Step 1 can now view and modify all the users, groups, and roles that were specified.

Setting Access Privileges for Publishing

You set default access privileges for basic documents, BQY documents, and BQY jobs in the Preferences tab section of the Browse module. You can also specify access privileges for a file when you publish it.

For detailed instructions on setting access privileges, see the *Foundation User's Guide*.

Summary

Management of organizational access to the Hyperion Performance Suite system involves adding users, providing them with access to the system, and allowing them to share information with one another. It also involves inactivating users and modifying or removing their access privileges as needed. To facilitate organizational management, users can be associated with roles that provide specified access privileges. They can also be given membership to groups, through which all members of each group get the access privileges assigned to the group.

5 Authentication and Login

This chapter discusses the authentication of users and groups. Hyperion Performance Suite provides an authentication system or you can configure Hyperion Performance Suite to use an external authentication system. This chapter also discusses available login methods.

Note The ability to access content from multiple Hyperion applications through Hyperion Performance Suite requires the use of the security platform driver which is an external authentication system. Hyperion recommends the use of the security platform driver over the other Hyperion supplied drivers.

In This Chapter

Authentication Service Function 5-2
Synchronization with External Systems 5-5
Configuring Login 5-8
Configuring Transparent Login 5-12

Authentication Service Function

The Authentication Service handles the authentication of users and manages user and group information. A set of users and groups that are managed together is an *authentication system.*

On login, a user must be authenticated using an Authentication Service that manages the authentication system to which the user belongs. If no Authentication Service running manages the user's authentication system, the user will not be able to login.

What an Authentication Service Manages

Each Authentication Service manages exactly **one** authentication system against which it validates user and password information. While this is true, each Authentication Service can access all user and group information, regardless of which authentication system an Authentication Service manages.

Note Multiple Authentication Services can manage the same authentication system. All Authentication Services that manage the same authentication system are peers of each other.

A user or group must be created in an authentication system, using an Authentication Service that manages that authentication system.

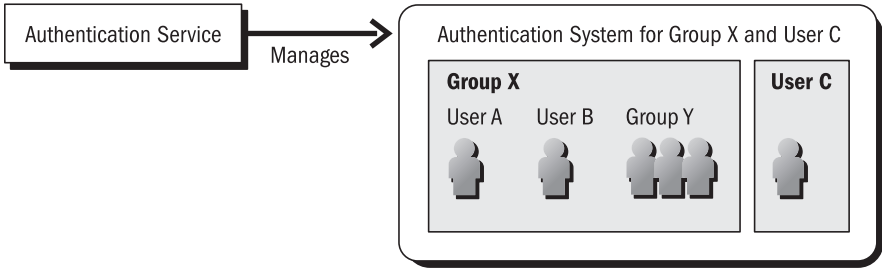


Figure 5-1 Each Authentication Service Manages Exactly One Authentication System

Types of Authentication

Authentication can either be native or external. Hyperion Performance Suite supports the use of both native and external authentication.

Native Authentication

Hyperion Performance Suite manages all the user and group information, including user passwords, in its own database, the Authentication Service repository (ASR). It does not use an authentication driver.

A special case of native authentication is System authentication. System authentication stores System users and groups, for example, administrator and globaladministrator. The Hyperion Performance Suite installer also creates a user in System authentication system for each Install_Home, for example, *Server1 on host stardust.* This authentication system does not require an Authentication Service to manage it. It always exists and cannot be deleted. In addition, no new users or groups can be created in this authentication system.

Users in the System authentication system can always log in using any Authentication Service. This means that the users *administrator* and *globaladministrator* can always log in, regardless of authentication system specified.

External Authentication

External authentication means that the user login information needed by Hyperion applications is stored outside the applications. The information is maintained in a central authentication directory, such as Lightweight Directory Access Protocol (LDAP) Directory, Microsoft Active Directory, or Windows NT LAN Manager.

External authentication uses a driver to access an external system from which user and group information can be retrieved.

The names of the users and groups are copied from the external system to the Hyperion Performance Suite database and periodically synchronized. However, password information is not copied. Thus, a user who is associated with an external authentication system is always authenticated directly against the external system through the external driver (unless the system is configured with a trusted password, and the servlets are configured to authenticate using this).

Security Platform Driver

Use the security platform driver to provide single sign-on access when multiple Hyperion applications are deployed.

The following types of authentication repositories are supported by the security platform driver:

- Windows NT LAN Manager (NTLM), 4.0 or higher
- Lightweight Directory Access Protocol (LDAP)
- Microsoft Active Directory server (MSAD), Windows 2000 sp1 or higher

When using the security platform driver, you must modify the XML-based security configuration file (`css_config.xml`) associated with your product to specify correct information pertaining to your corporate authentication directory.

Only one Authentication System can be configured using the security platform driver, but multiple Authentication Services can be setup to manage this Authentication system. Each service should either use the same `css_config.xml` file or should point to the same URL.

For more information on using the security platform driver for external authentication, see Chapter 6, "Integrating Hyperion Applications."

Other Drivers

For custom drivers, contact Hyperion customer support.

For legacy purposes, Hyperion Performance Suite provides other drivers for external authentication. These drivers must implement the `com.sqribe.transformer.drivers.authentication.AuthDrive` interface.

Synchronization with External Systems

At a specified interval, the list of external users or groups is synchronized with the list maintained in the ASR. When the external users or groups are imported into the system an owner is assigned to the imported users or groups. The user who is assigned as the owner can be configured using the Local Service Configurator (LSC) by modifying the "owner" property of the authentication system. The owner's default publishing access privileges are used to set the initial access control on imported users or groups.

If multiple Authentication Services manage one authentication system, only one Authentication Service does the synchronization.

User Synchronization

When importing users from an external system, only names are imported, not passwords. If external users are automatically imported, then the names of any users in external system not in internal system are imported. However, if external users are manually imported, then users must be created using the Administration servlet (or imported via API) and must be valid users in the external system. For authentication, the system always goes to an external system to validate an imported user on login.

On synchronization, any imported internal users not found in external system are deactivated. Where external users are automatically imported to the system, a user newly added to external system, might log in before synchronization occurs. In such a case, on login, the user is added dynamically to the ASR.

Group Synchronization

If an authentication system is configured to import external groups, the following information is imported:

- Names of any groups in the external system not in internal system
- Membership information for users is imported

If external groups are not imported, groups can be created in the Administration servlet (see "Adding a Group" on page 4-14) or created via the API. The existence of such groups in the external system is *not* validated. The group membership must also be manually defined.

Pass-Through for Jobs and BQY Files

The pass-through feature allows users to login once and access their reports' data sources without additional prompting for authentication. Pass-through is enabled per authentication system and then per OCE for BQY documents and per job for SQR and generic jobs.

In order to provide transparent access for users to data sources for foreground jobs and for BQY files, the administrator must first enable pass-through in the users' authentication system. Pass-through must then be enabled on a per-OCE basis (for BQY files and BQY jobs) and on a per-job basis, for SQR and generic jobs.

Note Pass-through does not work in the following scenarios:

- If a job is a background or scheduled job.
- If the user accesses Hyperion Performance Suite through another Hyperion application.
- If the system is configured with a Security Agent, such as Netegrity.
- If the servlet is configured to use TRUSTED_PASSWORD.

You can configure pass-through to use either a user's login credentials or credentials set in Browse Preferences or you can leave the credential choice up to the item owner.

Note The administrator user and the globaladministrator user are authenticated by the System authentication system. In order for pass-through to work for these users you need to enable pass-through for the System authentication system.

To enable jobs and BQY documents for pass-through:

1. **The administrator must enable the authentication system to use pass-through.**

   Use the LSC Configurator to configure the authentication system, see "Pass-Through and Trusted Password" on page 10-11.

2 **For BQY jobs and documents, the OCE owner must enable an OCE per data source to use pass-through.**

If a BQY job or document is pass-through enabled, then all of the OCEs that are used for that BQY must also be pass-through enabled. In addition, all of the data sources the BQY processes against must have the same username and password specified. Pass-through allows only one username and password to be specified.

For specific instructions, see the *Foundation User's Guide* for publishing OCE files.

3 **For SQR and generic jobs, the job owner must enable the job to use pass-through.**

For specific instructions, see the *Foundation User's Guide* for publishing SQR and generic jobs.

Caution! All pass-through enabled OCEs specified in a BQY job or file must have identical database credentials in order for all queries to process in that BQY job or file.

Configuring Login

A user can log in directly to Hyperion Performance Suite or an administrator can configure login to be transparent to the user who is logging in.

Logging in Directly

When users log in directly to the system, they type the requested information in a screen similar to the following:

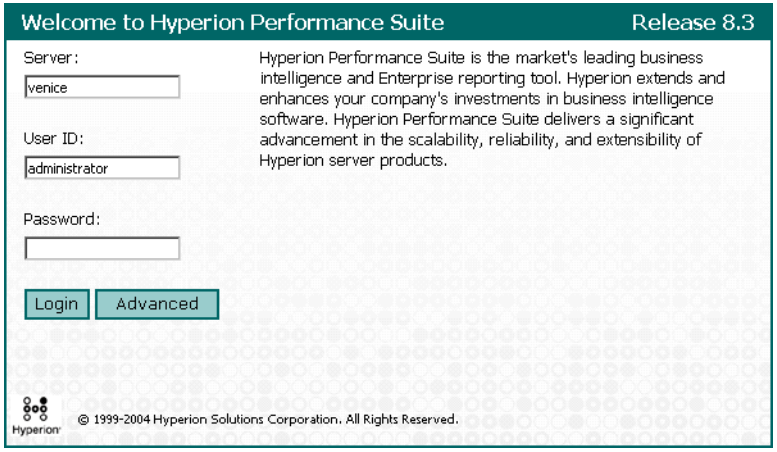


Figure 5-2 Hyperion Performance Suite Login Screen

Note If the user name and the user ID are different, only the user ID will log in a user.

At login, the default authentication system is used if no authentication system is specified. You can configure the default authentication system:

- On a per-servlet basis in the Servlet Configurator
- On a per-system basis in the Local Service Configurator

If no authentication system is specified at login, a default one is found from the following locations, tried in the order listed:

- The default authentication system specified for the servlet
- The system-wide default
- The *System* authentication system

On login, users can specify their associated authentication system by choosing the Advanced button. A new screen appears with a field that allows the user to select one of the available authentication systems. You can add authentication systems using the Local Service Configurator (see “Authentication Service” on page 10-7).

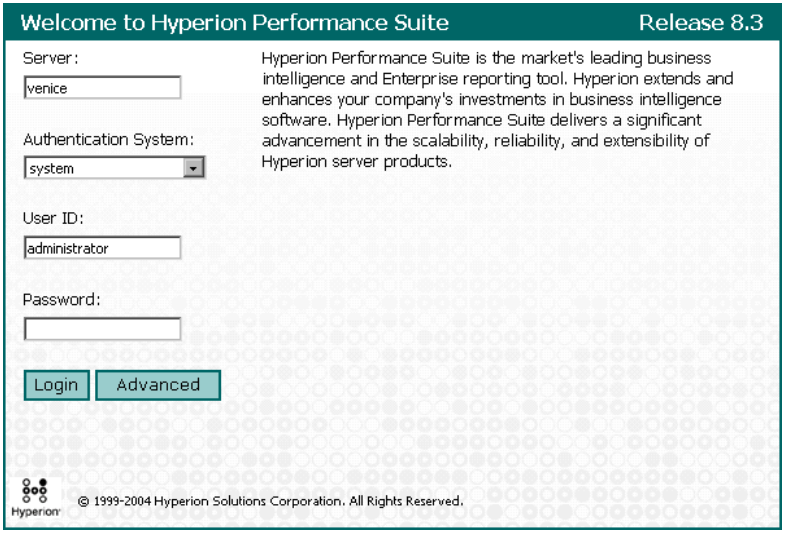


Figure 5-3 Advanced Login Screen

Transparent Login

If your site has implemented a reliable security policy and system, you can bypass the product login screen. A mechanism to allow trusted users to log in to Hyperion Performance Suite is provided.

For example, your site is a good candidate for transparent login if:

- The web server's security system is used to secure access to all Hyperion Performance Suite URLs.
- A security module interfaces with an external security system to pre-authenticate all users before allowing access to any web-based applications. By doing this, no user can access Hyperion Performance Suite without entering a user name and password to gain access to the web server.

In these cases, you do not want users to have to type in their user names and passwords twice. Transparent login allows you to more seamlessly integrate Hyperion Performance Suite into your company's infrastructure.

Prerequisites for Transparent Login

To seamlessly integrate Hyperion Foundation's login into the existing infrastructure, you should meet the following prerequisites:

- Understand how Hyperion Performance Suite users and groups will be organized.
- Be very familiar with your organization's current web architecture and security infrastructure.
- Decide whether you want to integrate transparent login as part of Hyperion Performance Suite URL, using a remote user environment variable, using HTTP authentication, or by implementing your own custom login scheme. (You may want to read this section, "Configuring Transparent Login," in its entirety before deciding.)

Note If the security platform driver is used, support for integrating with Netegrity SiteMinder is provided. For more information, see "Configuring for SiteMinder Single Sign-On" on page 6-21.

- Know how Hyperion Performance Suite finds login information.

Once you meet these prerequisites, you can proceed with integrating transparent login. The following steps present the general concept for transparent login integration:

1. Determine the password scheme to use in Hyperion Performance Suite. If an external system will authenticate users, the Hyperion Performance Suite password is less significant for the purpose of authenticating the user and the system should be configured internally to use trusted password.
2. Establish a method of passing authenticated user information to Hyperion Performance Suite. Passing this information in the URL is supported by the system. When the system receives a request from an authenticated user who does not have a Hyperion Performance Suite login connection, it uses the policy or mechanism to retrieve the user's name and the password configured in Hyperion Performance Suite to create the connection to the system. The subsequent information in this chapter provides details on these topics.

Note If you are running external authentication, you can have Hyperion Performance Suite synchronize its users list with the external authentication system's users list. For more information, see "Authentication Service" on page 10-7.

Configuring Transparent Login

This section discusses where Hyperion Performance Suite can find login information and various ways to configure your system for transparent login.

When using transparent login, be sure to have users start the product using the following URL:

server:*port*/Hyperion/*servlet*/main

where *server* is the name or IP address of the host on which Hyperion Performance Suite is running, *port* is the number of the port, and *servlet* is one of the five Hyperion Foundation servlets (browse, administration, personalpages, dashboard, or jobmanager), where the server listens for HTTP requests.

Note Depending on how you implement transparent login, you may want to disable user logout. (Upon logout, the login form normally appears. You can prevent this by disabling user logout.) For more information, see "User Interface Properties" on page 11-5.

Note Logging in as administrator or globaladministrator always resolves to the corresponding user in the system AuthenticationSystem, regardless of the AuthenticationSystem specified. This is an issue when using an external authentication system and an administrator or globaladministrator exists in the external system. For example, if you log into NT as the administrator, your password will probably not match the pre-defined administrator password and you are not going to be able to login.

Sources for Login Information

When a custom user name or password policy (any policy other than $NONE$) is set in the Servlet Configurator, that custom policy is used for all users. The custom policy is used even if another value for user name or password is provided in the login form, the URL, or a cookie. However, if the user name, password, or server specification is incorrect, the system looks in other places for the login information.

Hyperion Performance Suite looks for each piece of login information from the following sources, *in this order:*

- *Custom username policy* (*Custom password policy*) setting

  If set to $NONE$, the system proceeds to next source in this list.

- Login form

  The system obtains user name (password) value from configuration properties or user input.

- URL
- Cookie

The sections that follow explain transparent login using URLs, the custom policy properties, macros, and your web server's authentication.

Automatic Login with URLs

The default login screen permits users to log in to Hyperion Performance Suite by completing an HTML form and choosing **Login**. This login technique is the default.

One way to provide transparent login is to pass the user name, password, and server as part of a URL. Users can set up a bookmark that will automatically log them into Hyperion Performance Suite. If any of the parameters are omitted, the system will display the Login screen to prompt for the missing information.

The following three examples illustrate different ways to use a URL to provide transparent login.

Note Providing a password in clear text in a URL is not secure and is not recommended.

URL Bypassing the Login Screen

The following URL bypasses the login screen. It logs in the user and shows the initial product screen—the default personal page on the *Personal* tab.

The *server:port* is the IP domain name and port number where the user accesses Hyperion Performance Suite, *username* is the user name, *mypass* is the user's password, and *servname* is the name of the host running the General Service Manager (GSM).

```
http://server:port/Hyperion/servlet/main?
user=username&pass=mypass&server=servname
```

```
http://11.222.33.44:8100/Hyperion/browse/main?user=lynn&pass
=dani2&server=gemini
```

URL Invoking Login with User Name, Password Initialized

The following URL displays the login screen and initializes its fields with *username*, *mypass* and *servname*.

```
http://server:port/Hyperion/servlet/main?
user=username&pass=mypass&server=servname&autologin=no
```

```
http://11.222.33.44:8100/Hyperion/administration/main?user=lynn
& pass=dani2&server=gemini&autologin=no
```

URL Invoking Login with User Name, Trusted Password

A trusted password can be used to enable transparent login where the client is responsible for authentication. The servlet passes the trusted password to the Authentication Service, after doing its own authentication of the user. There is no need to change the passwords of all users.

However, for security reasons, the *System* authentication system's users *administrator* and *globaladministrator* cannot be authenticated using a trusted password.

The following URL displays the login screen and initializes its fields with *username* and *servname*:

```
http://hostname/Hyperion/servlet/main?user=username&server=servname&autologin=no
```

This example shows the use of the host's IP address instead of its name:

```
http://11.222.33.44:11111/Hyperion/browse/main?user=lynn&server=gemini&autologin=no
```

Note Before this example will work, you must configure the trusted password and reset *mypass* to match this trusted password. See "Configuring a Trusted Password" on page 5-19 for more information.

URL Bypassing the Login Screen, Running a Job

The following URL brings the user to a specified job (*jobname*) within the system, performs the login automatically, and runs the job.

```
http://server:port/Hyperion/servlet/run/jobname?user=username&pass=mypass&server=servname
```

```
http://11.222.33.44:11111/Hyperion/personalpages/run/HRNames2&user=
1ynn&pass=dani2&server=gemini
```

Custom Policies and Macros

You can provide transparent login by using custom user name and password policies. These policies are set through two properties in the Servlet Configurator, in the *User Interface* →*Login* category.

Custom username policy controls where the system looks for user names for all users. *Custom password policy* controls where the system looks for passwords for all users. The values of these custom-policy properties are called *macros*.

A macro can also be passed in place of a user name or password. The following sections discuss many different uses of the macros for user name and password:

- User Name Macros
- Password Macros
- REMOTE_USER Property

User Name Macros

A macro specified as a user name, or as the *Custom username policy,* tells the system where to obtain the user name(s). Table 5-1 describes the user name macros supported.

Table 5-1 User Name Macros for Hyperion Performance Suite

`$CUSTOM_LOGIN$`	If the user name is set to `$CUSTOM_LOGIN$`, the system uses your custom login code to determine the user name. See `$Install Home/servlets/samples/loginsamples.jar` for more details on using custom login API.
`$REMOTE_USER$`	If the user name is set to $REMOTE_USER$,the system gets the user name from the REMOTE_USER environment variable.
`$HTTP_USER$`	If the user name is set to $HTTP_USER$, the system gets the user name from HTTP authorization information.
`$SECURITY_AGENT$`	Use when integrating Netegrity using the security platform driver.

Password Macros

A macro specified as a password, or as the *Custom password policy,* tells the system where to obtain the password(s). Table 5-2 describes the password macros supported.

Table 5-2 Password Macros for Hyperion Performance Suite

`$CUSTOM_LOGIN$`	If the password is set to `$CUSTOM_LOGIN$`, the system uses your custom login code to determine the password. See `$Install_Home/servlets/loginsamples.jar` for more details on using custom login API.
`$TRUSTEDPASS$`	If the password is set to `$TRUSTEDPASS$`, the system uses the trusted password. The Authentication System should be configured with the same `$TRUSTEDPASS$` in which the servlets are configured. To use the system with a trusted password, you must configure the trusted password, see "Configuring a Trusted Password" on page 5-19.
`$USERNAME$`	If the password is set to $USERNAME$, the system applies the user name as the default password. This means that each Hyperion Performance Suite user must be created with user name = password.
`$HTTP_PASSWORD$`	If the password is set to $HTTP_PASSWORD$, The system gets the password from HTTP authorization information.

Default Server Macros

A macro specified as the custom default server policy tells the system where to obtain the default server information. Go to "Set the Default Server To" drop-down. You can enter text information specifying the name of the program or you can enter a default value from a drop-down list.

Authentication Macros

A macro specified as Custom Authentication Policy tells the system where to obtain the Authentication information. You can enter text information specifying the name of the program or you can enter a default value from a drop-down list.

REMOTE_USER Property

If Hyperion Performance Suite is running as a servlet within a web server, and the web server is configured to authenticate users, you can employ the same authentication mechanism to log users in to Hyperion Performance Suite transparently. Doing so uses the Common Gateway Interface (CGI) property REMOTE_USER, set on the web server.

To use REMOTE_USER, set *Custom username policy* to $REMOTE_USER$. This causes the system to retrieve user names from the CGI property REMOTE_USER. When set, $REMOTE_USER$ (like any custom user name or password policy) overrides any user name supplied by the login screen, a URL query string, or a cookie.

In conjunction with using REMOTE_USER for the user names, you can get passwords transparently by setting *Custom Password Policy* to $TRUSTEDPASS$, $USERNAME$, $CUSTOM_LOGIN$ (if you have implemented your own login scheme), or $HTTP_PASSWORD$. See "Password Macros" on page 5-17 for details.

Configuring a Trusted Password

Configure your system to use a trusted password by setting a trusted password for the servlets and for the Authentication services.

To configure your system to use a trusted password:

1. **Open the Local Service Configurator.**
2. **For each Authentication system, enable *Set trusted password* and enter and confirm the the trusted password.**

   See "Pass-Through and Trusted Password" on page 10-11.
3. **Open the Servlet Configurator.**
4. **Change *Custom password* policy setting to $TRUSTEDPASS$ (Properties→User Interface→Login).**

   See "User Interface Properties" on page 11-5.
5. **Run** `settrustedpass.bat located in` *`Install_Home`*`\servlets\bin.`
6. **Enter the current password (default is** `123456`**).**
7. **Enter and confirm the new password.**
8. **Restart the Authentication Services.**
9. **Restart the servlets.**

Summary

Hyperion Performance Suite uses both native and external authentication systems. A user can log in to the Hyperion Foundation system either directly or using transparent login.

6 Integrating Hyperion Applications

This chapter discusses integrating Hyperion Performance Suite with other Hyperion applications, such as Hyperion Reports and Hyperion Analyzer. Single sign-on (through the security platform driver) and registration to Hyperion Hub gives your users access to the reports or views of registered applications with one login.

In This Chapter

About Single Sign-On 6-2
Support for SiteMinder 6-3
Setting Up the Environment for NT LAN Manager Support 6-5
Configuring the Security Platform Driver 6-9
Sample Deployment Scenarios 6-22
About Related Content and Hyperion Hub 6-37
Administrating Related Content 6-37

About Single Sign-On

Single sign-on is the ability of a user to access multiple Hyperion applications after logging on only once. The user is externally authenticated using the security platform driver the first time he logs in. An encrypted token is generated which contains the user credentials in the form of the following:

- The user name
- In some cases, the user password. The presence of a password in the token depends on the configuration. If you are using a trusted authentication directory, no password is present or required in the token.

As shown in Figure 6-1, the token is passed among other Hyperion applications and is used as needed to automatically re-authenticate the user when the user moves to another application. Single sign-on is effective in cases where one Hyperion application launches another. Note that if a user launches a second application independently, for example, from the Start Menu, a token cannot be passed between the applications, and the user must re-authenticate.

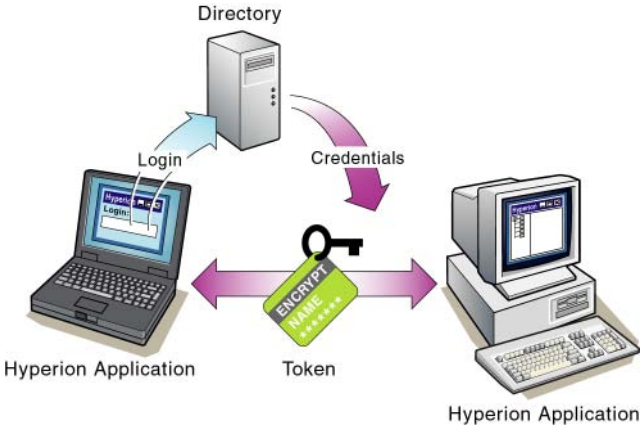


Figure 6-1 Authentication to External Provider Enables Sign-On to Reach Multiple Applications

Tokens are encrypted; however, additional security such as Secure Sockets Layer (SSL) protocol is recommended for prevention of replay attacks or man-in-the middle attacks.

To enable single sign-on between multiple Hyperion applications that launch one another, you must use a single XML configuration file that is shared by the multiple product installations. For more information, see "Configuring the Security Platform Driver" on page 6-9.

Support for SiteMinder

In addition to native Hyperion single sign-on, Hyperion applications can integrate with Web access management solutions such as the Netegrity SiteMinder product. SiteMinder is a Web access management solutions provider. Web access management solutions are employed by organizations to manage and enforce authentication, authorization, and single sign-on for web resources such as JSP files, ASP files, or HTML files. The Hyperion security platform enables single sign-on for a user into Web-based Hyperion applications from a Web access management solutions provider, also known as a security agent. Integration with a security agent requires configuration of the `<securityAgent>` element in the XML configuration file.

Note In this documentation, the terms security agent and Web security agent are interchangeable, and refer to any Web access management solutions provider such as Netegrity SiteMinder.

The following security agents are tested and supported for single sign-on with Hyperion applications using the Hyperion security platform:

- SiteMinder Policy Server 5.5 Service Pack 2
- SiteMinder Web Agent 5.5 Service Pack 2

If your corporation has implemented SiteMinder to protect company Web resources, you can configure the security platform to require only that users authenticate through SiteMinder, after which they will not be required to present credentials again when logging in to Hyperion applications.

For information about configuring the `<securityAgent>` element in the XML configuration file, see "Configuring for SiteMinder Single Sign-On" on page 6-21.

For a sample deployment scenario illustrating single sign-on with SiteMinder, see "Scenario 11: Single Sign-on with SiteMinder" on page 6-34.

Prerequisites

This section lists the prerequisites for using the security platform driver.

1 **You will need to decide which platform to use on the server in which the Authentication Service is running. Table 6-1 shows the supported authentication providers and platforms of the server running the Authentication Service.**

Table 6-1 Supported Authentication Providers and Platforms

Platform of the server running the Authentication Service	Lightweight Directory Access Protocol (LDAP) version 3 compatible directories	NT LAN Manager (NTLM)	Microsoft Active Directory
Windows NT 4.0, sp 6a or higher	X	X	X
Windows 2000 Server and Advanced Server, sp3 or higher	X	X	X
Windows 2003	X	X	X
UNIX	X	X - requires installation of Hyperion Remote Authentication Module	X

Note iPlanet 5.2 and Novell eDirectory 8.7 are the tested and supported LDAP servers. iPlanet is now known as Sun[tm] Open Net Environment (Sun ONE).

2 **If your company has implemented Siteminder to protect company Web resources, you can configure the security platform driver to enable single sign-on between Hyperion Performance Suite and Netegrity Siteminder.**

For more information on how to configure your system to use Netegrity Siteminder, see "Support for SiteMinder" on page 6-3.

3 **If you are implementing security using an NTLM provider and are using a UNIX system as the machine where the Hyperion application software is installed, ensure that the Hyperion Remote Authentication Module is installed on a Windows NT or Windows 2000 server. Install the Hyperion Remote Authentication Module from the Hyperion Download Center. After the Remote Authentication Module is installed, you must also provide its URL as a value to the `<remoteServer>` element in the security platform XML configuration file.**

4 **If you want to enable authentication of users from multiple Windows domains, but you do not want to set up trust relationships between those domains, install the Hyperion Remote Authentication Module on a separate Windows server. This enables users of Hyperion applications running on one domain to log into Hyperion applications on other domains. If multiple Hyperion applications are installed, each should be configured to use the same Hyperion Remote Authentication Module.HyperionHyperion.**

Setting Up the Environment for NT LAN Manager Support

The directions in this section apply to administrators who want to enable one or more Hyperion applications to use external authentication of users in a Windows NT LAN Manager (NTLM) domain.

To enable UNIX support for NT LAN Manager, see "UNIX Application Support for NT LAN Manager" on page 6-8.

Setting Up User Rights for NT LAN Manager

To enable use of the NTLM provider, certain access rights are required of the Windows NT user account on which the Common Services are running.

Note Make sure you set up these rights on the machine on which Hyperion Performance Suite runs.

Additionally, certain access rights are required for end users. The following access rights are required for external authentication to work with an NTLM provider:

- **Access this computer from the network** – End users of Hyperion Performance Suite using external authentication require this right (usually granted to Administrators).
- **Act as part of the operating system** – The account used to run Hyperion Performance Suite processes requires this right in order for external authentication to work (normally not granted to anyone).

See "Setting Up User Rights on Windows NT" on page 6-6 or "Setting Up User Rights on Windows 2000" on page 6-7, depending on which operating system you use.

Setting Up User Rights on Windows NT

1. From the Start Menu, select Programs→Administrative Tools (Common)→User Manager.
2. In the **User Manager** dialog box, select the appropriate user name.
3. Select Policies→User Rights. The **User Rights Policy** dialog box is displayed.
4. From the Right drop-down list box, select **Access this computer from network**.
5. The users or groups who have the selected policy setting are shown in the **Grant To** list box. If the appropriate user is shown in this list box, click **Cancel** and skip to Step 7.
6. To grant the selected right, click **Add**, and complete the **Add Users and Groups** dialog box.
7. In the User Rights Policy dialog box, check **Show Advanced User Rights**.
8. From the Right drop-down list box, select **Act as part of the operating system**.

   The users or groups who have the selected policy setting are shown in the **Grant To** list box.
9. If the appropriate user is shown in the **Grant To** list box, click **Cancel** and skip the rest of this procedure.
10. To grant the selected right, click, and complete the **Add Users and Groups** dialog box.

Setting Up User Rights on Windows 2000

1. From the Start Menu, select Settings→Control Panel→Administrative Tools→Local Security Policy.

   The **Local Security Settings** dialog box opens.

2. Expand the **Local Policies** folder, in the left-pane tree of the **Local Security Settings** dialog box.

3. Click the **User Rights Assignment** folder, and, in the right area of the dialog box, double-click the **Access this computer from the network** policy.

   The Local Security Policy Setting dialog box for the Access this computer from the network policy is displayed.

4. If the relevant user account has the policy checked, click **Cancel** and skip to Step 9.

5. Click **Add**.

6. Select the name of the appropriate user or group needing the right.

7. Click **Add**.

8. Click **OK**.

9. In the right pane of the dialog box, double-click **Act as part of the operating system** policy.

   The Local Security Policy Setting dialog box for the Act as part of the operating system policy is displayed.

10. If the relevant user account has the policy checked, click **Cancel** and skip the rest of this procedure.

11. Click **Add**.

12. Select the name of the appropriate user or group needing the right.

13. Click **Add**.

14. Click **OK**.

UNIX Application Support for NT LAN Manager

If you are implementing external authentication with an NTLM provider and wish to support the use of a UNIX machine for the client application, you must also ensure that the Hyperion NTLM Remote Server is installed on a Windows NT/2000 server.

To provide support for NTLM authentication for a UNIX client application:

1. On the Windows NT/2000 server, install the Hyperion NTLM Remote Server.
2. Accept the license agreement and click **Next**.
3. Click **Next** on the Welcome page.
4. Choose a destination location for the NTLM Remote Server, and click **Next**.
5. Enter the host name and port number for the machine hosting the NTLM Remote Server, and click **Next**.
6. If you will be using Secure Sockets Layer with your NTLM deployment, select the option to support SSL, and click **Next**.
7. For configuration information, see "Optional Configuration for NTLM" on page 6-20.
8. In the **Start Copying Files** dialog box, click **Next** to begin the installation.
9. Click **Finish** to complete the installation.
10. Run the remote server by choosing Start→Programs→Hyperion Solutions→NTLM Remote Server→Run NTLM Remote Server.
11. On the UNIX machine that hosts Hyperion Performance Suite, ensure that the machine is configured as shown in Scenario 3 in the deployment scenarios section.
12. On the UNIX machine that hosts the application, modify the values in the `<location>` tags in the `<remoteServer>` section of `css_config.xml` to tell the application where to find the remote NTLM server. For more information, see "Optional Configuration for NTLM" on page 6-20.

Configuring the Security Platform Driver

This section explains how to configure Hyperion Performance Suite to support authentication of users that are stored in LDAP, Active Directory, or Windows NT LAN Manager (NTLM) external-authentication providers when using the security platform driver. Configuration also applies to supporting single sign-on.

To enable single sign-on in cases where one Hyperion product launches another, you must use a single XML configuration file that is shared by both product installations.

To configure the security platform driver:

1. **Set-up external authentication using the security platform driver. See "Adding a New External Authentication System" on page 10-19.**

2. **Edit the `css_config.xml`, located at *`Install_Home`*`\BrioPlatform\etc`, to configure the property values for Hyperion Performance Suite and provider scenarios.**

   The properties are presented in the form of XML tags representing property types and modifiable values of the XML tags, representing the values for each property.

   For each supported authentication scenario, there is a set of properties to edit in the `css_config.xml` file, depending on the deployment scenario. See "Sample Deployment Scenarios" on page 6-22.

   The `css_config.xml` file contains the minimum set of properties that must be configured for your application and provider scenario.

Configuring the Preferred Logging Priority

The following configuration requirement applies to LDAP, Active Directory, and NTLM providers. For additional requirements specific to either provider, see "Configuring an LDAP or Active Directory Provider" on page 6-12 or "Configuring an NTLM Provider" on page 6-19.

To configure the error level setting for applications supporting external authentication and single sign-on:

1. **In a text editor, open `css_config.xml`.**

2. **Locate the following section of `css_config.xml`:**

```
<logger>
  <priority>DEBUG</priority>
</logger>
```

3 **Change the error-reporting value from `DEBUG` to the level of authentication-related error messages that you want the application to log.**

If the entire `<logger></logger>` section, including the tags, is deleted, the default value of `DEBUG` is used. Do not delete only the values inside the tags.

In the following list of valid values, each level is inclusive of the levels below it:

- **`DEBUG`** – Includes extensive information useful for debugging
- **`INFO`** – Includes information on the status of operations and requests
- **`WARN`** – Includes cautionary information, if relevant, for some operations and requests
- **`ERROR`** – Includes only statements pertaining to failed operations and requests
- **`FATAL`** – Includes only information about errors that result in a disconnection

4 **Save the `css_config.xml` file.**

Configuring the Provider Search Order

The search order provides the external authentication mechanism with the ability to access multiple providers in a sequential manner. Search order must be defined even if there is only a single authentication provider; in this case, the search order property has a single entry.

To define the provider search order:

1 **In a text editor, open `css_config.xml`.**

2 **Locate the `<searchOrder>` section of `css_config.xml`, which looks like the following but may have different values:**

```
<searchOrder>
 <el>ntlmServer</el>
 <el>ldapServer</el>
 <el>msadServer</el>
</searchOrder>
```

3 **Move the `<el>` sections around as needed to place the provider types in the order that they should be searched whenever a user tries to log on to a Hyperion application.**

It would make sense to place the provider containing the *most* users of Hyperion applications *first* in the search order, if that information is known.

For example, in the following section, the NTLM provider would be searched first for user information.

```
<searchOrder>
 <el>ntlmServer</el>
 <el>ldapServer</el>
 <el>msadServer</el>
</searchOrder>
```

You may add or remove providers as needed. For example, you might add an `<el>ldapServer2</el>` section if you have a second LDAP provider named `ldapServer2`.

4 **If you are using an LDAP provider, between the appropriate `<el></el>` tags, replace `ldapServer` with the desired name to represent the configuration for the LDAP server.**

The name must be the same as the name you specify in the LDAP provider section, in Step 3 on page 6-13.

This name is the same as the Provider on the properties page of a user or group in the Administration module.

5 **If you are using an NT LAN Manager provider, between the appropriate `<el></el>` tags, replace `ntlmServer` with the desired name to represent the configuration for the NTLM provider.**

The name must be the same as the name that you specify in the NTLM provider section, in Step 3 on page 6-19.

6 **Save the `css_config.xml` file.**

Configuring Token Timeout

When an externally authenticated user logs in to a Hyperion application, a token is generated to contain the login credentials. You can configure the token to expire after a specified number of minutes, instead of the default of 480 minutes.

To define the length of time a token is valid:

1 In a text editor, open `css_config.xml`.

2 Locate the `<token></token>` section of `css_config.xml`, which looks like the following but may have different values:

```
<token>
 <timeout>60</timeout>
</token>
```

3 Between the `<timeout></timeout>` tags, enter the number of minutes that should pass in before a user is required to authenticate again.

The default length of a token is 480 minutes (8 hours). In other words, if the `<token></token>` element and all its contents are removed from the configuration file, the security platform will assign a default token timeout of 8 hours.

4 Save the `.xml` configuration file.

Configuring an LDAP or Active Directory Provider

The section shows how to modify the properties that apply to configuring the provider implementations for Lightweight Directory Access Protocol (LDAP). Use these instructions if your application supports an LDAP or Microsoft Active Directory provider.

Note These instructions assume that you have already completed the generic configuration steps described in "Configuring the Preferred Logging Priority" on page 6-9 and "Configuring the Provider Search Order" on page 6-10.

Basic Configuration for LDAP or Active Directory

To complete basic configuration for LDAP:

1 **In a text editor, open** `css_config.xml`.

2 **If you are configuring for an LDAP directory such as iPlanet or Novell LDAP server, locate the following section of** `css_config.xml` **or the entire section including and between the tags** `<ldap name="ldapServer">` **and** `</ldap>`:

```
<ldap name="ldapServer">
  <trusted>true</trusted>
  <url>ldap://host:portNo/DIT</url>
  <userDN>cn=User Name</userDN>
  <password>userPassword</password>
  <user>
    <url>ou=People</url>
  </user>
  <group>
    <url>ou=Groups</url>
```

```
  </group>
</ldap>
```

If you are configuring for Microsoft Active Directory, locate the section within the following tags instead: `<msad name="msadServer"></msad>`, and then configure the properties the same way as for iPlanet or Novell LDAP.

3 **In the first line of the above section, change `ldapServer` or `msadServer` to the name you want to use to indicate the configuration for this LDAP or Microsoft Active Directory provider.**

The name must be the same as the name that you specified in the search order section, in Step 4 on page 6-11.

This name is the same as the Provider on the properties page of a user or group in the Administration module.

4 **Between the `<trusted></trusted>` tags, leave the default value of `true`, or, if the specified provider is not a trusted LDAP or Active Directory provider, replace the value with `false`.**

If the entire `<trusted></trusted>` section including the tags is deleted, the default value of `true` is used. Do not delete only the values of the tags.

If the trust setting is `true`, a password is not present or required in the token generated upon user authentication.

If the trust setting is `false`, a password is part of the token.

Note If your corporation uses a security agent such as Netegrity SiteMinder to protect company Web resources, the provider must be trusted. For more information, see "Configuring for SiteMinder Single Sign-On" on page 6-21.

5 **Between the `<url></url>` tags, replace `ldap://host:portNo/DIT` with the URL that specifies the location of the LDAP or Active Directory provider.**

You must include the domainComponent attributes (DCs) in the URL.

The following is an example of a URL that includes a directory information tree (`DIT`):

```
ldap://ldap_server:389/DC=company,DC=com
```

Note Do not include extra spaces in the URL.

6 **Between the `<userDN></userDN>` and `<password></password>` tags, modify the sample values, `cn=User Name` and `userPassword`, with information from a user account that has read-only access to the directory stores.**

If you want to provide anonymous access, delete the entire `<userDN></userDN>` and `<password></password>` sections. Delete the tags and the values; do not delete only the values.

7 **Between the `<url></url>` tags for user, replace `ou=People` with the information that indicates the branch in the directory server that contains user entries.**

The user-URL property is relative to the URL specified for the LDAP or Active Directory provider. If you want the provider to search the whole directory specified by URL in the provider section, delete the entire `<url></url>` section that is in the `<user>` section. Do not leave the `<url></url>` tags empty, without a value.

For example, if users on the LDAP or Active Directory provider are stored in an organizational unit directory named People, the following sample is correct:

```
<user>
 <url>ou=People</url>
</user>
```

8 **Between the `<url></url>` tags for group, replace `ou=Groups` with the information that indicates the branch in the directory server that contains group entries.**

The group-URL property is relative to the URL specified in the provider section. If you want the provider to search the whole directory specified by the URL in the provider section, delete the entire `<url></url>` section that is in the `<group>` section. Do not leave the `<url></url>` tags empty, without a value.

For example, if groups for the LDAP or Active Directory provider are stored in an organizational unit directory named Groups, the following sample is correct:

```
<group>
  <url>ou=Groups</url>
</group>
```

9 **Save the `css_config.xml` file.**

Optional Configuration for LDAP or Active Directory

The following XML elements represent the complete configuration that can be specified for LDAP or Active Directory (MSAD).

```
<ldap name="ldapServer">
        <trusted>true</trusted>
        <url>ldap://host:portNo/DIT</url>
        <userDN>cn=User Name</userDN>
        <password>userPassword</password>
        <authType>simple</authType>
        <authProtocol>ssl</authProtocol>
     <maxSize>200</maxSize>
        <identityAttribute>dn</identityAttribute>
        <user>
                <url>ou=people</url>
                <loginAttribute>uid</loginAttribute>
          <fnAttribute>givenname</fnAttribute>
                <snAttribute>sn</snAttribute>
                <emailAttribute>mail</emailAttribute>
            <objectclass>
                        <entry>person</entry>
                        <entry>organizationalPerson</entry>
                        <entry>inetOrgPerson</entry>
                </objectclass>
        </user>
        <group>
                <url>ou=Groups</url>
                <nameAttribute>cn</nameAttribute>
                <objectclass>

<entry>groupofuniquenames?uniquemember</entry>
                        <entry>groupOfNames?member</entry>
                </objectclass>
        </group>
</ldap>
```

To complete optional configuration for LDAP or Active Directory:

1. **In a text editor, open** `css_config.xml`.

2. **Between the** `<maxSize></maxSize>` **tags in the section for the LDAP or Active Directory provider, replace the sample value with the desired maximum number of entries that can be returned in a query.**

   If the `<maxSize></maxSize>` tags and their sample value are deleted from `css_config.xml`, the default value is `100`.

   If the Authentication System is configured to automatically import users, then the maxSize must be set to 0 (or the largest number of users or groups in the system).

If the Authentication System is configured to automatically import users, then the maxSize must be set to 0 (or the largest number of users or groups in the system). To allow return of the entire set of entries fetched by a search query, you can set the value to `0` to indicate an unlimited allowed result size. This may not be advisable, because on very large query results, it might consume too much memory.

3 **Between the `<authProtocol></authProtocol>` tags, indicate the value that corresponds to any additional security protocol you are using for secure data transmission to and from the authentication provider.**

The only valid value for the `<authProtocol></authProtocol>` tags in this release is `ssl`. If you are not using Secure Sockets Layer, delete the `<authProtocol></authProtocol>` tags, and their sample value, from `css_config.xml`.

If you are using Secure Sockets Layer (SSL), also complete the following tasks:

- On the directory server, ensure that a certificate is installed and available.
- On the Java Virtual Machine that runs your application, create a certificate database if one does not exist.
- On the Java Virtual Machine that runs your application, trust the Certificate Authority (CA) that issues the server certificate.

The security platform uses the LDAP service provider from SUN to authenticate users stored externally in an LDAP-compatible directory such as Novell eDirectory, Sun™ Open Net Environment (Sun ONE) (formerly iPlanet), or Microsoft Active Directory. The LDAP service provider runs on the Java Virtual Machine for your application. When SSL is used as the secure medium to connect to the directory server, the LDAP service provider of the security platform uses Java Secure Socket Extension (JSSE) software for its SSL support.

For more information about setting up SSL, please see the documentation for your directory server and/or JRE.

4 **Between the `<authType></authType>` tags, use the value `simple`. If the `<authType></authType>` tags are omitted from `css_config.xml`, the default value is `simple`. Only the simple authentication type is supported for this release.**

5 **Between the `<identityAttribute></identityAttribute>` tags, modify the sample value to match an attribute in the directory that uniquely identifies entries.**

The attribute may be the DN, or a customized attribute such as `employee_ID`, or any other attribute commonly used in the directory nodes of users and groups. If the `<identityAttribute>` section is deleted, the default value is `dn`.

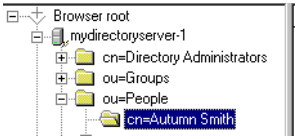
6 **Between the `<loginAttribute></loginAttribute>` tags within the `<user>` section, modify the sample value to match an attribute in the directory that uniquely identifies user entries.**

The attribute may be part of the DN, such as `cn` or `uid`, or a customized attribute, such as `employee_ID`, or any other attribute commonly used in the directory nodes of users. If the `<loginAttribute>` section is deleted, the default value is `cn`.

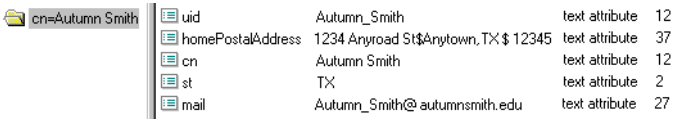
The following sample configuration states that the user names in which we are interested are using the "common name" attribute:

```
<loginAttribute>cn</loginAttribute>
```

The sample above is correct if it is true that all user names are identified by `cn = UserName`, as is Autumn Smith in the following LDAP browser view of a corporate directory store:



The above example highlights a subset of the DN. However, the `loginAttribute` property can instead refer to an attribute under the directory node for the user; for example, `loginAttribute` can point to `uid`, as shown in the following entry detail:



7 **Between the `<fnAttribute></fnAttribute>` tags within the <user> section, replace the sample value to match the attribute associated with first-name entries in the directory. If the `<fnAttribute> </fnAttribute>` tags and their contents are deleted, the default value for the first-name attribute is `givenname`.**

8 **Between the `<snAttribute></snAttribute>` tags within the <user> section, replace the sample value to match the attribute associated with last-name entries in the LDAP directory. If the `<snAttribute> </snAttribute>` tags and their contents are deleted, the default value for the last-name attribute is `sn`.**

9 **In the `<objectclass>` section within the <user> section, you may add `<entry></entry>` tags and values if your corporate directory schema requires specialized object classes to describe users, and those object classes are not present in the existing entries.**

The provided (default) user object classes for LDAP are `person`, `organizationalPerson`, and `inetOrgPerson`.

The provided (default) user object classes for Active Directory are `person`, `organizationalPerson`, and `user`.

10 **Between the `<nameAttribute></nameAttribute>` tags within the <group> section, replace the sample value of `cn` to point to an attribute in the corporate directory through which a group entry can be discovered. The default value is `cn` if the `<nameAttribute>` section is deleted.**

The following sample states that the group names containing the relevant user entries are using the Common Name attribute:

```
<nameAttribute>cn</nameAttribute>
```

In the `<objectclass>` section within the <group> section, you may add `<entry></entry>` tags and values if your corporate directory schema requires specialized object classes to describe groups, and those object classes are not present in the existing entries.

The provided (default) group object classes for LDAP are `groupofuniquenames?uniquemember` and `groupOfNames?member`.

The provided (default) group object class for Active Directory is `group?member`.

For additional entries you make, the `<entry>` tag values must be of the format `ObjectClassName?AttributeName`

For example:

```
<entry>group?member</entry>
```

where `group` is the name of the objectClass and `member` is the attribute that holds the distinguished Name of the member of this group.

11 **Save the `css_config.xml` file.**

Configuring an NTLM Provider

The instructions in this section show how to modify the properties that apply to configuring the provider implementations for Windows NT LAN Manager (NTLM), if your application supports an NTLM provider.

Basic Configuration for NTLM

To complete basic configuration for NTLM,

1. **In a text editor, open** `css_config.xml`.
2. **Locate the following section of** `css_config.xml` **(or, the entire section including and between the tags** `<ntlm name="ntlmServer">` **and** `</ntlm>`**:**

```
<ntlm name="ntlmServer">
  <trusted>false</trusted>
  <domain>THIS_IS_DOMAIN_NAME</domain>
</ntlm>
```

3. **In the first line of the above section, change** `ntlmServer` **to the desired name to indicate the configuration for this NTLM provider.**

   The name must be the same as the name you specified in the search order section, in Step 5 on page 6-11.

4. **Between the** `<trusted></trusted>` **tags, leave the default value of** `true`**, or replace the value with** `false` **if this is not a trusted NTLM provider.**

   - If the trust setting is `true`, a password is not present or required in the token generated upon user authentication. The user still must log in with a user name and password, but the password is not stored in the token.
   - If the trust setting is `false`, a password is part of the token, and this is required for this NTLM provider.

Note If your corporation uses a security agent such as Netegrity SiteMinder to protect company Web resources, the provider must be trusted. For more information, see "Configuring for SiteMinder Single Sign-On" on page 6-21.

5. **Between the** `<domain></domain>` **tags, replace** `THIS_IS_DOMAIN_NAME` **with the correct name of the Windows domain.**

If a domain is specified, then the NTLM provider is responsible for performing operations on that domain. Alternatively, if the domain element is left empty (for example, `<domain></domain>`), then the NTLM provider performs operations on all the trusted domains.

6 **Save the `css_config.xml` file.**

Optional Configuration for NTLM

The following XML elements represent the complete configuration that can be specified for NT LAN Manager.

The **`bold`** elements are the optional configuration parameters explained in this section. The other parameters are explained in "Basic Configuration for NTLM" on page 6-19.

```
<ntlm name="ntlmServer">
     <trusted>false</trusted>
     <domain>DOMAIN_NAME</domain>
     <maxSize>300</maxSize>
     <remoteServer>
          <location>//host:1099/NTLMImpl</location>
     </remoteServer>
</ntlm>
```

To complete optional configuration for NTLM:

1 **In a text editor, open `css_config.xml`.**

2 **Between the `<maxSize></maxSize>` tags in the section for the NTLM provider, replace the sample value with the desired maximum number of entries that can be returned in a query.**

The default value is `100` if the `<maxSize></maxSize>` tags and their content are deleted from `css_config.xml`.

If the Authentication System is configured to automatically import users, then the maxSize must be set to 0 (or the largest number of users or groups in the system).

To allow return of the entire set of entries fetched by a search query, you can set the value to `0` to indicate an unlimited allowed result size. This may not be advisable, because on very large query results, it might consume too much memory.

3 **Between the `<location></location>` tags that are within the `<remoteServer></remoteServer>` tags,**

- If you support Hyperion applications only on Windows platforms, delete the content of these tags, as their configuration applies only to support for UNIX clients accessing information stored in an NTLM provider.
- If you support external authentication using NTLM for Hyperion applications that run on UNIX, replace the sample content of the `<location></location>` tags with the correct URL of the remote NTLM Provider. You must have installed the NTLM Remote Server as indicated in *UNIX Application support for NT LAN Manager*.

4 **Save the `css_config.xml` file.**

Configuring for SiteMinder Single Sign-On

To enable single sign-on to web-based Hyperion applications through the security agent when your corporate information is protected by Netegrity Siteminder:

1 **Make sure that the authentication repository containing user and group information is trusted.**

If your corporation uses a security agent to protect company Web resources, the authentication repository (for example, LDAP, Microsoft Active Directory, or NT LAN Manager) must be trusted, because the Hyperion security platform does not store a password in the token when a security agent is used.

2 **In a text editor, open `sample.xml`.**

3 **Add `<securityAgent name="NETEGRITY"/>` to the end of the configuration file, after the `<logger></logger>` section but before the line containing `</css>`**

```
    <logger>
      <priority>FATAL</priority>
    </logger>
    <securityAgent name="NETEGRITY"/>
  </css>
```

Note The security agent configuration is applicable only to web-based Hyperion applications.

4 **Save the `sample.xml` file.**

5 **Set the usename macro in the Servlet Configurator to `$SECURITY_AGENT$`.**

For more information on how to configure the username macro, see "Custom Policies and Macros" on page 5-16 and "User Interface Properties" on page 11-5.

Additionally, the SiteMinder administrator must set up protection for the appropriate Hyperion application's web resources. These resources could be HTML files, JSP files, ASP files, or other web-based resource files.

To do this, the SiteMinder administrator needs to configure a "response" that would enable a HTTP header to be added by SiteMinder. This HTTP header carries the login name of the user and makes the login name available to the web resources (the Hyperion application's resources, in this case). The header must be configured in the response to have the name `HYPLOGIN`, and the value should be configured to be the login name of the authenticated user. For example, if you are using an LDAP directory and `cn` is the login name attribute configured in the security platform XML configuration file, then the `HYPLOGIN` header should carry the `cn` value corresponding to the authenticated user in the LDAP directory. The administrator can configure the header to `SM_USERLOGINNAME`, an attribute that holds the user ID as specified by the user in the login attempt. For more details, please refer to the "Responses and Response Groups" section of the Netegrity Policy Design Guide.

Sample Deployment Scenarios

This section contains the following deployment scenarios as examples:

- Scenario 1: Single LDAP Directory
- Scenario 2: Single Microsoft Active Directory
- Scenario 3: UNIX Application and Single NTLM Domain
- Scenario 4: Windows Application and Single NTLM Domain
- Scenario 5: UNIX Application Against LDAP, Microsoft Active Directory, and NTLM
- Scenario 6: Windows Application Against LDAP, Microsoft Active Directory, and NTLM
- Scenario 7: Multiple Microsoft Active Directory Instances

- Scenario 8: Multiple LDAP Directory Instances
- Scenario 9: Multiple NTLM Domains
- Scenario 10: Multiple NTLM Domains Connected with Hyperion Remote Authentication Module
- Scenario 11: Single Sign-on with SiteMinder
- Deployment References from LDAP Product Vendors

Scenario 1: Single LDAP Directory

Figure 6-2 illustrates a deployment scenario that uses LDAP.

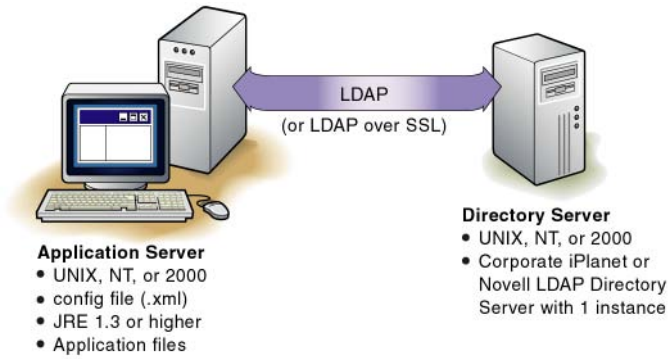


Figure 6-2 Authentication Against a Single Instance of an LDAP Directory

The configuration file is by default installed in *INSTALL_HOME*\BrioPlatform\etc and is used by the AuthenticationService to determine which directory server(s) to access. The directory server can reside on the same machine either locally or remotely.

A secure SSL connection can optionally be used.

In the single LDAP directory scenario,

- All users must have the same prefix, such as `cn` or `uid`.
- All groups must have the same prefix, such as `cn` or `ou`.
- Referrals are not supported.
- Users and groups should exist under nodes, such as `ou=People` and `ou=Groups`, for optimal data-retrieval performance.

Figure 6-3 shows a sample corporate directory schema.

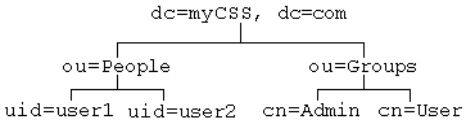


Figure 6-3 Sample Corporate Directory Schema

Scenario 2: Single Microsoft Active Directory

Figure 6-4 illustrates a deployment scenario that uses Microsoft Active Directory.

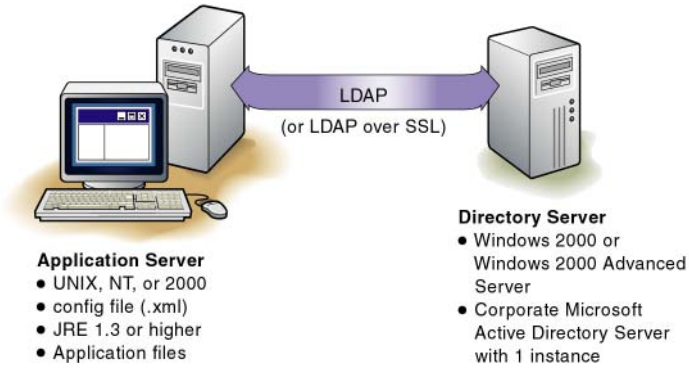


Figure 6-4 Authentication Against a Single Instance of Microsoft Active Directory

The configuration file is by default installed in *INSTALL_HOME*\BrioPlatform\etc and is used by the AuthenticationService to determine which directory server(s) to access. The directory server can reside on the same machine either locally or remotely.

A secure SSL connection can optionally be used.

In the single Microsoft Active Directory scenario,

- All users must have the same prefix, such as `cn` or `uid`.
- All groups must have the same prefix, such as `cn` or `ou`.
- Referrals are not supported.
- Users and groups should exist under nodes, such as `cn=Users`, for optimal data-retrieval performance.

Figure 6-5 shows a sample corporate directory schema.

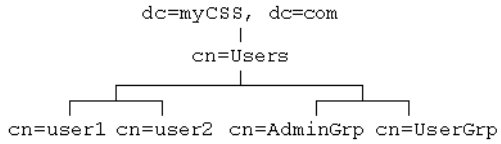


Figure 6-5 Sample Corporate Directory Schema

Scenario 3: UNIX Application and Single NTLM Domain

Figure 6-6 illustrates a deployment scenario in which a UNIX-based application accesses information from a Windows NT LAN Manager domain controller. This implementation depends also on the NTLM remote server that is configured and running on a Windows NT or 2000 machine. The Remote Authentication Module can be installed from the Hyperion Download Center. The Remote Authentication Module is needed because the external authentication mechanism depends on the NTLM support library file `(.dll)` for NTLM authentication, and dlls are not supported on UNIX.

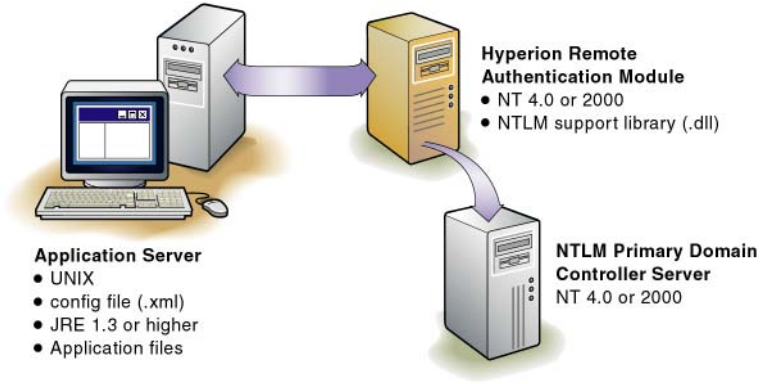


Figure 6-6 Authentication from a UNIX-Based Application Server Against a Single Instance of NTLM

Note The NTLM remote server enables communication between NTLM and a UNIX-based application. Install the NTLM remote server from the Hyperion application's installation software.

The configuration file is by default installed in *INSTALL_HOME*\BrioPlatform\etc and is used by the AuthenticationService to determine which directory server(s) to access. The NTLM support library file `(.dll)` file is also required, for the NTLM connectivity. The configuration for external authentication should be done as described in the rest of this document. The NTLM server can be on a Windows NT 4.0 server or a Windows 2000 server that has backward-compatibility to NT 4.0. The NTLM remote server should be on Windows NT 4.0 server or Windows 2000 server. Combining the NTLM remote server with the NTLM Primary Domain Controller is not recommended. The NTLM remote server machine needs to be in the same domain as the NTLM Primary Domain Controller.

Scenario 4: Windows Application and Single NTLM Domain

Figure 6-7 illustrates a deployment scenario in which a Windows-based application accesses information from a Windows NT LAN Manager domain controller.

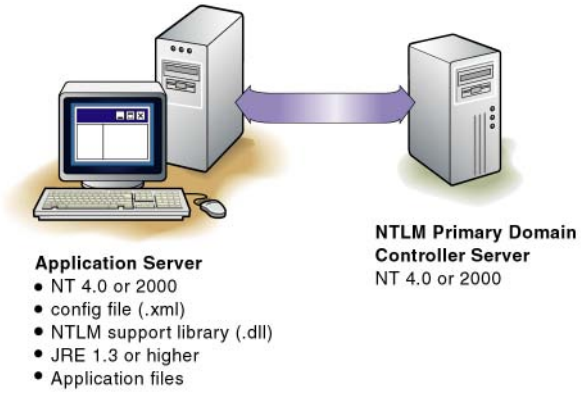


Figure 6-7 Authentication from a Windows-Based Application Server Against a Single Instance of NTLM

The configuration file is by default installed in *INSTALL_HOME*\BrioPlatform\etc and is used by the AuthenticationService to determine which directory server(s) to access. The NTLM support library file `(.dll)` file is also required, for the NTLM connectivity. The configuration for external authentication should be done as described in the rest of this

document. The NTLM Primary Domain Controller can be on a Windows NT 4.0 server or a Windows 2000 server that has backward-compatibility to NT 4.0.

Scenario 5: UNIX Application Against LDAP, Microsoft Active Directory, and NTLM

Figure 6-8 illustrates a deployment scenario in which a UNIX-based application accesses information from multiple directory stores. The NTLM remote server is required for access to the Windows NT LAN Manager domain, as in Scenario 3. Configuration of the search order becomes important in this scenario.

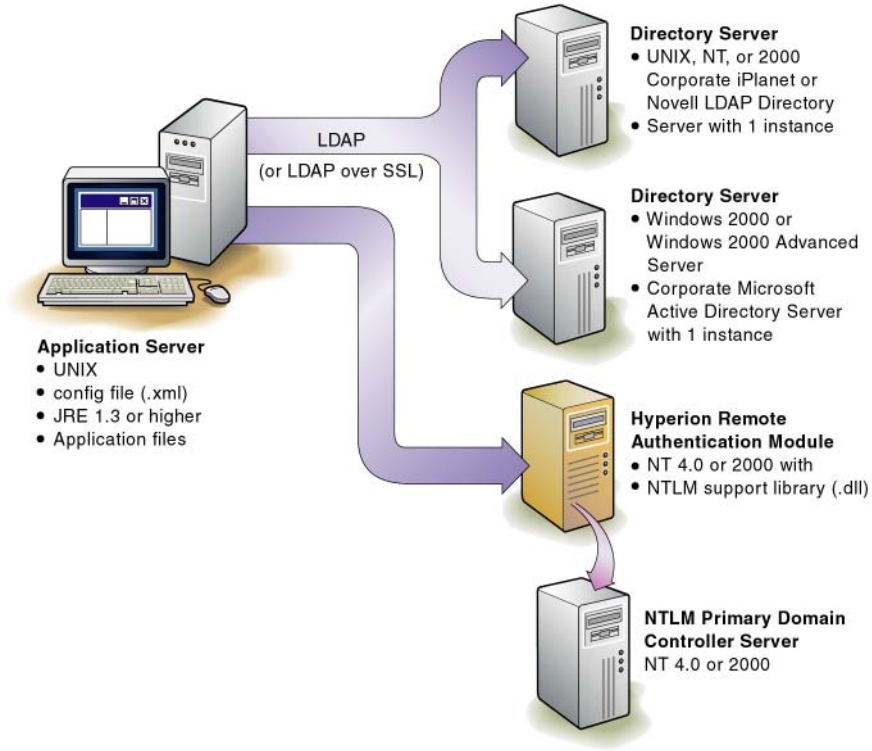


Figure 6-8 Authentication from a UNIX-Based Application Server Against an LDAP Directory, Microsoft Active Directory, and NTLM

Note The NTLM remote server enables communication between NTLM and a UNIX-based application. Install the NTLM remote server from the Hyperion application's installation software.

The configuration file is by default installed in *INSTALL_HOME*\BrioPlatform\etc and is used by the AuthenticationService to determine which directory server(s) to access. The NTLM support library file `(.dll)` file is also required, for the NTLM connectivity. The configuration for external authentication should be done as described in the rest of this document. The NTLM Primary Domain Controller server can be on a Windows NT 4.0 Server or a Windows 2000 server that has backward-compatibility to NT 4.0. The NTLM remote server machine needs to be in the same domain as the NTLM Primary Domain Controller.

For LDAP-compatible directories, a secure SSL connection can optionally be used.

The configuration of the search order property in the `.xml` configuration file determines the order in which each directory store receives requests for information from the application. For example, the first instance of a requested user found while going through the search order is the instance that is used to retrieve and return information about the user to the application. Therefore, although there are three directories that can host user information, it is recommended that user information not be duplicated across the directories. Duplication can lead to the incorrect user object being authenticated.

For information about configuring the search order, see "Configuring the Provider Search Order" on page 6-10.

Scenario 6: Windows Application Against LDAP, Microsoft Active Directory, and NTLM

Figure 6-9 illustrates a deployment scenario in which a Windows-based application accesses information from multiple directory stores.

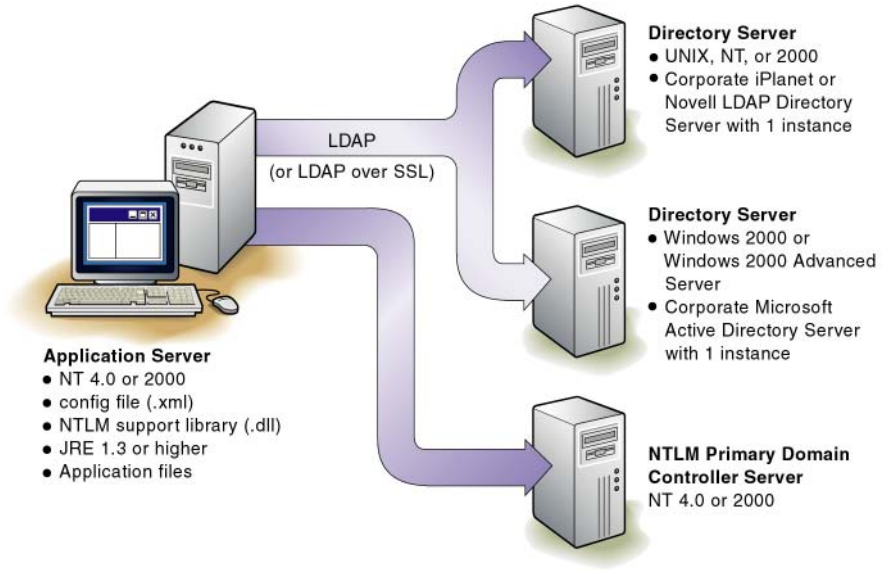


Figure 6-9 Authentication from a Windows-Based Application Server Against an LDAP Directory, Microsoft Active Directory, and NTLM

The configuration file is by default installed in *INSTALL_HOME*\BrioPlatform\etc and is used by the AuthenticationService to determine which directory server(s) to access. The NTLM support library file `(.dll)` file is also required, for the NTLM connectivity. The configuration for external authentication should be done as described in the rest of this document. The NTLM Primary Domain Controller can be on a Windows NT 4.0 server or a Windows 2000 server that has backward-compatibility to NT 4.0.

For LDAP-compatible directories, a secure SSL connection can optionally be used.

The configuration of the search order property in the XML configuration file determines the order in which each directory store receives requests for information from the application. For example, the first instance of a requested user found while going through the search order is the instance that is used by the external authentication mechanism to retrieve and return information about the user to the application. Therefore, although there are three directories that can host user information, it is recommended that user information not be duplicated across the directories. Duplication can lead to the incorrect user object being authenticated.

For information about configuring the search order, see "Configuring the Provider Search Order" on page 6-10.

Scenario 7: Multiple Microsoft Active Directory Instances

When there are multiple Microsoft Active Directory instances which hold user authentication information, you must create a single instance of Active Directory which hosts all the user information. Enabling a single instance to use for external authentication is left to the individual installation. One solution is to enable replication between the instances to the master directory server, as shown in Figure 6-10.

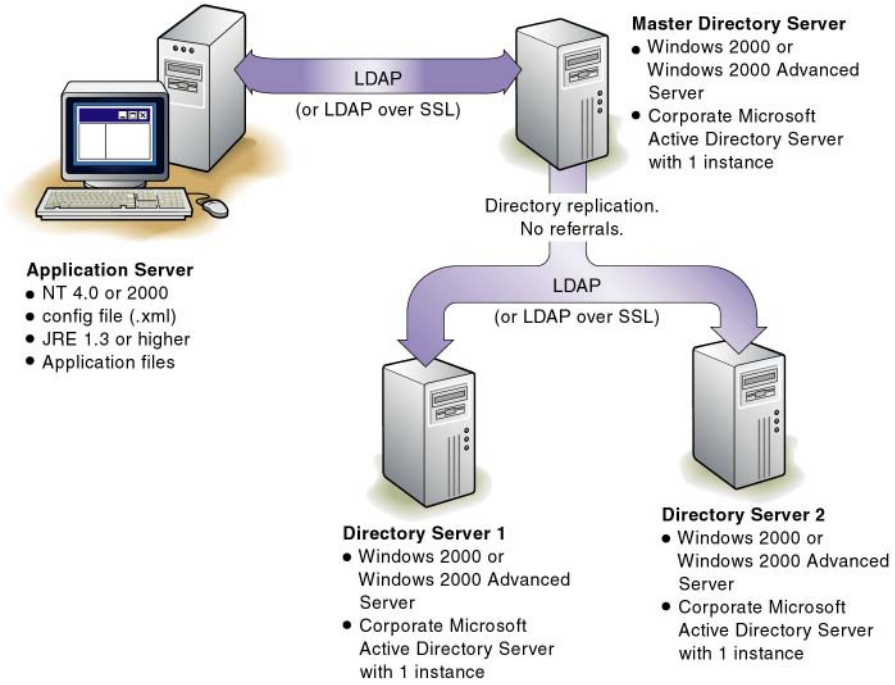


Figure 6-10 Authentication with Multiple Microsoft Active Directory Instances

The configuration file is by default installed in *INSTALL_HOME*\BrioPlatform\etc and is used by the AuthenticationService to determine which directory server(s) to access. The configuration for external authentication should be done as described in the rest of this document.

A secure SSL connection can optionally be used.

Scenario 8: Multiple LDAP Directory Instances

When there are multiple LDAP directory instances which hold user authentication information, you must create a single instance of LDAP which hosts all the user information. Enabling a single instance to use for external authentication is left to the individual installation. One solution is to enable replication between the instances to the master directory server, as shown in Figure 6-11.

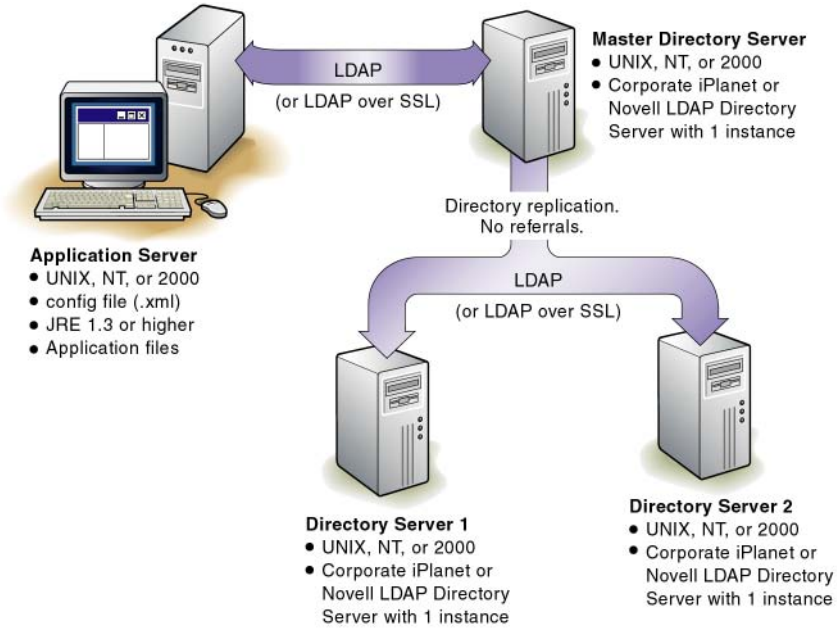


Figure 6-11 Authentication with Multiple LDAP Directory Instances

The configuration file is by default installed in *INSTALL_HOME*\BrioPlatform\etc and is used by the AuthenticationService to determine which directory server(s) to access. The configuration for external authentication should be done as described in the rest of this document.

Scenario 9: Multiple NTLM Domains

When there are multiple Windows NT LAN Manager domains which hold user authentication information, you must create a single domain which hosts all the user information. Enabling a single domain to use for external authentication is left to the individual installation. One solution is to establish trust relationships between the domains, as shown in Figure 6-12.

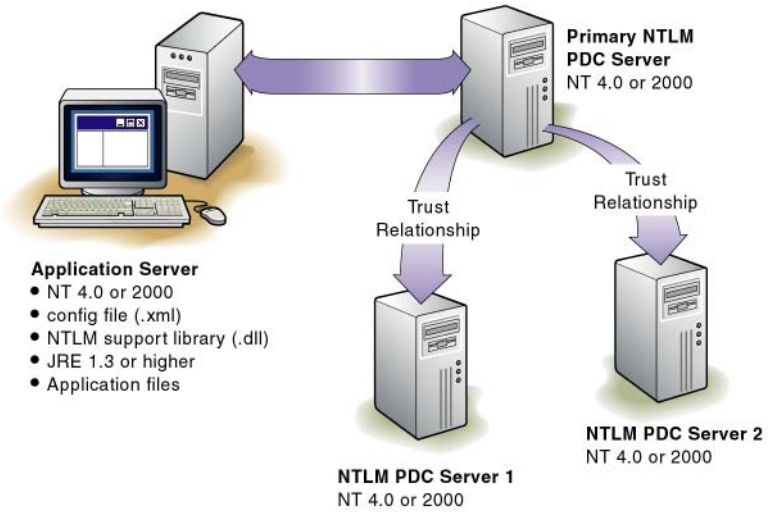


Figure 6-12 Authentication with Multiple NTLM Domains

The configuration file is by default installed in *INSTALL_HOME*\BrioPlatform\etc and is used by the AuthenticationService to determine which directory server(s) to access. The NTLM support library file `(.dll)` file is also required, for the NTLM connectivity. The configuration for external authentication should be done as described in the rest of this document. The NTLM Primary Domain Controllers can be on Windows NT 4.0 servers or Windows 2000 servers that have backward-compatibility to NT 4.0.

Scenario 10: Multiple NTLM Domains Connected with Hyperion Remote Authentication Module

When there are multiple Windows NT LAN Manager domains which hold user authentication information, an additional solution is to link the domains using the Hyperion Remote Authentication Module (compare to "Scenario 9:

Multiple NTLM Domains" on page 6-32). This scenario eliminates the necessity of establishing trust relationships between the domains, as shown in Figure 6-13.

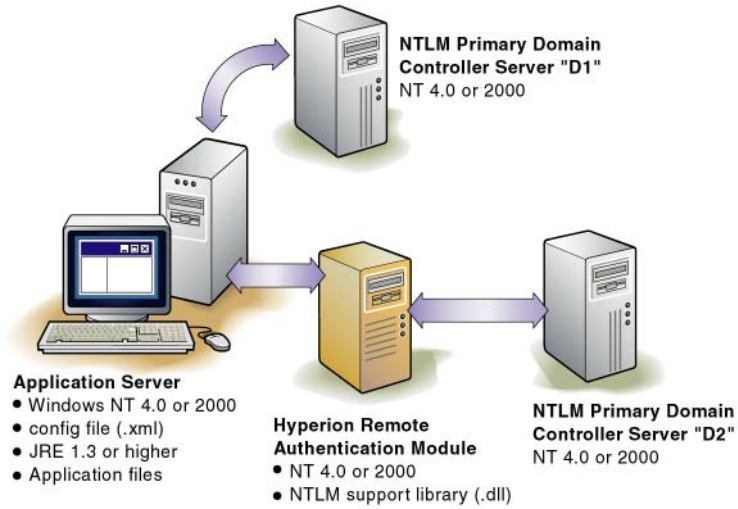


Figure 6-13 Authentication with Multiple Untrusted NTLM Domains

The Hyperion Remote Authentication Module gives users of Hyperion applications on Windows the ability to log in using multiple domains, without the need for the administrator to create trust relationships between the domains. In the figure above, Windows users may optionally log in using domain "D2" in addition to the more commonly used domain "D1," because the Hyperion Remote Authentication Module is running, giving access to domain "D2." Note that D1 does not trust D2.

The configuration file is by default installed in *INSTALL_HOME*\BrioPlatform\etc and is used by the AuthenticationService to determine which directory server(s) to access. The NTLM support library file `(.dll)` file is also required, for the NTLM connectivity. The configuration for external authentication should be done as described in the rest of this document. The NTLM Primary Domain Controllers can be on Windows NT 4.0 servers or Windows 2000 servers.

The security platform can communicate over a secure medium such as Secure Sockets Layer (SSL) with the Hyperion Remote Authentication Module. If you need to use SSL, select the SSL option when installing the Hyperion Remote

Authentication Module. For complete installation instructions, download and read the installation and setup instructions provided with the Hyperion Remote Authentication Module on the Hyperion Download Center.

Scenario 11: Single Sign-on with SiteMinder

SiteMinder is a Web access management solutions provider sometimes employed by companies to manage and enforce authentication, authorization, and single sign-on for company Web resources. The Hyperion security platform enables single sign-on for a user into a Web-based Hyperion application without challenging the user for credentials, as long as SiteMinder has already authenticated the user. Integration with SiteMinder requires configuration of the `<securityAgent></securityAgent>` element in the XML configuration file.

Note If your corporation uses a security agent to protect company Web resources, the corporate authentication repository (for example, LDAP, Microsoft Active Directory, or NT LAN Manager) must be trusted, because the Hyperion security platform does not store a password in the token when a security agent is used.

Figure 6-14 illustrates a scenario enabling single sign-on with SiteMinder and a Hyperion application using the Hyperion security platform:

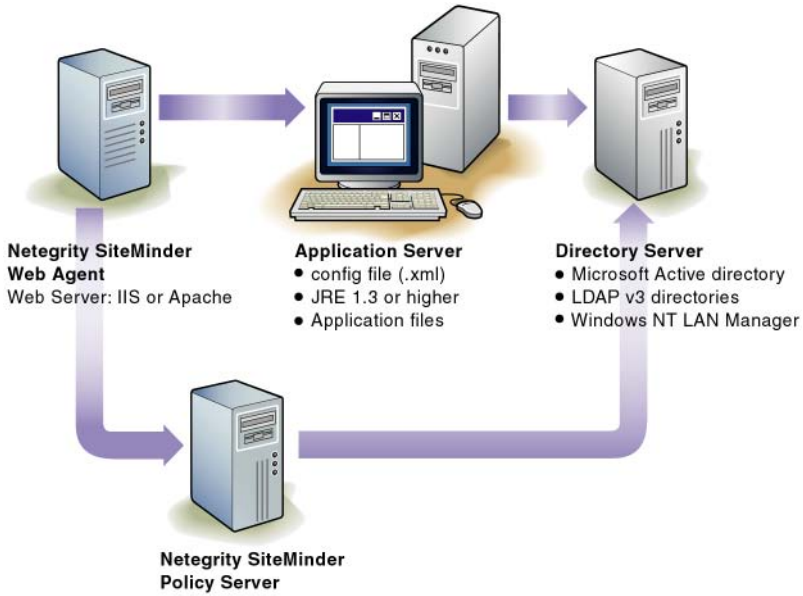


Figure 6-14 Single Sign-on with Siteminder as the Security Agent

The Hyperion application trusts the authentication and authorization information sent by SiteMinder with regards to the protected resources on the directory server. Therefore, the Hyperion security platform supports Tier 1 integration with SiteMinder.

The Web agent is installed on a Web server that intercepts requests for the Hyperion application's Web resources, such as JSP files, ASP files, or HTML files on the application server. If these web resources are protected, the Web agent issues a challenge for unauthenticated users. Once the user is authenticated, the policy server adds to the HTTP headers another header, named `HYPLOGIN`, whose value is the login name of the authenticated user. Thereafter, the HTTP request is passed on to the Hyperion application's Web resources, and the login name is extracted from the headers. For more details on configuring the header `HYPLOGIN` and populating it, see "Configuring for SiteMinder Single Sign-On" on page 6-21.

Deployment References from LDAP Product Vendors

iPlanet Directory Deployment Guide for v5.1:

`http://192.18.99.138/816-5609-10/816-5609-10.pdf`

iPlanet Directory Deployment Guide for v4.16:

http://192.18.99.138/816-6679-10/816-6679-10.pdf

Active Directory Deployment Guide:

http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/activedirectory/deploy/default.mspx

About Related Content and Hyperion Hub

Related content is reports and views that can be shared by Hyperion applications. Related content from Hyperion Analyzer and Hyperion Reports can be accessed through the browse module of Hyperion Performance Suite. Conversely content in Hyperion Performance Suite can be accessed through Hyperion Analyzer and Hyperion Reports. For more information on related content, see "Viewing Related Content" in the *Hyperion Performance Suite Foundation User's Guide*.

Hyperion Hub is a central application which provides a business metadata repository for Hyperion applications and tools. Registering to Hyperion Hub provides integration between Hyperion applications. Currently Hyperion Performance Suite supports accessing content and being accessed from Hyperion Analyzer and Hyperion Reports

Administrating Related Content

As the administrator, you can configure Hyperion Performance Suite to provide related content for your users. Depending upon your needs, you can configure Hyperion Performance Suite to access content from registered Hyperion Analyzer and Hyperion Reports with or without allowing those applications access to content from Hyperion Performance Suite.

To configure Hyperion Performance Suite for related content:

1. **Configure users with the same authentication system using the security platform driver. See "Configuring the Security Platform Driver" on page 6-9.**

2. **Log on using a username authenticated with the security platform driver that has the administrator role.**

   Administrators that set-up and implement Related Content need access to a username authenticated with the security platform driver.

3. **Register with Hyperion Hub or set up a property file to use as a local registry.**

   See "Registering Hyperion Performance Suite to Hyperion Hub" on page 10-40 or "Using a Property File as a Local Registry" on page 6-38.

4. **Be sure all users involved have the related content viewer role.**

   The related content viewer role is included by default in the user role which is automatically given to every user.

Note If Hyperion Hub registration changes, you need to restart your application server.

Using a Property File as a Local Registry

Use this method to share content with other Hyperion applications when Hyperion Hub is not working.

To register using a property file:

1. **Navigate to the file,** `RelatedContents.properties`.

   Install_Home`\servlets\deployment\config\RelatedContents.properties`

2. **Set useHubregistry to false.**

   True is the default.

3. **Define the Related Content applications. Use the correct format , as shown in the file, for each Hyperion application.**

```
Hyperion Reports:
|HR|instance_name_1|http://server1:port/HReports/HRRepositoryXM
L.jsp?sso_token=$SSO_TOKEN$
Hyperion Analyzer:
|Analyzer|instance_name_2|http://server2:port/Analyzer7_Server/
DirectoryServlet?sso_token=$SSO_TOKEN$
```

Set Other Related Content Properties

The `RelatedContents.properties` file contains two other properties. The file is located at *Install_Home*`\servlets\deployment\config\RelatedContents.properties`.

The alias property provides a way to change the name of the host machine stored in Hyperion Hub. This property can be changed when you switch your Hyperion Performance Suite from one server to another.

```
# You can define aliases for related content applications here.
# The format will be
# alias.alias_name_1=http://server1:port1
# alias.alias_name_2=http://server2:port2
```

The performance tuning parameters allow you to change the cache size and cache time to live per Hyperion Performance Suite system. For the new values to take effect you must restart the servlets. The defaults are shown below.

```
#Performance Tuning Parameters
# size of the cache is max number of related content folders
that can be cached.
# TTL is the time to live in seconds for each related content
folder before it is fetched again.
# This cache is created for each user. If you change these
values, you will have to restart the servlets.
cache.size=10
cache.TTL=500
```

Summary

This chapter showed how to configure single sign-on using the security platform driver and related content.

PART III

Content

7 Administering Content

This chapter covers the administrative tasks associated with system content, the items and folders stored in the Repository.

In This Chapter

Organizing Items and Folders 7-2

Working with MIME Types 7-2

Administrating Pushed Content 7-5

Administering Personal Pages 7-6

Organizing Items and Folders

For efficient functioning of Hyperion Foundation, structure your folders so users can access items quickly and easily. Within your folder hierarchy, balance folder size against hierarchy depth. Do not let folders contain huge numbers of items, nor let the number of levels in the folder hierarchy become excessive.

Note If you frequently publish content into your Hyperion Foundation system, run a virus scan regularly on the root folder.

A hidden folder named *System* is designed for the administrator's use. It is visible only to administrators, and only when hidden items are revealed. Use *System* to store files you do not want users to see, such as the icon files for MIME types. You cannot rename, delete, or move the System folder.

Working with MIME Types

In order for an item to be published to the Repository, its *MIME type* must be defined in Hyperion Foundation. Although Hyperion Foundation has many built-in MIME types, you may need to create additional ones for your users. You can delete MIME types that you create, but not built-in MIME types.

You can associate a MIME type with more than one extension. For example, you can associate the extensions `.txt`, `.bat`, and `.dat` with the *text* type.

Different MIME types can have the same extension. For example, if your organization uses multiple versions of the same program, you may wish to define a MIME type for each version, though files of all versions use the same extension. When a user opens a file whose extension belongs to multiple MIME types, a dialog prompts the user to specify the program executable with which to open the file.

You manage MIME types in the Administration servlet, from the System tab. In the listing of MIME types, each type has a traffic-light icon that is either green (active) or red (inactive).

Creating a MIME Type

To create (define) a MIME type:

1. **In Administrator, select the System tab.**
2. **Select Add MIME Type in the navigation pane.**
3. **Fill in the properties for the MIME Type.**

   The Name, Description, and File Extensions fields are mandatory.

   To assign file extensions to the MIME type, type an extension in the lefthand box and choose **>>** to add it to the box on the right. Repeat to assign multiple extensions.

   When entering an extension, do not include the preceding period (.) character.
4. **Choose Finish.**

Modifying a MIME Type

To modify a MIME type:

1. **In Administrator, select the System tab.**
2. **Select Manage MIME Types in the navigation pane.**
3. **In the listing of MIME types, choose the Modify Properties icon for the MIME type you wish to modify.**

   Alternatively, you can choose the name of the MIME type. The properties page appears.
4. **Change properties as desired.**

   To remove a file extension, select it in the *Extensions* box and choose **<<**.
5. **Choose OK.**

Inactivating or Re-activating a MIME Type

You can inactivate a MIME type so that new items of that MIME type cannot be published. Existing items of an inactive MIME type are still accessible. When a user opens such an item, a dialog appears that asks what program to use to open the item.

You can re-activate an inactive MIME type at any time.

To inactivate or re-activate a MIME type:

1. **In Administrator, select the System tab.**
2. **Select Manage MIME Types in the navigation pane.**
3. **In the listing of MIME types, choose the Modify Properties icon for the MIME type you wish to modify.**

   Alternatively, you can choose the name of the MIME type. The properties page appears.
4. **Change the setting of the Active check box as follows:**
   - To inactivate the MIME type, clear the **Active** check box, and then choose **OK**.

     In the listing, this MIME type now has a red traffic-light icon.
   - To re-activate the MIME type, select the **Active** check box again, and then choose **OK**.

     In the listing, this MIME type now has a green traffic-light icon.

Deleting a MIME Type

Unlike inactivation of a MIME type, deletion is permanent and affects existing items. You cannot publish files that have any of the extensions of a deleted MIME type.

For items of a deleted MIME type, instead of a MIME type icon, the text "unknown file type" displays. When a user opens such an item, a dialog appears that asks what program to use to open the item.

You can delete MIME types that you add; however, you cannot delete Hyperion Foundation MIME types.

To delete a MIME Type:

1. **In Administrator, choose the System tab.**
2. **Choose Manage MIME Types in the navigation pane.**
3. **Choose the Delete icon of the MIME type you wish to delete.**

Administrating Pushed Content

Each user's View Manager module can contain subscribed and pushed content. Subscribed content is added to a user's View Manager when the user subscribes to it. Pushed content is added to a user's View Manager when an administrator with the View Manager Content Pusher role pushes the content to the user. For example, Chris, the marketing manager, wants everyone in the marketing group to have easy access to the marketing schedule document. Chris (who has the View Manager Content Pusher role) publishes the schedule and pushes this item to the marketing group. Now members of the marketing group can view the schedule from the View Manager rather than having to navigate through the Browse module to the schedule document.

For specific instructions on how to push items, see the *Hyperion Foundation User Guide*.

Administering Personal Pages

As the administrator, you set up the generated Personal Page and content for users' Personal Pages. For information about using the Personal Pages, see the *Foundation User's Guide*. For details about the configuration properties of the Personal Pages servlet, see "Personal Pages Properties" on page 11-14.

Setting Up the Generated Personal Page

When a new user logs into Hyperion Performance Suite for the first time, the first page that appears is the *generated Personal Page*, see Figure 7-1. Hyperion Foundation automatically generates each new user's Personal Page at the time of the first login.

The page is then saved as part of the user's own Personal Pages. Changes the administrator makes for subsequent new users do not affect users who have already logged in once. Therefore, the exact content of a user's generated Personal Page depends on when that user first logs in.

After logging in for the first time, users modify their own Personal Pages. They can also create additional Personal Pages.

Due to users' different access privileges, the generated page may be quite different for different users. By carefully setting the access control on the files used for the generated page, you can arrange, for example, to have new users in the Sales department see entirely different content on the generated page than do new users in the Production department.

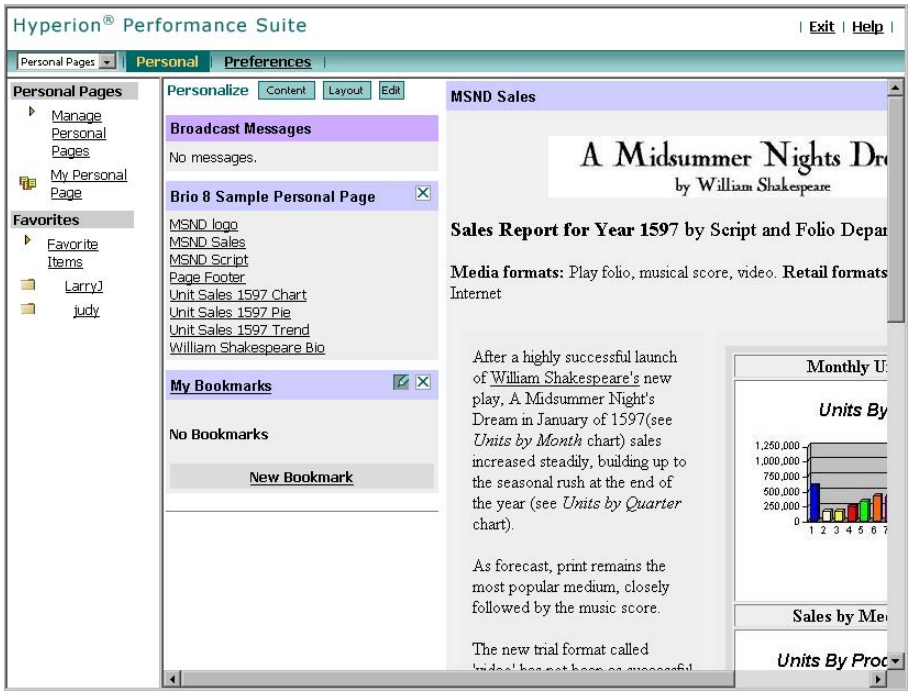


Figure 7-1 Generated Personal Page Example

The following are included on the generated Personal Page by default:

- One Broadcast Messages content window that displays links to all items in the Broadcast Messages folder.
- One Broadcast Messages file content window for each displayable item that resides in the Broadcast Messages folder.
- One content window for each of the first two pre-configured folders.
- The first (as sorted) displayable HTML item in any pre-configured folder.
- The My Bookmarks content window.
- The Exceptions Dashboard content window.

You can customize the preceding list by setting the Generated Personal Page properties in the Servlet Configurator. For details on the Generated Personal Page properties, see Table 11-15 on page 11-15.

To configure the generated Personal Page, you can do any or all of the following:

- Set the Generated Personal Page properties in the Servlet Configurator to include what you want.
- Populate the Broadcast Messages folder with any combination of nondisplayable items for which links display on the generated Personal Page, and displayable HTML files or external links, whose content displays there.

  All these items appear as links and together constitute one content window under the Broadcast Messages heading. Some of the displayable items may also appear as separate file content windows, depending on your configuration settings in the Generated Personal Page properties.
- In the Broadcast Messages folder, create pre-configured subfolders to appear when users log in for the first time. Populate these folders with displayable HTML items and/or nondisplayable items. For each pre-configured folder, a content window appears, containing links to all the items in the folder. Each displayable item also appears as a separate file content window.

Tip As with any content, only users who have the required access privileges can see items and folders in the Broadcast Messages folder and other pre-configured folders.

To tailor the generated page for particular groups, put folders and items intended for specific groups in the Broadcast Messages folder and the pre-configured folders, and assign access privileges to the target groups. For example, if each group has access to a different subset of the pre-configured folders, then users of each group see different content windows when they log in for the first time.

Understanding Broadcast Messages

The Broadcast Messages folder broadcasts messages to all the users in your system, except as restricted by the access privileges granted on the individual items it contains. Put announcements and documents for wide distribution in this folder.

The terms “Broadcast Messages content windows” and “Broadcast Messages” for short, refer only to the content of the Broadcast Messages folder itself, excluding the content of its subfolders (the pre-configured folders).

Broadcast Messages include:

- One content window that displays links to all items in the Broadcast Messages folder.
- An additional file content window for each displayable item that resides in the Broadcast Messages folder.

Unlike all other types of content windows, Broadcast Messages cannot be deleted from a user’s Personal Pages.

If a user makes another page their default Personal Page, the Broadcast Messages remain on the Personal Page that was originally generated. The user can delete the generated page only if the user has added the Broadcast Messages folder to another Personal Page. (A user can acquire multiple pages containing the Broadcast Messages by copying published Personal Pages.)

Setting Up Content for Broadcast Messages

The Broadcast Messages folder is your vehicle for customizing what users see according to enterprise or administration needs. By including content for various groups and setting the access control on each item or folder to ensure that only its intended group has access, you push specific content to a user’s browser.

Renaming Broadcast Messages Folders

When you rename the Broadcast Messages folder, the changed folder name appears in the title bar of the Broadcast Messages content window in the Browse module and on users' Personal Pages. The system property *Folder containing broadcast messages* changes automatically to reflect the new name. However, after renaming either the Broadcast Messages folder or its subfolder, *PersonalPage Content*, you must manually change another property, *Location*. The *Location* property is found in the Servlet Configurator, in the Personal Pages/Publish section (see Table 11-14 on page 11-15).

Providing Optional Personal Page Content to Users

Beyond what you set up for the generated Personal Page, you can also set up optional content for users to include on their Personal Pages.

All of the pre-configured folders are optional content for users and appear on the Content page for users to add to a Personal Page. A pre-configured folder displays on a Personal Page as a content window when a user adds it to a Personal Page, displaying links to the items it contains.

Publish all content to the pre-configured folders using the Browse web module. For information on how to publish content, see the *Foundation User's Guide*.

Displaying an HTML File as a File Content Window

Hyperion Foundation allows users to display HTML files on their Personal Pages as file content windows. This means that, rather than having a link to the file, the file's *contents* display on the Personal Page.

By default, the first displayable item in a pre-configured folder automatically displays as a file content window on each new user's generated Personal Page. As an administrator, you can ensure that users with the required access privileges see the content of additional HTML items by subscribing to the item.

See the *Foundation User's Guide* for more information on displaying HTML files as file content windows.

Setting Up Graphics for Bookmarks

To provide graphics that users can easily use for image bookmarks, place the pre-configured graphic files in the *wsmedia/personalize* folder in your servlets deployment directory.

You can also add customized image icon files for individual users upon request. Add these image files to the *wsmedia* folder or any other folder that is within the scope of the Context root (`/Hyperion`) and give the user a URL to point to that file, for example, `/wsmedia/sqr/vcr.gif`.

Note An icon will not display on Personal Pages if it has a DBCS filename or is in a DBCS directory.

Configuring Exceptions

To make an exceptions-capable job or file report exceptions, enable the Advanced Option *Allow users to add this file to the Exceptions Dashboard* when publishing through the Browse module.

For information on how users can add an exceptions-enabled job or file to their Exceptions Dashboard, see the *Foundation User's Guide*.

To give a job exceptions capability, you must design the job (usually, an SQR program) to write exceptions to the `output.properties` file. For more information, see the *Foundation User's Guide*.

For programmers' information about supporting exceptions in report programs, see the *Hyperion Foundation User's Guide*.

Example of Setting Up Content for Personal Pages

This section works through the following example:

Example

Using the Browse web module, an administrator sets up two pre-configured folders, William Shakespeare Sales and William Shakespeare's Life. In William Shakespeare Sales, the administrator sets up links to four items - two HTML files, one Word document, and one JPG file. The administrator, in this example started with the following Personal Page (Figure 7-2):

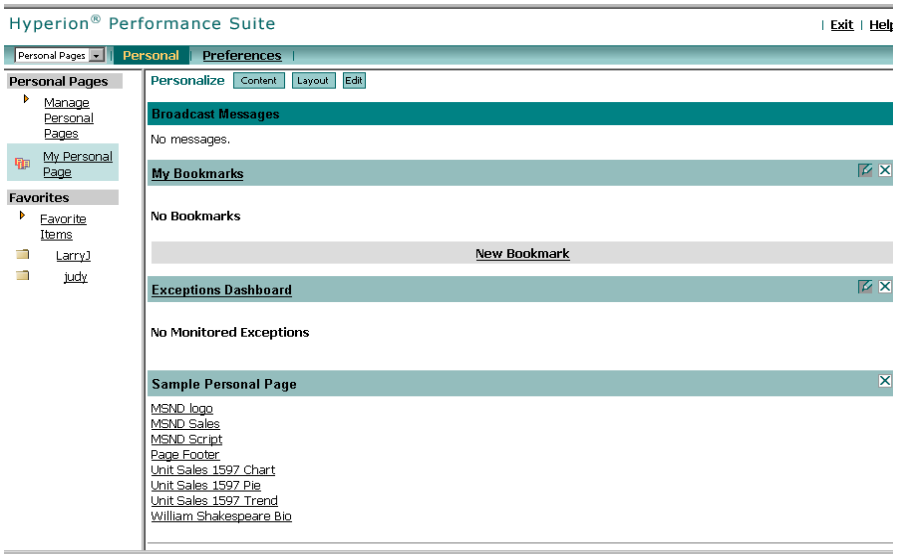


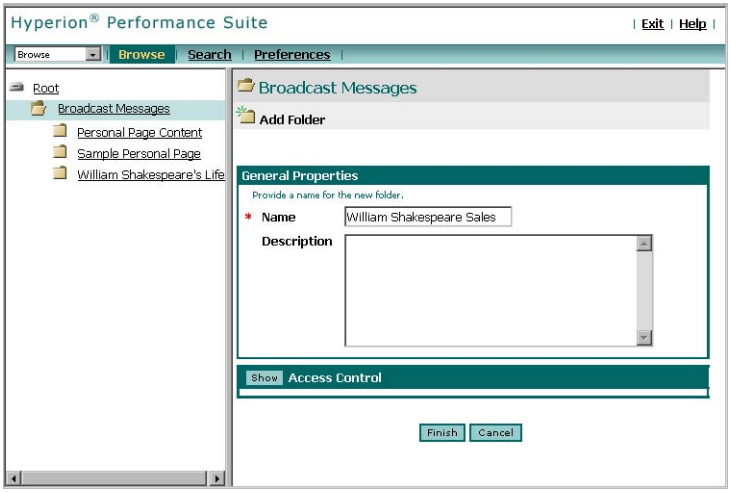
Figure 7-2 Starting Personal Page for this Example

Setting up Pre-Configured Folders

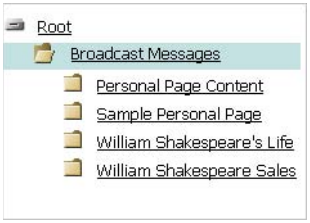
In this example, we will add subfolders called William Shakespeare Sales and William Shakespeare's Life to the Broadcast Messages folder.

To add a subfolder to the Broadcast Messages folder:

1. **Navigate to the Broadcast Messages folder in the Browse web module.**
2. **Choose Add Folder on the action menu.**
3. **Enter folder names *William Shakespeare Sales* and *William Shakespeare's Life one at a time*, and choose Finish.**



The William Shakespeare Sales and William Shakespeare's Life subfolders appear under the Broadcast Messages folder in the Browse web module.



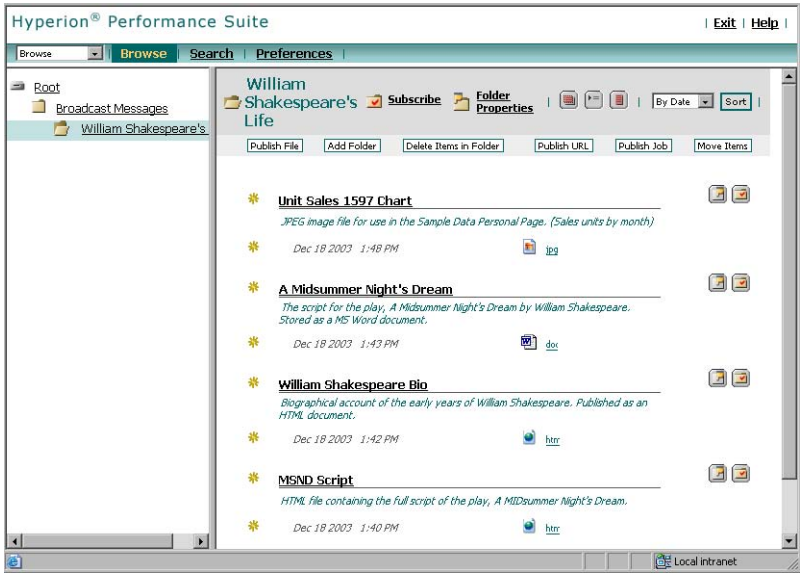
Setting up Items in a Folder

To set up items in a folder:

1 **Select the William Shakespeare Sales subfolder in the Browse web module.**

2 **Choose Publish File and follow the rest of the directions in the "General Publishing" chapter of the *Foundation User's Guide*.**

Add two HTML files, one Word document, and one JPG file. These objects appear on the Browse page as follows:



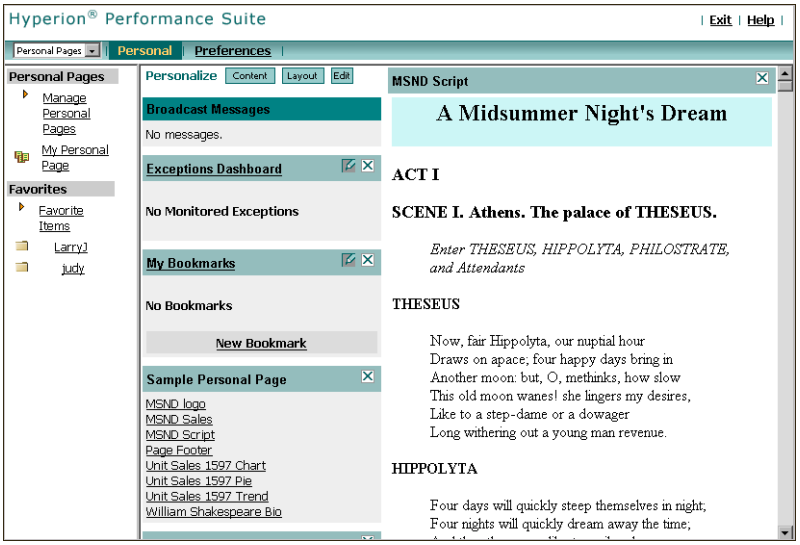
3 **In the Personal Page module, choose Content on the Personalize bar and move the William Shakespeare Sales folder and the MSND Script (displayable) from the Select Content window to the My Personal Page Content window.**

Follow the directions in the *Hyperion Foundation User's Guide* for adding content to a Personal Page.

Viewing the New Users' Personal Page

The content that you defined in the Browse web module appears in the Personal Page generated by Hyperion Foundation for a new user.

For the user in this example, the Personal Page appears as follows:



Publishing Personal Pages

As an administrator, you can publish Personal Pages so that users can copy them to their own Personal pages, and you can change the default Publish properties for publishing Personal Pages (see Table 11-14 on page 11-15). When a Personal Page is published, it is added to the Personal Page content folder, located in the Broadcast Messages folder (default folder location is *root/Broadcast Messages/Personal Page Content*).

Users can also publish Personal Pages when they have *modify* access to the Personal Page content folder.

For details on how to publish Personal Pages, see the *Foundation User's Guide*.

Note Make sure that users understand the following point: Even though two users can copy the same published page, they are not guaranteed identical results. Access privileges on items included on the published page determine what each user sees.

Configuring Other Personal Pages Properties

Using the Servlet Configurator, you can set many Personal Page configuration properties (see "Personal Pages Properties" on page 11-14). A few examples include:

- You can set up color schemes for Personal Pages by setting the Color Schemes properties.
- You can limit Personal Pages by setting the maximum number of Personal Pages a user can have.
- You can control whether the headings on content windows display by turning them on or off. (Headings are the colored bars that resemble title bars.)

Summary

The management of Hyperion Performance Suite content involves setting up MIME types for end users, providing Personal Page content for users, and setting up preconfigured graphic files for image bookmarks. You can push content to users View Manager using the subscribe feature.

8 Administering Jobs

This chapter explains the administrative tasks for setting up jobs, schedules, and the physical resources used for job output.

In This Chapter

Managing Calendars 8-2

Managing Job Elements 8-12

Administering Physical Resources 8-18

Managing Calendars

A custom calendar is a calendar you create, modify, and delete using the Calendar Manager. You can create calendars to schedule jobs based on fiscal or other internal or organizational calendars. Jobs scheduled against a custom calendar resolve dates and variable date limits against the quarterly and monthly dates specified in the custom calendar, rather than using the default calendar. The default calendar, based on the Gregorian calendar, cannot be modified except for the holiday designations and the start week day.

You invoke the Calendar Manager from the Job Utilities toolbar (Figure 8-1).

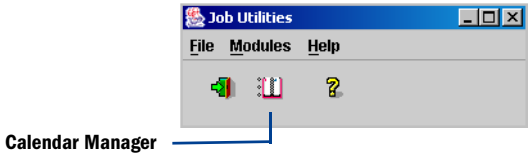


Figure 8-1 Job Utilities Toolbar

A login screen (Figure 8-2) appears where you must supply a user name and password, Hyperion Foundation host, and port number.

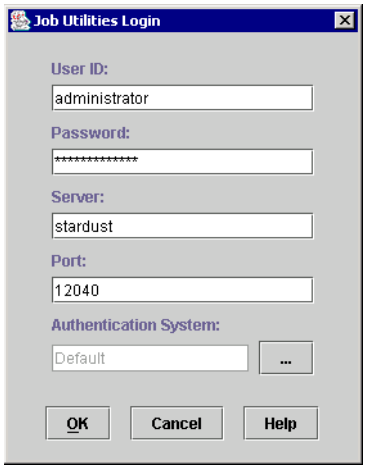


Figure 8-2 Job Utilities Login Screen

Once the system confirms these values, the Calendar Manager window appears (Figure 8-3). The navigation pane on the left lists the default calendar and the custom calendars with the specific years for each calendar in subfolders. You can choose a calendar name or year to modify or delete it.

From the navigation pane, choosing Calendars displays a blank Calendar Property screen. choosing a calendar name displays the Calendar Properties screen with the selected calendar record. Choosing a year displays the calendar Periods and Years screen with the selected calendar and year.

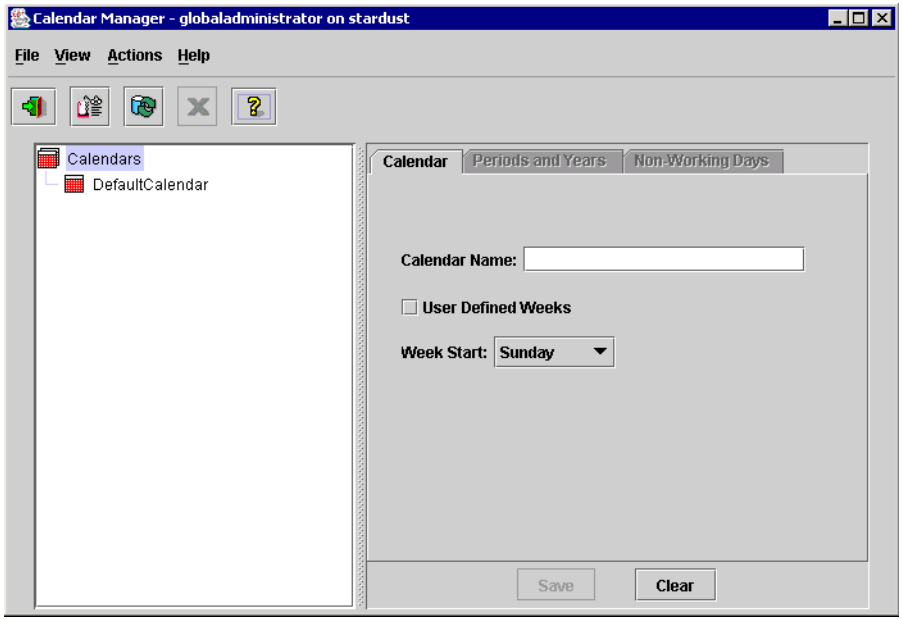


Figure 8-3 Calendar Property Screen

Creating a New Calendar

The default calendar the Calendar Manager comes with is the standard Gregorian calendar.

To create a new calendar:

1. **Invoke the Calendar Manager.**
2. **Choose Calendars from the left navigation pane.**
3. **Enter a name for your calendar.**
4. **Enter the information on the screens in the Calendar Manager, choosing Save at the end of each screen.**

   You must choose **New Year** and enter a year in the text box before you can save the calendar. For specific field information, see "Calendar Manager Properties" on page 8-6.

Deleting Calendars

You can either delete whole calendars or individual years of a calendar.

To delete a calendar or a year:

1. **Navigate to the calendar or year you want to delete.**

2. **Choose the Delete icon and verify that you want to delete the calendar or year.**

   You cannot delete the last year of a calendar. To delete the last year of a calendar you must delete the entire calendar.

Modifying Calendars

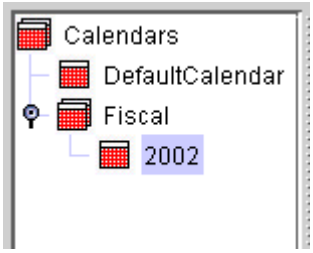
You can modify a year already specified or add another year to an existing calendar.

To modify a calendar:

1 **In the Calendar Manager navigate to the calendar you want to modify.**

Choose the calendar name to view the fields in Table 8-1.

Choose the year to modify the Periods or Years and the Non-working Days.



2 **Choose New Year to add another year to this calendar. Modify the necessary fields.**

When modifying the Periods or Years be sure the dates for weeks or periods are consecutive.

For specific field information, see "Calendar Manager Properties" on page 8-6.

3 **Choose Save.**

Calendar Manager Properties

In this section each tab in the Calendar Manager has a separate table describing the options.

The following figure and table showsFigure 8-4 and Table 8-1 show the general calendar properties.

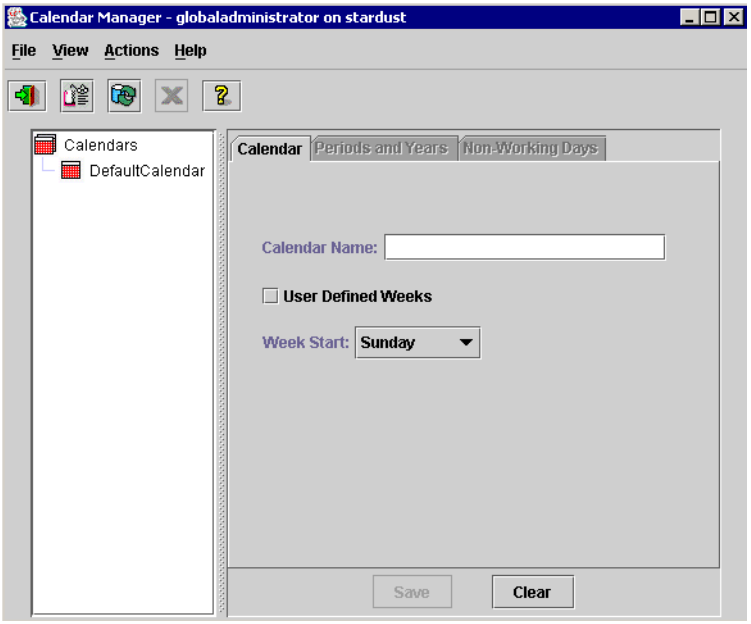


Figure 8-4 Calendar Properties

Table 8-1 Calendar Properties

Calendar Name	The name cannot be changed after it is saved.
User Defined Weeks	Enable if you want to select the start day of the week. The default week is 7 days long and is not associated with any other period of time. User defined weeks can be associated with periods, quarters, or months. Weeks, in either case, cannot span multiple periods. The start and end date cannot be overlapping and they must be sequential.
Week Start	If User Defined Weeks is enabled, select the first day of the week from the drop-down list.

Periods and Years

Define specific years in a custom calendar, define the periods within those years, and assign quarters and periods.

Figure 8-5 and Table 8-2 show the configuration for custom calendar periods and years.

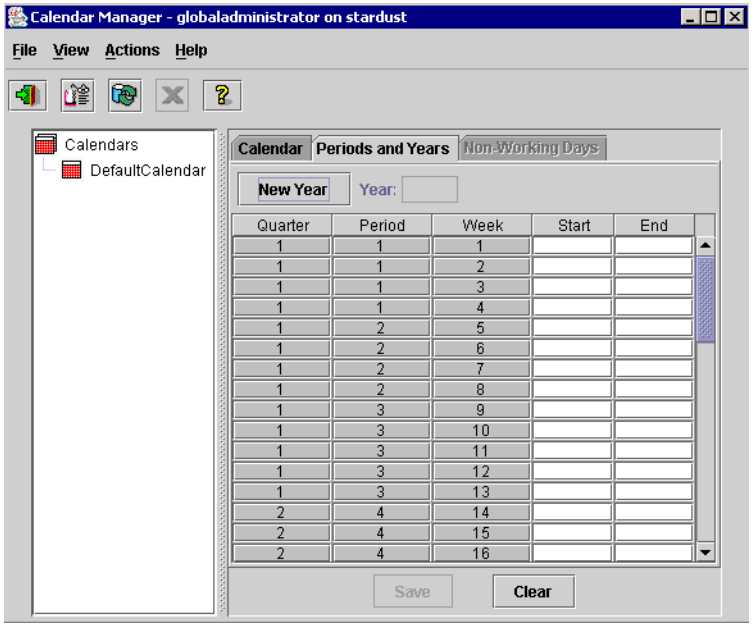


Figure 8-5 Calendar Periods and Years

Table 8-2 Calendar Periods and Years

New Year	Any year is valid if no other years are defined for tis calendar. If this is not the first year defined, the year entered must be sequential.
Quarter/Period/Week	The system automatically assigns the quarters sequential numbers. All calendars have 12 periods.
Start and End	Fill in the first Start and End date. The system automatically fills in the rest of the periods, assigns the quarters logically, and fills in the rest of the start and end dates. After the fields are filled in you can edit the start and end dates. The start and end dates cannot be overlapping and must be sequential.

Non-Working Days

You can select non-working days by *day* or by *day of the week*.

Figure 8-6 and Table 8-3 show custom calendar non-working days.

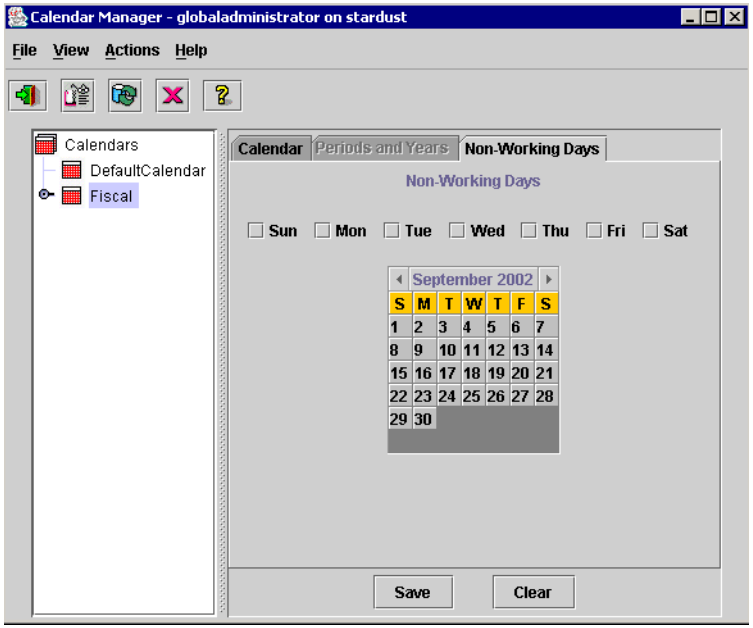


Figure 8-6 Non-Working Days

Table 8-3 Calendar Non-Working Days

Days of the week	Choosing on days of the week populates the calendar automatically.
Calendar	The calendar reflects the day starting the week as selected on the previous screen. Choosing the arrows on either side of the month/year name moves the calendar forward or back one month. You indicate working and non-working days on a day by day basis by selecting and de-selecting the days.

Viewing the Job Log

Calendar Manager keeps a log of events that relates to jobs. The Job Log contains information about the execution of schedules including the job name, start time, stop time, the name of the user that executed the job, the reason that the job was executed, whether the output was viewed, and the directory where the output is located. If the job did not yet complete, there is no value for the stop time.

You can choose to view all of the log entries or only those related to specific users.

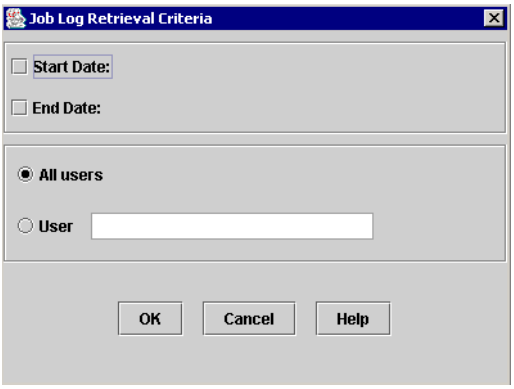
To view the Job Log:

1 **Choose the View Job Execution Log Entries icon.**

The Job Log Retrieval Criteria dialog box appears.

2 **Select start and end dates to specify a range of log entries to retrieve from the Job Log.**

To select a start date or end date, select **Start Date** or **End Date** and choose the corresponding list box. A calendar appears from which you can select a particular date. To omit the start date or end date, do *not* select **Start Date** or **End Date**. (If you omit a start date, Calendar Manager retrieves those entries with the defined end date, and vice versa.)



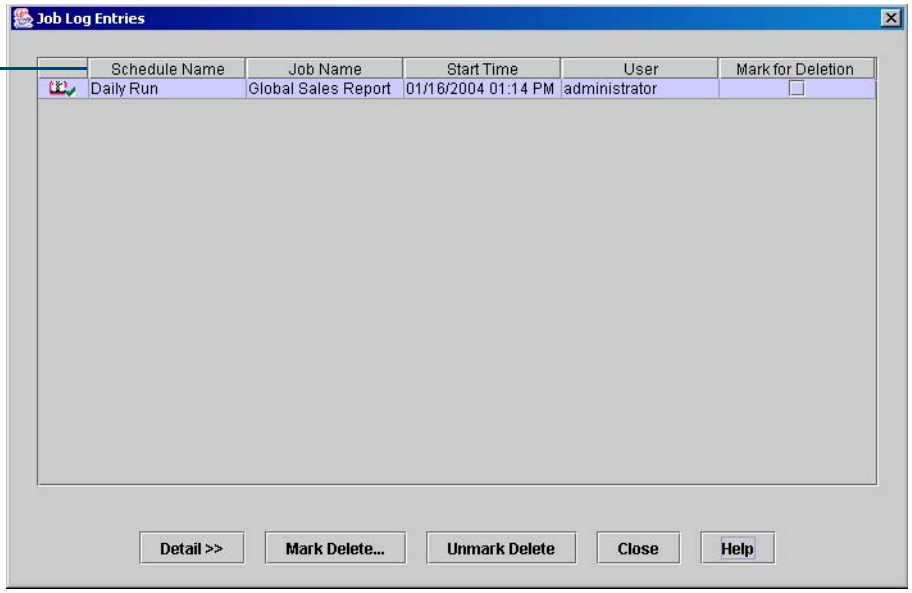
3 **Select All Users to retrieve all entries from the Job Log, or User to retrieve only those entries specific to a particular user.**

If you select **User**, specify a valid Hyperion Performance Suite user name in the field provided.

4 **Choose OK to retrieve the log.**

A new dialog box appears that displays the log entries that you requested.

To sort a column in ascending order, choose the column heading.
To sort a column in descending order, [Shift+click] the column heading.

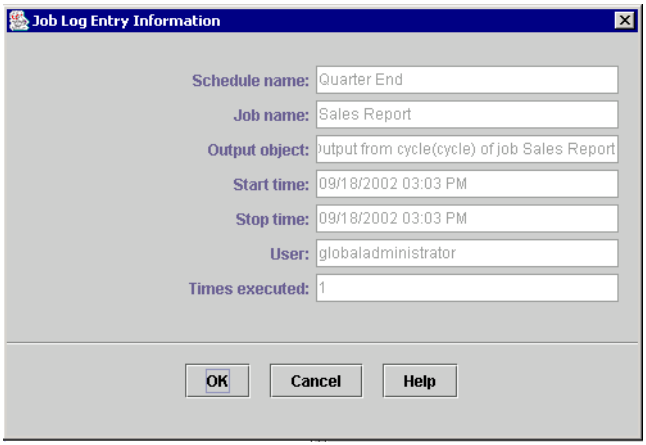


Log entries are initially sorted in ascending order by *schedule name*. You can sort by any of the columns (Schedule Name, Job Name, Start Time, User, Mark for Deletion) by simply choosing the column heading. To sort a column in descending order, [Shift+click] the column.

To change the order in which the columns are displayed, choose a column heading and drag it to the desired location. For example, to move the Job Name column after the Start Time column, choose the Job Name column and drag it to the right.

5 **Select a log entry and choose Detail to view more information.**

A dialog box appears with details about the selected event.



6 **Choose OK to return to the Job Log Entries dialog box. Then, select any log entries that you want to delete and choose Mark Delete.**

To select multiple log entries, use the Shift or Ctrl key, and choose the entries to delete. Choose **Yes** in the dialog box that appears to indicate that you want to remove the selected log entries. Entries marked for deletion are not deleted until the next Hyperion Performance Suite server cycle. (A Hyperion Performance Suite server cycle is a recurring event where Hyperion Performance Suite performs routine maintenance tasks such as deleting items marked for deletion.)

7 **After you review the information, choose OK to close the dialog box.**

Managing Job Elements

This section provides information on managing the following job elements:

- Public Time Events
- Public Job Parameters
- OCE Files
- Database Pass-Through

Note The system automatically creates a textual log file for each job when it is run. This log file appears under the job in the browse item list. You can suppress all job log files by adding the java system property, `-Dbqlogfile_isprimary=false`, to the common services and the job factory startup scripts. You will also need to stop and restart the services. See Chapter 2, "Administration Tools and Tasks", for more information on stopping and starting the services.

Managing Time Events

Different types of time events are managed by users with different roles. Only time events that need the Scheduler Administration role to create are discussed in this guide. Users with the Scheduler Administration role can create public recurring time events and externally triggered events which can be viewed and accessed by other users. For more information on roles, see Chapter 3, "Role-Based Access Control".

To create, modify, and delete public recurring time events follow the procedures for personal recurring time events.

For information on types of time events and for procedures on how to create, modify, or delete public recurring time events, see the *Foundation User's Guide*.

Creating Externally Triggered Events

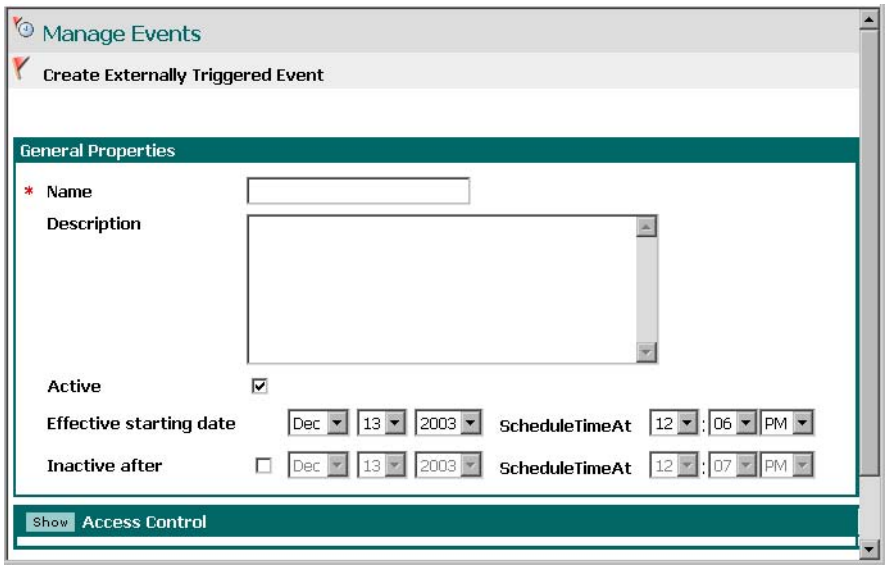
Externally triggered events are non-time events that jobs are scheduled against. A job scheduled against an externally triggered event runs after the event is triggered.

To create an externally triggered event:

1 **Choose Manage Events from the navigation pane of the Job Manager module.**

2 **Select Externally Triggered Event from the Add Another list box on the bottom of the page and choose Go.**

The Create Externally Triggered Event page appears.



3 **Enter a name and description for the event you are creating.**

It is recommended, but not required, that the event name be unique.

4 **Enable the Active option.**

This field is enabled by default. If the Active field is not enabled the externally triggered event will not work.

5 **Select the *Effective starting date*.**

The Effective starting date defaults to the current date.

6 **Select the *Inactive after date*.**

7 **Set the access control. For how to set access privileges, see the *Foundation User's Guide*.**

This gives you the option to allow specific roles, users, or groups to view and use the public recurring time event you are creating.

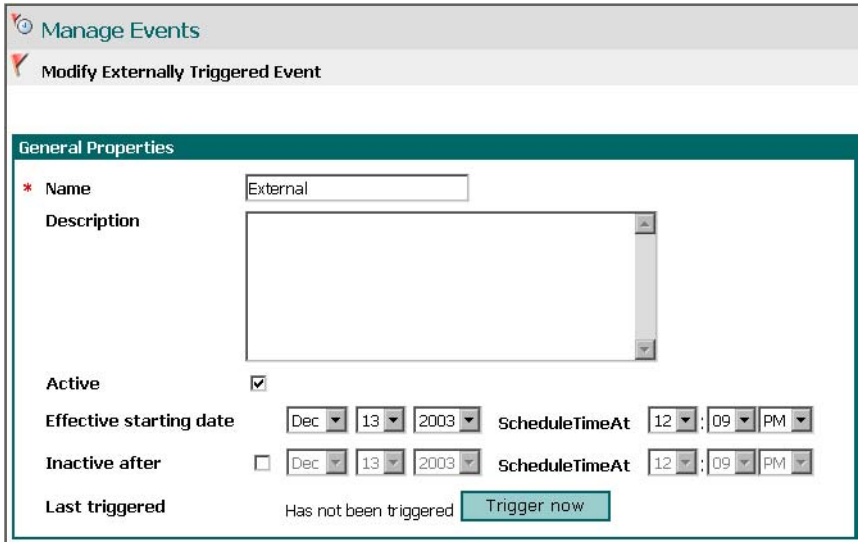
8 **Choose Finish.**

Triggering an Externally Triggered Event

Externally triggered events are non-time events that are triggered manually through the Job Manager module. You can also trigger an external event programmatically using the `triggerETE()` method specified in the Externally Triggered Event interface of the Hyperion Performance Suite SDK. For more information, see the Hyperion Performance Suite SDK.

To trigger an externally triggered event through the Job Manager module:

1. Select **Manage Events** from the navigation pane of the Job Manager module.
2. Select **Modify** next to the event that you want to trigger.
3. Choose **Trigger Now.**



4. Choose **OK.**

The Event List displays.

Administering Public Job Parameters

Different types of job parameters are managed by users with different roles. Only public job parameters, which are managed by users with the Scheduler Administration role, are discussed in this guide. Users with the Scheduler Administration role can create, modify, and delete public job parameters.

To create, modify, and delete public job parameters follow the procedures for personal job parameters except save the parameters as public instead of personal. Use the access control system to allow specific roles, groups, and users to use the public job parameters you created.

For information on how to create, modify, or delete public job parameters, see the *Hyperion Performance Suite Foundation User's Guide*.

Managing OCE Files

OCE files are used by BQY jobs or BQY files to connect to databases. A separate OCE file can be specified for each query of a BQY file or job. If no OCE file is specified for a query at publishing time, the user will not be able to process that query unless it is a query that uses only Local Results. It is, therefore, important that you publish and give access to common OCEs to users who will be publishing BQY jobs and BQY files.

For publishing OCE files, see the *Foundation User's Guide*.

Note To process BQY documents or job outputs using the Hyperion Intelligence Client or the Hyperion Intelligence iServer Client, no explicit access to the OCE is required when the SC_ENABLE flag is set to *true* (this is the default).

When the SC_ENABLE flag is set to *false*, only users who have been given explicit access by the publisher to the OCE associated with the BQY document/job output will have access.

Use the ConfigFileAdmin utility to toggle the flag and to set the ServletUser password. See "Using the ConfigFile Utility" on page 9-49 for detailed instructions.

Managing Pass-Through for Jobs and BQY Files

The pass-through feature allows users to log in once to Hyperion Performance Suite and access their reports' databases without additional authentication. Pass-through is enabled per authentication system and then per specific job or BQY document.

As the administrator you can provide transparent access to databases for foreground jobs and for BQY files that use a particular authentication system by enabling pass-through for that authentication system. When pass-through is enabled, item owners can then enable or disable pass-through for specific jobs and BQY documents.

You can configure pass-through to use either a user's login credentials or credentials set in Browse Preferences or you can leave the credential choose up to the item owner.

For configuration details, see "Pass-Through and Trusted Password" on page 10-11.

Managing Scheduled Jobs

Scheduled jobs are managed through the Job Manager Module. For information on the Job Manager Module, see the *Hyperion Performance Suite Foundation User's Guide*.

Administering Physical Resources

Physical resources, such as printers or output directories, are used as destinations for BQY report output. You administer physical resources from the System tab of the Administration module.

Related Topic:

Adding a Physical Resource

You add physical resources from the System tab of the Administration module.

To add a physical resource:

1. **In the navigation pane, choose Add Printer or Add Output Directory.**
2. **Specify the required properties, and any of the optional properties.**

   For more information, see "Access Privileges" on page 8-19. For information about printer properties, see "Properties of Printers" on page 8-20. For information about output directory properties, see "Properties of Output Directories" on page 8-21.
3. **When finished, choose Finish.**

Modifying a Physical Resource

You modify physical resources from the System tab of the Administration module.

To modify a physical resource:

1. **In the navigation pane, choose Manage Physical Resources.**
2. **Choose Modify for the resource you wish to modify.**
3. **Make your changes, and then choose OK.**

Deleting a Physical Resource

You delete physical resources from the System tab of the Administration module.

To delete a physical resource:

1 **In the navigation pane, choose Manage Physical Resources.**

A list of all resources is displayed. The list includes all types of physical resources.

2 **Choose the Delete button next to the resource you want to delete.**

Confirm the deletion when prompted.

The resource is now deleted.

Access Privileges

Unlike other objects in Hyperion Foundation, which offer several access levels, physical resources offer only two access levels: *Access* and *No Access*.

You add another role, group, or user to the Access Privileges list, and set their access privileges, in exactly the same way as for other objects (items, users, and so on). See *Foundation User's Guide* for instructions on setting access privileges.

Properties of Printers

You use printer resources as destinations for out put of BQY jobs. You should assign the requisite access control and make end-users aware of which printer to use. Users should see only the printers they are supposed to use. The printer must be accessible to each server where the Intelligence Service is running.

When you add or modify a printer, the properties shown below in Figure 8-7 and Table 8-4 are presented for editing:

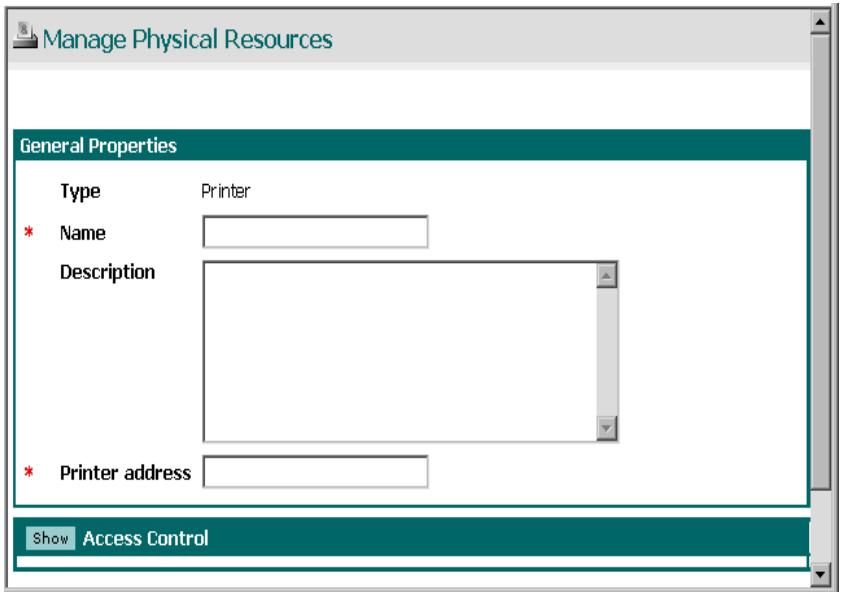


Figure 8-7 Properties Page for a Printer

Table 8-4 General Properties of Printers

Type	Read-only property; set as *Printer*.
Name	The name for the printer that the end-user sees.
Description	A meaningful description to help administrators and users identify the printer.
Printer Address	The network address of the printer. For example, `\\f3prt\techpubs`. End-users will not see this address. **Note:** The printer must be visible to the server on which the Intelligence Service is running.

Properties of Output Directories

You use output directories as destinations for SQR or BQY job output. You should assign the requisite access control and make end-users aware of which output directories to use. Users should see only the output directories they are supposed to use. The output directories must be accessible to each server where the Intelligence Service is running.

When you add or modify an output directory, the following properties shown in Figure 8-8 and Table 8-5 are presented for editing.

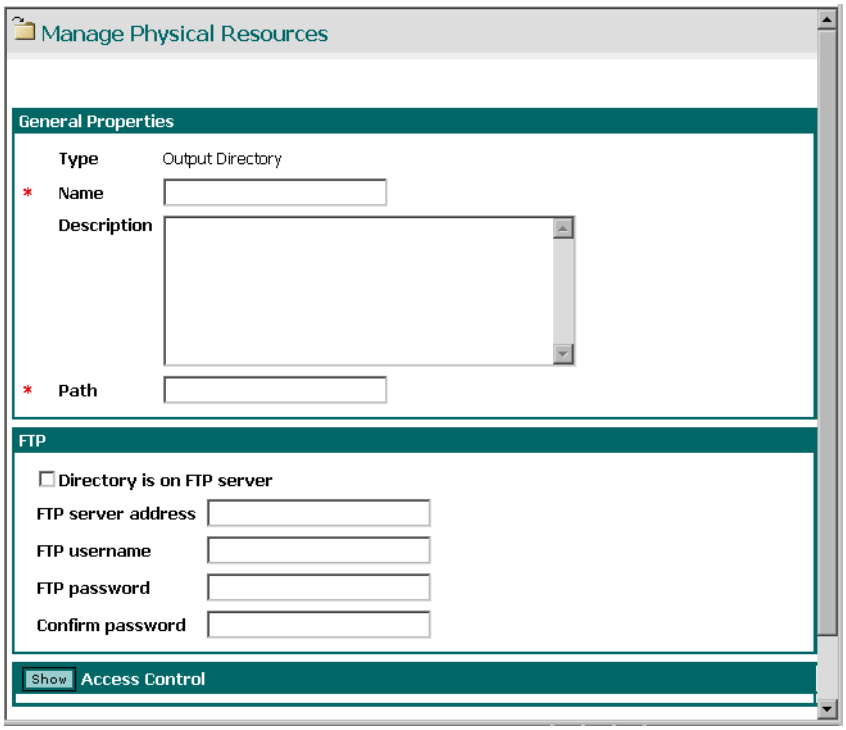


Figure 8-8 Properties Page for an Output Directory

Table 8-5 General Properties of Output Directories

Type	Read-only property; set as *Output Directory*.
Name	Name for the output directory. End-users will see this *Name*.
Description	A meaningful description to help administrators and users identify the directory.
Path	The directory's full network path. For example, `\\apollo\Inventory_Reports`

Table 8-6 FTP Properties (Optional) of Output Directories

Directory is on FTP Server	Enable this option if the output directory is located on an FTP server, and then set the next three properties.
FTP Server Address	Address of the FTP server where the output directory is located. For example, `ftp2.hyperion.com`.
FTP User Name	User name to access the FTP output directory.
FTP Password	Password for *FTP User Name.*

Summary

This chapter showed how to set up custom calendars, physical resources, and other elements necessary for end-users to run BQY, SQR, and generic jobs.

PART IV

Configuration and Maintenance

9 Configuring the RSC Services

All of the Hyperion Foundation services have configurable properties that you can modify using the Local Service Configurator (LSC) or the Remote Service Configurator (RSC). The LSC and RSC handle different services. The two sets of services are referred to, respectively, as the LSC services and the RSC services.

This chapter explains how to use the RSC and describes the properties of all of the RSC services. In addition, the chapter discusses the configuration of a Job Service, including an example of the entire configuration process, publication of a job, and execution of the job.

In This Chapter

Using the Remote Service Configurator (RSC) 9-2

Common Properties 9-24

Job Service-Specific Properties 9-29

Job Service Overview 9-40

Using the ConfigFile Utility 9-49

Using the Remote Service Configurator (RSC)

The Remote Service Configurator (RSC) allows you to modify the properties of existing installations of the following services:

- Name Service
- Repository Service
- Service Broker
- Job Service
- Event Service

With the RSC, you can modify service properties or delete services. However, you cannot add services. To add a service, use the Hyperion Performance Suite installation program.

Note When you delete services, a warning appears letting you know that an error message will display during uninstallation. You can safely ignore the message.

The RSC can configure the services on any host of a distributed Hyperion Performance Suite system. The RSC modifies the `config.dat` file that resides on the target host. You can run the RSC from any server host in the system.

In addition to modifying or deleting services, you can use the RSC to do the following:

- Add, delete, and modify hosts
- Add, delete, and modify database servers
- Change the database password used by the RSC services

Starting the Remote Service Configurator

To invoke the Remote Service Configurator, do either of the following:

- Choose the **Remote Service Configuration** icon on the main Service Configurator toolbar, as shown in Figure 9-1.
- Select **Remote Service Configurator** from the Module menu on the main Service Configuration toolbar.

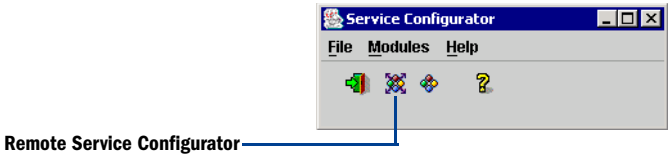


Figure 9-1 Service Configurator Toolbar

Supply the following on the login screen that appears:

- **User ID** – An administrative user ID.
- **Password** – The password for the user name.
- **Server** – The Hyperion Performance Suite host of the services you wish to configure.
- **Port** – The Hyperion Performance Suite port number on the server host.
- **Authentication System** – The authentication system that handles the user you are logging in as. Note that the users *globaladministrator* and *administrator* can be authenticated by any authentication system.

The Service Configurator Login Screen is displayed in Figure 9-2.

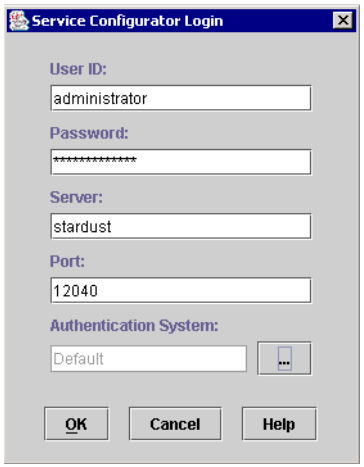


Figure 9-2 Service Configurator Login Screen

Changing the Authentication System

Choose the Advanced button **[...]** on the login screen to select a different authentication system. Select an authentication system from the provided listing and choose **OK** to return to the main login screen. (The default authentication system is the authentication system displayed on the login screen the first time you log in.)

Figure 9-3 shows the advanced page for RSC login.

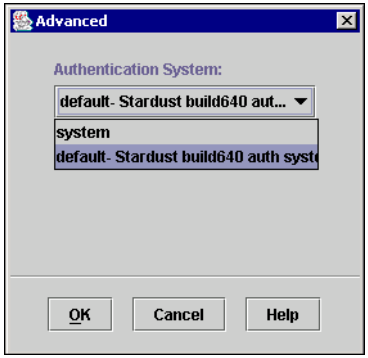


Figure 9-3 Advanced Login Screen

The left pane of the main Remote Service Configurator window lists the installed services of the host you have logged into. Basic properties of the highlighted service display on the right.

Figure 9-4 shows the main window of the RSC.

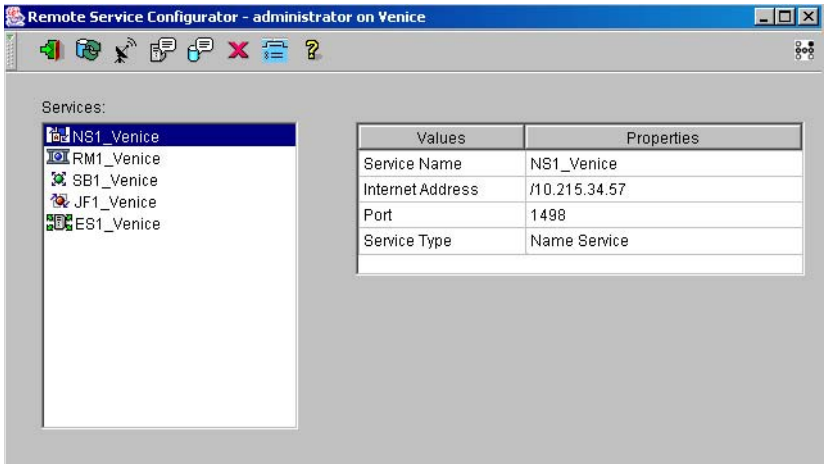


Figure 9-4 Main Window of the Remote Service Configurator

The RSC Toolbar

The toolbar on the main window offers several action icons.

Figure 9-5 shows the RSC toolbar.

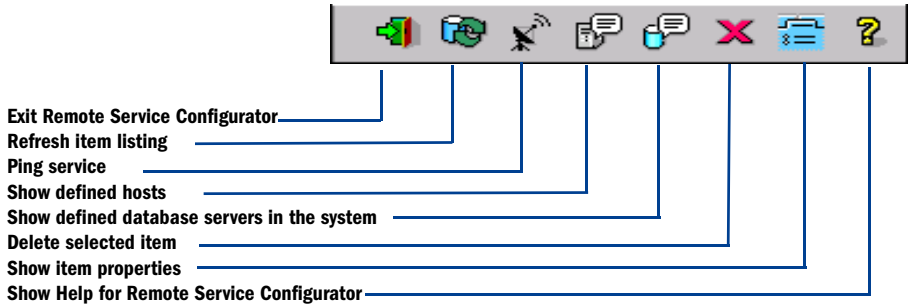


Figure 9-5 RSC Toolbar

The toolbar icons have the following functions:

- **Exit Remote Service Configurator** – Closes the RSC after user's confirmation.
- **Refresh item listing** – Updates the list of services and the basic properties of the selected service.
- **Ping service** – Checks whether the selected service is "alive".
- **Show defined hosts** – Displays the Defined Hosts window, where you can define, delete, or modify hosts.
- **Show defined database servers in the system** – Displays the Defined Database Servers window, where you can add, delete, and modify database servers.
- **Delete selected item** – Deletes the selected service after the user's confirmation.
- **Show item properties** – Displays properties of the selected service for editing.
- **Show Help for Remote Service Configurator** – Displays online help for the RSC.

Deleting a Service

To delete a service from the Remote Service Configurator module:

1 **Select the service from the left pane of the main Remote Service Configurator window and choose Delete selected item.**

A prompt asks you to confirm deletion.

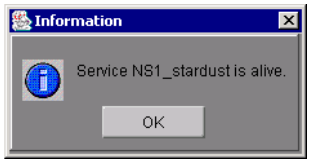
2 **Choose Yes to delete the service.**

Note You cannot delete the Name Service, Repository Service, or Event Service.

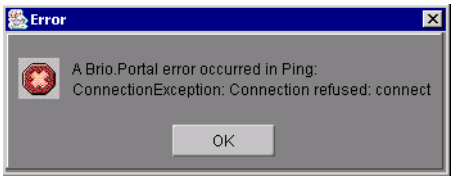
Pinging a Service

Sometimes errors occur because a service has not been started correctly, or has for some reason stopped working properly. An easy way to test the availability of a service is to "ping" it; that is, to send a message to see if it responds.

To ping a service from the Remote Service Configurator, select the service on the main RSC window and choose **Ping Service**. If the service is responsive, the following message appears:



If the service is not responsive, the following message appears:



This typically indicates that the service is not running. If you receive an error such as this, refer to the service's log file to investigate why the error occurred.

Defining Hosts

The Defined Hosts dialog box lists the currently-defined hosts in the Hyperion Performance Suite system and identifies the host name and platform.

You can add, modify, or delete hosts. The following sections discuss:

- Adding a New Host
- Modifying a Host
- Deleting a Host

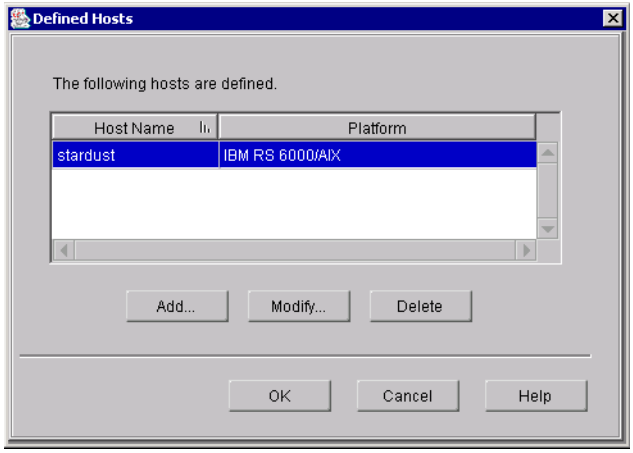
Adding a New Host

After installing services on a machine, add (define) the machine as a new host in the Hyperion Performance Suite system.

To add a new host:

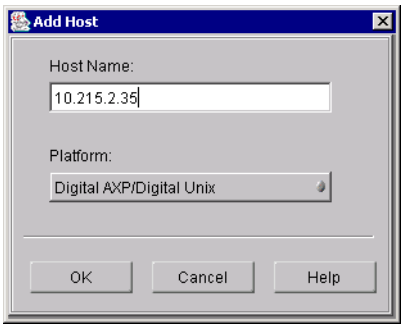
1 **Choose the Show defined hosts icon from the main Remote Service Configurator window.**

The Defined Hosts dialog box appears.



2 **Choose Add.**

The Add Host dialog box appears.



Note The host name cannot start with numerals. The Data Access Service and the Intelligence Service does not work when the host name starts with numerals.

Enter information as defined in the following table:

Table 9-1 Add Host

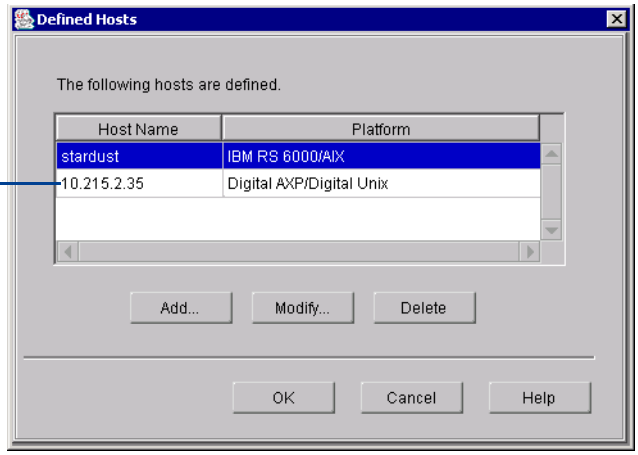
Host name	Enter the name of the host to add. The Data Access Service and the Intelligence Service will not work if the host name starts with numerals.
Platform	Select the host's platform from the drop-down list.

3 **Choose OK.**

After you choose **OK**, Hyperion Performance Suite "pings" the host to make sure it is on the network. If the ping fails, an error message displays.

After Hyperion Performance Suite successfully pings the host and validates the host name, Hyperion Performance Suite adds the host and lists it in the Defined Hosts dialog box.

The new host you add appears in the Defined Hosts dialog box.



4 **Choose OK to close the Defined Hosts dialog box.**

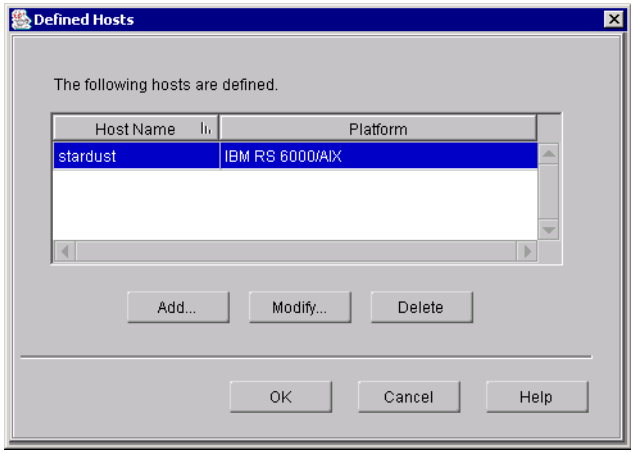
If you change this property, you must restart the Hyperion Performance Suite server and Job Service in order for the new host to take effect.

Modifying a Host

To modify a host:

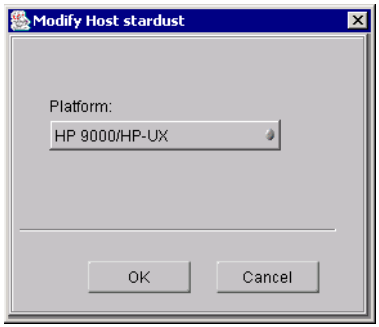
1 **Choose the Show defined hosts icon from the main Remote Service Configurator window.**

The Defined Hosts dialog box appears.



2 **Select a host from the list and choose Modify.**

The Modify Host dialog box appears.



3 **From the Platform list box, select a different platform for the host.**

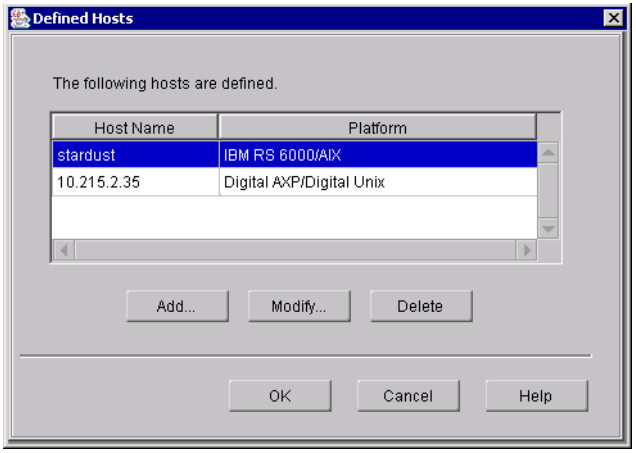
4 **Choose OK to close the Modify Host dialog box.**

Deleting a Host

To delete a host:

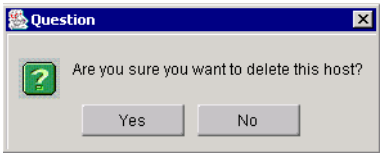
1 **Choose the Show defined hosts icon from the main Remote Service Configurator window.**

The Defined Hosts dialog box appears.



2 **Select the host you wish to delete from the list and choose Delete.**

A prompt asks you to confirm deletion of the host.



3 **Choose Yes to delete the host, then choose OK to close the Defined Hosts dialog box.**

Note You cannot delete a host if services are installed on it.

Changing the Database Password

When you change the password that the services use to access the Repository database, the order of steps is critical. Carefully read all of the instructions before beginning to follow them.

Note Make sure to change the password in Hyperion Performance Suite before changing it in the RDBMS.

Caution! If you perform the steps in the wrong order, you may lose the ability to run Hyperion Performance Suite.

To change the database password:

1. **From the Remote Service Configurator, select one of the services whose password you want to change. It must be one of the service types in the following list:**
   - Name Service
   - Repository Service
   - Event Service
2. **Choose the Show item properties icon and then the Storage tab.**
3. **Change the password and choose OK.**
4. **Repeat Step 1 through Step 3 for all services of the types listed in Step 1, making certain to enter exactly the same new password for each one.**

   If any services of the types listed in Step 1 have different database accounts, perform this step only for those that use the account whose password you are changing.

5 Close the Remote Service Configurator.

6 In the Local Service Configurator, choose the **Show host properties** icon and then the **Database** tab.

7 Change the password and choose **OK**.

This password property (like the other properties on the Database tab) applies to all of the LSC services on the local host. All of them use the same database account.

For more information about the LSC, see Chapter 10, "Configuring the LSC Services and Other System Configuration.".

8 Repeat Step 6 and Step 7 on every host that has any LSC services, making certain to enter the password exactly the same way each time.

9 If you are using the same database for row level security, change the password for row level security on the system tab of the Administration module.

10 Stop the Hyperion Performance Suite services.

11 Change the password in the RDBMS, making certain to enter it exactly as you did for the Hyperion Performance Suite services.

12 Restart the services.

Changing the Database Driver or JDBC URL

When you change the driver for the Repository database or its URL, the order of steps is critical. Carefully read all of the instructions before beginning to follow them.

Caution! If you perform the steps in the wrong order, you may lose the ability to run Hyperion Performance Suite.

If any part of the JDBC URL has changed, such as the database server name, port #, or SID, you must update the JDBC URL property. To do so, perform the JDBC URL portions of the instructions below.

To change the database driver:

1. **Stop the Hyperion Performance Suite services.**
2. **Back up config.dat and server.xml, located in the** `*Install_Home*/BrioPlatform/etc` **directory.**
3. **Start the Local Service Configurator.**
4. **Choose the Show host properties icon and then the Database tab.**
5. **Update the *Database driver* and *JDBC URL* properties.**
6. **Start the ConfigFile utility.**

   For information about this utility, see "Modifying the Config.dat File" on page 9-51.
7. **Enter 3 to choose *Get Name Server Data* from the menu. You can use this data listing to preserve all of the Name Service properties you do not wish to change.**

8 Type **4** to choose *Modify Name Server Data* from the menu. As the program prompts you for each property, refer to the listing you just displayed, and enter the same values for all properties except *Name Server JDBC URL* and *Name Server JDBC Driver*. Enter the new values for these properties.

For example:

```
Name Server JDBC URL
jdbc:brio:oracle://brio8host:1521;SID=brio8
Name Server JDBC driver
com.brio.jdbc.Oracle.OracleDriver
```

9 Run the following SQL against the Repository database:

```
update v8_jdbc set jdbc_driver='newDriverName',
jdbc_url='newJdbcUrl'
```

For example:

```
update v8_jdbc set jdbc_driver=
'com.brio.jdbc.Oracle.OracleDriver',
jdbc_url='jdbc:brio:oracle://brio8host:1521;SID=brio8'
```

10 Copy the new driver files to the *Install_Home*/BrioPlatform/lib directory.

11 Update the variable BP_DBDRIVER in all of the start scripts.

The start scripts are startCommonServices.bat (or .sh), and the individual services' scripts, such as ES_Host_start.bat (or .sh).

For example:

```
set BP_DBDRIVER=C:\Brio\BrioPlatform\lib\BPoracle.jar;
C:\Brio\BrioPlatform\lib\BPutil.jar;C:\Brio\BrioPlatform\lib\BP
base.jar
```

12 Add the new JDBC driver to the Java classpath.

13 Restart the services.

Defining Database Servers

The *Defined Database Servers* dialog box lists the currently defined Repository database servers, identifying the database server name, type, and location (host) of each.

You can add, delete, or modify database servers from the Remote Service Configurator module. The following sections discuss the following tasks:

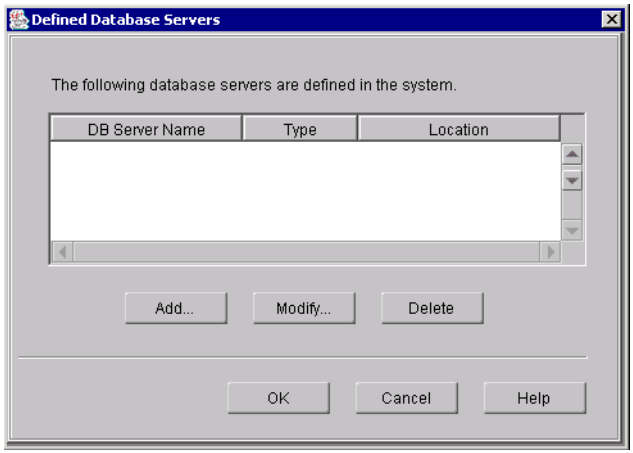
- Adding a Database Server
- Associating a Database Server with a Job Service
- Modifying a Database Server
- Deleting a Database Server

Adding a Database Server

To add a database server:

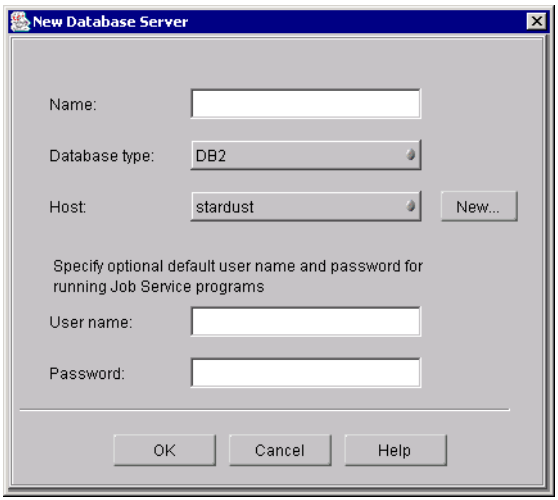
1 Choose **Show defined database servers in the system.**

The *Defined Database Servers* dialog box appears.



2 Choose **Add.**

The New Database Server dialog box appears.



3 **Provide the necessary information, as described in Table 9-2.**

Table 9-2 Properties for a New Database Server

Name	Alphanumeric name for the database server you want to add; it must be at least five characters long.
Database type	The type of database server you are using. Select the appropriate type from the drop-down list.
Host	The host where the database server resides. Choose a host from the drop-down list, or choose **New** to add a new host.
User name	The default user name used by the Job Service for running SQR programs on this database server. This user name is used if the job publisher does not supply a database user name/password when publishing a given job.
Password	The valid password for the *User name*.

4 **Choose OK to save the information and exit from the New Database Server dialog box.**

Associating a Database Server with a Job Service

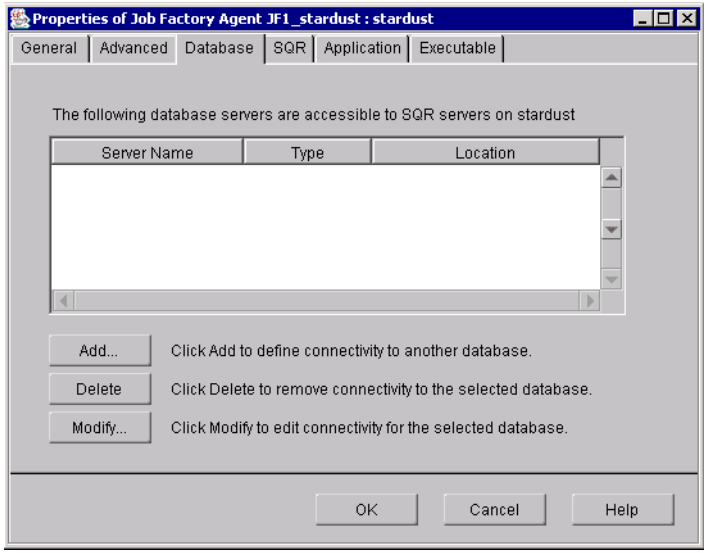
After you successfully add a database server, you need to associate it with a Job Service.

To associate a database server with a Job Service:

1 **From the main RSC window, select the Job Service you want to associate with the database server.**

2 Choose **Show item properties.**

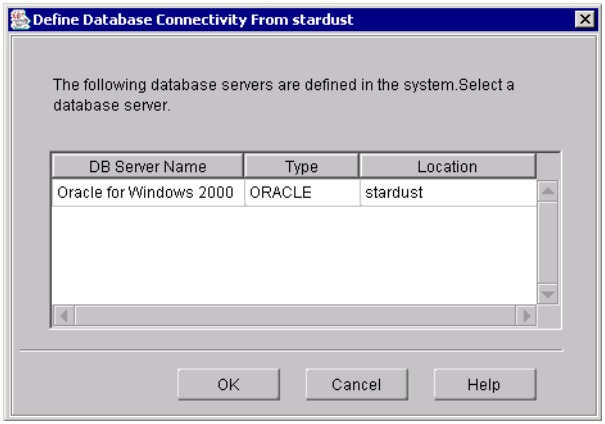
The Properties dialog box appears.



3 Choose the **Database** tab.

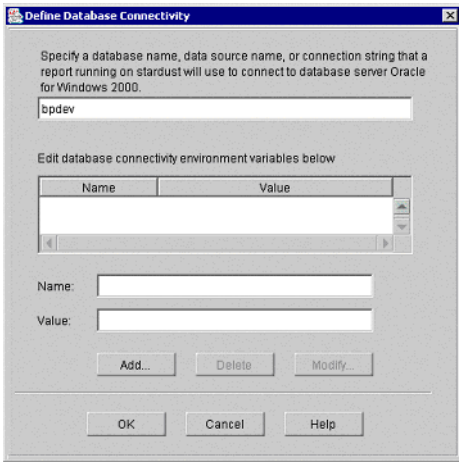
4 Choose **Add.**

The Define Database Connectivity dialog box appears.



5 **Select the database server you want to associate with the Job Service, and choose OK.**

Another Define Database Connectivity dialog box appears.



6 **Specify connectivity information for the Job Service.**

Depending upon the type of database, you have to supply connectivity information. For example, for an Oracle database, you must supply a connect string.

7 **Enter environment variables if desired.**

If you plan to execute SQR jobs against this database, enter the appropriate environment variables here. These environment variables are typically used to specify database-specific information, as well as any shared library information that may be required to run SQR.

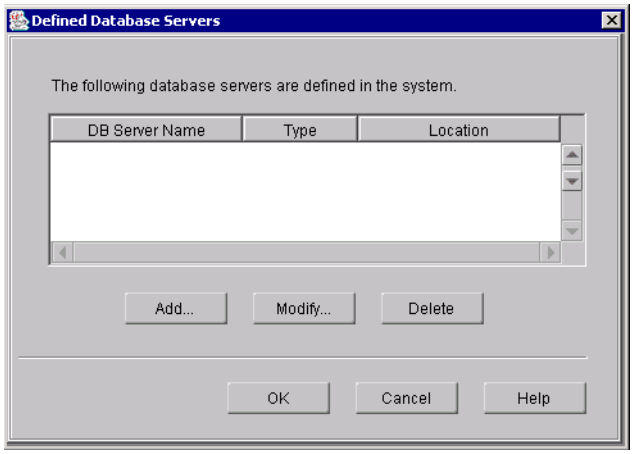
8 **Choose OK to save your changes.**

Modifying a Database Server

To modify a database server:

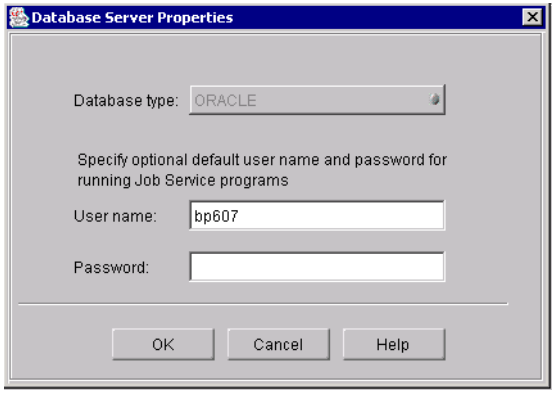
1 **Choose Show defined database servers.**

The Define Database Server dialog box appears.



2 **Select a database server from the list and Choose Modify.**

The Database Server Properties dialog box appears.



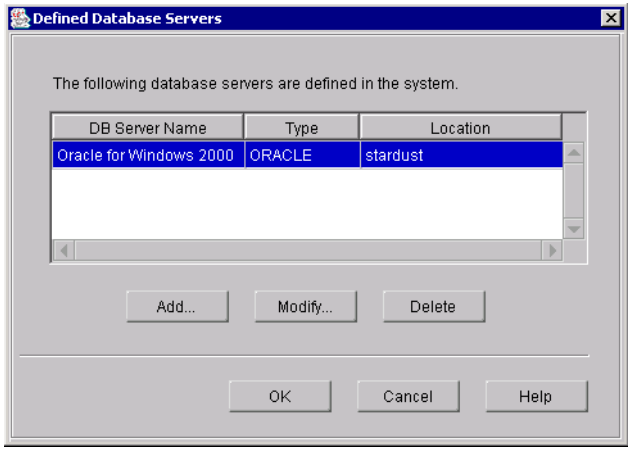
3 **Change properties as designated in Table 9-2 and Choose OK.**

Deleting a Database Server

To delete a database server:

1 **Choose Show defined database servers in the system.**

The Database Servers dialog box appears.



2 **Select a database server from the list and Choose Delete.**

A prompt asks you to verify that you want to delete this database server.

3 **Choose Yes to delete the database; then choose OK to exit from the Database Server Setup dialog box.**

Adding Services

To add a RSC service to your Hyperion Performance Suite system:

1. **Run the Hyperion Performance Suite installation program to install the service software on the desired host machine.**

2. **Configure the new service during the installation process.**

   For information about creating a new Hyperion Performance Suite service, see your installation guide.

   After the service is installed, you can reconfigure it using the RSC.

Note After you install a new RSC service, all Service Brokers in your system are notified about the new service and begin dispatching requests to it.

Modifying Service Properties

To view or modify the properties of a service, from the main RSC window, do either of the following:

- Double-click the name of the service.
- Select the name of the service and choose **Show item properties** on the RSC toolbar.

A properties page displays for editing. Choose a tab to view or modify a group of properties. For example, choose the Storage tab to modify properties that define where persistent storage of business data is. The groups of properties are:

- General Properties
- Advanced Properties
- Storage Properties
- Database Properties
- SQR Properties
- Application Properties
- Executable Properties

Not every service has all of the property groups.

When you modify properties of a service, the service receives notification of the changes and immediately updates its configuration. Most properties are used while the service is running and take effect immediately. Examples of such properties are *Max Connections* and *Logging Levels*.

Properties that are only used at startup time, however, do not take effect until the next time the service starts. Such properties include *Host*, *Directory*, *Log File*, and *IP Port*.

Note The Job Service has more properties than mentioned here. See "Job Service-Specific Properties" on page 9-29 for complete information.

The next topic, "Common Properties," describes the groups of properties that all or most of the RSC services have. The subsequent topics describe the other properties of each service.

Note Any RSC services not mentioned explicitly in this chapter have only common properties.

Common Properties

All RSC services have the General and Advanced property groups, and the majority have the Storage properties.

General Properties

The General properties provide the description of the service, host, IP port, and directory. All RSC services have General properties.

The General Properties are detailed in the Figure 9-6 and Table 9-3.

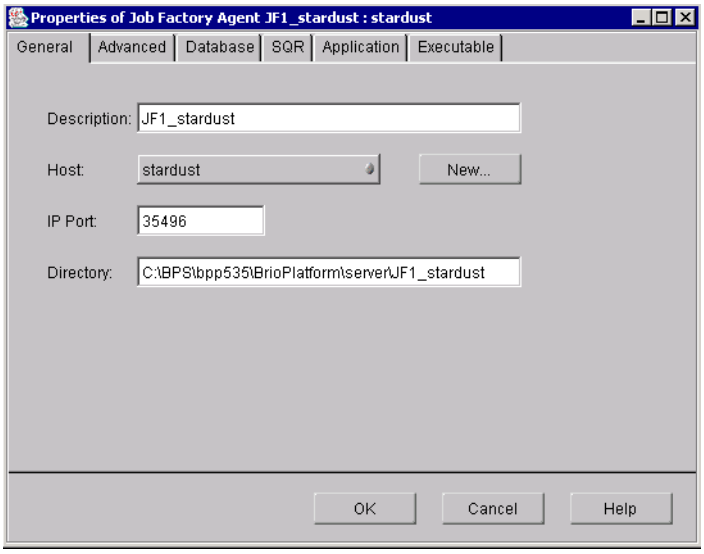


Figure 9-6 RSC Services General Properties

Table 9-3 General Properties

Description	A brief description of the service.
Host	The host on which the service resides. Choose a host from the list or choose **New** to define a new host. If you define a new host, enter a name that makes the service easily identifiable within your organization. The maximum number of characters allowed is 64. For complete information, see "Defining Hosts" on page 9-7. Changes to this property do not take effect until the service is restarted.
IP Port	The service's IP port number. The wizard assigns a unique port to each service. Even if you install multiple services of a particular type—Job Services, for example—on the same host, the wizard automatically enters a unique IP port number for each one. Changes to this property do not take effect until the service is restarted.
Directory	The location where the service resides. Adopt a convention for naming the directories where you store service information. For example, for a Event Service named ES_apollo, the *Directory* might be `j:\Brio\Brio8\server\ES_apollo.` Changes to this property do not take effect until the service is restarted.

Advanced Properties

The Advanced properties describe the service's log level and the maximum number of connections the service supports. All services have Advanced properties.

The Advanced Properties are detailed in the Figure 9-7 and Table 9-4.

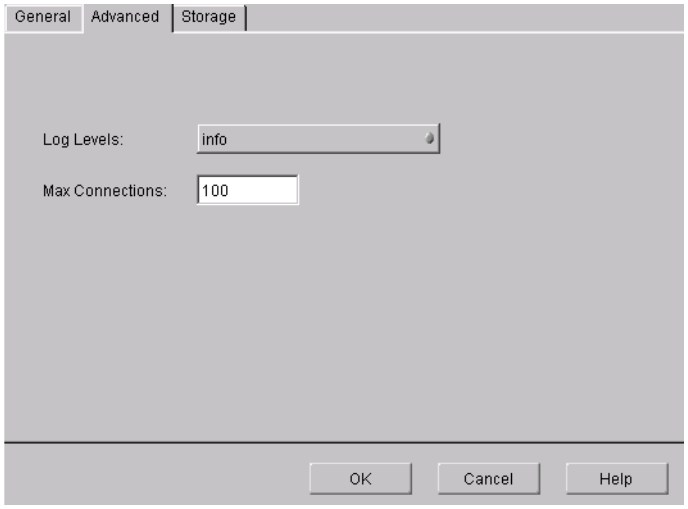


Figure 9-7 RSC Services Advanced Properties

Table 9-4 Advanced Properties

Log Levels	Select the logging level for this service. See "Configuring Log Levels" on page 14-11. A change to this property takes effect immediately. Therefore when errors occur and you want more debugging information, you can change the logging level without restarting the service.
Max Connections	The maximum number of connections allowed. Consider memory allocation for the connections you allow. You must also increase the maximum number of file descriptors on some systems, such as UNIX. A change to this property takes effect immediately. Changing the ***Max Connections*** setting without restarting the service is useful to dynamically tune the service at run-time.

Storage Properties

The Storage Properties are used by a service to connect to the database where it stores its data. The following services store data of their own:

- Name Service
- Repository Service
- Event Service

For example, the Event Service stores information about schedules and subscriptions. The Repository Service stores your Hyperion Performance Suite content's metadata. (Service Broker and Job Service do not have the Storage properties.)

The service-specific data for all these services is stored in a single database. The Storage Properties define connectivity for this database, which is usually referred to as the "Repository database."

The Storage Properties are detailed in Figure 9-8 and Table 9-5.

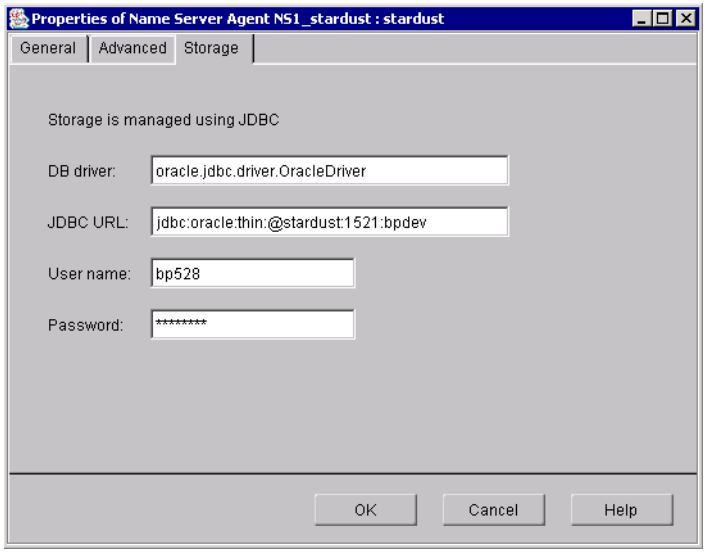


Figure 9-8 RSC Services Storage Properties

Note Hyperion Performance Suite only supports configurations in which all services connect to the same database. For this reason, change the settings on this tab only if you are an experienced Hyperion Performance Suite administrator, or get the assistance of Hyperion's technical support.

The Storage properties settings rarely need to be changed. The circumstances that would require changes include, for example, assignment of new host names on your network, need to change a database user account (name or password), or need to change database type (as from Oracle to Sybase). Such changes require extensive changes to external systems' configuration as well.

Table 9-5 Storage Properties for Services

DB Driver	The name of the driver used to access the database. This is database-dependent, and should only be changed by an experienced administrator. If you change the *DB Driver*, you must change other files, properties, data in the database, and the Java classpath. For details, see "Changing the Database Driver or JDBC URL" on page 9-14.
JDBC URL	(**J**ava **D**ata**B**ase **C**onnectivity **U**niform **R**esource **L**ocator) The URL for Java access to the database via the JDBC driver. The services use this URL to connect to the database server. If you change the *JDBC URL*, you must change other files, properties, and data in the database. For details, see "Changing the Database Driver or JDBC URL" on page 9-14.
User Name	The user name for the database account. All services should use the same database account.
Password	The password for the database account.

Job Service-Specific Properties

The Job Service has some properties unique to it, including the property groups Database, SQR, Application, and Executable. This section describes these properties as well as other tasks that start from the Job Service's Properties dialog box.

When you modify properties of a Job Service, the service receives notification of the changes and updates its configuration immediately. Properties used while the service is running take effect immediately. Such properties include *Max Connections*, *Logging Levels*, and all properties on the Database, SQR, Application, and Executable tabs.

The Job Service properties tabs are detailed in Figure 9-9.

Figure 9-9 Job Service Properties Tabs

Properties only used at startup time, however, do not take effect until the next time Job Service starts. Such properties include *Directory*, *Log File*, and *IP Port*.

Database Properties

The Database properties provide the information needed for a Job Service to connect to the databases against which it runs jobs. Specifically, on the Database page you define connectivity for all database servers this Job Service needs to access.

The Database Properties are detailed in Figure 9-10 and Table 9-6.

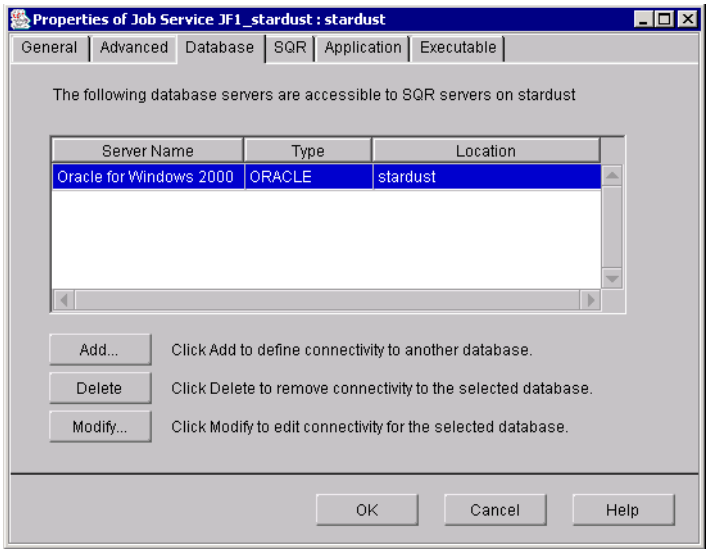


Figure 9-10 Database Properties for Job Service

Table 9-6 Database Properties for Job Services

Server Name	The name of the database server.
Type	The type of database server you are using.
Location	The host where the database server resides.

As you create or edit the list of database servers and their connectivity properties, use the following buttons:

- **Add** – Allows you to define connectivity between the Job Service and an additional database. When you choose **Add**, a dialog box appears that displays the database servers in your Hyperion Performance Suite system. Select a new database from the list, and define any necessary connection strings or environment variables.

  Adding connectivity to a local database server enables the Job Service to run a program that can connect directly to a local database. (For information on adding database servers, see "Adding a Database Server" on page 9-16.)

- **Delete** – Allows you to delete a database's connectivity from the Job Service. Select a database from the list and choose **Delete**.

- **Modify** – Allows you to modify the connectivity properties of a database. Select a database from the list and choose **Modify**. A dialog box appears where you can choose existing environment variables from the list or create new ones in the Name and Value fields. For example, `name=ORACLE_SID, value=PAYROLL`.

Note The Database Servers list combined with the SQR Servers list is used to construct data sources for publishing SQR reports.

SQR Properties

The SQR properties define the SQR servers in the system.

The SQR page lists the SQR servers that are currently defined and available on the same host as the Job Service.

The SQR Properties are detailed in Figure 9-11.

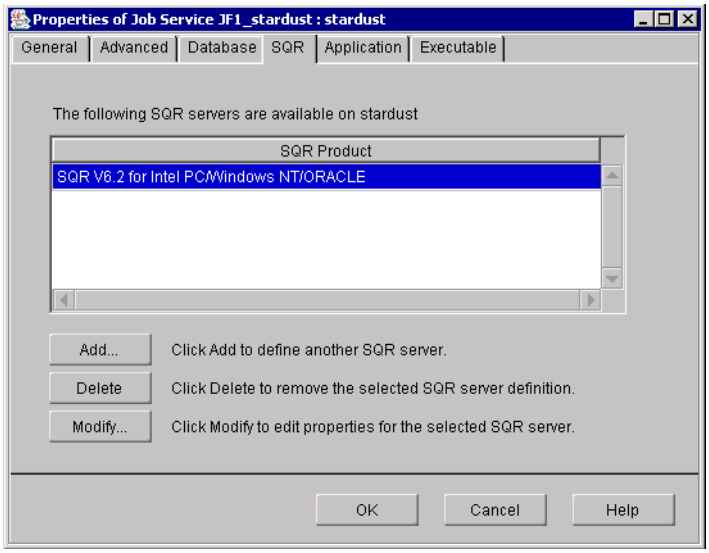


Figure 9-11 SQR Properties for Job Service

You can choose any of the following buttons on the SQR tab:

- **Add** – Allows you to define an additional SQR Server to use for running SQR jobs. When you choose **Add**, a dialog box appears that lists the available SQR Servers. Select a new SQR Server from the list and choose **OK**.
- **Delete** – Allows you to delete an SQR Server. Select a server from the list and choose **Delete**.
- **Modify** – Allows you to modify the properties of an SQR Server. Select a server from the list and choose **Modify**. A dialog box appears, where you can change the path of the SQR Server.

Application Properties

The Application properties describe the application used by a Job Service.

If you use the Job Service to run generic jobs, choose the **Application** tab. This tab is where you view or modify the properties of the application(s) associated with the Job Service.

The Application Properties are detailed in Figure 9-12 and Table 9-7.

Note You can configure a single Job Service to run any combination of the three types of jobs: SQR, BQY, and generic.

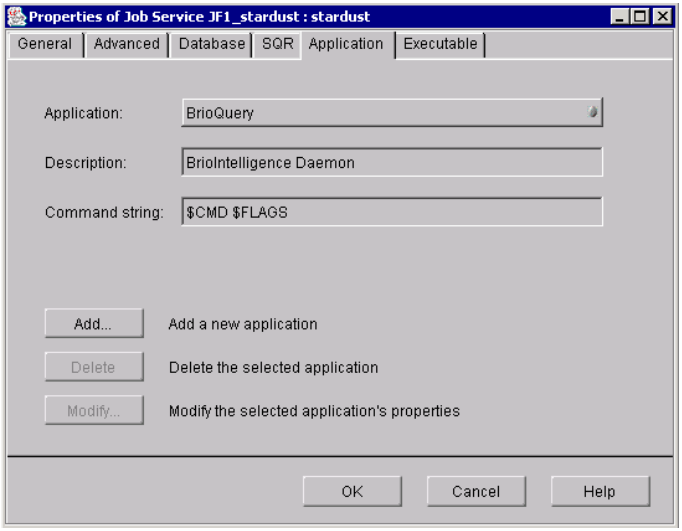


Figure 9-12 Application Properties for Job Service

Table 9-7 Application Properties for Job Service

Application	The name of the application. Select an application from the drop-down list, or choose **Add** to add a new application. The drop-down list displays all the applications defined in Hyperion Performance Suite. An application can have multiple executables, each on a different Job Service to distribute the load.
Description	An optional description of the application. The description field on this page is read-only. To change the description, choose **Modify**.
Command String	Command string to pass to the application when it runs. The Command String field is read-only. To modify the command string, choose **Modify**.

As you edit the properties of an application, use the following buttons on the Application tab:

- **Add** – Allows you to add a new application. When you choose **Add**, the Application Properties dialog box appears, where you can enter information about the application. After you add an application, you must define its executable. Select the Executable Properties tab to do so.
- **Delete** – Allows you to delete an application. You can delete an application only if it has no associated executables. Select an application, choose **Delete**, and choose **Yes** to confirm.
- **Modify** – Allows you to modify the properties of an application. Choose **Modify**, change the properties as desired, and choose **OK**.

As outlined above, when you choose **Add** to add a new application or **Modify** to modify the properties of an existing application, the Application Properties dialog box appears.

The properties on the application properties dialog box are detailed in Figure 9-13.

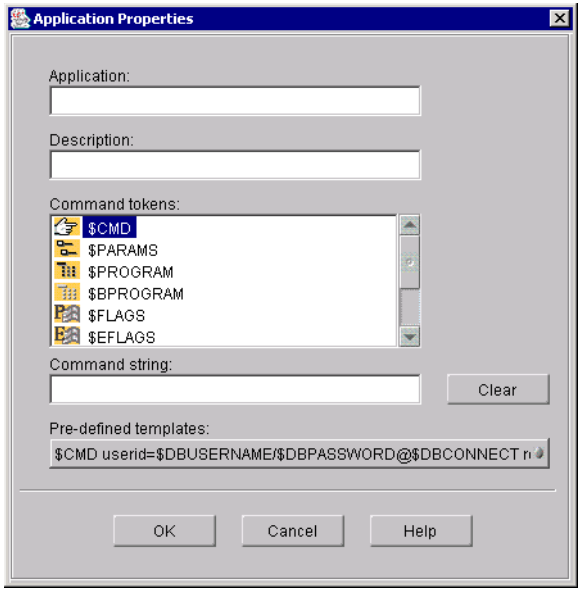


Figure 9-13 Applications Properties Dialog Box

In the Application Properties dialog box, enter a name and description for the application.

It is important to understand that you must specify both the *application* and an *executable*. An application may be installed on multiple hosts. Each installation of the application has a different executable, or program file and path, which you define on the Executable tab.

For example, your system might have Oracle Reports (an application) installed on two hosts, *apollo* and *zeus*. The Job Services on apollo and zeus might have identical Application properties, but their executables would be different, since each host has its own executable file. For more information about Executable properties, see "Executable Properties" on page 9-38.

After setting the Application properties, provide a command string to pass to the application when it runs. Either select a pre-defined template from the drop-down list, or enter the command string in the Command String field. You can build a command string using the tokens that the dialog box displays.

Table 9-8 explains the tokens that you can use to build a command string. Examples of command strings follow the table.

Table 9-8 Tokens Used to Create Command Strings

`$CMD`	Represents the full path and name of the executable.
`$PARAMS`	Represents the parameters defined for the program. You can set prompt and default values for individual parameters in the program properties.
`$PROGRAM`	Represents the program to run. Examples of programs include shell scripts, SQL scripts, or an Oracle Report.
`$BPROGRAM`	Represents the program name with the file extension stripped off. You can use this in combination with hardcoded text to specify a name for an error file, a log file, or another such file. An example would be `log=$BPROGRAM.log`.
`$FLAGS`	Represents the flags associated with the program.
`$EFLAGS`	Represents the flags associated with the executable or an instance of it. All jobs associated with this executable use these flags.
`$DBCONNECT`	Represents the database connect string associated with the program. If this is set, the end user does not have the option to specify a different connect string at runtime.
`$DBUSERNAME`	Represents the database user name associated with the program. If this is set, the end user does not have the option to specify a different user name at runtime.
`$DBPASSWORD`	Represents the database password associated with the program. If this is set, the end user does not have the option to specify a different password at runtime.
`$BPUSERNAME`	Represents the Hyperion Performance Suite user name. If the user name is required as an input parameter to the job, specifying this token instructs the system to include the user name in the command line automatically, rather than prompting the user.
`$RMUSERNAME`	Supported only for backward compatibility. Use $BPUSERNAME instead.

Command String Examples

The following are examples of command strings:

- This command string template runs Oracle Reports:

  ```
  $CMD userid=$DBUSERNAME/$DBPASSWORD@$DBCONNECT
  report=$PROGRAM destype=file desname=$BPROGRAM.html
  batch=yes errfile=$BPROGRAM.err desformat=html
  ```

  When the tokens in the above command string for Oracle Reports are replaced with their actual values, the command that actually gets executed in the Job Service looks like the following code sample.

  ```
  r30run32 userid=scott/tiger@Brio8 report=inventory
  destype=file desname=inventory.html batch=yes
  errfile=inventory.err desformat=html
  ```

- This command string template runs shell scripts on a Job Service running on UNIX:

  ```
  $CMD $PROGRAM $PARAMS
  ```

  When the tokens in the above command string for running shell scripts are replaced with their actual values, the command that actually gets executed in the Job Service looks like:

  ```
  sh runscript.sh p1 p2 p3
  ```

- This command string template runs batch files on a Job Service running on a Windows system:

  ```
  $PROGRAM $PARAMS
  ```

  When the tokens in the above command string for running batch files are replaced with their actual values, the command that actually gets executed in the Job Service looks like:

  ```
  Runbat.bat p1 p2 p3
  ```

Executable Properties

The Executable properties provide detailed information for running an application used by a Job Service. Only Job Services have Executable properties.

The Executable Properties are detailed in Figure 9-14 and Table 9-9.

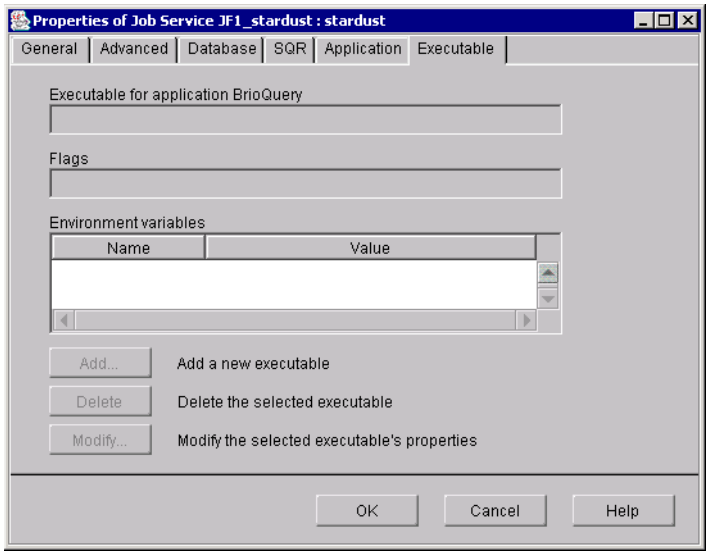


Figure 9-14 Executable Properties for Job Service

Table 9-9 Executable Properties for Job Service

Executable	Defines the location of the executable program for the application (full path and executable name). It must be located on the same host as the Job Service.
Flags	This value is used in the command line as the value for the token `$EFLAGS`. The `$EFLAGS` token represents the flags associated with the program.
Environment Variables	You can modify the environment variables associated with the application, for example, `$PATH, $ORACLE_HOME`.

As you edit the properties of the executable, you can choose any of the following buttons on the Executable tab:

- **Add** – Allows you to define an executable for a new application. (Applications are defined on the Application Properties tab.) The Add button is only active when you need to define an executable for a new application. When you choose **Add**, a dialog box appears where you can enter the path and name of the executable, command-line flags, and environment variables.
- **Delete** – Allows you to delete an executable. Select an executable, choose **Delete**, and choose **Yes** to confirm.
- **Modify** – Allows you to modify the properties of an application's executable. When you choose **Modify**, a dialog box appears where you can change the path and name of the executable and modify command-line flags and environment variables.

Job Service Overview

This section explains how to set up a Job Service to run the desired types of jobs.

A Job Service is a Hyperion Foundation service that compiles and executes content-creation programs. The Job Service "listens" for Hyperion Performance Suite job requests (such as a request initiated by a user from the Browse module), manages program execution, and returns the results to the requester. In addition, it stores the results in the Repository.

About Job Services

The three types of jobs that Hyperion Foundation can store and run are:

- **BQY job –** A BQY document published in Hyperion Foundation as a job, and its associated files.
- **SQR job –** An SQR report program and its associated files. An SQR job can be secure or nonsecure.
- **Generic job –** A report program from another software provider (for example, an Oracle report or a Crystal report), and its associated files.

For BQY jobs, no special configuration is necessary. Every Job Service is preconfigured to run BQY jobs.

For users to run SQR or generic jobs, you must configure a Job Service to run the appropriate report engine or application program. A single Job Service can run multiple types of jobs, as long as it is configured for each type (except BQY).

Adding an Application to a Job Service

You can configure any Job Service for multiple applications, so that it can run jobs processed by any of those applications.

To configure an existing Job Service for an additional application:

1. **On the RSC main page, select the Job Service to configure, and choose Show Item Properties.**
2. **In the Properties dialog that displays, select the Application tab.**
3. **On the Application page, choose the Add... button.**
4. **Complete the Application properties, and choose OK.**

   See "Application Properties" on page 9-33 for a description of the Application properties.
5. **In the Properties dialog, select the Executable tab.**
6. **On the Executable page, choose the Add... button.**
7. **Complete the Executable properties, and choose OK.**

   See "Executable Properties" on page 9-38 for a description of the Executable properties.
8. **If you want to add another application to the same Job Service, repeat from Step 2; otherwise, choose OK to return to the main RSC page.**

Modifying Executable Properties of an Application

To modify the Executable properties of an application for which the Job Service is already configured:

1. **Go to the Application tab of the Job Service's properties dialog box.**

   For explicit instructions, see "Adding an Application to a Job Service" on page 9-41.

2. **Select the application whose Executable properties are to be modified.**

   This step is necessary before modifying properties on the Executable tab.

3. **Proceed with the modifications.**

Enterprise-Reporting Applications

The Hyperion Performance Suite architecture is designed for distributed, enterprise implementations. As such, for optimum performance we recommend the following:

- Replicate Job Services (more than one Job Service assigned to a given data source on different machines) to increase overall reliability and decrease job turn-around time.
- Install a Job Service on the same machine as the database to conserve valuable network resources.

Note Normally, you should have a single Job Service on a given host. You can configure a Job Service to run several different applications.

To run jobs against an enterprise application, configure the parameters described in Table 9-10.

Table 9-10 Parameters for Enterprise Applications

Host	The host is the physical machine identified to the system by host name.
Job Service	The Job Service on the host using Remote Service Configurator.
Application	An application is typically a third-party vendor application designed to run in the background. Application examples include Hyperion SQR, Oracle Reports, or public domain application shells such as PERL.
Program	A program is typically a source used to drive a specific invocation of an application. For example, a user might submit an SQR program that generates a Sales report to an SQR application on a given host through a Job Service.

From Adding a Job Service to Running a Job

This section synthesizes the process of configuration for running jobs into a single set of steps, taking you from service installation to the successful execution of a job.

To run a job in Hyperion Foundation, complete the following steps. They are explained in detail in other sections throughout this chapter.

1. Install the report application's executable on the host where you run the Job Service. Use the installation program that comes with the report application.
2. On the desired host, install the Job Service software from your Hyperion Performance Suite server installation CD.
3. Configure the new Job Service in the Remote Service Configurator.
4. Start the new Job Service.
5. For generic jobs, add an application and executable. For SQR jobs, add an SQR executable, and define a database server and database connectivity properties. BQY jobs do not need any special configuration.
6. Publish a job (a report or program) to run against the application.

   This can be an SQR, BQY, or generic job.
7. A user can now run the job from the Browse module.

Example: Configuring a Job Service for SAP

An example of modifying Job Service's properties is configuring an existing Job Service for an additional application. The high-level steps for configuring an existing Job Service for SAP and DDO are:

- Add a Database Server for DDO and SAP
- Define Connectivity to the DDO Database Server
- Add an SQR Server

The detailed steps to configure an existing Job Service for SAP and DDO appear below.

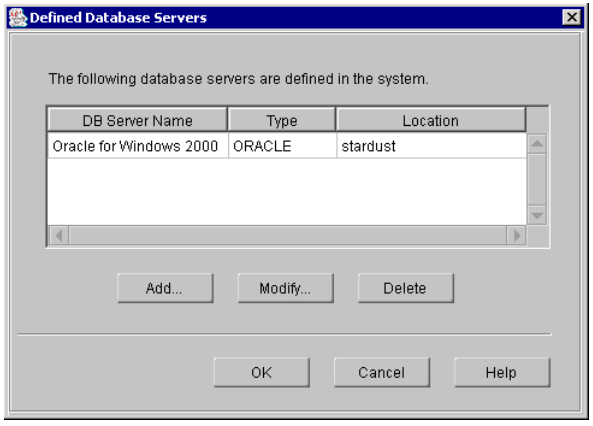
Add a Database Server for DDO and SAP

DDO is part of Hyperion's SQR/DDO, a data-access middleware product. The steps below define a DDO data source (which the dialog boxes call a Database Server). These steps create a configuration in which SQR accesses SAP by using the DDO middleware.

To add a database server for DDO and SAP:

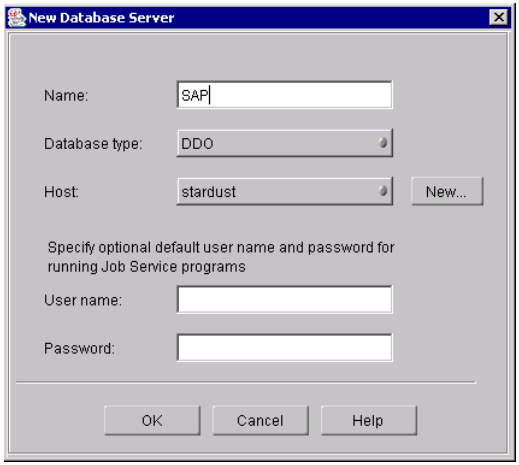
1 **Choose the Show defined database servers icon in Remote Service Configurator.**

The Database Servers dialog box appears.



2 **Choose Add.**

The New Database Server dialog box opens.



3 In the Name field, type **SAP**.

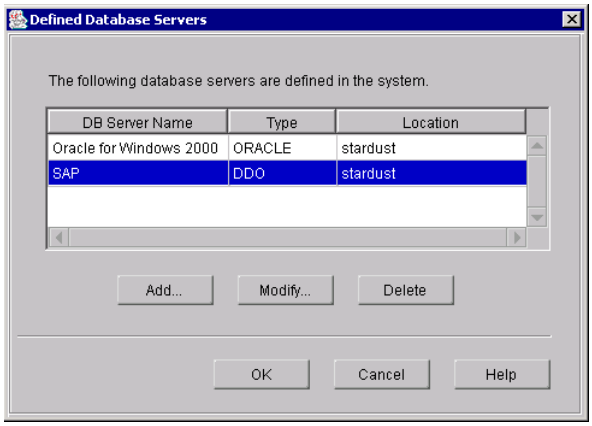
4 In the Type field, select **DDO**.

5 Choose your DDO host from the list.

Note If your DDO host is not in the list, choose **New** and create a new host. For more information about creating a host, see "Adding a New Host" on page 9-7.

6 (Optional) Enter a user name and password for SAP.

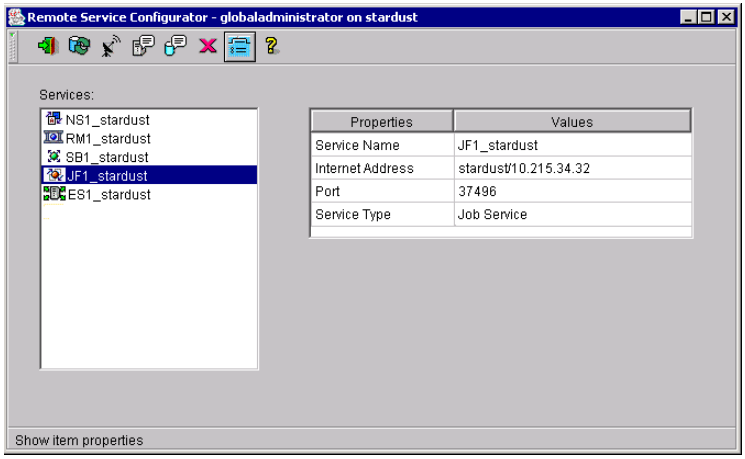
7 Choose **OK** to add the server.



Define Connectivity to the DDO Database Server

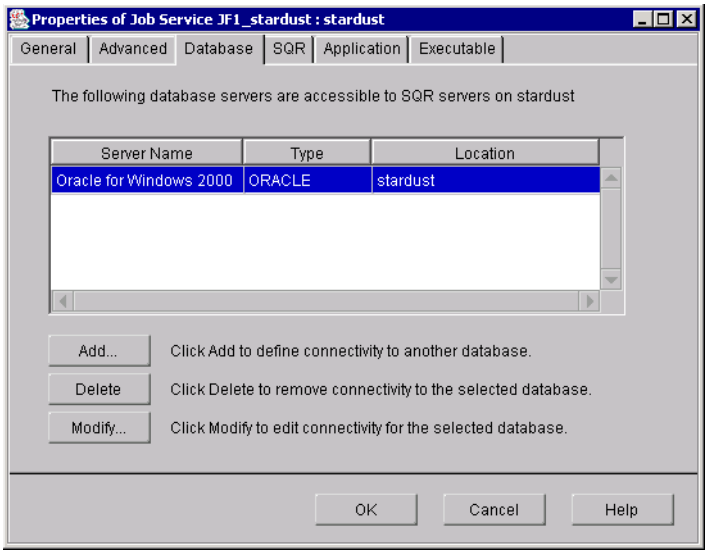
To define connectivity to the DDO Database Server:

1 **Select the Job Service you want to configure for SAP.**

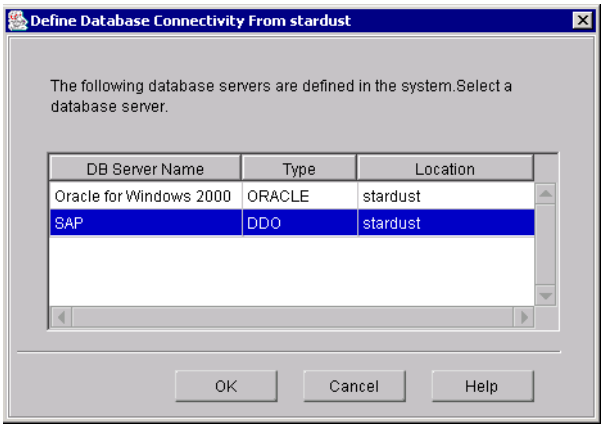


2 Choose the **Show item properties** icon.

3 Select the **Database** tab and choose **Add.**

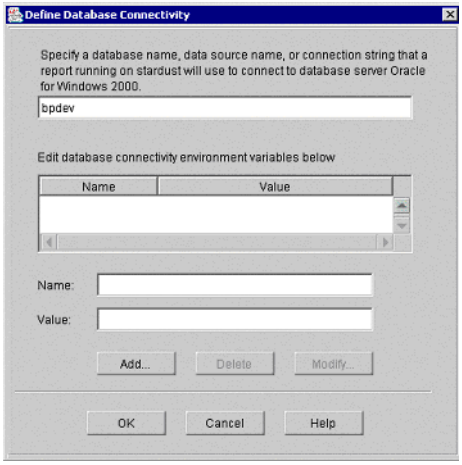


4 **In the Define Database Connectivity From dialog box, choose the SAP database server, and then choose OK.**



5 **In the Define Database Connectivity dialog box, enter the DDO Registry Data Source Name in the first field and choose OK.**

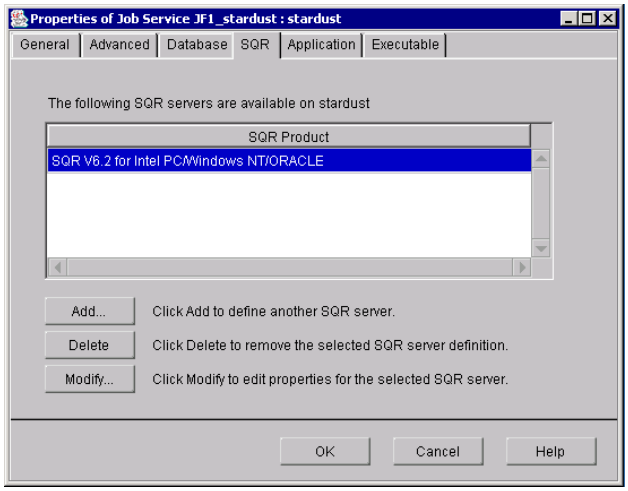
You do not need to enter any environment variables. Your SAP client number and language are defined in the DDO Registry, so you do not need to enter them here.



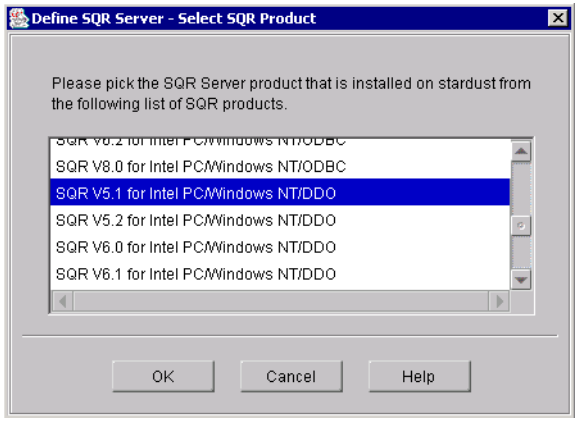
Add an SQR Server

To add a SQR Server:

1 Select the **SQR** tab and choose **Add.**



2 In the Define SQR Server dialog box, select your version of SQR for DDO and choose **OK.**



3 In the Setup SQR Server dialog box, enter the path for SQR and choose **OK.**

4 Choose **OK** to close the Properties dialog box.

Using the ConfigFile Utility

This section discusses how to modify the `config.dat` file and how to set up explicit access to process BQY documents and BQY job output using the ConfigFile utility.

config.dat

Regardless of whether the services are running on Windows or UNIX operating systems, and whether they are running in the common services' process or in separate processes, the RSC services always use the `config.dat` file to begin their startup process.

The `config.dat` file resides in *`Install_Home`*`\BrioPlatform\etc` directory. All RSC services on a host (within an Install_Home) share a `config.dat` file. If you distribute RSC services across several machines, each machine has its own `config.dat` file.

When Name Service starts, it reads the `config.dat` file to get database connectivity and login information. Each of the other RSC services reads this file to get its password, host, and port for Name Service. Name Service gets its configuration information directly from the database. The other RSC services connect to Name Service to get their configuration information.

The `config.dat` file uses plain ASCII text. The passwords contained in the file are encrypted, and you can only modify them using the Remote Service Configurator or the `ConfigFile` utility. This ensures that only people who know the `config.dat` password can modify the service passwords in the file. For details about the `ConfigFile` utility, see "Modifying the Config.dat File" on page 9-51.

To modify the configuration information in `config.dat`, modify service properties using the Remote Service Configurator. The RSC writes your changes to the `config.dat` file.

An example `config.dat` file:

```
++++++++++ BEGIN FILE +++++++++++++
[Setup]
Key=28729638
Password=3A09CF0E38ADEE1FB7273CD9E411

[NameServer]
Name=NS1_KPEREYRA
Login=kpereyra80
Password=3C7752F7785BB0A0A077AB944
JDBC_URL=jdbc:brio:oracle://jasper:1521;SID=jasper
JDBC_DRIVER=com.brio.jdbc.oracle.OracleDriver
Host=KPEREYRA
Port=1498
SAPassword=09DB781FE8A15B866669CA5
[AGENT=RM1_KPEREYRA]
Password=E37EF8D7EC2D7356639FF939B
[AGENT=SB1_KPEREYRA]
Password=64F9F2913D858BD07B5626EBA
[AGENT=JF1_KPEREYRA]
Password=862E7BA8D3C8E2894E7A12D5E5
[AGENT=ES1_KPEREYRA]
Password=240E81E735C5CCC38DEC1B0046
++++++++ END FILE +++++++++++++
```

Modifying the Config.dat File

You can view or modify information in the `config.dat` file by using a simple utility run from the command line, named `ConfigFileAdmin.bat (Windows) or ConfigFile.sh (UNIX)`. This file is located in the directory *`Install_Home`*`\BrioPlatform\bin`.

To run the `ConfigFile` program, specify the `config.dat` file password on the command line after the file name. For example, with the default password, you would type `configfileadmin.bat administrator` (on Windows) or `configfilemenu.sh administrator` (on UNIX).

Some of the tasks you can accomplish with the `ConfigFile` program are:

- Delete a service
- Change services' passwords
- Change the password for access to `config.dat`
- Change the ServletUser password

The main menu of ConfigFileAdmin offers these commands:

```
0) Exit
1) Create New Config File
2) Load Existing Config File
3) Get Name Server Data
4) Modify Name Server Data
5) Add Service Agent
6) Delete Service Agent
7) List Service Agents
8) Get Service Agent Password
9) Change Service Agent Password
10) Change Config File Password
11) Validate Password
12) Encode Password
13) Encrypt Password
14) Miscellaneous Commands Menu
```

To list the properties of the Name Service, such as its database login name and password, select option **3**.

When the Hyperion Performance Suite installation creates a `config.dat` file, it assigns a default `config.dat` file password, namely, *administrator*. This is different from the administrator account password. As a routine matter of system security, you should change the `config.dat` password. You can change it using the `ConfigFile` utility itself, by selecting option **10**.

You can use option **4** to modify the database password that the Name Service uses to connect to the Repository database. Alternatively, you can use the Remote Service Configurator to do so.

Explicit OCE Access to Process BQY Documents/Job Output

By default, no explicit access to the OCE is required to process BQY documents or job outputs using the plug-in or the iHTML interface. To require explicit access, as when a specific database is associated with the BQY document or job output, use the ConfigFileAdmin utility.

This flag is stored in the Repository.

To set a requirement for explicit OCE access to process BQY documents/job out:

1. **At the command prompt, go to the directory** *Install_Home*`\BrioPlatform\bin` **of the Hyperion Foundation server. Enter:**

   `configfileadmin` *`password`*

2. **From the ConfigFileAdmin menu, choose item 14.**

```
.
.
.
11) Validate Password
12) Encode Password
13) Encrypt Password
14) Miscellaneous Commands Menu
```

   Supply the requested information for the database (user) name, database password, database URL, and database driver. You can find this information in the <xref>... section of the `server.xml` file.

3 **From the menu that displays, select item 1.**

```
0) Exit
1) Toggle the SC_ENABLED flag for ServletUser (enables/disables
feature)
2) Update the ServletUser password and re-generate properties
file.
```

4 **After toggling, restart the server, since the Repository Service caches this information.**

ServletUser Password

The special user *ServletUser* has read-only administrative privileges. When the SC_ENABLE flag is set to *true,* the ServletUser sends a request for access to the BQY document/job output on behalf of the user who does not have explicit access to the OCE associated with the document/job output. When the SC_ENABLE flag is set to *false*, the ServletUser cannot make such a request. Only users who have been given explicit access by the publisher to the OCE associated with the BQY document/job output will have access.

The password for the ServletUser is updated in the Repository and stored, encrypted, in *Install_Home*`\servlets\deployment\config\sc.properties`.

To change the password for ServletUser:

1 **At the command prompt, go to the directory** *Install_Home*`\BrioPlatform\bin` **of the Hyperion Foundation server. Enter:**

`configfileadmin` *password*

2 **From the ConfigFileAdmin menu, choose item 14.**

```
.
.
.
11) Validate Password
12) Encode Password
13) Encrypt Password
14) Miscellaneous Commands Menu
```

3 **From the menu that displays, select item 2.**

```
0) Exit
1) Toggle the SC_ENABLED flag for ServletUser (enables/disables
feature)
2) Update the ServletUser password and re-generate properties
file.
```

4 **Enter the information requested.**

5 **Manually update the** `sc.properties` **file on all HPS servlet installations.**

Summary

This chapter details all the properties that can be configured using the RSC Configurator. The properties in the config.dat file, also detailed in this chapter, are configured manually.

10 Configuring the LSC Services and Other System Configuration

All of the Hyperion Foundation services have configurable properties, which you can modify using the Local Service Configurator (LSC) or the Remote Service Configurator (RSC). The LSC and RSC handle different services. In this documentation, these services are referred to simply as LSC services and RSC services.

This chapter explains how to use the LSC Configurator and describes the properties of all of the LSC services. It also explains the properties you can configure in the file `portal.properties`.

In This Chapter

The Local Service Configurator (LSC) 10-2

Modifying Properties of LSC Services 10-5

Modifying the Host Properties. 10-29

Modifying the System Properties 10-34

Registering Hyperion Performance Suite to Hyperion Hub 10-40

The portal.properties File 10-42

The Local Service Configurator (LSC)

The Local Service Configurator allows you to modify the properties of existing installations of the following services:

- Authentication Service
- Authorization Service
- Publisher Service
- Session Manager
- Super Service
- Intelligence Service
- Data Access Service
- Usage Service
- Logging Service
- Global Service Manager
- Local Service Manager

The LSC only modifies service properties; it neither creates nor removes services. To add a service, use the Hyperion Performance Suite installation program. To remove a service, use the ConfigFile... tool. For more information about the ConfigFile... tool, see "Using the ConfigFile Utility" on page 9-49. The LSC cannot configure services on a remote host (nor in a different Install_Home on the same host) or on a system with no GUI capability. The LSC edits the `server.xml` file, as well as some Repository information. The `server.xml` file resides in *`Install_Home`*`\etc`.

Note It is possible to have more than one Hyperion Performance Suite installation, or Install_Home, on a single physical host. A server installation is a set of installed services in the same *Install_Home* directory that run in a single process space. If there are two *Install_Home* directories on a host, they require two separate process spaces.

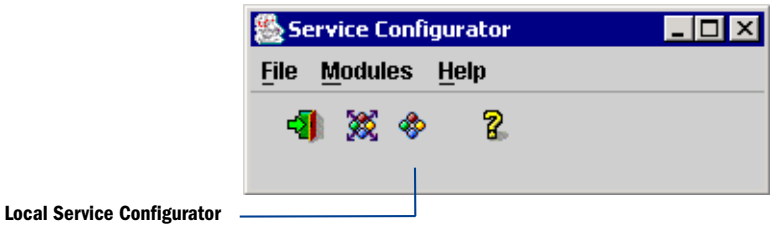
The LSC always edits the `server.xml` in its own Install_Home, which holds configuration information only for the services in that Install_Home.

Starting the Local Service Configurator

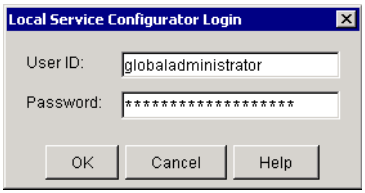
To invoke the Local Service Configurator:

1 **Do either of the following:**

- Choose the **LSC** icon on the main Service Configurator toolbar.
- Select **LSC** from the Module menu on the main Service Configurator toolbar.



2 **Enter your user ID and password in the LSC Login window that appears.**



Note If you log in with a normal user account, you cannot modify authentication systems. You can do everything else. To modify authentication systems, you must be logged in as *globaladministrator*.

The main LSC window appears as shown in Figure 10-2.

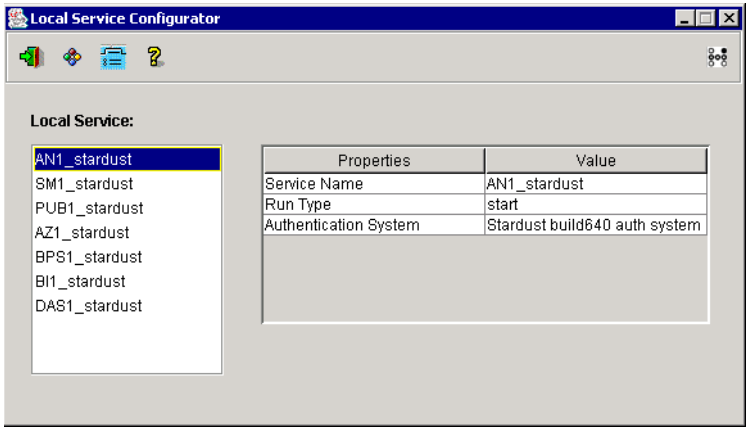


Figure 10-1 Main LSC Window

The left pane of the main window lists the installed services of the Hyperion Performance Suite installation (*Install_Home*) the LSC is running on. Basic properties of the selected service are displayed on the right.

The LSC Toolbar

The toolbar at the top of the main page presents four icons as shown in Figure 10-2.

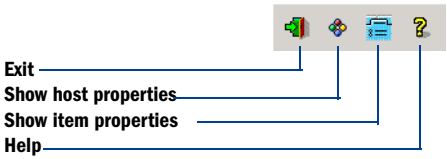


Figure 10-2 LSC toolbar

Choosing the icons results in the following actions:

- **Exit** – Closes the LSC after user's confirmation.
- **Show host properties** – Displays the general properties of the host for editing.
- **Show item properties** – Displays the properties of the selected service for editing.
- **Help** – Displays online help.

The main page consists of a list of the locally installed services and a few basic properties.

Modifying Properties of LSC Services

This section explains how to modify a service's properties, and describes all of the properties you can modify using the LSC.

Figure 10-3 shows the main page of the LSC.

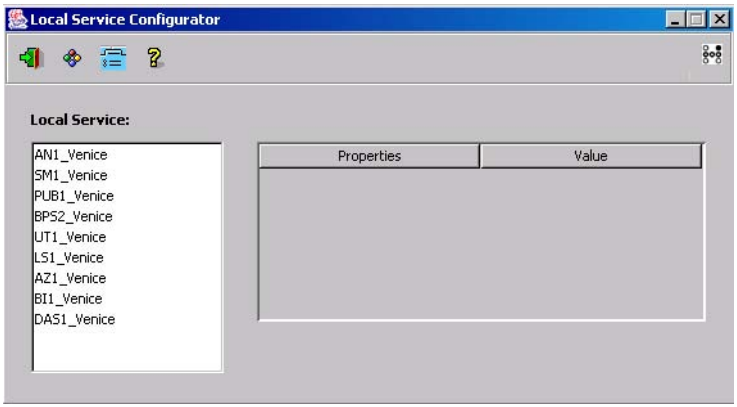


Figure 10-3 Main Page

To modify the properties of a service, do either of the following from the main page of the Local Service Configurator:

- Double-click the name of the service.

- Select the name of the service and choose the **Show service properties** icon on the LSC toolbar.

A tabbed window with editable properties displays. The following sections describe the properties of each service.

Services with Only the Standard Properties

Several of the services have only two properties, which are on the *General* properties page. All LSC services have these two standard properties.

The services that have *only* the two standard properties are:

- Session Manager
- Publisher Service
- Authorization Service
- Usage Service
- Logging Service
- Super service (a special service used only to start the RSC services)

The standard properties are displayed on the General Properties page as shown in Figure 10-4 and Table 10-2.

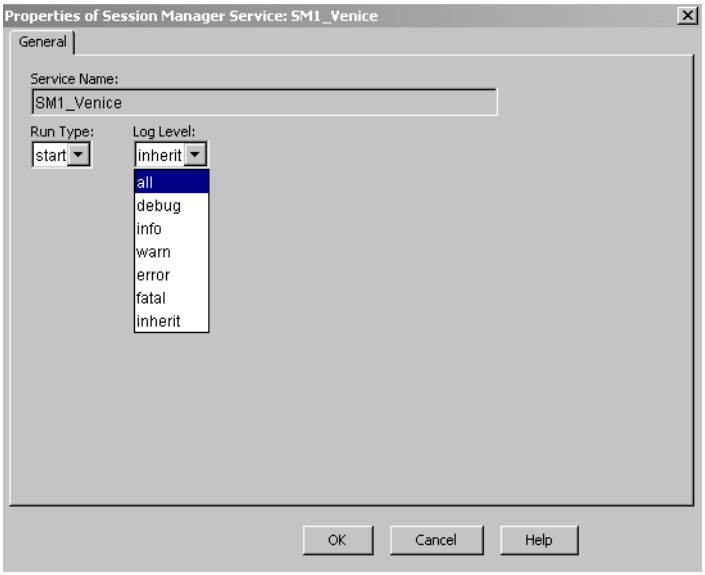


Figure 10-4 General Properties Page

Table 10-1 Standard General Properties

Service Name	(Read-only) The name of the service, assigned during installation.
Run Type	Controls whether the service is started with the other services (by the startCommonServices script or the BrioPlatform Server). Setting *Run Type* to **Start** makes the service active, so it starts with the others. Setting *Run Type* to **Hold** inactivates the service, so it does *not* start with the others. The **Hold** setting is useful for troubleshooting, to temporarily limit which services start.
Log Level	Select the logging level for this service. See “Configuring Log Levels” on page 14-11.

Authentication Service

An Authentication Service has two pages of properties, *General* and *External Driver*.

General Properties

This section describes the properties on the General properties page of an Authentication Service as shown in Figure 10-5 and Table 10-2.

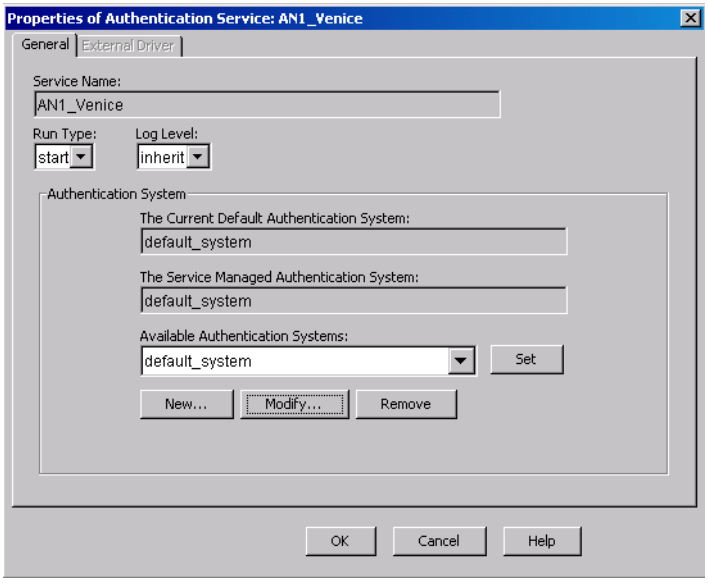


Figure 10-5 Authentication Service’s General Properties Page

Table 10-2 General Properties (Authentication Service)

Service Name	(Read-only) The name of the service, assigned when the service was installed.
Run Type	Controls whether the service is started with the other services (by the startCommonServices script or the BrioPlatform Server). Setting *Run Type* to **Start** makes the service active, so it starts with the others. Setting *Run Type* to **Hold** inactivates the service, so it does *not* start with the others. The **Hold** setting is useful for troubleshooting, to temporarily limit which services start.
Log Level	Set the log level for this service. For detail information on log levels, see "Configuring Log Levels" on page 14-11.
The Current Default Authentication System	(Read-only) Authentication system used if user does not specify one at login. To change which authentication system is the default, modify the system you want to be the default system, and check the *Make this the new default* check box. **Note:** *Current Default Authentication System* applies globally. You can also set the default authentication system at the servlets level, using the Servlet Configurator. When a user logs in, the system looks for an authentication system to use, going through the following list, in order: 1. Authentication system specified by the user in the (Advanced) login dialog 2. The servlets' default authentication system 3. This (global) *Current Default Authentication System* 4. The System authentication system
The Service Managed Authentication System	The authentication system that the local Authentication Service manages. Each Authentication Service can authenticate only users who belong to its *Service Managed Authentication System.*
Available Authentication Systems	To change the current authentication system, choose the desired authentication system from this list, and then choose **Set**.

External Driver Properties

Figure 10-6 shows the page on which you modify the external driver properties of the Authentication Service. Table 10-3 describes the property.

Note Only one authentication system using the security platform driver can be created. Multiple Authentication Services can be set-up to manage this authentication system. Each service should either use the same `css_config.xml` file or should point to the same URL.

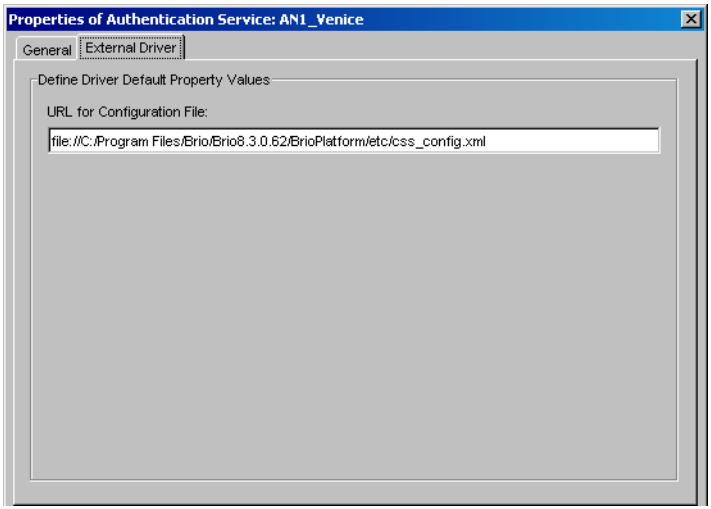


Figure 10-6 External Driver Properties

Table 10-3 External Driver Properties (Authentication Service)

URL for Configuration File	For security platform driver only. Location of the configuration file. The default location is file://localhost/INSTALL_HOME/BrioPlatform/etc/css_config.xml.

Authentication System: Definition and Default Properties

The Definition and Default page of the New/Modify Authentication System wizard appears when you choose **New** or **Modify** from the *General* properties page of the Authentication Service.

Figure 10-7 and Table 10-4 describe the authentication system definition and default properties.

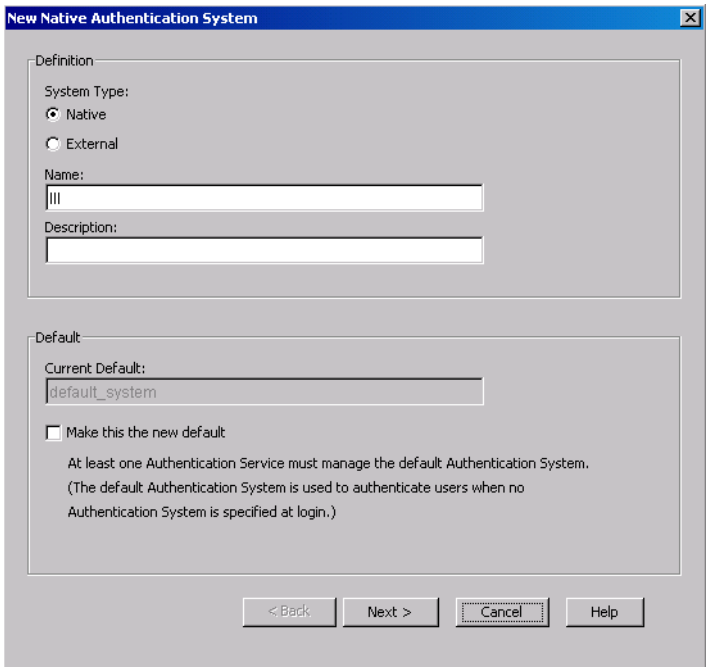


Figure 10-7 Definition and Default Page

Table 10-4 Definition Properties (Authentication System)

Type of Authentication System	*Native:* Authentication system provided by Hyperion Performance Suite. *External:* Allows you to connect to an authentication system outside of Hyperion Performance Suite.
Name	Your name for the authentication system.
Description	Your description of the authentication system.
Current Default	Shows the current default authentication system. At login, a user may choose to specify an authentication system. If the user does not specify one, then *Current Default* is used.
Make This the New Default	To change the default authentication system to the system you are creating or modifying, check this check box.

Pass-Through and Trusted Password

The Pass-Through and Trusted Password page appears when you choose **Next** on the Authentication System Definition and Default page.

For pass-through, it is not necessary to allow the end user to specify their own credentials if database authentication is used, and the reports' data source is the same as the authentication data source. If NT or LDAP authentication is used, or if the user requires the flexibility of using pass-through for multiple data sources, you should require the user to specify their own credentials. You can enable both pass-through options to allow users to choose in Browse Preference if they want to use their login credentials or use credentials specified in Browse Preference.

Note The administrator user and the globaladministrator user are authenticated by the system authentication system. In order for pass-through to work for these users you will need to enable pass-through for the system authentication system.

Figure 10-8 and Table 10-5 describe the authentication system pass-through and trusted password properties.

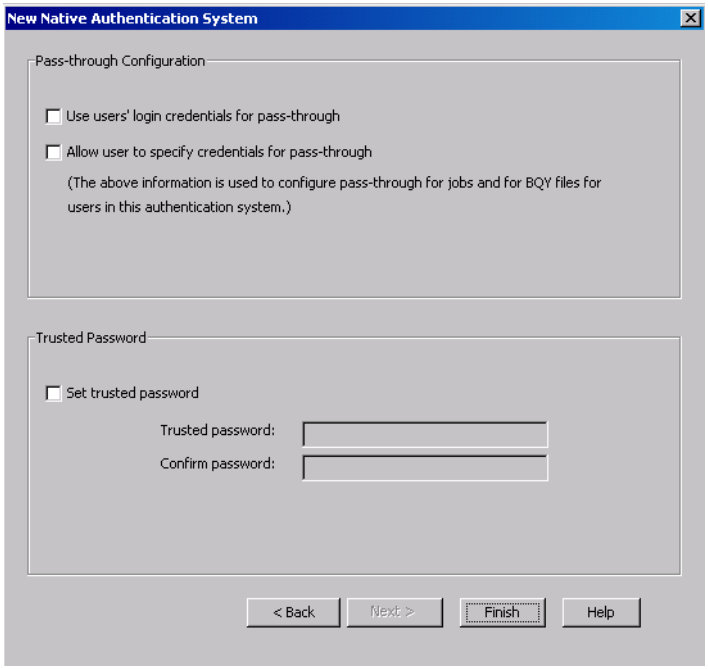


Figure 10-8 Pass-Through and Trusted Password Properties

Table 10-5 Pass-Through and Trusted Password Properties (Authentication System)

Use user's login credentials for pass-through	Pass-through is enabled using the user's login credentials.
Allow user to specify credentials for pass-through	Pass-through is enabled using the credentials the user specifies in Browse Preferences. If no credentials are specified in Browse Preferences, an error message displays each time the user attempts to open a BQY file or run a job.
Trusted Password	To use a trusted password for this authentication system, enable this property. After you check the check box, enter the password in each password field. For more information on trusted passwords, see "Transparent Login" on page 5-10. **Note:** For security reasons, the *administrator* and *globaladministrator* users cannot be authenticated using a trusted password.

External Authentication System: Owner and Driver Properties

The properties for a New External Authentication System display on an additional three pages. Figure 10-9 and Table 10-6 show the owner and driver information properties.

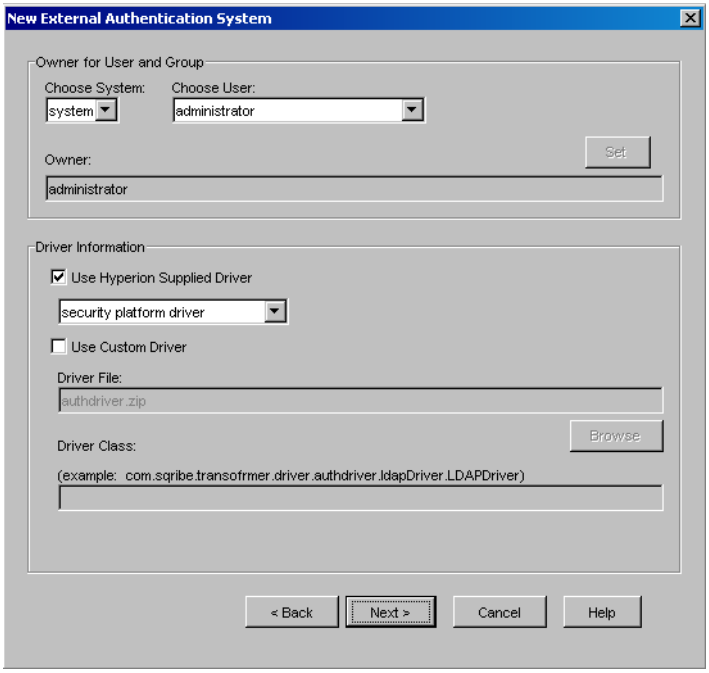


Figure 10-9 Owner and Driver Properties

Table 10-6 Owner and Driver Information (External Authentication System)

Click System	Select an authentication system. The list of users shown in the *Click User* list will be restricted to those in the authentication system specified here.
Click User	Select a user from the drop-down list. To change the Owner field to the currently selected user, choose Set.
Owner	The user that is set as the owner for the users and groups that are automatically imported from the external system. The default publishing access privileges of the owner are used to set the initial access control on these imported users and groups.

Table 10-6 Owner and Driver Information (External Authentication System) *(Continued)*

Use Hyperion Supplied Driver **Use Custom Driver**	Check the applicable box to use either Hyperion-supplied or Custom drivers. Choose the Security Platform Driver to integrate with other Hyperion products using LDAP, MSAD, or NTLM authentication.
Driver File	Name of the driver file. If multiple driver files are specified then they are separated by semi-colons. The semi-colons are automatically added if the user is using the Browse button. If the user types the driver file names, then the semi-colons must by entered manually.
Driver Class	Class of the external authentication driver you want to use.

Note In Hyperion Foundation, the Authentication Service's Repository maintains a complete model of the users and groups in the external system. It does this by synchronizing its view of the users and groups with the external system's list of users and groups at periodic intervals. The last three fields of the Parameters page described in Table 10-7 are for defining how often to do this synchronization.

External Authentication System: Parameters Properties

Figure 10-10 and Table 10-7 show the properties that collect information about importing users and groups from an external authentication system.

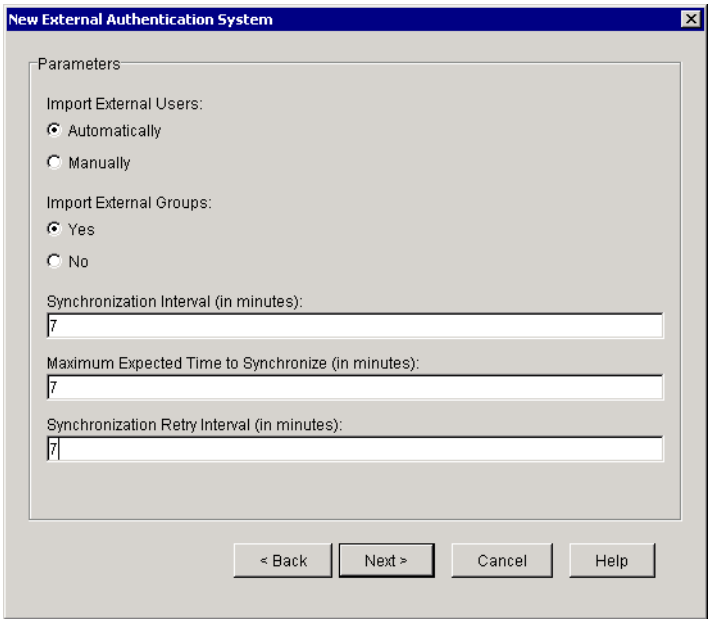


Figure 10-10 Parameter Properties

Table 10-7 Parameters Properties (External Authentication System)

Import External Users	If set to **Automatically**, then users are automatically imported from the external system into the Hyperion Performance Suite system. If set to **Manually**, then users must be manually created (using either the Administration module or the Hyperion Performance Suite API). Each user created in Hyperion Performance Suite must correspond to a valid user in the external system.
Import External Groups	If set to **Yes**, then the groups in the external system are automatically imported. The relationships between users and groups is also automatically imported. If set to **No**, then the external groups are not imported. Groups must be manually created (either via the Administration module or Hyperion Performance Suite API). The group membership must also be manually defined.
Synchronization Interval	How often synchronization should occur, in minutes. In Hyperion Foundation, the Authentication Service's Repository maintains a complete model of the users and groups in the external system. It does this by synchronizing its view of the users and groups with the external system's list of users and groups at periodic intervals.
Maximum Expected TIme to Synchronize	This should be set to the maximum time that synchronization is expected to take, in minutes. This value is used if there are multiple Authentication Services that have been set up to manage the same Authentication System. In this case, only one Authentication Service will be synchronizing at any one time. This value is used by the peer Authentication Services (who are not synchronizing) to determine if the Authentication Service that is synchronizing has died before completing synchronization.
Synchronization Retry Interval	If synchronization fails, this is used to indicate how long to wait, in minutes, before retrying synchronization.

External Authentication System: Driver Default Properties

Figure 10-11 and Table 10-8 show the external driver property values.

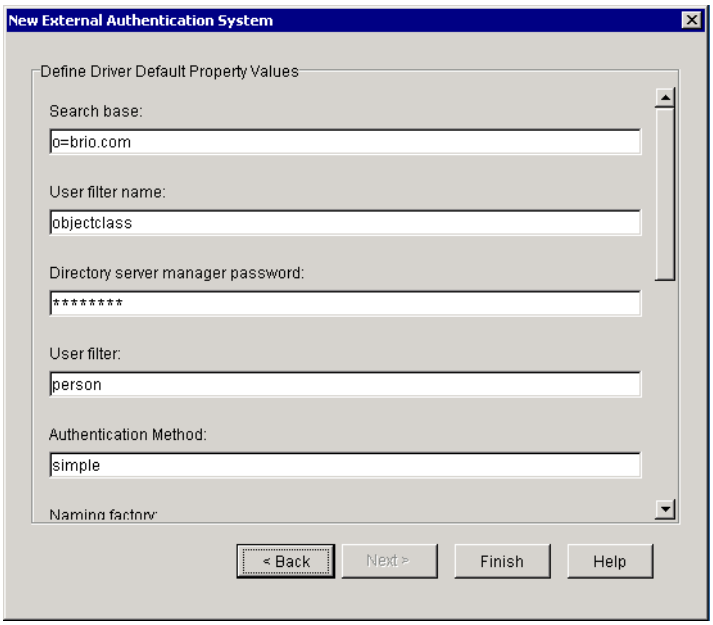


Figure 10-11 Driver Default Properties

Note The dialog you see may differ from the figure and the descriptions, according to which driver's properties you are viewing. All of the properties described in the table are those of an LDAP driver except for the first property.

Table 10-8 External Driver Properties (External Authentication System)

URL for Configuration File	For security platform drivers only. Location of the configuration file. The default location is file://localhost/INSTALL_HOME/BrioPlatform/etc/css_config.xml.
Naming factory	Name of Java class that implements the InitialContextFactory interface.
Directory server URL	URL to access the directory server.
Search Base	The path to the entry in the directory tree at which to search for users and groups.

Table 10-8 External Driver Properties (External Authentication System) *(Continued)*

Directory server manager	The distinguished name of the directory manager (or other user) entry. This user should have read access to the entire sub-tree specified in the Search Base. For example, *CN=Directory Manager*, *O=Hyperion*, *C=US*.
Directory server manager password	Password for the directory server manager account.
User identification symbol	The identification for the user attribute in the Distinguished Names (DN).
Group filter name	Identifier for the object class attribute for a group.
Group filter	Name of the object class for a group.
User filter name	Identifier for the object class attribute for a user.
User filter	Name of the object class for a user.
Group membership filter	Identifier for the group membership attribute.
Authentication method	Preference for the strength of authentication. Only *simple* is supported.

Adding a New *Native* Authentication System

To add a new native authentication system:

1. **Choose New from the Authentication System Properties page.**

   The Authentication System Definition and Default Page appears.

2. **Under System Type, select Native.**

3. **Fill in the remaining authentication system definition properties as described in Table 10-4 and choose Next.**

   The Pass-through and trusted password Authentication System Page appears.

4. **View the default authentication properties as described in Table 10-5.**

5. **Choose Finish.**

6. **Choose Yes when prompted to save the new authentication system to the database.**

Adding a New *External* Authentication System

Only one authentication system using the security platform driver is allowed per system.

To add a new external authentication system:

1. **Choose New from the Authentication System Properties page.**

   The Authentication System Definition Page appears.

2. **Under *System Type*, select External.**

3. **Fill in the authentication system definition and view the default properties as described in Table 10-4 and choose Next.**

   The Pass-through and Trusted Password Authentication System Page appears.

4. **Fill in the pass-through and trusted password properties as described in Table 10-5 and choose Next.**

   The Owner and Driver Information Page appears.

5. **Fill in the owner and driver information as described in Table 10-6 and choose Next.**

   The Parameters Page appears.

6. **Fill in the parameters as described in Table 10-7 and choose Next.**

   The Define Driver Default Property Values Page appears.

7. **Fill in the parameters as described in Table 10-3.**

8. **Choose Finish.**

9. **Choose Yes when prompted to save the new authentication system to the database.**

Note If you develop a *custom* external authentication driver, use the `setConfidential` method on confidential properties, such as passwords. All properties of external authentication drivers are logged *except* those marked as confidential by the `setConfidential` method. For more information, see the Hyperion Performance Suite SDK.

Intelligence Service

The Intelligence Service has additional General properties.

General Properties

Figure 10-12 and Table 10-9 display the Intelligence Service's General properties:

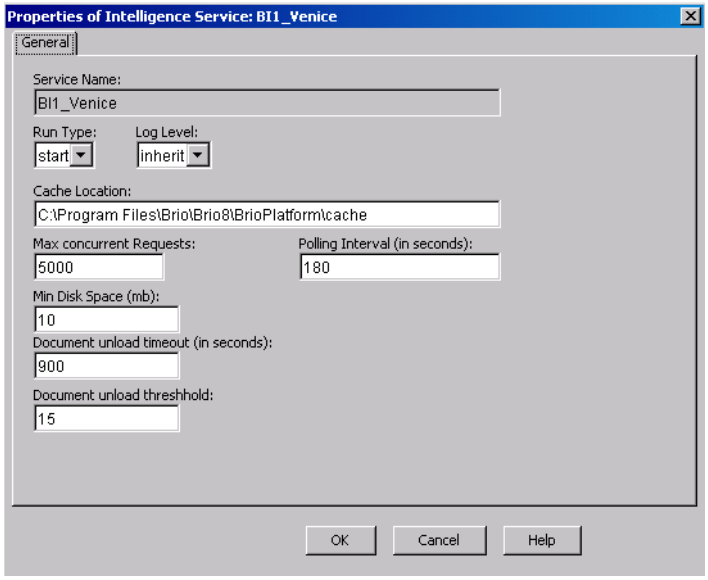


Figure 10-12 Intelligence Service General Properties

Table 10-9 General Properties

Service Name	(Read-only) The name of the service, assigned when the service was installed.
Run Type	Controls whether the service is started with the other services (by the startCommonServices script or the BrioPlatform Server). Setting *Run Type* to **Start** makes the service active, so it starts with the others. Setting *Run Type* to **Hold** inactivates the service, so it does *not* start with the others. The **Hold** setting is useful for troubleshooting, to temporarily limit which services start.
Log Level	Set the log level for this service. For detail information on the log levels, see "Configuring Log Levels" on page 14-11.
Cache Location	The name of the directory where the service's temporary files are stored. For example, if you want to set the cache location to your d: drive, you would type: **D:\\temp**.
Max Concurrent Requests	The maximum number of concurrent requests the service supports. Requests that exceed the number in this field will be blocked. For example, if you want to block the number of concurrent requests after 4999, you would type: **5000**.
Polling Interval	Controls how often the service checks for the "Document Unload Timeout" setting. For example, if you want the service to poll every 180 seconds, you would type: **180**.
Min. Disk space (mb)	Sets the minimum disk space (Mb) required to service a new request. For example. if you want to allocate 10 Mb as the minimum disk space, you would type: **10**.
Document Unload Timeout	Sets the inactive time in seconds after which the document can be unloaded from memory to conserve system resources. For example, if you want a document to remain in memory no longer than 30 minutes after it was last used, you would type **1800**.
Document Unload Threshold	The document unloading mechanism is activated when the number of open documents exceeds the number specified here. For example, if you want a maximum of 15 open documents, you would type: **15**.

Fonts for Unix

If your Unix users want their BQY documents to have a consistent look and feel, you need to make either Type1, TrueType, or OpenType fonts available to the Intelligence Service. For a Windows-like look and feel you should download Microsoft's TrueType web fonts.

If you currently have Type1, TrueType, or OpenType fonts, perform Step 5 and Step 6 below to make your fonts available to the Intelligence Service.

If you currently have Type1, TrueType, or OpenType fonts, but do not have a fonts.dir file, you will need to perform Step 4, Step 5, and Step 6 below.

To make Microsoft's TrueType web fonts available to the Intelligence Service when you do not have Type1, Truetype, or OpenType fonts:

1. **Download the Microsoft TrueType web fonts from** `http://sourceforge.net/projects/corefonts/ or other source.`

2. **Create a new directory, <directory>.**

3. **Extract each CAB file (*.exe) into the newly created directory using the cabextract utility located in** *Install_Home*/BrioPlatform/bin.

   Install_Home/BrioPlatform/bin/cabextract -d <directory> <CAB file>

4. **Create a fonts.dir file in the directory containing the font files using the ttmkfdir utility located in** *Install_Home*/BrioPlatform/bin.

   Install_Home/BrioPlatform/bin/ttmkfdir -d <directory> -o <directory>/fonts.dir

5. **Set the environmental variable** BQ_FONT_PATH **to the directory where the fonts.dir file was created.**

   Add this variable to the start-up script to save your changes.

   In the start-up script, BQ_FONT_PATH=<directory>, export BQ_FONT_PATH.

   This environmental variable can contain colon separated paths to directories containing the fonts.dir file.

6. **Restart the Intelligence Service.**

Data Access Service

The Data Access Service properties are displayed on two tabs: General Properties and Data Source Properties. The General Properties are for fine-tuning the DAS performance and the Data Source Properties all pertain to DAS and database connections.

General Properties

All of the following advanced option settings can be used to fine-tune the Data Access Service (DAS) performance.

Figure 10-13 and Table 10-10 detail the Data Access Service's General properties:

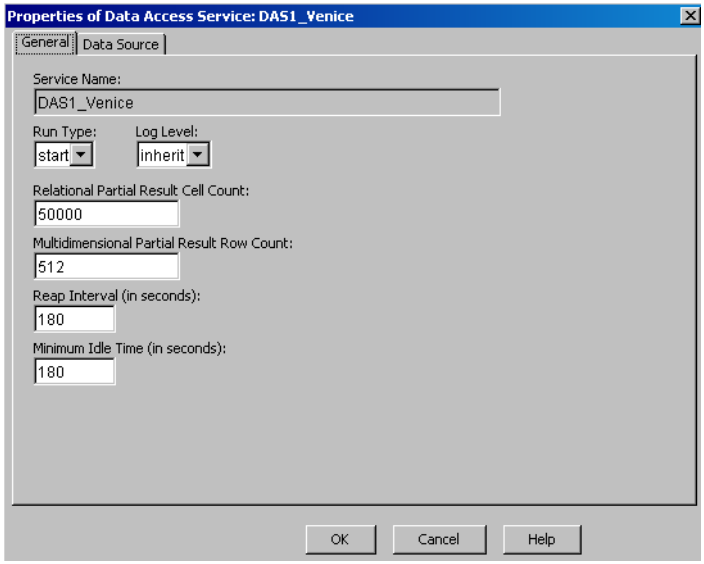


Figure 10-13 Data Access Service's General Properties

Table 10-10 General Properties

Service Name	(Read-only) The name of the service, assigned when the service was installed.
Run Type	Controls whether the service is started with the other services (by the startCommonServices script or the BrioPlatform Server). Setting *Run Type* to **Start** makes the service active, so it starts with the others. Setting *Run Type* to **Hold** inactivates the service, so it does *not* start with the others. The **Hold** setting is useful for troubleshooting, to temporarily limit which services start.
Log Level	Set the log level for this service. For detail information on the log levels, see "Configuring Log Levels" on page 14-11.
Relational Partial Result Cell Count	Determines the maximum number of relational data table cells that a block of result data from a query can contain when sent from the DAS to the client. The default value is 2048; the minimum is 1.
Multidimensional Partial Result Row Count	Determines the maximum number of multidimensional data table rows that a block of result data from a query can contain when sent from the DAS to the client. The default value is 512; the minimum is 1.
Reap Interval	Determines the frequency in seconds that the DAS program should try to clear any query data from memory whose requesting client is assumed to have disconnected. The default value is 180; the minimum is 5.
Minimum Idle Time	Determines the minimum number of seconds that query data should be kept in memory for the client to retrieve before assuming that the client has disconnected. The default value is 180; the minimum is 0.

Data Source Properties

The Data Source properties page lists all of the currently defined data sources for the current Data Access Service. Scroll to the right, using the horizontal scroll bar, to see properties that are not initially visible.

Figure 10-14 and Table 10-11 display the data source properties.

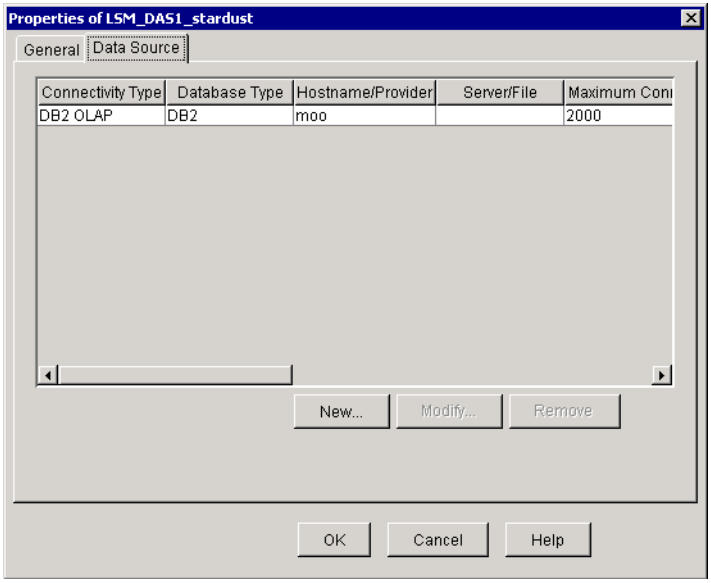


Figure 10-14 Data Source Properties

From the Data Source properties page, you can do the following:

- **Modify properties of an existing data source** – Select the data source you want to modify, and then choose **Modify**.
- **Create a new data source** – choose **New**.
- **Remove a data source** – Select the data source you want to remove, and choose **Remove**.

The dialog boxes for modifying or adding a data source present the same fields as are displayed on the Data Source page.

Table 10-11 Data Source Properties

Connectivity Type	Choose a database driver for the data source. The chosen driver must be installed on the host of a DAS. The *Connectivity Type* is used only to route requests to an appropriate DAS. It is assumed that the appropriate database client software to actually connect to the requested database is installed and properly configured on each host where DAS is configured to accept routed requests for database access.
Database Type	Choose the vendor-specific database type for the data source. The *Database Type* is used only to route requests to an appropriate DAS. It is assumed that the appropriate database client software to actually connect to the requested database is installed and properly configured on each host where DAS is configured to accept routed requests for database access. Whether a DAS can connect to a specific database is determined by the OCE file and the database drivers installed.
Name of data source	The database host name or logical data source name. The *Name of Data Source* is used only to route requests to an appropriate DAS.It is assumed that the appropriate database client software to actually connect to the requested database is installed and properly configured on each host where DAS is configured to accept routed requests for database access. For OLE DB database connections, this corresponds to the OLE DB Provider identifier.
Server/File	(For OLE DB only) The server file or data source name used for database connections. The *Server/File* is used only to route requests to an appropriate DAS. It is assumed that the appropriate database client software to actually connect to the requested database is installed and properly configured on each host where DAS is configured to accept routed requests for database access.
Maximum Connections to DB	Determines the maximum number of connections permitted from the DAS process to the datasource, using the current driver. The default value is 2048; the minimum is 0.

Table 10-11 Data Source Properties *(Continued)*

Maximum Queue Size	Determines the maximum number of requests that can simultaneously wait to obtain a connection to the database server. The default value is 100; the minimum is 0.
Minimum Idle Time	Determines the minimum number of seconds that an unused database connection should be kept open before closing it. The default value is 180; the minimum is 0.
Reap Interval	Frequency (in seconds) at which the system should check for unused database connections and close them.The default value is 180; the minimum is 5.
Maximum Connections in Pool	Determines the upper limit of the number of unused database connections that can be kept open at any time for a particular database user name/OCE combination. The default value is 1000; the minimum is 0.
Minimum Pool Idle Time	Minimum number of seconds that unused connections for a particular database user name/OCE combination should be kept in memory. The default value is 180; the minimum is 0.

Adding a New Data Source

When adding new data source you must match certain DAS properties with corresponding OCE properties. An OCE file is used by the client program to determine which DAS to use and an OCE file is used by DAS to make the connection to the database. Table 10-12 shows the DAS properties (set in the LSC) that must match specific OCE properties (set in Hyperion Intelligence Designer):

Table 10-12 Corresponding DAS and OCE Properties

DAS Properties (in LSC)	OCE Properties (in Designer)
Connectivity type	Connection software
Database type	Database type
Name of data source	Host or provider (OLE DB)

After you choose **New** from the Data Source properties page, the following dialog box (shown in the following figureFigure 10-15) displays:

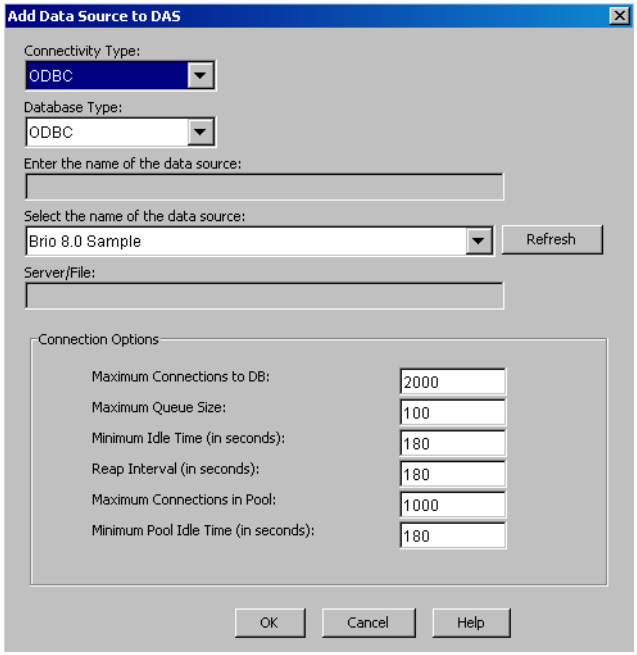


Figure 10-15 New Data Source Properties

Fill in the fields to create the new data source. The properties are described in "Data Source Properties" on page 10-25.

To create a new OLE DB data source connection:

1. **Select OLE DB for the connectivity type.**
2. **Select OLE DB for the database type.**
3. **Select the name of the data source from the drop-down list.**
4. **For the server/file field, enter the host name where the database is running.**
5. **Restart the services and the servlets.**

Modifying the Host Properties

You can use the LSC to modify properties of the host (or *Install_Home*) on which you are running the LSC.

Note Services that are installed under the same *Install_Home* directory are collectively called a "Install_Home." They run in a single process space. There can be more than one Install_Home on a single physical host, running in separate process spaces.

The "host" properties technically belong to the current Install_Home, rather than the host. In the case of a host that has multiple Install_Homes, these properties pertain to the Install_Home whose LSC you are running. Nonetheless, for simplicity, and because most hosts have only one Install_Home, these properties are referred to as the "host's" properties.

The host properties display on two tabs:

- General Properties

  Includes properties of the GSM and LSM that manage this host/*Install_Home*.

- Database Properties

  Includes properties related to the Repository database, such as the database driver and the database password used by the services.

To modify the host properties:

1. **From the main window of the Local Service Configurator, choose the Open General Properties Dialog icon (second from the left on the toolbar).**
2. **Set properties as desired on each of the three tabs.**

   The properties are described in the tables following these steps.
3. **Choose OK when finished.**

General Properties

The properties on the host's (Install_Home's) General tab include specification of the system's Global Service Manager (GSM) and the host's Local Service Manager (LSM). The General tab properties are as follows:

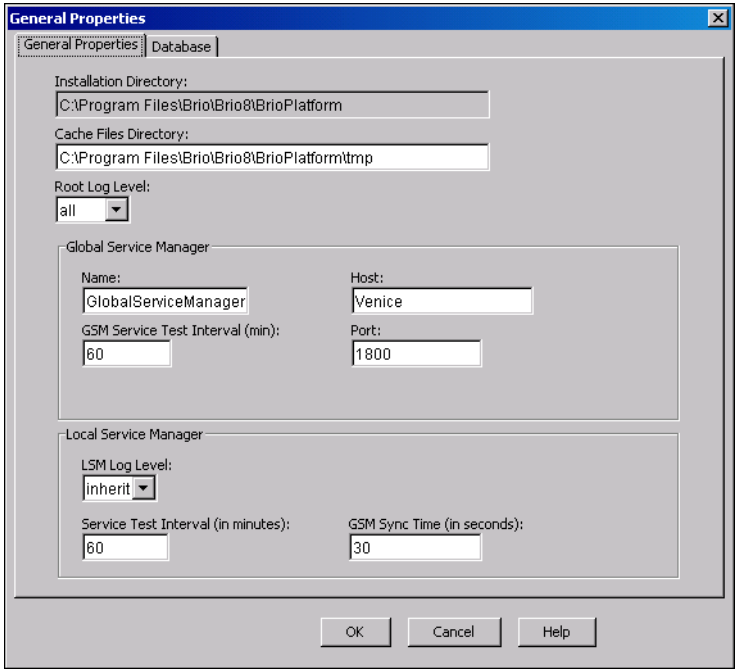


Table 10-13 General Properties of Host

Installation Directory	(Read-only) Path to the BrioPlatform directory where the Hyperion Foundation services are installed.
Cache Files Directory	Directory where temp files are stored for caching of user interface elements and listings of content.
Root Log Level	Set the log level for all of the services. For detail information on the log levels, see “Configuring Log Levels” on page 14-11.
GSM: Name	(Read-only) The name of the GSM that manages the host’s (or Install_Home’s) services.
GSM: Service Test Interval	Indicates in minutes how often the GSM checks whether registered services on all hosts are running.
GSM: Host	Machine on which the GSM is installed. This is the *Server* referred to in the Login screen.
GSM: Port	Port number on which the GSM is running. This is the *Port* referred to in the Login screen.
LSM: Log Level	Set the log level for this service. For detail information on the log levels, see “Configuring Log Levels” on page 14-11.
LSM: Service Test Interval	Indicates in minutes how often the LSM checks that the other local services are running.
LSM: GSM Sync Time	Indicates in seconds how often the LSM synchronizes its information with the GSM.

Database Properties

The Database properties of a host (Install_Home) are as follows:

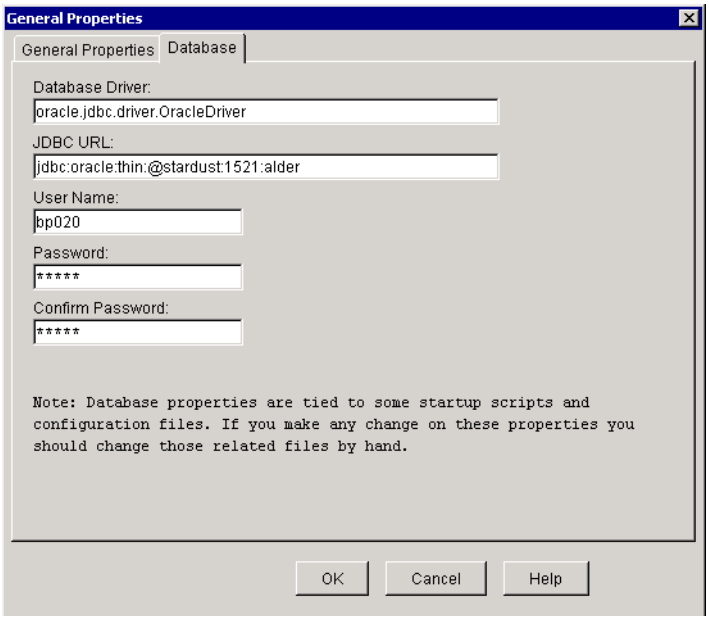


Table 10-14 Database Properties of Host

Database Driver	The name of the driver used to access the database. This is database-dependent, and should only be changed by an experienced administrator. If you change the *Database Driver*, you must change other files, properties, data in the database, and the Java classpath. For details, see "Changing the Database Driver or JDBC URL" on page 9-14.
JDBC URL	The URL for Java access to the database via the JDBC driver. If you change the *JDBC URL*, you must change other files, properties, and data in the database. For details, see "Changing the Database Driver or JDBC URL" on page 9-14.
User Name	The user name that the services will use to access the database containing their metadata. This name must be the same for all installations using the same GSM.
Password	The valid password for the *User Name*.

The Database Properties of a host (or Install_Home) rarely should be changed. But if you do need to change any of them, you must also change other files. The following all have database information for services and must be kept in sync:

- `server.xml` – Use the LSC to modify this configuration file.
- `config.dat` – Use the configFile... utility to modify this configuration file.
- Every RSC service – You must set properties on *every* RSC service individually
- `startCommonServices` script
- All service-specific start scripts

Specific instructions for changing some of the database properties are given in "Changing the Database Password" on page 9-12, and in "Changing the Database Driver or JDBC URL" on page 9-14.

Modifying the System Properties

The *system properties* apply globally to a Hyperion Performance Suite system. The system properties are accessed from the Administration module.

To modify the system properties:

1. **Select Administration from the module drop-down list.**
2. **Select System tab and navigate to the properties you want to modify.**

   See the tables below for detailed information about the properties.
3. **Choose Save Properties.**

Note Properties that require restarting the system server are noted in the tables.

General Properties

The system properties on the General page are detailed in Figure 10-16 and Table 10-15:

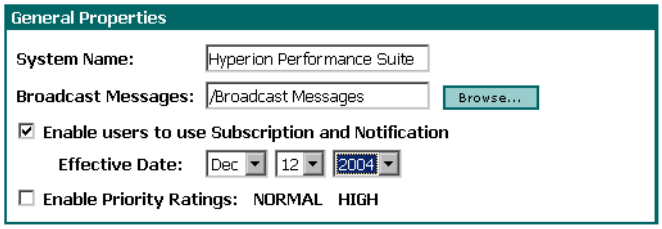


Figure 10-16 General Properties

Table 10-15 General Properties (System)

System Name	This is the name you use to define your installation and distinguish it from other Hyperion Performance Suite installations. An installation can be defined as the system served by exactly one GSM.
Broadcast Messages	Enter the name of the folder in which you want to store broadcast messages for users of the Browse module. The folder must already exist.
Enable users to use Subscription and Notification	Enable to use the subscription and notification features. When this option is on, publishing events are logged. The publishing event log enables the Event Service to identify subscription matches and notify users of changes in items they have subscribed to.
Effective Date	Enter a date for the logging to begin.
Enable Priority Ratings	Turn this property on to allow users to set priority ratings on items they publish in the Browse module.

Notification Properties

The system properties on the Notification page are detailed in Figure 10-17 and Table 10-16:

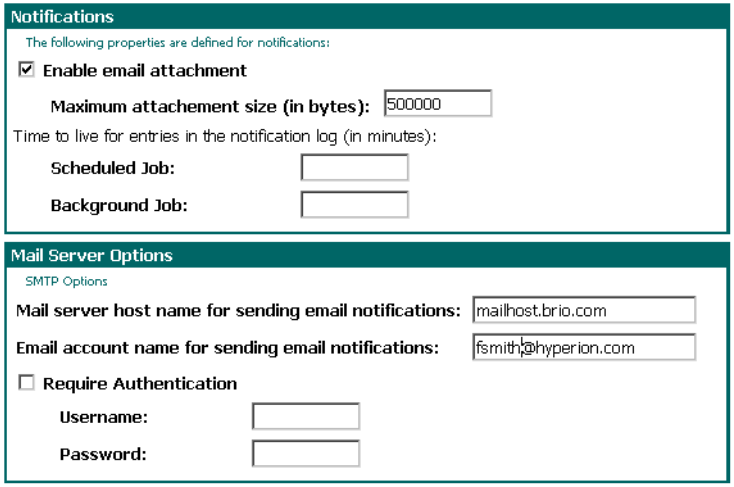


Figure 10-17 Notification Properties

Table 10-16 Notification Properties (System)

Enable email attachment	Enable to allow users to send file attachments with their email notifications. For a job that generates only one output file, that file is attached to the email, regardless of its type. For a job that generates multiple output files: if one is a PDF file, that file is attached; if there is no PDF output file, the email has no attachment. If you change this property, you must restart the Hyperion Performance Suite server for the new setting to take effect.
Maximum attachment size	Specify the maximum allowed size for attachments, in bytes. If you change this property, you must restart the Hyperion Performance Suite server for the new maximum attachment size to take effect.
Time to live for entries in the notification log	Enter a time (in minutes) after which events will be removed from the notification log and will no longer appear to users in the Browse module. You can specify different expiration times for scheduled jobs and background jobs.
Mail server host name for sending email notifications	Enter the mail server host name for sending notifications. If you change this property, you must restart the Hyperion Performance Suite server for the new mail server host name to take effect.
Email account name for sending email notifications	Enter the email account name for sending email notifications. If you change this property, you must restart the Hyperion Performance Suite server for the new email account name to take effect.
Require authentication	Enable to require authentication (ASMTP). Enter username and password when enabled. Default is disabled.

After specifying the appropriate notification properties, you can select **Send Test Email**, which displays a pop-up indicating your entries for mail server and an interface to enter the destination email address.

SmartCut Properties

SmartCut properties are used to construct SmartCuts that are included in email notifications. The URL for any SmartCut is the following:

`http://Host:IP Port/Root/SmartCut`

(Alternatively, a SmartCut may start with `https` instead of `http`.) For more information about SmartCuts, see

The SmartCut page of the system properties is detailed in the following figure and tableFigure 10-18 and Table 10-17:

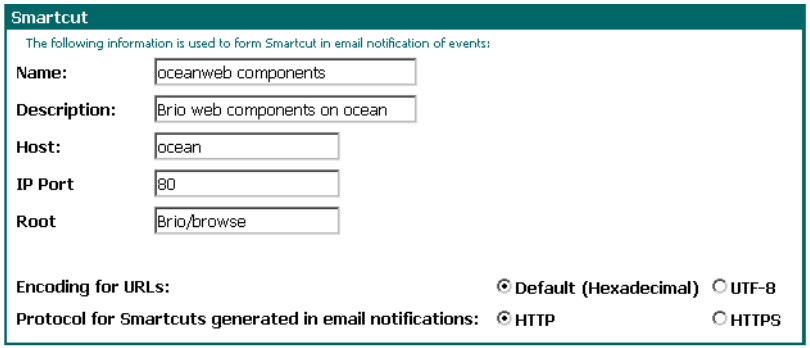


Figure 10-18 SmartCut Properties

Table 10-17 SmartCuts Properties (System)

Name	Enter a name for the Browse servlet referenced in any SmartCuts that are part of email notifications sent to users. If you change this property, you must restart the Hyperion Performance Suite server and Job Service for the new name to take effect.
Description	Enter a description of the Browse servlet. If you change this property, you must restart the Hyperion Performance Suite server and Job Service for the new description to take effect.
Host	From the drop-down list, select the host on which the Browse servlet resides. If the host is not in the list, choose **New**, enter the name and platform of the host, and choose **OK**. If you change this property, you must restart the Hyperion Performance Suite server and Job Service for the new host to take effect.

Table 10-17 SmartCuts Properties (System) *(Continued)*

IP Port	Enter the port number on which the Browse servlet runs. If you change this property, you must restart the Hyperion Performance Suite server and Job Service for the new IP Port to take effect.
Root	The web application deployment name for the Browse servlet, as set in your web server software. Typically, this path is `Hyperion\browse`. The last segment (typically, `browse`) must match the servlet name specified during installation. If you change this property, you must restart the Hyperion Performance Suite server and Job Service for the new setting to take effect.
Protocol for SmartCuts generated in email notifications	Specify either HTTP or HTTPS as the protocol to use for SmartCuts generated in email notifications. If you change this property, you must restart the Hyperion Performance Suite server for the new setting to take effect.
Encoding for URLs	Specify how Hyperion Performance Suite encodes (and decodes) URLs. This property can take one of two values: *Default* – Uses the standard encoding of URLs as defined in RFC 2396. In particular, the subset of ASCII characters which are valid in URLs are left as is. The space character is converted to `%20`. All other characters are converted into the 3-character string "%xy" where xy is the two-digit hexadecimal representation of the lower 8-bits of the character. Since this encoding uses only the lower 8-bits of a character, this default encoding is only appropriate for installations using Latin-1 languages. *UTF-8* – Uses the encoding of URLs as recommended in RFC 2718. In particular, non-allowable characters are first converted into UTF8 and then each resulting byte is converted to its %xy representation. This encoding must be used for installations supporting non-Latin-1 languages or installations using the WebSphere or Sun ONE native servlet engines.

User Interface

You, as the administrator, set how many users/groups/roles will be displayed in the access control group when users set or modify the access control of an item.

The User Interface properties are detailed in Figure 10-19 and Table 10-18:

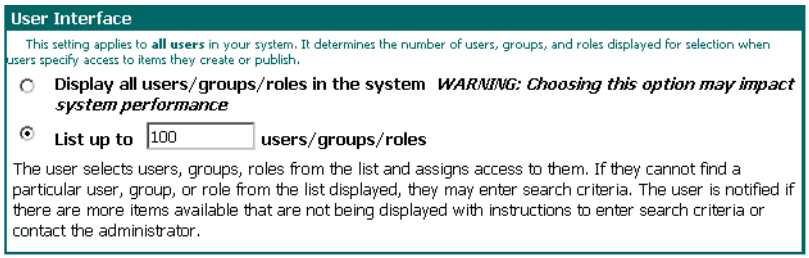


Figure 10-19 User Interface Properties

Table 10-18 User Interface Properties

Display all users/groups/roles in the system	Enable this to display all users/groups/roles in the system that the user has access to when they are setting or modifying access control. Choosing this option may impact system performance.
List up to __ users/groups/roles	Enable this to set how many users/groups/roles will be displayed when the user is setting or modifying access control. This option, set at 100, is the default. If this is set too low users could possibly not get the full list of users/groups/roles that they have access to.

Registering Hyperion Performance Suite to Hyperion Hub

You will need access to a username authenticated through the security platform driver. This username must also be authenticated on the same external system for all of the applications you want to access. For example, you use username Tom to register to Hyperion Hub. Tom is authenticated against NT for Hyperion Report, Hyperion Hub, and for Hyperion Performance Suite. Tom is authenticated against LDAP for Hyperion Analyzer. The Hyperion Performance Suite will not have access to Hyperion Analyzer in this scenario.

You can register to Hyperion Hub so other applications can or cannot access content from Hyperion Performance Suite . See Figure 10-20 and Table 10-19 below for detailed information about which properties to use for each scenario.

To configure Hyperion Hub properties using the Administration module:

1. Select **Administration** from the drop-down module list.
2. Select the **System** tab.
3. Select **Manage Settings under Hyperion Hub on** the navigation pane.
4. Configure or modify the properties.

   See Figure 10-20 and Table 10-19 below for detailed information about the properties.
5. Choose **Apply** to save settings.

Note If Hyperion Hub registration changes, you need to restart your application server.

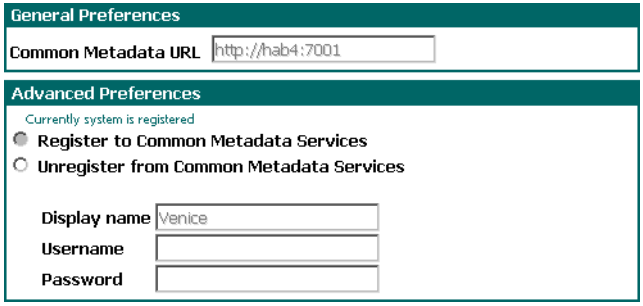


Figure 10-20 Hyperion Hub Properties

Table 10-19 Hyperion Hub Properties

Hyperion Hub URL	Specify the URL to the Hyperion Hub. This field cannot be changed when registered to the Hyperion Hub.
Register to Hyperion Hub	Select to register Hyperion Performance Suite. This option allows sharing contents between all registered Hyperion applications.
Unregister from Hyperion Hub	Select to unregister Hyperion Performance Suite. This option does not give other Hyperion applications access to contents from Hyperion Performance Suite.
Display Name	Usually the host name, but can be any unique name used to identify this system. Grayed out when not registered.
Username	For non-security platform driver users, enter a valid user who was authenticated by the platform security driver. Grayed out when not registered.
Password	For non-security platform driver users, enter a the password for the user above. Grayed out when not registered.

Managing Row-Level Security

Configure properties for row-level security through the system tab of the Administration module. The properties are stored in the database repository.

To configure properties for row-level security:

1. **Select Administration from the drop-down module list.**
2. **Select the System tab.**
3. **Select Manage Row Level Security from the navigation pane.**
4. **Change the properties.**

   See the table below for property details.
5. **Choose Save Properties.**

   See Appendix A, “Row-Level Security in BQY Documents,” for row-level security implementation details.

The row-level security properties are explained in Figure 10-21 and Table 10-20:

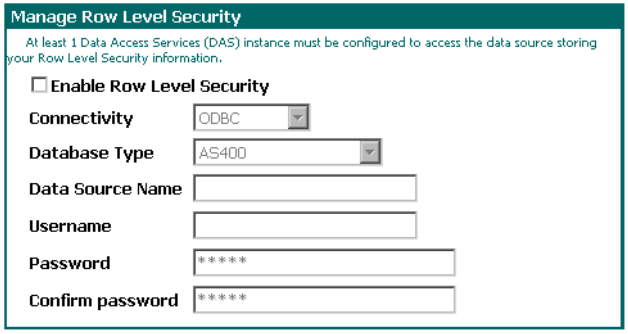


Figure 10-21 Row-Level Security Properties

Table 10-20 Row -Level Security Properties of Host

Enable Row Level Security	Enable when using Row-Level Security. The default is disabled.
Connectivity	Database connectivity information for reports' source data. Select the appropriate connectivity information from the drop-down list.
Database Type	Type of database that you are using. Select the appropriate database type from the drop-down list. The list of database types is dependent on the connectivity selection.
Data Source Name	The host of the report data source database.
User Name	The default database user name used by Job Service for running SQR programs on this database server. This user name is used for jobs that were published with no database user name/password specified.
Password	The valid password for the *User Name*.

The portal.properties File

A few properties are configured in a text file that you edit directly. This file is `portal.properties`, located in *`Install_Home`*`\BrioPlatform\lib\msgs`. The following table describes the properties it contains.

To edit `portal.properties`, use any plain text editor. To change the value of any property, edit the string that follows its equal sign (=). Change any or all value strings. However, do not modify the file in any other way. When saving the file, be sure to preserve its name and file extension.

Table 10-21 Properties in the `portal.properties` File

defaultCalendarName	The default name for a new calendar.
listenerThreadPollingPeriod	Frequency with which the system should poll for externally triggered events (in minutes).
multiValueSQRParamSeparator	For SQR jobs: The character to use as a separator between values of a multi-value parameter.
bqDocsTimeOut	The interval (in seconds) that services should wait for the Intelligence Service to open a BQY document.
defaultCategoryUuid	The name of the root folder.
outputLabel	The name of a set of job output files, is composed of the *outputLabel* value, followed by the job name.
outputLabel1	Part of the job output label identifying a cycle of a BQY job.
bqlogfilenameprefix	With this property and the following one, you define the entire name of the log file for BQY job output. This property defines the name without the file extension.
bqlogfileext	This property defines the file extension of the log file for BQY job output.

Summary

This chapter details all of the properties that can be configured using the LSC Configurator. The system properties and Row-Level Security properties, also detailed in this chapter, are configured through the Administration module.

11 Configuring the Servlets

This chapter explains how to configure the Hyperion Foundation servlets, including descriptions of all the properties. It also explains the "zero administration" of the Hyperion Intelligence Client.

Configuring the servlets enables Hyperion Performance Suite to more precisely meet the needs of your organization. Your particular configuration settings depend on aspects of your organization's environment such as how the system handles user passwords, usage volume, and how your users expect to interface with Hyperion Performance Suite.

Note For information on customizing parameter forms for SQR and generic jobs, see the *Hyperion Performance Suite Foundation User's Guide*. For customizing the user interface of web modules, refer to the *Hyperion Performance Suite Foundation Developer's Guide*

In This Chapter

Using the Servlet Configurator 11-2

The Properties 11-5

Changing Application Context. 11-25

Zero Administration and the Hyperion Intelligence Client 11-27

Load Testing Hyperion Intelligence Clients. 11-29

Using the Servlet Configurator

You can configure many details of the servlets' behavior with the Servlet Configurator. The Servlet Configurator configures all of the locally-installed servlets. You must install the Servlet Configurator and the file it edits on each web server that hosts the Hyperion Foundation servlets.

The configuration file, called `ws.conf`, is installed in:

Install_Home`\servlets\deployment\config`

To start the Servlet Configurator, do the following:

- *Windows:* From the **Start** menu, choose **Programs→Hyperion→Foundation Services→Servlet Configurator**.
- *UNIX:* Run the servletconfig.sh file, installed in *Install_Home*`/servlets/bin`.

Figure 11-1 shows the Servlet Configurator.

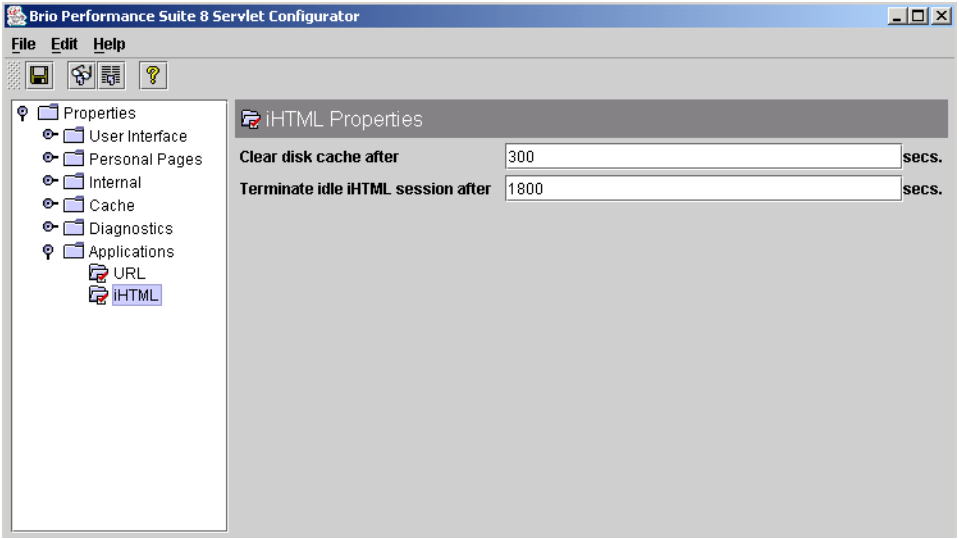
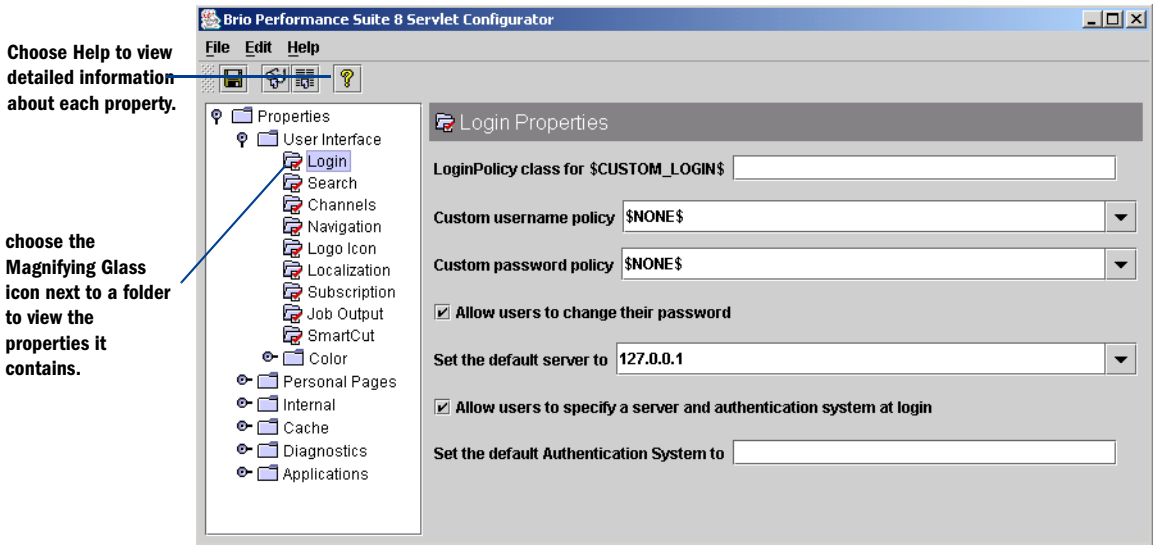


Figure 11-1 Servlet Configurator

The folders of properties appear in the navigation frame of the window. To view the properties in a folder, choose the “magnifying glass” icon next to the folder. For example, to view the user interface properties, choose the “magnifying glass” icon next to User Interface.



The configuration toolbar appears above the navigation pane. The toolbar contains the following icons:

Saves all the configuration settings. (Keyboard shortcut: Alt+S)

Sets the visible configuration settings to their default values. (The visible settings are those currently displayed in the right-hand frame.)

Sets all the configuration settings to their default values.

Displays the online help.

After modifying settings in the Servlet Configurator:

1. **Save your settings.**
2. **Make the new settings effective by restarting the servlets.**

Note The configuration settings are stored in the file `ws.conf`, which resides in `servlets\deployment\config`. If you have replicated the servlets in your system and want to make the configurations match, copy the `ws.conf` file from one servlet host to the other, and then check for host-specific settings.

The Properties

The pages that follow describe the properties configurable through the Servlet Configurator. You can configure any of the following properties:

- User Interface Properties
- Personal Pages Properties
- Internal Properties
- Cache Properties
- Diagnostics Properties
- Applications Properties

User Interface Properties

There are several subfolders of properties under User Interface. Each subfolder has a separate table in this section.

The Login properties pertain to the common login mechanism for all servlets.

Table 11-1 Login Properties

LoginPolicy class for $CUSTOM_LOGIN$	If you are using a custom login implementation, enter the name of the class that implements the LoginPolicy interface. Include the full package-qualified name, but omit the `.class` extension. For more information about custom login, see the `loginsamples.jar` file in the `doc\customlogin` subdirectory of the servlets directory.
Custom user name policy	If set to a value other than $NONE$, uses the specified user name policy to obtain the user name for all users logging into any Hyperion Foundation servlet. You can set this property to $SECURITY_AGENT$, $REMOTE_USER$, $HTTP_USER$, CUSTOM_LOGIN$ (the custom policies), or to $NONE$. If the custom user name policy is set to $SECURITY_AGENT$, the custom password policy must be set to $TRUSTEDPASS$. Set this option to $NONE$ unless you implement a custom login or configure transparent login. Use $CUSTOM_LOGIN$ only if you use a custom implementation for the user name value.

Table 11-1 Login Properties *(Continued)*

Custom password policy	If set to a value other than $NONE$, uses the specified password policy to obtain the password for all users logging into any Hyperion Foundation servlet. You can set the password to $HTTP_PASSWORD$, $TRUSTEDPASS$, $USERNAME$, CUSTOM_LOGIN$ (the custom policies), or to $NONE$. If the custom user name policy is set to $SECURITY_AGENT$, the custom password policy must be set to $TRUSTEDPASS$. Set this option to $NONE$ unless you have implemented a custom login or have set up transparent login. Use $CUSTOM_LOGIN$ only if you use a custom implementation for the password value.
Allow users to change their password	Turn this option on to display the Change Password link in Browse (on Preferences tab). If you do not select this option, the *change password* link is hidden from all screens. If you have set up transparent login, do not select this option.
Set default server to	Specifies the default server. You can set this option to either $CUSTOM_LOGIN$ or to a *server*:*port* designation. If you want the system to obtain the default server from custom login code, Choose $CUSTOM_LOGIN$ from the drop-down list. Otherwise, enter the IP address or name for the server hosting the GSM, and optional port number. The server and port are separated by a colon (:). If the port number is omitted, the default GSM port number 1800 is used. Both of the following examples are valid entries: apollo:2220 (uses port 2220) apollo (uses default port 1800) The default server is used only if a user enters *default* as the server, or if none of the following specifies one: ■ the login form's *Server* field ■ a URL query parameter `server=GSMHost` ■ the `usrsvr` cookie To override a server specification from the login form or a cookie and force use of custom login code instead, include the following in the URL: `?server=$CUSTOM_LOGIN$`
Allow users to specify a server and authentication system at login	Enable this option to allow a user to enter a GSM in the *Server* field of the login form and to enter an authentication system. This option is enabled by default. When this option is disabled, the *Server* field does not appear on the login form, and the default GSM is used.

Table 11-1 Login Properties *(Continued)*

Set the default Authentication System to	Default authentication system, which a user can override at login.

The Search properties apply to the Search tab in the Browse module.

Table 11-2 Search Properties

Enable search features	If you disable this option, the Search tab in the Browse module does not appear, so all search features are inaccessible.
Search matches displayed	Indicates the maximum number of items returned as a result of a search. Select **All** to return all of the items (with no limit). When the number of matches found is greater than this setting, the *Sort results by* order (set on the search page) governs which results are displayed.

The Navigation properties control the display of navigation elements.

Table 11-3 Navigation Properties

Show the tabs	Shows the navigation tabs whenever HTML output displays.
Show the Exit button	Displays the Exit button in the servlets. If you do not select this option, the Exit button is hidden from all screens. If you implement transparent login, keep this option off.

The Logo Icon properties enable you to customize the logo that the servlets display in the upper left of the browser window:

Table 11-4 Logo Icon Properties

Hyperlink logo to	URL to a web page that displays when a user chooses the company logo.
Use company logo	The filename of the logo image file. The file must reside in the `servlets\deployment\img` of the servlets' host.
Preferred logo width	The preferred width of the logo, in pixels.
Preferred logo height	The preferred height of the logo, in pixels.

The Localization properties enable you to customize time, date, and language settings for a particular locale.

Table 11-5 Localization Properties

Format times using	Defines how to format the time. The servlets can display time fields in a 12-hour (AM/PM) format or in a 24-hour format. For example, in a 24-hour format, the servlets would display 6:30pm as 18:30.
Date display order	Defines how to format the date. The servlets can display dates in either month day year order (for example, May 1 2004) or day month year order (for example, 1 May 2004).

Table 11-5 Localization Properties *(Continued)*

Use locale-sensitive sort	Defines whether to use the default locale when sorting names. If you do not define a locale-sensitive sort, the servlets use a lexicographical sort. A locale-sensitive sort is slightly slower but more user-intuitive. For example, 'A' and 'a' are sorted together in a locale-sensitive sort, whereas they are not in a lexicographical sort.
	The lowercase, two-letter code for the language most commonly used by end users of your web modules. For example, **en** for English or **fr** for French. A complete list of codes is located in: `http://www.ics.uci.edu/pub/ietf/http/related/iso639.txt`
	A user can use the web modules in the language of their choice (if templates exist in that language) by setting their browser's language option. (In Internet Explorer, Choose Tools–Internet Options, General tab, Languages button. In Netscape Navigator, choose Edit–Preferences–Navigator/Languages.)
	The *Default local language code* value is used in conjunction with the *Country code* and *Local variant* values to determine the set of templates the servlet reads upon startup and in what language to display pages. The system checks for localization settings in the following order (until a non-*Default* value is found): 1. The user's browser 2. Localization properties for the specific servlet (iHTML or Data Access) 3. Default localization properties for Hyperion Foundation servlets 4. Default locale specified on the web server
Default local language code	The Localization settings found are then used in this order (until a *Default* value is found): a. Language code b. Country code c. Local variant
	For example, the Browse web module checks the user's browser first. If it has no language setting, then Browse, which does not have its own specific localization settings, checks the default localization settings. This check begins with *Default local language code*. If that setting is specified (is not *Default),* Browse checks *Default local country code* to refine localization. If it too is specified, Browse checks *Default local variant.* If, on the other hand, *Default local language code* was set to *Default*, Browse would skip the default localization settings and check the locale for which the servlets host is configured.

Table 11-5 Localization Properties *(Continued)*

Default local country code	The uppercase, two-letter code for the country. (For example, **US** for the United States, **CA** for Canada, and so on). This value is used in conjunction with the *Language code* and *Local variant* parameters to obtain and display data for the user. A complete list of codes is located in: `http://ftp.ics.uci.edu/pub/websoft/wwwstat/country-codes.txt` This value is only used if the *Default local language code* is specified (is not set to *Default)*. If you set *Country code* to *Default*, the iHTML servlet uses the *Language code* value to determine the locale of the user. For more information, see Default local language code in this table.
Default local variant	Optional localization property used for a finer granularity of localization in messages for an audience of users with the same language and country codes. For example, if you specify a variant of WEST_COAST, the system can use it to deliver specialized data, such as time for the local time zone. The *Default local variant* is only used if the *Default local country code* is not set to *Default*. If you set *Default local variant* to *Default*, the servlet uses the *Default local language code* and *Default local country code* values to determine the locale for users. For more information, see Default local language code in this table.

The Subscription property enables you to turn subscriptions on or off.

Table 11-6 Subscription Property

Enable subscription features	Turn this option on to enable users to subscribe to items from the Browse module. If you do not turn on this option, users cannot receive notifications when items are modified.

The Job Output properties allow you to customize the format of job output.

Table 11-7 Job Output Properties

Display HTML icon when displaying SQR job output in listing pages	If you turn off this option, the HTML format for SQR job output will not be available from the Browse listing pages.
Output format to display after an SQR job is run	Choose the default job output format displayed after an SQR job is run.

The SmartCut property affects how SmartCuts display.

Table 11-8 SmartCut Property

Show SmartCut as link	Turn this option on to display SmartCuts as links. If this option is off, SmartCuts display as plain text. The default setting is *off*.

The Color properties enable you to customize the colors of the servlets' user interface. There are several subfolders under Color, pertaining to different areas of the servlet display.

Note The Color properties apply only to the HTML templates of the user interface, not to the JSPs. Therefore, for consistency across the user interface, when you change colors here (in the Servlet Configurator), do the same in the stylesheets, located in the `css` directory. For example, `Install_Home\servlets\deployment\CSS`.

Table 11-9 Color—Main Frame—General Properties

Main frame: Background color	The background color of the main frame (or pane). Does not apply to Personal Pages. If you leave this option blank, your platform's default background color is used.
Miscellaneous highlight color	Color of highlight that does not denote selection, such as the highlight behind *Page names - Descriptions* on the My Personal Pages page.
Personal Page wizard: Background color	The Personal Page wizard is the sequence of pages displayed after a user chooses *New Personal Page*. Wizard pages have two colors, a main background color and the color of its top and bottom borders.
Personal Page wizard: Border color	See preceding paragraph.

Table 11-9 Color—Main Frame—General Properties *(Continued)*

Even row color	Some listings, for readability, use two colors, alternating rows. This option sets the color of the “even” rows.
Odd row color	Some listings, for readability, use two colors, alternating rows. This option sets the color of the “odd” rows.

Table 11-10 Color—Main Frame—Title Properties

Title text color	Title colors apply to the title of each web module page and to the column headings on listings. Examples of page titles are F*avorite Items* (on the Personal tab) or *Item Subscription* (on the Preferences tab). Examples of column headings are *Item Name* and *Location* on the Preferences tab's *Favorite Items* page.
Title underline color	Where titles are underlined, this option sets the underline color.

Table 11-11 Color—Main Frame—Text Properties

Regular text color	Regular text is most of the text on web module pages. If you leave this option blank, the browser's default is used.
Messages/information text color	Messages/informational text refers to text such as "You do not have any folders..." on the *Favorite folders* page when there are no favorite folders.
Date/time text color	Color used for the date and time on listings such as any Browse tab listing of items.
Miscellaneous special text color	An additional text color used where needed. For example, if a search returns multiple pages, the text "Page 1 of 3" appears in this additional color.
Link text color	Color of links on which the user has not (recently) chosen.
Visited link text color	Color of links on which the user has (recently) chosen.

Table 11-12 Color—Navigation Frame Properties

Navigation frame: Background color	Background color of the navigation frame (narrow frame on the left).
Navigation frame: Text color	Background color of the navigation frame (narrow frame on the left).
Navigation frame: Title underline color	Color of the underline beneath the title (tab name) displayed in the navigation frame.

Personal Pages Properties

The properties in the Personal Pages folder enable you to control users' capabilities in the Personal Pages module. There are several subfolders of properties under Personal Pages, each of which has a separate table in this section.

The General properties involve the Personal Pages themselves:

Table 11-13 General Properties

Max Personal Pages per user	The maximum number of Personal Pages a user can have. This value should be 20 or less. The default value is 5.
Max initial published Personal Pages	The maximum number of Personal Pages to be copied from the published Personal Pages when a user first logs in. Set this value to at least 1 less than the value of *Max Personal Pages per user*. The default value is 2.
Users can click default Personal Page	Enabling this option allows users to change their default Personal Page. Users change their default by putting the desired default Personal Page at the top of the list on the My Personal Pages page in the servlets. When this option is disabled, users cannot delete or reorder the default Personal Page. The default value is enabled. Note: To ensure that users see the Personal Page containing the Broadcast Messages every time they log in, disable this option.
Show headings of Content Windows on Personal Pages	By default, this option is enabled, and content windows display with headings (title bars). To suppress the headings, disable this option.

The Publish properties pertain to users publishing their Personal Pages for others to use:

Table 11-14 Publish Properties

Location	The folder path and name of the folder that contains published Personal Pages. This folder must be under the Broadcast Messages folder (whose location and name are set in the System properties of the root folder, using the system tab of the Administration module) The default value of this option is /Broadcast Messages/Personal Page Content. By default, this folder is not browsable.
Show publisher's groups	Controls whether the Publish page displays the option to give permissions to a user's own groups, with a drop-down list of those groups. This option is enabled by default.
Allow publisher to enter group name	Controls whether the Publish page displays the option to give permissions to a specified group. This option is enabled by default.
Allow publishing to all users	Controls whether the Publish page displays the option to give permissions to all users. This option is enabled by default. At least one of the last three Publish properties must be enabled.

The Generated Personal Page properties involve the Personal Page that is generated for each new user the first time that user logs into Personal Pages. You can prepare different versions of this page for different users. The page is generated by the servlet.

Table 11-15 Generated Personal Page Properties

Show My Bookmarks	Controls whether the generated Personal Page includes the *My Bookmarks* content window. This option is enabled by default.
Show Exceptions Dashboard	Controls whether the generated Personal Page includes the *Exceptions Dashboard*. This option is enabled by default.
Number of folders	Controls how many pre-configured folders (subfolders of the Broadcast Messages folder) display on the generated Personal Page. The default value is 3.
Number of File Content Windows	Controls how many displayable items in pre-configured folders (subfolders of the Broadcast Messages folder) display as content windows on the generated Personal Page. The default value is 1.
Default color scheme	Controls which of the color schemes on the *Edit Personal Page* page is the default one. Also designates the color scheme used for a users' generated Personal Page.

The Color Scheme properties let you prepare sets of colors for users to apply to their Personal Pages. There are four color schemes, originally set to default values. You can rename each one and set its colors for particular parts of a Personal Page. Each of the color schemes has the following properties:

Table 11-16 Color Scheme Properties

Name	A name for the color scheme (required).
Headings color	Background color of the heading (title bar) of each content window.
Background color	Background color of content windows in the main (wide) column.
Text color	Color of servlet-generated text on Personal Pages, such as the names of content windows.
Link color	Color of the text of servlet-generated links on a Personal Page, such as bookmarks in *My Bookmarks*.
Broadcast Messages color	Color of the heading of each Broadcast Messages content window.
Header background color	Background color of content windows in the optional header area at the top of a Personal Page.
Footer background color	Background color of content windows in the optional footer area at the bottom of the page.
Left column background color	Background color of content windows in the optional narrow column on the left side of a Personal Page.
Right column background color	Background color of content windows in the optional narrow column on the right-hand side of a Personal Page.

Internal Properties

The Internal properties do not pertain to the user interface, but rather the workings of the servlets or the Hyperion Foundation server. Each subfolder under Internal has a separate table in this section.

Note The session time-out value is configured on the Servlet Engine. For example on JRun, the http session time-out value can be modified for the JVM.

The Redirect properties involve redirecting URLs:

Table 11-17 Redirect Properties

Redirect URLs using	Select an option to specify how to redirect URLs. The servlets can redirect URLs using HTTP or JavaScript. Since HTTP redirection is more efficient, it is the preferred method.
Allow redirect to parent	Indicates whether the servlets should ever do a redirect to a parent frame. Typically, you should select this option; however, do not select this option if the servlets are driven externally by another frame-based application.

The Cookies property concerns the cookies that the servlets create and use:

Table 11-18 Cookies Property

Keep cookies between browser sessions	Selecting this option causes the servlets to save information between browser sessions. The last user name and server the user used to log in is saved. The user name and server is used to initialize the login screen in subsequent logins.

The Transfer property controls how data is passed between the services and the servlets:

Table 11-19 Transfer Properties

Pass data using streams instead of files	Enabling (checking) this option causes the servlets to retrieve files from the services using streamed I/O and a direct connection instead of temporary file system storage. When this option is enabled, data is transferred out-of-band over a separate socket connection between the Repository Service and the servlets. When this option is disabled, data is transferred in-band and stored in a file (or in memory if the data is <500KB) both for the servlets (in a temporary directory) and the Service Broker. Data is transferred from the Repository Service to the Service Broker and then to the servlets. In general, you should enable this option, since streamed I/O is more efficient. However, if your system has a firewall between the servlets and the services, and the servlets cannot open additional sockets for file transfer, then you should disable (un-check) this option. Note about firewalls: When this option is enabled (that is, when streams are used), the system opens a new socket for a file transfer. The operating system generates the port number, and you cannot control this number. A firewall, however, prohibits access through random port numbers. Therefore, you must disable this option, which causes file transfers to use the open socket already in use by the Service Broker.

The Jobs property pertains to messages that appear after job execution:

Table 11-20 Jobs Properties

Show confirmation screens for	The number of seconds for which the background job confirmation screens appear when running a background job.

The Upload property pertains to publishing files:

Table 11-21 Upload Properties

Max file size allowed for publish	Specify the maximum size of a file you want to enable users to publish into the Repository. The default setting is 100MB.

Cache Properties

The Cache properties set limits on how long the web modules can cache various data. These properties affect the responsiveness of the user interface, so setting them involves the trade-off between performance and the freshness of data displayed.

Example

The *Cache folders for* property can be described in any of the following ways: (1) The maximum time to cache folders, in seconds. (2) The maximum delay between when a modification is made to a folder in the Repository and when the user sees the change in the Browse module. (3) The maximum time interval during which a user will see the old contents of a folder.

Increasing the value of *Cache folders for* makes pages display more quickly to the user, but increases the length of time that the user sees stale folder contents. Decreasing the value of *Cache folders for* reduces the duration that the user can see stale folder contents, but slows the display of pages.

The Cache properties include several subfolders. Each subfolder under Cache has a separate table in this section.

The Objects properties concern the caching of particular object types:

Table 11-22 Objects Properties

Number of folders cached	Determines the size of the cache for folders.
Cache folders for	The maximum time to cache folders. Stated in practical terms, the limit for the delay between changes to a folder's contents and the Browse module's display of the changes. Enter the value in seconds. The value can be 0 or greater. A user sees the old contents of a folder for no more than the number of seconds you enter here.
Cache browse queries for	The maximum amount of time it takes for changes to browse queries in the Hyperion Foundation servers to be reflected in the servlets. Enter the value in seconds. The value can be 0 or greater.
Cache jobs for	The maximum amount of time it takes for changes to jobs in the Hyperion Foundation servers to be reflected in the servlets. Enter the value in seconds. The value can be 0 or greater.

Table 11-22 Objects Properties *(Continued)*

Cache parameter lists for	The maximum amount of time that the servlets should cache the parameter lists for a job. Enter the value in seconds. The default is 60.
Cache published Personal Pages for	The maximum amount of time that the servlets should cache the content of the *Personal Page Content* folder (whose location is set by the Personal Pages–Publish property *Location*). Enter the value in seconds. The value must be greater than 0. By default, it is set to 60 seconds. Note that this cache is refreshed whenever a new Personal Page is published via the Personal Pages servlet.
Cache Content Windows on Personal Pages for	The maximum amount of time it takes for changes to Broadcast messages on a Personal Page to be reflected in the Personal Pages servlet. Enter the value in seconds. The value must be greater than 0. By default, it is set to 60 seconds.
Cache Content Windows being modified for	The maximum amount of time the Browse, Administration, or Job Manager module should cache content while it is being modified. Enter the value in seconds.
Cache list items for	The maximum amount of time that item lists should be cached. Enter the value in seconds. The default value is 900 seconds. Pertains to listings of items or resources in Browse, Administration, and Job Manager modules.
Max items to cache for listing	The maximum number of items in a listing that should be cached. The default value is 100.

The System property concerns caching of properties that apply to the system as a whole:

Table 11-23 System Property

Cache system properties for	The number of seconds the servlets should keep system properties information before refreshing it from the server. Use the system tab of the Administration module to view or modify the system properties. Note that refreshing system properties makes the updated settings effective only for new users. Users who are already logged in when a refresh is done are not affected.

The Templates property concerns caching of user interface templates:

Table 11-24 Templates Property

Cache parsed HTML templates	Controls whether the servlets cache templates. Normally, this option should be enabled. It is enabled by default. While testing customized templates, it is useful to disable this option so that template changes display immediately.

The Notification property pertains to the *View Job Status* page of the Job Manager servlet:

Table 11-25 Notifications Property

Refresh notifications every	The frequency of refreshing the *View Jobs Status* page in the Job Manager module. That is, the maximum amount of time between the Event Service issuing a notification and the notification appearing on the user's *View Jobs Status* page. Enter the value in seconds. Values can be 0 or greater.

The Browser property involves the output of BQY jobs:

Table 11-26 Browser Property

Max BQY job outputs listed for modification	The maximum number of job output collections to list in the *Versions* area of a BQY job's properties page. Accordingly, the maximum number of output collections whose properties can be modified.

Diagnostics Properties

The Diagnostics properties folder contains just one subfolder, Log.

The configuration log properties define the logging service server and the path of the Servlet Configurator log configuration file, `servletLog4jConfig.xml`.

Logging Service Server	The hostname of the server with the Logging Service.
Configuration	The path of the Servlet Configurator log configuration file, `servletLog4jConfig.xml` or use the default path.

Applications Properties

There are three subfolders under the Applications properties folder. Each subfolder under Applications has a separate table in this section.

The URL properties concern the locations of each servlet:

Table 11-27 URL Properties

Browse	The location of the Browse servlet. Enter this location exactly as it appears in the `web.xml` file.
Administration	The location of the Administration servlet. Enter this location exactly as it appears in the `web.xml` file.
Personal Pages	The location of the Personal Pages servlet. Enter this location exactly as it appears in the `web.xml` file.
Dashboard	The location of the View Manager servlet. Enter this location exactly as it appears in the `web.xml` file.
Job Manager	The location of the Job Manager servlet. Enter this location exactly as it appears in the `web.xml` file.
iHTML	The location of the iHTML servlet. Enter this location exactly as it appears in the `web.xml` file.
Data Access	The location of the Data Access servlet. Enter this location exactly as it appears in the `web.xml` file.

The iHTML properties pertain only to the iHTML servlet:

Table 11-28 iHTML Properties

Clear disk cache after	Maximum time interval between clearing of disk cache, in seconds. Default is 300.
Terminate idle iHTML session after	Number of seconds for iHTML servlet to wait for a response from the Intelligence Service before timing out. This changes the BQServiceResponseTimeout property in the ws.conf file. If the time limit is exceeded the Intelligence Service will not respond. The iHTML servlet will return the following message: The Intelligence Service timed out. Default is 1800.

Data Access Properties

The Data Access properties pertain only to the Data Access servlet:

Table 11-29 Data Access Properties

DAS response timeout	Number of seconds for DAS servlet to wait for a response before timing out. This changes the DASResponseTimeout property in the ws.conf file. Default is 1800.
Hyperion Intelligence Client Backward Compatibility Support	Set to true to enable Hyperion Intelligence Clients of prior versions (8.2.1 and earlier) to communicate with Hyperion Performance Suite 8.3 servers. This changes the BackwardCompatibility property in the ws.conf file. Default is false. Enable backward compatibility for testing or diagnostic purposes only, as it is not recommended for production.

Changing Application Context

This section shows where you need to make changes in the system in order to customize the URL.

To customize the URL:

1 **Open** `ws.conf` **located in** *`Install_Home`*`\servlets\deployment\config`.

2 **Set the desired URL in these lines: ## Application definitions**

```
WebClient.Applications.URL.Browser=/Hyperion/browse/
WebClient.Applications.URL.Admin=/Hyperion/administration/
WebClient.Applications.URL.Personal=/Hyperion/personalpages/
WebClient.Applications.URL.Dashboard=/Hyperion/viewmanager/
WebClient.Applications.URL.Scheduler=/Hyperion/jobmanager/
WebClient.Applications.URL.iHTMLServlet=/Hyperion/ihtml/
WebClient.Applications.URL.DAServlet=/Hyperion/dataaccess/
```

Note If you change `/Hyperion`, you must change the servlet context root for the deployment of the web applications on the Application Server.

3 **Go to** ***Install_Home*****\servlets\deployment\WEB-INF and open web.xml.**

Set the following:

```
<servlet-mapping>        <servlet-name>Administrator</servlet-name>
<url-pattern>/administration/*</url-pattern>
</servlet-mapping>
<servlet-mapping>        <servlet-name>Browser</servlet-name>
<url-pattern>/browse/*</url-pattern>
</servlet-mapping>
<servlet-mapping>        <servlet-name>PersonalPage</servlet-name>
<url-pattern>/personalpages/*</url-pattern>
</servlet-mapping>
<servlet-mapping>
<servlet-name>Viewmanager</servlet-name>
<url-pattern>/viewmanager/*</url-pattern>
</servlet-mapping>
<servlet-mapping>        <servlet-name>Scheduler</servlet-name>
<url-pattern>/jobmanager/*</url-pattern>
</servlet-mapping>
<!-- iHTML Servlet URI mappings -->
<servlet-mapping>     <servlet-name>iHTMLServlet</servlet-name>
<url-pattern>/ihtml/*</url-pattern>
</servlet-mapping>
<!-- Data Access Servlet URI mappings -->
```

```
<servlet-mapping>     <servlet-name>DAServlet</servlet-name>
<url-pattern>/dataaccess/*</url-pattern>
```

4 In the servlet administration application change the URL mapping and the java arguments to `-Dbrio.content.path=/Hyperion`.

5 Restart the servlet engine.

Zero Administration and the Hyperion Intelligence Client

Zero Administration is triggered when a user chooses a Hyperion Intelligence Server URL link for a BQY file or job either from the browser application or using a SmartCut.

Zero administration identifies the version number of the most up-to-date Hyperion Intelligence Client on the server.

The Hyperion Intelligence Client's capabilities are made available according to the user's roles and adaptive states. The higher level access functions include processing database queries and the full analytical features of Hyperion Intelligence Designer.

The Hyperion Intelligence Client's download starts when the user chooses a BQY document. The user has the option to download the online help files or use the help files from the web server.

Server Processing

The zero administration files (JSP, HTML, and all XPI, and CAB files) are hosted on the web server's file system. The Hyperion Intelligence Client version numbers are stored in the registry for Netscape and Window browsers.

Server URL Mapping

Your users may have problems using locally saved BQYs when their web server deployment changes or you migrate to a different version of Hyperion Performance Suite. You can set-up URL mappings to automatically redirect to the new URLs when the Intelligence Client is installed.

To set-up URL redirection, add commands that establish any required redirections to *Install_Home*`\servlets\deployment\jsp\dataaccess\zeroadmin\zeroadmin.jsp` for each deployment of the servlets. These mappings are made by adding calls to the Map6xUrlTo8() method and should be added to the `CustomizeInstallForIE(insight)` function.

`The Map6xUrlTo8(Old_URL, New_URL)` method establishes a new URL mapping. Passing an empty string as `New_URL` cancels the URL redirection. `Clear6xUrlMap()` function removes all URL redirections established so far. The `CustomizeInstallForIE(insight)` function only runs when the Intelligence Server is downloaded. The mappings are saved in the Windows

registry for use with locally saved documents. If the mappings need to be updated dynamically (once per session) then the call to the `CustomizeInstallForIE(insight)` function should also be called from the Zero Administration main function.

Example:

```
function CustomizeInstallForIE(insight) {
insight.Map6xUrlTo8("http://brio6x_host/ods-
isapi/ods.ods",
"http://hyperion8x_host/Hyperion/dataaccess/Browse") }
```

Client Processing

At each chose in the Browse module on a BQY document, the web browser retrieves and parses the HTML documents from the web server. The JSP logic for zero administration, which is included in these HTML files, runs in the client's web browser.

The zeroadmin.jsp file is retrieved from the web server. The version numbers from that file are compared to the version numbers on the client's computer. There are three possible outcomes:

- If no version number is found on the client, the user is prompted to install.
- If the numbers are equal (meaning the client has the same version number as the zeroadmin.jsp file), or if the client version is greater than the zeroadmin.jsp version, the BQY document is opened using the previously installed Hyperion Intelligence Client.
- If the version number on the client is less than the version in the zeroadmin.jsp file, the client is prompted to upgrade their product.

Netscape browsers store the Hyperion Intelligence Client version in the registry. You can view the registry by choosing About Plugins from the Netscape browser's Help menu.

Window browsers can interrogate the Hyperion Intelligence Client itself to find out what version it is. You can view this information by locating the DLL files (for example, the `axbqs32.dll` file for Hyperion Intelligence Client under Internet Explorer, or the `npbqs32.dll` file for Hyperion Intelligence Client under Netscape) and displaying their file properties.

Most popular web browsers allow automatic download and installation and provide a digital certificate for an extra layer of security.

The JSP automatically provides the correct application (plug-ins for Windows in a browser-compatible file format).

Tip Netscape users: Set the following preferences in Netscape (Edit, Preferences): Enable Java, Accept all cookies, Enable JavaScript, Enable Software Installation. Then restart your browser.

Load Testing Hyperion Intelligence Clients

Hyperion Intelligence Clients use unique request ids for each request sent to the server, as well as expiring keys to encrypt the DB credentials and SQL string sent over the wire. Due to this, customers using load-testing tools like load-runner, silk performer, etc. will face difficulty conducting their tests.

In order to load test the following tasks need to be considered:

- Assign unique request Ids to URL parameter `CURRENT_REQUEST_ID`

One way to generate the unique ids for LoadRunner is to use the datetimestamp and virtual user id as below:

```
Url=Browse?REQUEST_TYPE=getSectionMap&DOC_NAME={BQY_Files}.bqy&
DOC_UUID={par_sDocUUID}&DOC_VERSION=1&MULTI_PART=0&CURRENT_REQU
EST_ID={DateTimeStamp}{UserRuntimeID}", "Referer=", ENDITEM,
```

Where,

DateTimeStamp is Date/Time parameter type with format %Y%m%d%H%M%S

UserRuntimeID is a VUserID parameter type with format %03s

- Enable Static key encryption for recording the scripts as well as running the scripts within Hyperion Performance Suite

This setting is not recommended for production environments.

Data Access Servlet

Add the following property into `ws.conf` and restart web server.

```
WebClient.Applications.DAServlet.UseStaticKeyForEncryption=true
```

Data Access Service

Add the following new property in `server.xml` and restart Data Access Service for all installed homes. Make sure the new property is defined inside `<properties>` sub-node of `<service type="DataAccess">` node and outside of this node, `<propertylist defid="0ad70321-0002-08aa-000000e738090110" name="DAS_EVENT_MONITOR_PROPERTY_LIST”>`

```
<property defid="0ad70321-0001-08aa-000000e738090110"
name="USE_STATIC_KEY_FOR_ENCRYPTION">true</property>
```

Intelligence Service

Add the following new property in server.xml and restart Intelligence Service for all installed homes.

The new property must be inside <properties> sub-node of `<service type="BrioQuery">` node and outside of this node, `<propertylist defid="0ad70321-0002-08aa-000000e738090110" name="BQ_EVENT_MONITOR_PROPERTY_LIST">`

```
<property defid="0ad70321-0001-08aa-000000e738090110"
name="USE_STATIC_KEY_FOR_ENCRYPTION">true</property>
```

Note Setting only one of the above properties can cause processing (running of BQY jobs, querying from Hyperion intelligence Client, querying from zero-client) to fail since the source and target encryption schemes will not match.

Summary

This chapter explains the properties of the Servlet Configurator and how Zero Administration works for Hyperion Intelligence Clients.

12 Backing Up

Standard data center policies for database backups include incremental daily backups and weekly full backups with off-site storage to protect the organization's investment. When you back up your Hyperion Performance Suite system, you should plan the backup in the same way that you plan other database backups.

This chapter explains how to back up your Hyperion Performance Suite servers and Repository content. It specifies what you need to back up, and when.

In This Chapter

What to Backup 12-2
General Backup Procedure 12-2
Backing Up the Hyperion Performance Suite File System 12-3
Sample Backup Script 12-7
Backing Up the Repository Database 12-8
Backing Up the Clients 12-8

What to Backup

You must back up the following items in your system:

- File system, which contains your Hyperion Performance Suite *content* and other system information (including files in other directories and on other hosts)
- Repository database, which contains user and item metadata
- Report registry keys from the same point in time (Windows only)

Hyperion Performance Suite maintains an item repository in the native file system and stores metadata, or descriptive information, about each user and object in a Relational Database Management System (RDBMS).

Note To recover data, restore the database and file system backups (and registry if required), and restart the services.

General Backup Procedure

To backup your Hyperion Performance Suite system:

1. **Shut down the Hyperion Foundation services.**
2. **Back up the Hyperion Foundation file system.**
3. **Back up the Hyperion Foundation Repository database.**
4. **Save the backup (on tape or CD).**

Note If you use *Windows*, export the Hyperion Performance Suite registry key. If you use *UNIX*, backup the `/etc/rc` or the `/etc/init.d` boot startup scripts.

Backing Up the Hyperion Performance Suite File System

There are five types of backups, distinguished by when you perform them. These backup types are:

- **Complete** – A backup of the entire system. Your organization's policies and procedures determine whether and how often you perform a complete backup.
- **Post-installation** – A backup of certain directories, performed after completing an installation and before using the system.
- **Daily incremental** – A daily backup that includes only files that are *new or modified* since the previous day. Daily incremental backups involve directories that contain frequently changing information, such as the Repository content and log files.
- **Weekly full** – A weekly backup that includes *all* the files in the directories of which you do incremental backups on a daily basis.
- **As Needed** – A backup done only after changes are made, rather than on a regular schedule. As-needed backups involve directories containing files that are customizable but are not modified regularly.

The *Install_Home* directory contains the Hyperion Performance Suite products you have installed on the host. Subdirectories of *Install_Home* include `\admin` and `\BrioPlatform`, among others. Figure 12-1 shows the contents of *Install_Home*.

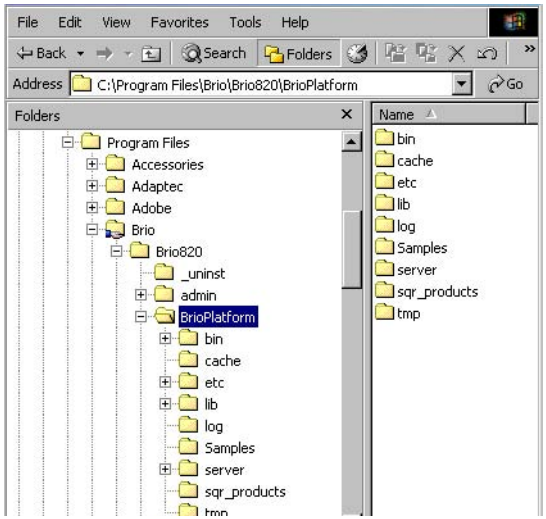


Figure 12-1 Hyperion Performance Suite Directory Structure

Complete Backup

To back up your system comprehensively, back up the directories specified in Table 12-1.

Table 12-1 Tables to Back Up

Directory	Description
Install_Home	Directory in which you installed all Hyperion products on a given host.

Post-Installation

Immediately after installing, back up the directories specified in Table 12-2.

Table 12-2 Directories for Post-Installation Backup

Directory	Description
Install_Home\Install	Contains all configuration information defined during installation. Back up this directory on all hosts and zip each backup.
Install_Home\BrioPlatform\bin	Holds the startup batch scripts for each service. The `bin` directory also contains the `ConfigFileAdmin.bat` utility used by the administrator to decode and change passwords. Typically, the only password of interest is the RDBMS login password. On Windows 2000 systems, this directory also contains the `Setup.exe` program file. `Setup.exe` is used to create or delete services running as Windows 2000 Services. You can also use `Setup.exe` to update the Windows 2000 Registry information.
Install_Home\etc	Holds service configuration files used at service startup, including: ❒ `server.xml` ❒ `config.dat` ❒ `BrioPlatform#_`*`localHost_gsmHost_gsmPort`*`.dat`
Install_Home\Install\lib	Contains jar files required by one or more Hyperion Performance Suite components.
Install_Home\BrioPlatform\lib	Contains all the drivers required to run the Hyperion Foundation services.
Install_Home\Admin\lib	Contains library files for the Job Utilities (SQR Publisher, Calendar Manager) as well as the Local and Remote Service Configurators.
Install_Home\sqr_products	Contains the files necessary to manipulate the metadata for versions of SQR.

Weekly Full and Daily Incremental

The following directories in Table 12-3 should be backed up fully once a week and incrementally every day.

Table 12-3 Directories for Weekly Full and Daily Incremental Backup

Directory	Description
Install_Home\log	Holds log files for services operating on this machine.
Install_Home\BrioPlatform\Server\RM_*host*	Holds content (Repository files).

As Needed

Table 12-4 specifies the directories to be backed up as needed.

Table 12-4 Directories for As-Needed Backup

Directory	Description
Install_Home\BrioPlatform\bin	Holds the startup batch scripts for each service. The `bin` directory also contains the `ConfigFileAdmin.bat` utility used by the administrator to decode and change passwords. Typically, the only password of interest is the RDBMS login password.
Install_Home\etc	Holds service configuration files used at service startup as well as `server.xml` and `config.dat`.
Install_Home\BrioPlatform\Server	Contains directories associated with the services.

Reference Table for All File Backups

Table 12-5 lists the directories for all types of backups and is sorted alphabetically by directory.

Table 12-5 Alphabetical Reference to Directories for All Backups

Directory	Description	Backup Requirements
Install_Home	Directory in which all Hyperion products on a given host are installed.	Back up this directory for a complete backup of all your Hyperion products.
Install_Home\Admin\lib	Contains library files for Job Utilities (SQR Publisher, Calendar Manager, Local and Remote Service Configurator).	After the initial installation.
Install_Home\BrioPlatform\bin	Holds the Hyperion Foundation startup batch scripts for each service. The `bin` directory also contains the `ConfigFileAdmin.bat` utility used by the administrator to decode and change passwords. Typically, the only password of interest is the RDBMS login password. On Windows 2000 systems, this directory also contains the `Setup.exe` program file. `Setup.exe` is used to create or delete services running as Windows 2000 Services. You can also use `Setup.exe` to update the Windows 2000 Registry information.	After the initial installation and after any changes are made to the startup scripts.
Install_Home\BrioPlatform\lib	Contains all the drivers required to run the Hyperion Foundation services.	After the initial installation.
Install_Home\BrioPlatform\server\RM_*host*	Holds content (Repository files).	Daily incrementals, weekly fulls-consistent with company backup policy.
Install_Home\etc	Holds service configuration files used at service startup as well as `server.xml` and `config.dat`.	After the initial installation, before and after subsequent service configuration changes that focus on adding and removing services to a given domain.

Table 12-5 Alphabetical Reference to Directories for All Backups *(Continued)*

Directory	Description	Backup Requirements
Install_Home\Install	Contains all configuration information defined during installation.	Perform after initial installation. on each host. Back up this directory on each host and zip each backup.
Install_Home\Install\lib	Contains jar files required by one or more Hyperion components.	After the initial installation.
Install_Home\log	Holds log files for services operating on this machine.	Daily incrementals, weekly fulls-consistent with company backup policy.
Install_Home\sqr_products	Contains the files necessary to manipulate the metadata for versions of SQR.	After the initial installation.

Sample Backup Script

The following is a sample script for a file-system backup of a Sun Solaris deployment of Hyperion Performance Suite:

```
Backup Utility: Solaris Dump
Backup Type: Full Level 0 Dump
Backup Frequency: Weekly run on Saturday at 1 AM

#!/bin/sh

PARMS="0ucbsdf 126 5000 61000"
DEVISE="/dev/rmt/0hn"
CMD="/usr/sbin/ufsdump"
FileSystems="/Hyperion/log
/Hyperion/BrioPlatform/Server/RM_Solar12"

# ---------------------------------------------------------
#        Perform Level 0 Dump of all listed filesystems
# ---------------------------------------------------------

echo "Starting Backup set for the following filesystems:"
echo ""

for i in $FileSystems
do
   echo "backing up filesystem: "
   echo $i
   $CMD $PARMS $DEVISE $i
done
```

Backing Up the Repository Database

The Repository database should be backed up according to your company policy for database backups, and taking into account the volume of Repository usage.

A backup of the Hyperion Performance Suite Repository database is RDBMS- (or vendor-) dependent. For details about the backup procedure for your particular RDBMS, see its documentation.

Backing Up the Clients

The backup needs of Hyperion Performance Suite client installations are minimal. You should perform a standard post-installation full backup, according to your company policy. Thereafter, the only files you need to backup are the following servlet files:

- The servlet configuration file, `ws.conf` on Windows or `wsrun_`*`platform`* on UNIX, located in *`Install_Home`*`/servlets/deployment/config`
- Any other modified files in *`Install_Home`*`/servlets/deployment/config`
- `web.xml`, in *`Install_Home`*`/servlets/deployment/WEB-INF`
- Any customized JSPs
- Any customized HTML templates

Summary

In this chapter, the Hyperion Performance Suite system back-up procedures are detailed for both the repository database and the clients. Sample backup scripts are also included.

PART V

System Management

13 Usage Tracking

Usage tracking provides a historical view of system usage. It covers usage of the Foundation functions of logging in, publishing files, and more.

In This Chapter

About Usage Tracking 13-2

Managing Usage Tracking 13-4

Sample Usage Tracking Reports 13-7

About Usage Tracking

Usage Tracking is a service that records information about specific Hyperion Performance Suite activities as they occur. This information can answer questions like the following:

- Who logged in yesterday?
- How often do users in the Purchasing group login?
- Which Hyperion Performance Suite reports are accessed most frequently?

Hyperion recommends that Usage Tracking use its own schema in the same database as the repository. For more information about setting up the Usage Tracking schema, see the *Hyperion Performance Suite Installation Guide*.

How Does Usage Tracking Work

Activities are recorded as events in the repository database. Each event is recorded with the necessary information to distinguish that event from other events and also to provide pertinent information about the event.

You can configure your system to track the events in which you are interested. For example, you can track opening, closing, and processing BQY documents or you can track only opening BQY documents.

The usage service can be replicated and all usage services access the same database. Events are deleted from the database in a configurable time frame.

The usage service must be running in order to track the events set in the user interface.

What Events Can Be Tracked

Each tracked event becomes a record in the usage tracking database views. You can configure the usage service to track the following events through the Administration module:

- Foundation Login
- Database Login (for BQY only)
- Open BQY Document
- Close BQY Document (when using the Hyperion Intelligence iServer)
- Open Standard document (by MIME type)
- Run BQY Job
- Run SQR Job
- Run Generic Job
- Process BQY Document
- View BQY Job Output
- View SQR Job Output
- View Generic Job Output

Server Time

Event times are stored in GMT.

Managing Usage Tracking

Usage tracking configuration is managed through the Administrator web module and the Local Service Configurator. All configurable properties, except run type, are managed in the Administration web module. To modify the run type, see "Services with Only the Standard Properties" on page 10-6.

To access Manage Usage Tracking in the Administration web module:

1. Choose **Administration** from the module list.
2. Choose the **System** tab.
3. Choose either **Manage Usage Tracking** or **Track Events** from the navigation pane.
4. Change the properties as necessary.

   For property details, see "Usage Tracking Properties" on page 13-4.
5. Choose **Apply**.

Usage Tracking Properties

Records are the usage tracking events in the database. The Figure 13-1 and Table 13-1 lists the usage tracking general properties.

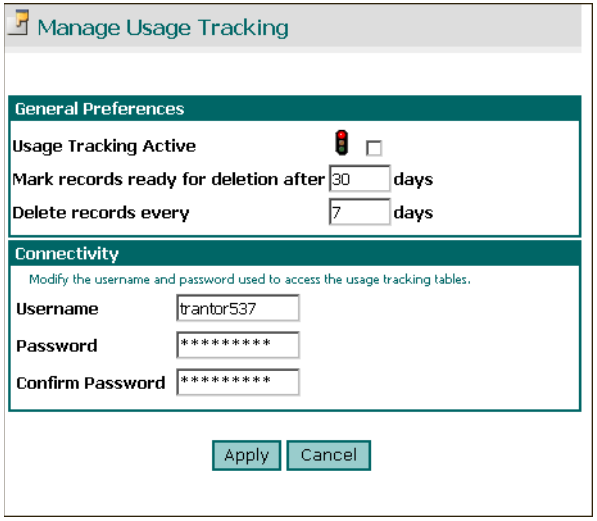


Figure 13-1 Usage Tracking General Properties

Table 13-1 General Properties

Usage Tracking Active	Select to turn on usage tracking.
Mark records ready for deletion after_days	Mark records for deletion during the next garbage collection after (n) number of days in the system. Default is 30 days.
Delete records every_days	Run the garbage collection utility after (n) number of days. Default is 7 days.
Username	Database username auto-populates from the usage tracking database. This only needs to be changed if the database is moved.
Password	Database password auto-populates from the usage tracking database. This only needs to be changed if the database is moved.
Confirm Password	Database password auto-populates from the usage tracking database. This only needs to be changed if the database is moved.

The Figure 13-2, Figure 13-3, and Table 13-2 display all of the possible events that can be tracked. The usage service must be running in order to track the selected events. No tracking events are selected by default.

Track Events

To enable tracking of an event, check the box next to its name

Event	Description
☐ System Logins	Tracks each system login
☐ Database Logins	Track each database login
☐ Timed Query Event	Track each time a BQY query is processed
☐ Open BQY Document	Track each time a BQY document is opened
☐ Process BQY Document	Track each time a BQY document is processed
☐ Close BQY Document	Track each time a BQY document is closed
☐ Run BQY Job	Track each time a BQY job is executed
☐ View BQY Job Output	Track each time output from a BQY job is viewed
☐ Run SQR Job	Track each time a SQR job is executed
☐ View SQR Job Output	Track each time output from a SQR job is viewed
☐ Run Generic Job	Track each time a generic job is executed
☐ View Generic Job Output	Track each time output from a generic job is viewed

Figure 13-2 Track Events Section

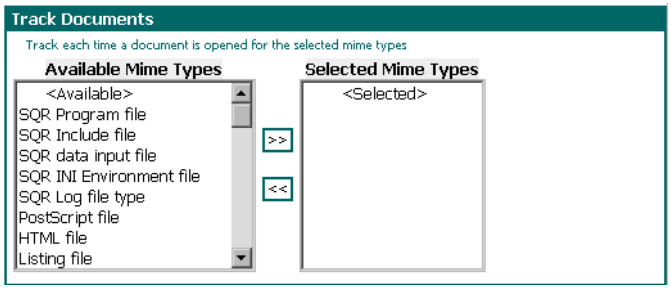


Figure 13-3 Track Documents MIME Types

Table 13-2 Track Events

System Logins	Track each login to the system.
Database Logins	Track each login to a database.
Timed Query	Track each timed query.
Open BQY Document	Track each time a BQY document is opened using the Hyperion Intelligence Client or the Hyperion Intelligence iServer.
Process BQY Document	Track each time a BQY document is processed.
Close BQY Document	Track each time a BQY document is closed using the Hyperion Intelligence iServer.
Run BQY Job	Track each time a BQY job is run.
View BQY Job Output	Track each time BQY job output is accessed.
Run SQR Job	Track each time an SQR job is run.
View SQR Job Output	Track each time SQR job output is opened using the Hyperion SQR iServer.
Run Genic Job	Track each time a generic job is run.
View Generic Job Output	Track each time generic job output is accessed.
Track Documents	Track each time a document with one of the selected MIME types is opened.

Sample Usage Tracking Reports

The sample Usage Tracking Reports allow you to get standard Hyperion Performance Suite usage reports right away. You can modify the standard reports as necessary or create your own reports. The reports are in BQY format and require access to one of the Intelligence products.

The BQY document, Sample-Usage Tracking.bqy, which generates the usage tracking reports, is located on the documentation CD in the Usage Tracking folder. The Readme file in this folder contains connection instructions.

Note The sample reports could contain sensitive company information when used with your data. Use access control when publishing the reports so only the intended audience has access.

Summary

Usage tracking collects the information about your Hyperion Performance Suite system that you request. You can use this information to fine tune your system.

14 Troubleshooting

Log messages can be generated throughout Hyperion Performance Suite to help technicians identify system or environmental problems or to help developers debug reports or API programs.

In This Chapter

Logging Architecture 14-2
Log File Basics 14-4
Configuring Log Files for Troubleshooting 14-9
Analyzing Log Files. 14-17
What to Send to Customer Support 14-24

Logging Architecture

All logging messages are routed through the Logging Service and stored in a central location. The Logging Service writes the log messages to one or more files. A viewer can be used to read these files.

Log4j (version 1.2) is used as the basis for the logging framework and configuration files. The Log Management Helper is used by the C++ services (Intelligence and Data Access Services) in conjunction with the log4j framework and the Logging Service.

The product comes with pre-configured loggers and appenders. *Loggers* correspond to the area in the code (class) where the log message originated. *Appenders* correspond to the output destinations of the log messages. You can troubleshoot specific components of your system by setting the log level of the loggers.

Log4j

The log4j package allows logging statements to remain in shipped code without incurring a heavy performance cost. As part of the Jakarta project, it is distributed under the Apache Software License, a popular open source license certified by the Open Source Initiative (OSI). Logging behavior is controlled through XML configuration files at runtime. In the configuration files, log statements can be turned on and off per service or class (via the loggers) and log levels for each logger can be set. This provides the ability to diagnose problems down to the class level. Multiple and different destinations can be configured for each logger.

The log4j environment has the following main components:

- **Loggers** – Control which logging statements are enabled or disabled. Loggers may be assigned the levels `ALL`, `DEBUG`, `INFO`, `WARN`, `ERROR`, `FATAL`, or `INHERIT`.
- **Appenders** – Send formatted output to its destinations.

Note For more information on log4j, see www.apache.org or *The complete log4j manual* by Ceki Gülcü (QOS.ch, 2003).

The Logging Service

The Logging Service stores all log files in a central location. If the logging service is unavailable the logging messages are sent to the backup logging file. When the logging service is restored the messages in the backup file are automatically sent to the logging service, which then stores them in the appropriate log file. The backup file is then deleted.

The Logging Service cannot be replicated.

Note The servlets support sending logs to multiple Logging Services because servlets support clients that are logged into different servers each using their own Logging Service.

Log Management Helper

The Log Management Helper (LMH) consolidates all logs from DAS or BI services and sends them to the logging service. There is one LMH process for each DAS service and one for each BI service per Install_Home. The logging service consolidates all log messages in one log file for DAS and one log file for BI per Hyperion Performance Suite system.

Server Synchronization

Since log files are timestamped and written in chronological order, time synchronization between servers is important. Time synchronization is the responsibility of the administrator. Many products, both free and commercial, are available to manage the synchronization of the server clocks.

Log File Basics

In order to use the log files for troubleshooting you need to know the following:

- Location of Log Files
- Log File Naming Convention
- File Format of Log Messages

Location of Log Files

The log files are located on the machine where the logging service is running in the `Install_Home\BrioPlatform\log` directory. The components below log messages centrally using the logging service:

- Services
- Servlets
- Process Monitor
- Web services

Local Log Files

The Local Service Configurator, Remote Service Configurator, and the Calendar Manager log messages locally to `Install_Home/admin/log`.

Intelligence and DAS Service Local Log Files

The Intelligence and DAS services have additional log files that are stored in the directory where the service is run. These log files collect log messages before the Intelligence and DAS services connect to the logging service. The log messages in these files are not routed to the logging service log files. Start-up problems are collected in the following two logs, `BIstartup.log` and `DASstartup.log`. Other log messages generated when the logging service is not available are collected in the following log files:

- `BI1_hostname.log` – when not using a process monitor to start the service
- `0_BI1_hostname.log` – when using a process monitor to start the service
- `DAS_hostname.log` – when not using a process monitor to start the service
- `0_DAS_hostname.log` – when using a process monitor to start the service

If you change the name or location of these files, you need to change the entry in the `server.xml` file that points to them. The `server.xml` file resides in *`Install_Home`*`\etc`.

Log File Naming Convention

Each service or servlet has its own log file. In a multi-Install_Home installation, all services of the same type will log their messages to the same file. Separate log files are generated for the license information, the configuration and/or environment information, and stdout messages.

Services and servlets log filenames are constructed as follows:

*Install_Home_hostname_hostname_port number*_messages_*OriginatorType*.log

whereas

Install_Home is the root directory

host name is the name of the machine

port number is the port number

OriginatorType is one of the components listed below:

- Servlets
  - BrowseServlet
  - AdministrationServlet
  - PersonalPagesServlet
  - JobManagerServlet
  - ViewManagerServlet
  - DataAccessServlet
  - iHTMLServlet
- Services:
  - AuthenticationService
  - AuthorizationService
  - CommonServices
  - PublisherService
  - SessionManager
  - LSM
  - GSM

- IntelligenceService
- DataAccessService
- JobService
- EventService
- NameService
- ServiceBroker
- RepositoryService
- Usage Service

- Miscellaneous
  - BIProcessMonitor
  - DASProcessMonitor
  - CalendarManager
  - ExternalDriverSynchronizer
  - WebService
  - SDK
  - EventComponent
  - LocalServiceConfigurator
  - RemoteServiceConfigurator
  - Installer

Special log files are:

- license_messages.log – Contains license information.
- configuration_messages.log – Contains basic environment and configuration information.
- *name*_backupMessages_*ip-address_port*.log – Where name is the process name. This file contains logging messages when the logging service is unavailable (for example, BI_PM_sla1_backupMessages_10_215_34_160_1800.log).
- stdout_console.log – Contains messages sent to stdout and stderr.

File Format of Log Messages

Each log message contains the information below in the following order:

- Logger – Name of the logger that generated the logging message
- Timestamp – Timestamps are saved in UTC, to ensure that messages from different time zones can be correlated. The administrator is responsible for time synchronization between servers.
- Level – Log level
- Thread – Name of thread
- Sequence Number – Unique number to identify messages with the same timestamp
- Time – The time the log message was generated
- Context – Specific information about which component generated the log message
  - Subject – Name of the user
  - Session ID – UUID of the session
  - Originator Type – Name of the type of component
  - Originator Name – Name of the component
  - Host – Name of the host
- Message – The log message
- Throwable – Records the stack trace of a throwable error

The format for the backup log file is the same as the format for the regular logs.

Note If the schedule for a job is later modified, it will not be possible to correlate the parameters.

Configuration Log

Basic configuration information is logged to `configuration_messages.log` located in `BrioPlatform/log`. The file format is the same as the service and servlet log files.

This log file contains java system property information, jar files' version information, and database information.

Configuring Log Files for Troubleshooting

In order to troubleshoot your Hyperion Performance Suite system, you can configure the following logging properties:

- Log Levels
- Loggers
- Appenders
- Log Rotation

Loggers, log levels, and appenders are configured in XML files. The log rotation property is a Java system property and is configured in the `startcommonservices.bat file`.

Log levels for LSC services, RSC services, and the root logger are configured using the LSC Configurator and the RSC Configurator. All other configuration changes can be made by editing the XML files.

Configuration Files

There are two types of configuration files, main files and imported files. The imported files are used by the main files and organize the loggers and appenders into separate XML files.

The service configuration files are located in *`Install_Home`*`\BrioPlatform\etc\log4j.` The servlet configuration files are located in `Install_Home\servlets\deployment\config.` The paths of `serviceLog4jConfig.xml` and `remoteServiceLog4jConfig.xml` are stored in `server.xml.` The path of `servletLog4jConfig.xml` is stored in `ws.conf`. If you change the location of these configuration files, you must update the path in the appropriate file.

The product has the following main configuration files:

- `serviceLog4jConfig.xml` – Main configuration file for services.
- `remoteServiceLog4jConfig.xml` – Main configuration file for Intelligence Service and Data Access Service and for the RSC services when started remotely.

- `adminLog4jConfig.xml` – Main configuration file for LSC, RSC, and Calendar Manager applications.
- `servletLog4JConfig.xml` – Main configuration file for the servlets.

The product has the following imported configuration files:

- `appenders.xml` – Appender configuration file imported by `serviceLog4jConfig.xml`, `servletLog4JConfig.xml`, and `remoteServiceLog4jConfig.xml`. Appenders can be added by referencing them in <logger> and <root> elements using <appender-ref> elements.
- `serviceloggers.xml` – Service logging configuration file imported by `serviceLog4jConfig.xml` and `remoteServiceLog4jConfig.xml`. Configure through the LSC Configurators.
- `debugLoggers.xml` – Contains definitions for specific loggers that can be enabled to debug specific problems in the services. Imported by `serviceLog4jConfig.xml` file and `remoteServiceLog4jConfig.xml.` Located in *`Install_Home`*`\BrioPlatform\ etc\log4j.`
- `debugLoggers.xml` – Contains definitions for specific loggers that can be enabled to debug specific problems in the servlets. Imported by `servletLog4jConfig.xml`. Located in `Install_Home\servlets\deployment\config.`

Configuring Log Levels

The log level sets the amount and type of information that is written to the log file. Except for the inherit level, the levels in Table 14-1are listed from the most verbose to the least verbose. The levels at the top of the list contain all the levels below it. For example, if you set the log level at WARN, the WARN, ERROR, and FATAL messages will be sent to the log file.

The default log level, which is set on the root, is WARN. You can change this for the entire system or on a service/servlet basis. If a given logger is not assigned a level (or its level is set to INHERIT), it inherits the level from its closest ancestor with an assigned level. The root logger resides at the top of the logger hierarchy and always has an assigned level.

Table 14-1 System Wide Logging Levels

Level	Description
INHERIT	Uses the log level set at its closest ancestor with an assigned level. (Not available at the root level.)
ALL	Logs all of the messages below.
DEBUG	Minor and frequently occurring normal events. This level should only be used when trying to troubleshoot.
INFO	Normal significant events of the application.
WARN	Minor problems caused by factors external to the application.
ERROR	Usually indicates a Java exception error. Error conditions do not necessarily cause the application to crash and the application may continue to service subsequent requests.
FATAL	Implies the imminent crash of the application or the relevant sub-component. (rarely used)

Configuring Loggers

Configure log levels for RSC services using the RSC Configurator, see "Advanced Properties" on page 9-26. RSC log levels are stored in the database. Configure log levels for LSC services and the root logger using the LSC Configurator, see "General Properties" on page 10-30. LSC log levels are stored in `serviceLoggers.xml`.

Configure the servlet root logger level in `servletLog4JConfig.xml`. Configure all other servlet loggers in the servlet debug configuration file (`debugLoggers.xml`).

To configure the servlet root logger:

1. **Open** `servletLog4JConfig.xml located in Install_Home\servlets\deployment\config.`

2. **Scroll to the end of the file and change the log level for the root.**

   For example, change WARN to INFO.

```
<root>
<level value="WARN"/>
<appender-ref ref="LOG_REMOTELY"/>
</root>
```

3. **Save the file.**

Configuring Debug Loggers

The debug loggers can be enabled by changing their log level from INHERITED to DEBUG. These loggers should be used in conjunction with help from customer support.

Note A number of java properties, such as `print_config`, `print_query` debug, and `echo are mapped to debug loggers in` *`Install_Home`*`\BrioPlatform\ etc\log4j\debugLoggers.xml.`

Configuring Appenders

You can send log messages to multiple destinations by adding appenders to a logger. Appenders are defined in the `appenders.xml` file.

To add an appender to a logger:

1. **Locate the appender you want to add in the `appenders.xml` file.**
2. **Copy the name of the appender.**
3. **Open the XML file of the logger in which you want to add this appender.**
4. **Paste the name of the appender after `<appender-ref ref=` under the logger in which you want to add this appender.**

   For example,

   ```
   <appender-ref ref="LOG_LOCALLY_BY_LOGGING_SERVICE"/>
   ```

5. **Save the file.**

Configuring Synchronous or Asynchronous Messaging

Log messages can be sent either synchronously (the default) or asynchronously. Asynchronous mode offers performance advantages while synchronous mode provides reliability in that all messages get logged. You can also change the BufferSize parameter in order to limit the number of messages that might be lost in the system.

To enable asynchronous messaging:

1. **Open the `appenders.xml` file and locate the asynchronous appender.**

   ```
   <appender name="SEND_TO_LOGGING_SERVICE_ASYNC"
   class="org.apache.log4j.AsyncAppender">
   ```

2. **Change the BufferSize parameter if desired.**

   ```
   <param name="BufferSize" value="128" />
   ```

3. **Copy the name of this appender, `"SEND_TO_LOGGING_SERVICE_ASYNC"`.**

4 **Locate the root logger in the appropriate XML file.**

You can change the default appender for the service or the servlet root logger by opening the appropriate XML file.

5 **Replace the name of the default appender, `"LOG_LOCALLY_BY_LOGGING_SERVICE"`, with the name of the asynchronous appender, `"SEND_TO_LOGGING_SERVICE_ASYNC"`.**

6 **Save the file.**

Configuring Root Level Appenders

In the main configuration file for services, `serviceLog4jconfig.xml`, the default appender for the root level logs locally by the logging service. If the server does not contain the logging service, the appender `LOG_REMOTELY` will be uncommented. You can also uncomment the second appender, `LOG_LOCALLY`, if you want to send the log messages both remotely and locally.

The following code, copied from the `serviceLog4jconfig.xml`, file, shows the root level appenders:

```
<!-- The following appender should be enabled if the server does
not contain the logging service -->
        <!-- <appender-ref ref="LOG_REMOTELY"/> -->

       <!-- The following appender can be enabled in conjunction
with the remote appender to also send log messages locally -->
        <!-- <appender-ref ref="LOG_LOCALLY"/> -->

       <!-- The following appender should only be enabled if the
server contains the logging service -->
        <appender-ref ref="LOG_LOCALLY_BY_LOGGING_SERVICE"/>
```

Configuring Log Rotation

You can configure to roll and delete log files by time intervals or by file size. File size log rotation is controlled by the CompositeRollingAppender. Time interval log rotation is controlled by the CompositeRollingAppender and a Java property in the start file of the common services.

By default the system rolls logs every 12 hours and the oldest log file is deleted when the number of logs is greater than 5. Log files are created and deleted by originator type. For more information on originator types, see "Log File Naming Convention" on page 14-6.

All appenders in the XML configuration files are configured to use the default values for the CompositeRollingAppender. You can configure the CompositeRollingAppender's properties for each appender separately.

Note If you want all of your log files to rotate using the same criteria, change the configuration for each CompositeRollingAppender defined in both `appenders.xml` files.

To change the log rotation settings:

1. **Open** `appenders.xml` **located in** *`Install_Home`*`\BrioPlatform\etc\log4j` **for the services or in** *`Install_Home`*`\servlets\deployment\config` **for the servlets.**

2. **Locate the CompositeRollingAppender definition for the appender you want to change and change the properties as desired.**

   Table 14-2 details the CompositeRollingAppender properties.

   Here is a sample CompositeRollingAppender definition:

```
<appender name="BACKUP_MESSAGES_FILE"
class="org.apache.log4j.CompositeRollingAppender">
<param name="File"
value="${directory}/log/${name}_backupMessages.log"/>

<!-- Select rolling style (default is 2): 1=rolling by size,
2=rolling by time, 3=rolling by size and time. -->
<param name="RollingStyle" value="1"/>

<!-- If rolling style is set to 2 then by default log file will
be rolled every 12 hours. -->
<param name="DatePattern" value="'.'yyyy-MM-dd-a"/>
```

```
<!-- If rolling style is set to 1 then by default log file will
be rolled when it reaches size of 5MB. -->
<param name="MaxFileSize" value="5MB"/>

<!-- This is log file rotation number. This only works for log
files rolled by size-->
<param name="MaxSizeRollBackups" value="5"/>
<layout class="com.brio.one.mgmt.logging.xml.XMLFileLayout">
</layout>
</appender>
```

3 **If the RollingStyle is 2 or 3, set the maixmum log rotation number in** `startcommonservices.bat located in` *`Install_Home`*`/BrioPlatform/bin`.

```
set BP_ROTATIONNUM=-Dlog_rotation_num=5
```

Table 14-2 Composite Rolling Appender Properties

RollingStyle	There are three rolling styles: ■ 1 - Roll the logs by size ■ 2 - Roll the logs by time ■ 3 - Roll the logs by size and time. This option could provide confusing results in that the naming conventions for logs rolled by time and size are different and the deletion counters do not count logs rolled differently together.
DatePattern value	If RollingStyle=2 or 3, set the time interval to write log messages to a new log file. Set the Date Pattern value using the string, yyyy-MM-dd-mm; for example, yyyy-MM-dd-mm means every 60 minutes, yyyy-MM-dd-a means every 12 hours, and yyyy-mm-dd means every 24 hours. Default is every 12 hours.
MaxFileSize	If RollingStyle=1 or 3, when the maximum file size is reached the system will write log messages to a new file. Default is 5MB. You can use KB (kilo byte), MB (mega byte), or GB (gigabyte).
MaxSizeRoll-Backups	If RollingStyle=1 or 3, when the maximum number of log files per originator type (plus one for the current file) is reached the system will delete the oldest file. Default is 5. Log files rolled by time are not affected by this setting.

Analyzing Log Files

This section details how to view log files, which log files are always generated, and which log files to look at in order to troubleshoot specific tasks.

Viewing Log Files

You can view log messages by looking directly at log files or by using a log viewer. This version of Hyperion Performance Suite contains the log4j viewer, LogFactor5. This viewer provides a way to filter and sort log messages.

To use LogFactor5:

1. **Copy the name of the LogFactor5 appender,** `<appender-ref ref="LF5APPENDER"/>`.

2. **Paste the copied codeline under the logger in which you want to use LogFactor5.**

```
<root>
<level value="WARN"/>
<appender-ref ref="LF5APPENDER"/>
<appender-ref ref="LOG_REMOTELY"/>
</root>
```

LogFactor5 will start automatically when the component you added the appender to is started. If the component is ongoing, LogFactor5 will start in 30 seconds. The LogFactor5 screen displays when logging initializes. Log messages are displayed as they are posted.

For more information on LogFactor5 and Chainsaw, see www.apache.org.

Standard Console Log File

The stdout_console.log is always generated regardless of the operation being performed or the log level. This log represent standard output and standard errors (console output). Some errors that are caught by the application are logged here. Start-up failures also generally appear in this log file.

Analyzing Specific Log Files

This section details which logs to analyze for the following specific tasks:

- Logs for Publishing General Content
- Logs for Publishing BQY Content
- Logs for Running Jobs
- Logs for Login/Logout Errors
- Logs for Managing Users and Groups
- Logs for Managing Roles
- Logs for Access Control
- Logs for Configuration

Logs for Publishing General Content

When creating, modifying, and deleting files or folders, the following logs can be used to analyze errors:

- Server Logs
  - *root_hostname_hostname_port number*_messages_PublisherService.log
  - *root_hostname_hostname_port number*_messages_RepositoryService.log
  - *root_hostname_hostname_port number*_messages_ServiceBroker.log
- Client Logs
  - *root_hostname_hostname_port number*_messages_BrowseServlet.log

Logs for Publishing BQY Content

When creating, modifying, and deleting BQY documents or jobs, the following logs can be used to analyze errors:

- Logs for publishing general content
- Server Logs
  - BI1_*hostname*.log
  - DAS1_*hostname*.log
  - 0_DAS_*hostname*.log (when using a process monitor)
  - 0_BI_*hostname*.log (when using a process monitor)
  - *hostname*_BI1_LSM.log
  - *hostname*_DAS1_LSM.log
  - root_hostname_hostname_port number_messages_DataAccessService.log
  - root_hostname_hostname_port number_messages_IntelligenceService.log
- Client Logs
  - *root_hostname_hostname_port number*_messages_DataAccessServlet.log
  - *root_hostname_hostname_port number*_messages_iHTMLServlet.log

Logs for Running Jobs

The Job Service runs jobs either directly or through the Event Service. The following logs can be used to analyze errors:

- Server Logs
  - *root_hostname_hostname_port number*_messages_EventService.log
  - *root_hostname_hostname_port number*_messages_JobService.log
  - *root_hostname_hostname_port number*_messages_ServiceBoker.log
  - root_hostname_hostname_port number_messages_DataAccessService.log
  - root_hostname_hostname_port number_messages_IntelligenceService.log
  - DAS1_*hostname*.log
  - BI1_*hostname*.log
- Client Logs
  - *root_hostname_hostname_port number*_messages_BrowseServlet.log
  - *root_hostname_hostname_port number*_messages_JobManager.log

Logs for Login/Logout Errors

A user login requires information from multiple areas in the system, each of which can cause an error and the login to fail. Use the following logs to analyze errors:

- Server Logs
  - *root_hostname_hostname_port number*_messages_SessionManager.log
  - *root_hostname_hostname_port number*_messages_ExternalDriverSynchronizer.log
  - *root_hostname_hostname_port number*_messages_GSM.log
  - *root_hostname_hostname_port number*_messages_LSM.log
  - *root_hostname_hostname_port number*_messages_Authentication.log
  - *root_hostname_hostname_port number*_messages_Authorization.log
  - *root_hostname_hostname_port number*_messages_Publisher.log
  - *root_hostname_hostname_port number*_messages_ServiceBroker.log
  - *root_hostname_hostname_port number*_messages_RepositoryService.log
- Client Logs (Servlet)
  - *root_hostname_hostname_port number*_messages_BrowseServlet.log
  - *root_hostname_hostname_port number*_messages_AdministrationServlet.log
  - *root_hostname_hostname_port number*_messages_PersonalPagesServlet.log
  - *root_hostname_hostname_port number*_messages_JobManagerServlet.log
  - *root_hostname_hostname_port number*_messages_ViewManagerServlet.log

Logs for Managing Users and Groups

Users and groups are managed by the Authentication Service. Users and groups can only be created by the Authentication Service that manages the authentication system in which they will belong. Use the following logs to analyze errors:

- Server Logs
  - *root_hostname_hostname_port number*_messages_Authentication.log
  - *root_hostname_hostname_port number*_messages_ExternalDriverSynchronizer.log
- Client Logs (Servlet)
  - *root_hostname_hostname_port number*_messages_AdministrationServlet.log
  - *root_hostname_hostname_port number*_messages_BrowseServlet.log

Logs for Managing Roles

Roles are managed by the Authorization Service. Use the following logs to analyze errors:

- Server Logs
  - *root_hostname_hostname_port number*_messages_Authentication or Authorization.log
- Client Logs (Servlet)
  - *root_hostname_hostname_port number*_messages_AdministrationServlet.log
  - *root_hostname_hostname_port number*_messages_BrowseServlet.log

Logs for Access Control

Access control is maintained by the Authorization Service. Use the following logs to analyze errors:

- Server Logs
  - *root_hostname_hostname_port number*_messages_Authorization.log
  - Specific logs for the service involved in the operation being performed
- Client Logs (Servlet)
  - *root_hostname_hostname_port number*_messages_BrowseServlet.log
  - *root_hostname_hostname_port number*_messages_AdministrationServlet.log
  - *root_hostname_hostname_port number*_messages_PersonalPagesServlet.log
  - *root_hostname_hostname_port number*_messages_JobManagerServlet.log
  - *root_hostname_hostname_port number*_messages_ViewManagerServlet.log

Logs for Configuration

Configuration errors for RSC services show at startup in the `stdout_console.log` or in the `root_hostname_hostname_port number_messages_NameService.log` file. It also might be helpful to look at `configuration_messages.log`.

What to Send to Customer Support

When a problem occurs and it is necessary to seek help from Hyperion customer support, send all application server logs for the instance being used. If it is applicable, compress the log directory.

For services and servlets, zip and send all logs under the `BrioPlatform/log` folder.

Summary

Generating the log messages you need to troubleshoot problems helps technicians, developers, administrators, and customer support debug all types of errors and problems.

PART VI

Appendices, Glossary, and Index

Row-Level Security in BQY Documents

This appendix explains the row-level security feature: what it is and how to implement it for BQY documents.

About Row-Level Security

Properly implemented, row-level security gives individuals in an organization access to only the information they need to make informed decisions. For example, managers need payroll information on their direct reports. Managers do not need to know payroll information for other departments within the organization. Row-level security allows this level of granularity.

The Row-Level Security Paradigm

Most database administrators understand the concept of row-level security. Returning to the payroll data example, all detailed compensation data on the employees of an organization is stored in the same table(s) within the database. Typically, some column within this table can be used as a limit, either directly or by a join to another table with its own set of limits, to restrict access to the data within the table based on the identification of the user accessing the data. Following the payroll example, an employee ID often identifies the sensitive compensation data. A join to a separate employee information table, which contains non-compensation related information such as home address and title, would include a department number. A manager would be limited to details on the employees for her/his particular department.

Row-level security, implemented at the database level, is often done by means of a view. To an application, accessing a view is no different than accessing a table. However, the view is instantiated based on the appropriate limits. Coupled with the GRANT and corresponding REVOKE data definition statements available with the prevalent Relational Database Management Systems (RDBMS), the base tables can be made inaccessible to most users, and the views on that data, filtered based on user identification, made accessible instead. Multiple views may sometimes be required to fully implement a security scheme, depending on how the tables are defined and how the information contained therein must be shared. For instance, a different view for managers versus those in human resources might be required.

Column level security, a companion concept to row-level security, can be similarly enforced. Views can easily hide a piece of information. For example, in the payroll example, the salary column can be left out of the view, but other types of information about an employee can still be accessible to those who need it. This type of security can impart a special problem for standardized reports, available throughout the organization but for audiences with different access permissions. The reporting software might have difficulty dealing with the missing information, consequently requiring different implementations of these otherwise similar reports.

Hyperion Performance Suite and Row-Level Security

The Hyperion Performance Suite approach to data security is server based. Both the Intelligence Server and the Intelligence iServer are designed to fully implement a secure data access platform. The non-server based clients do not participate in this security mechanism. Users of the Designer and Explorer clients need access beyond that of most users to effectively create the dashboards, and analytic reports required by the majority of the data consumers. In addition, the security information can be placed in a centralized location for the servers (the repository). For the desktop clients, it would in some cases need to be dispersed to multiple databases and maintained separately.

To effectively control access, the servers key off the user's identification when connecting to it. This is the user's logon name, used to establish a session with the Hyperion Foundation services.

Beyond this user name, the servers make no assumptions about the user's place within the organization. A security system can be built entirely independent of any existing grouping of users. New groupings can be defined in lieu of existing ones. This is especially important where groups were not defined with data security as a primary goal. Row-level security can also take full advantage of the existing structures where data security was built into the user and group structure. In many cases, row-level security will work within existing database role definitions and third-party software security systems.

Column Level Security

Hyperion Intelligence servers can easily handle the challenge of column level security. Such hidden information is replaced with an administrator-supplied value (possibly NULL, zero, blanks, or a similar placeholder value), and thus it will not cause existing reports to fail when encountering this type of a security constraint.

Performance Issues

The system is designed to not impose any significant performance penalty. The security information is collected at the time the user opens a document from the server's repository, and only then if the server knows the security controls are enabled. When a user opens a locally saved document from a previous session with the Hyperion Foundation services, the security information is recollected when reconnecting to the server in case it has changed.

Publishing in a Secure Environment

A powerful feature of the Intelligence clients is the ability to take data "on the road." Once data has been extracted from the database, which is where the row-level security restrictions are enforced, that data can be saved with the BQY document for offline analysis and reporting. Users who publish should be aware of the implications of their audience when publishing data and reports.

If the publication of the data is difficult to control in the current configuration of users and groups known to the server, consider the following options:

- Publish without the detailed results of the queries, leaving only the summary charts and Pivots for the "general" audience. If they need to drill into the summary data, they will need to rerun the queries, at which time their particular security restrictions will be applied. (Even some charts and Pivots can reveal too much, so there is still a need for prudence when publishing these documents.)
- Create the documents with `OnStartup` scripts to reprocess queries as the document is opened. This will always give the user only the data to which they are entitled.

All users should take similar precautions when sharing information generated from Hyperion Foundation Intelligence clients. This includes exchanging the report files (BQY extensions) themselves by email or shared network directories, exporting the data as HTML files and publishing them to a web site, posting the data on FTP servers as the result of a job action, and creating PDF files from the reports.

Securing the Security Information

The row-level security feature is implemented by means of database tables. The servers read this data and never update it. Hyperion recommends these tables actually be defined somewhere other than the repository schema, and that read-only access be granted to only the select few that should be able to update the security information.

As additional protection, the actual tables can be hidden via a view, and a WHERE clause can be added to each view definition so that only the server's user identification, by which it connects to the database to read the row-level security tables, can read the content, if the database supports it. Table A-1 shows examples of Where clauses if the repository connection is made as user *brioserver*.

Table A-1 Repository Connection Made as *brioserver*

Database	Sample Where Clause on CREATE VIEW
DB2	WHERE USER = 'BRIOSERVER'
Oracle	WHERE USER = 'BRIOSERVER'
SQL Server	WHERE USER = 'brioserver'

Note Be aware of case sensitivity with the user name and allow that, for SQL Server, the user might be 'dbo'.

Each view has the same name as its underlying table, and all available columns from that table would be selected.

Row-Level Security Tables

Two tables implement the row-level security features for the plug-in and Intelligence iServer clients. Because the tables can be populated in a manner appropriate to the site's requirements, no predefined user interface to maintain the tables is provided as part of the Hyperion Intelligence product. However, on the Documents CD, a BQY document, `row level security.bqy` can be modified to suit an ad hoc implementation of the row-level security feature, and as a tutorial or test tool when setting up a production system. The only requirement is that the basic set of column definitions be retained. The sample document can be used in all cases as a reporting tool for the row-level security data as the servers see it.

Implementing a secure data access environment using row-level security requires an understanding of SQL. First, knowing how the database relationships are defined is critical. Second, specifying the restrictions is directly translated into the SQL ultimately processed at the database.

Creating the Row-Level Security Tables

When the Hyperion Performance Suite components are installed using the *custom* option, the installer prompts for whether or not to create the row-level security tables and in what database.

If the Hyperion Performance Suite components are installed using the *express* option, or it is elected not to create the row-level security tables during a custom install, then the tables must be created manually. The BQY file mentioned above can create the tables, the necessary SQL DDL can be created based on the table definitions found in this documentation, or the script that creates them during the install can be run. To locate these scripts, look on the install CD under the DATA directory, and then under the appropriate database brand or vendor. The script of interest is named `CreateRLS.sql`.

When creating the tables post-install, use the web-based Administration module to tell the system where the tables are located. The information required includes the data source name, the database type, the API used to access the database, and the database credentials needed to access the row-level security tables. For details on setting the row-level security properties, see "Managing Row-Level Security" on page 10-41.

There is also a setting to enable or disable the row-level security feature. This setting is intended to enhance performance in systems where the feature is not needed. When disabled, no attempt is made to access these tables. The feature should always be enabled if data security is to be enforced.

The BRIOSECG Table

The BRIOSECG table defines the users and groups that are subject to row-level security restrictions. There are two columns, BUSER and BGROUP, both of varying character length (VARCHAR(n)). The maximum length is not fixed by the server; set it to a practical value.

A user name is defined as the server authentication name (`ODSUsername` is the property of the ActiveDocument object in the Brio Object Model). For jobs, it is the user who scheduled the job.

Group names are arbitrary. The data security administrator is free to define these as required. When both columns of a row are populated with non-null values, the user name defined in the BUSER column is a member of the group name defined in BGROUP.

As maintained by the sample BQY file, `row level security.bqy`, when a user is added, a row is added to the table with a NULL value in the BGROUP column. When a group is added, a NULL value is stored in the BUSER column. This is a device used by the sample document to maintain the table and is recommended practice, but it is not a requirement for correct operation of row-level security.

This table is theoretically optional. Without it, however, all users exist as single individuals; they cannot be grouped to apply a single set of restrictions to all members. For example, Vidhya and Chi are members of the PAYROLL group. If this relationship is not defined in BRIOSECG, then any restrictions that apply to Vidhya that should also apply to Chi have to be defined twice. By defining the PAYROLL group and its members, Vidhya and Chi, the restrictions can be defined only once and applied to PAYROLL group.

A group name cannot be used in BUSER; that is, groups cannot be members of other groups. Users, of course, can be members of multiple groups, and this can effectively set up a group/subgroup hierarchy. For example, a PAYROLL group might contain users Sally, Michael, Kathy, David, Bill, Paul, and Dan. Sally, Dan, and Michael are managers, and so they can be made members of a PAYROLL MANAGER group. Certain restrictions on the PAYROLL group can be overridden by the PAYROLL MANAGER group, and Dan, to whom Sally and Michael report, can have specific overrides to those restrictions placed explicitly on the PAYROLL MANAGER group.

Where the database supports it, and if the user's authentication name in Hyperion Performance Suite corresponds, this table can be a view created from the roles this user has in the database. For example, in Oracle:

```
CREATE VIEW BRIOSECG (BGROUP, BUSER) AS
   SELECT GRANTED_ROLE, GRANTEE FROM DBA_ROLE_PRIVS
```

DBA_ROLE_PRIVS is a restricted table. Since the server reads the view using a configured database logon, it would not be appropriate to use USER_ROLE_PRIVS instead of DBA_ROLE_PRIVS, because that user view will reflect only the server's roles, not the user on whose behalf the server is operating. Again, this is an Oracle example; other RDBMS may or may not provide a similar mechanism. In some cases, depending on the database, a stored procedure could collect the role information for the users and populate a BRIOSECG table if a simple SELECT is inadequate to collect the information. This would require some means to invoke the procedure each time role definitions were changed.

When using the database's catalog or some other means to populate `BRIOSECG`, the sample document, `row level security.bqy`, cannot be used to maintain user and group information.

A special group, PUBLIC, exists. It does not need to be explicitly defined in BRIOSECG. All users are members of the PUBLIC group. Any data access restriction defined against the PUBLIC group applies to every user unless explicitly overridden, as described later.

All users can be made part of a group at once by inserting a row where BUSER is 'PUBLIC' and BGROUP is that group name. While this may seem redundant, given the existence of the PUBLIC group, it offers some benefits:

- It allows the database catalog technique described above to work. For example, in Oracle, a role can be granted to PUBLIC.
- It allows restrictions for a group other than PUBLIC to quickly be applied to or removed from everyone in an instant.
- It provides more flexibility when using override specifications as described later.

Note Restrictions are never applied against a user named PUBLIC, but only the group PUBLIC. For this reason, do not use PUBLIC as a user name. Similarly, to avoid problems, do not name a group the same as a user name.

The BRIOSECR Table

The BRIOSECR table is the heart of the row-level security feature. It defines the specific restrictions to be applied to users and the groups (including PUBLIC) to which they belong. These restrictions take the form of join operations (a user cannot access a column in the employee salary table unless it is joined to the employee table), and limits (WHERE clause expressions) to be applied to either the source table (SALARY) or table(s) (EMPLOYEE) to which it is joined.

Table A-2 lists the columns in the `BRIOSECR` table.

Table A-2 Columns in the BRIOSECR Table

Column Name	Column Type	Functional Use
UNIQUE_ID	INT	This column contains an arbitrary numeric value. It should be unique, and it is useful for maintaining the table by whatever means the customer chooses. The servers do not rely upon this column, and the servers never access this column. To that extent, it is an optional column but recommended. (It is required when using the sample file, `row level security.bqy`.) When the RDBMS supports it, a unique constraint or unique index should be applied to the table on this column.
USER_GRP	VARCHAR	The name of the user or the name of a group to which a user belongs. If PUBLIC, the restrictions are applied to all users.
SRCDB	VARCHAR, can be null	Used to identify a topic in the Data Model. (In the Intelligence clients, a topic typically corresponds to a table in the database, but it could be a view in the database.) If the physical name property of the topic is of the form name1.name2.name3, this represents name1. Most often, this represents the database in which the topic exists. This field is optional unless required by the connection in use. The most likely circumstance in which to encounter this requirement will be with Sybase or Microsoft SQL Servers where the OCE (the connection definition file) is set for access to multiple databases.
SRCOWNER	VARCHAR, can be null	Used to identify the owner/schema of the topic in the Data Model. This would be name2 in the three-part naming scheme shown above. If the topic property, physical name contains an owner, then it must be used here as well.
SRCTBL	VARCHAR	Used to identify the table/relation identified by the topic in the Data Model. This is name3 in the three-part naming scheme.
SRCCOL	VARCHAR	Used to identify a column in SRCTBL. This is a topic item in Data Model terminology, and is an item that might appear on the Request line in a query built from the Data Model. In the context of the security implementation, the item named here is the object of the restrictions being defined by this row of the security table BRIOSECR. If this column contains an *, all columns in `SRCTBL` are restricted.
JOINDB	VARCHAR, can be null	If present, defines the database name qualifier of a table/relation that must be joined to `SRCTBL`.
JOINOWNR	VARCHAR, can be null	If present, defines the schema/owner name qualifier of a table/relation that must be joined to `SRCTBL`.
JOINTBL	VARCHAR, can be null	If present, names the table/relation that must be joined to `SRCTBL`.
JOINCOLS	VARCHAR, can be null	If present, names the column name from `SRCTBL` to be joined to a column from `JOINTBL`.

Table A-2 Columns in the BRIOSECR Table

Column Name	Column Type	Functional Use
JOINCOLJ	VARCHAR, can be null	If present, names the column name in JOINTBL that will be joined (always an equal join) to the column named in JOINCOLS.
CONSTRTT	CHAR(1), can be null	If present, identifies a table/relation to be used for applying a constraint (limit). This is a coded value. If the value in this column is *S*, the column to be limited is in SRCTBL. If *J*, a column in JOINTBL is to be limited. If the value in this column is *O*, it indicates that for the current user/group, the restriction on the source column for the group/user named in column OVRRIDEG is lifted, rendering it ineffective. If this value is NULL, then no additional restriction is defined. If the JOIN* columns are also all NULL, the column is not accessible at all to the user/group. This implements column level security. See the functional use description of CONSTRTV for more information on column level security.
CONSTRTC	VARCHAR, can be null	The column in the table/relation identified by CONSTRTT to which a limit is applied.
CONSTRTO	VARCHAR, can be null	The constraint operator, such as =, <> (not equal), etc. BETWEEN and IN are valid operators. Basically, any valid operator for the database can be supplied.
CONSTRTV	VARCHAR, can be null	The value(s) to be used as a limit. The value(s) properly form a condition that together with the content of CONSTRTC and CONSTRTO columns create valid SQL syntax for a "condition" in a WHERE clause. Subquery expressions, therefore, are allowed. Literal values should be enclosed in single quotes or whatever delimiter is needed by the database for the type of literal being defined. If the operator is BETWEEN, the AND keyword would separate values. If :USER is used in the value, then the user name is the limit value. If :GROUP is used, all groups of which the user is a member are used as the limiting values. Both :USER and :GROUP can be specified, separated by commas. The public group must be named explicitly; it is not supplied by reference to :GROUP. When applying column level security, CONSTRTV provides the SQL expression that will effectively replace the column on the Request line. For example, the value zero (0) might appear to replace a numeric value that is used in the document but should not be accessible by the specified user/group. While any valid SQL expression that can be used in a SELECT list is permitted, pick a value that is acceptable for the likely use. For example, the word NULL is permitted, but note that in some cases, it might not be the appropriate choice, as it could also end up in a GROUP BY clause.
OVRRIDEG	VARCHAR, can be null	The name of a group or user. Used when CONSTRTT is set to O. If the group named in OVRRIDEG has a restriction on the source element, then this restriction is effectively ignored for the user/group named in USER_GRP. SRCDB, SRCOWNER, SRCTBL, and SRCCOL as a collection must be equal between the row specifying the override and the row specifying the conditions to be overridden. (See examples.)

As suggested earlier, existing security definitions can sometimes be translated into the format described here. A view, stored procedure, or programmatic mechanism can be used to translate and/or populate the information needed in `BRIOSECR` by the Hyperion Performance Suite servers. When these methods are used, the servers require the column names and data types defined above. And again, do not attempt to use the sample document, `row level security.bqy`, to manage this information.

If a join table is specified and it does not already exist in the data model the user accesses, it will still be added to the final SQL generated to ensure the security restrictions are enforced. This process is iterative. When a table is added and the present user, either directly or by group membership, has restricted access to that added table, those restrictions will also be applied, which may mean additional tables will be added, and those restrictions will also be checked, and so on. Circular references will result in an error if they are defined.

Row-Level Security Examples

The examples are based on the sample Access database, `Brio 8 Sample Database.mdb`, provided by option when installing Hyperion Performance Suite on a Windows platform, using the connection file `Brio 8 Sample.oce`.

For these examples, the users BRIO and VIEW&PROCESS require access to data that is denied to the rest of the users. These two users both belong to the group AMERICAS, which corresponds to a region of the same name. However, the user BRIO is a corporate officer who should be able to see all data.

Only one piece of data will be accessed in the course of these examples: the amount sales column from the sales fact table. The examples are more far-reaching than this might seem.

Screenshots for these examples come from the document to which processing restrictions are applied, and from the sample document, `row level security.bqy`, mentioned earlier. For the screen shots from the sample document, the columns in the BRIOSECR table follow in a top down, left to right manner for the most part with the fields on the screen. Deviations from this will be noted where possible. In particular, though, note

that the UNIQUE_ID column is not shown in this sequence of fields, appropriate to its optional role to the functionality of the software, although it is used behind the scenes by the sample document.

Figure A-1 shows the layout of the data in the database, to illustrate the possible joins as intended by the database designer.

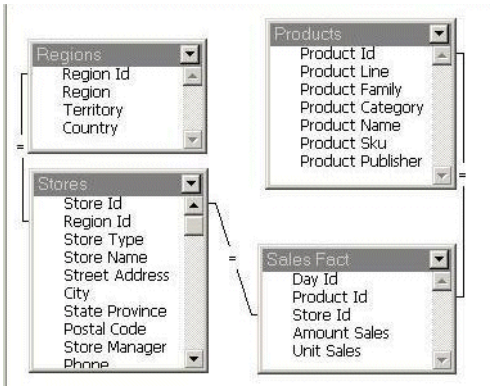


Figure A-1 Database Layout Showing Possible Joins

Figure A-2 shows the data model in the published document.

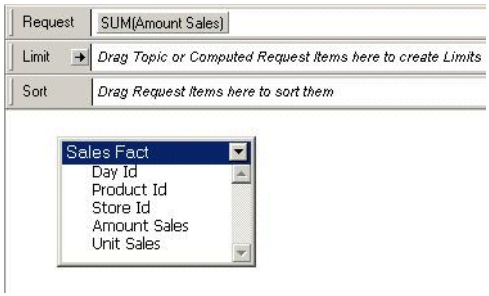


Figure A-2 Data Model in the Published Document

Defining the Users and Groups

Based on the above description of the users and groups involved in this example, insert a minimum of two rows into the BRIOSECG table, as shown in Table A-3.

Table A-3 Rows to Insert in the BRIOSECG Table

BGROUP	BUSER
AMERICAS	BRIO
AMERICAS	VIEW&PROCESS

In the sample document for maintaining row-level security information, once the information has been added, it would look something like Figure A-3 when the AMERICAS group is selected.

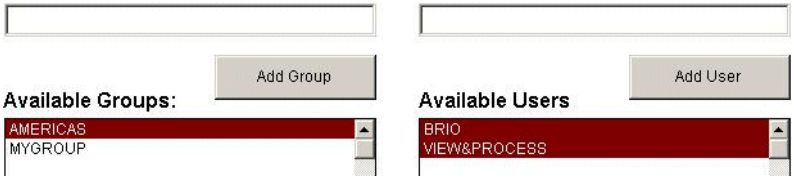


Figure A-3 Sample Document with AMERICAS Group Selected

Dealing with "The Rest of the Users"

The requirement here was that users who were not part of the AMERICAS group should have no access to this information. There are several ways to do this, and in part, what the best way is depends on who the "rest of the users" are.

If they are extranet users, this probably means no access; users outside of the corporate network should not get sales data, even summary data, as this might be considered proprietary and certainly not for any potential competitors. Using the PUBLIC group, restrict the entire SALES_FACT table from accessing this information by using the asterisk to reflect all columns (see Figure A-4).

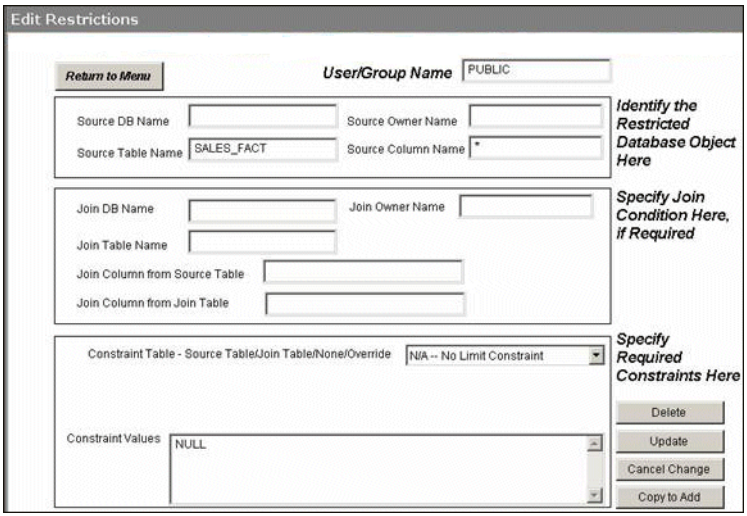


Figure A-4 Restriction on SALES_FACT Table

(This is an example of column level security. All values from this table, if they appear on the Request line, will be substituted with NULL.)

Where there are no extranet concerns, it might be appropriate for all the employees to know how their company is doing overall, such a blanket restriction is not recommended. Instead, restrict the use of the STORE_ID column, the only means by which the sales information can be tied back to any particular store, country, region, etc. This will look identical to the case above except that STORE_ID is specified instead of an asterisk for the Source Column Name.

Overriding Constraints

Obviously, members of the AMERICAS group are also members of PUBLIC. So, regardless of the way the PUBLIC group was restricted, those restrictions are not to be applied to the AMERICAS group for the sales information. That group might be restricted in different ways, or not at all, and the same mechanism ensures that happens while PUBLIC restrictions are in place. Figure A-5 shows this when using the sample document, `row level security.bqy`.

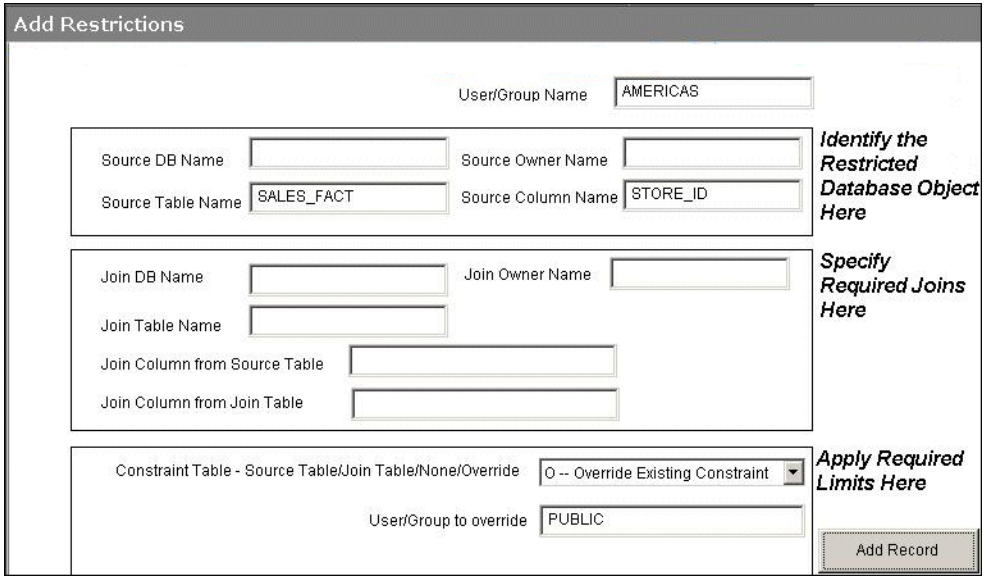


Figure A-5 Overriding Constraint on User/Group

This only overrides PUBLIC constraints for this particular column. Restrictions on PUBLIC against other columns are still enforced against members of the AMERICAS group as well. If the restriction is on all columns of a table, designated by an asterisk, the override must also be specified with an asterisk and then specific column constraints reapplied to groups as needed.

Cascading Restrictions

In order to give the members of the AMERICAS group access to sales information only for the appropriate region, the query includes references to columns in other tables which are not necessarily part of the existing data model. The row-level security will function the same whether or not the tables already existed in the data model.

As seen in the table relationships pictured above, the region information is bridged to the sales information by the store table. To implement a constraint that makes only sales information available for a particular region requires two entries in the BRIOSECR table, one to join sales to stores, and one to join stores to regions. This latter case also requires a limit value for the region name. (A limit on REGION_ID could also accomplish the same goal, but is not as readable, especially in an example. See the discussion to follow about subqueries for another perspective on limits on ID type columns.)

The first restriction required for this example is on the STORE_ID column. In order to use that column, a join must be made back to the STORES table. Figure A-6 shows how this join would be specified.

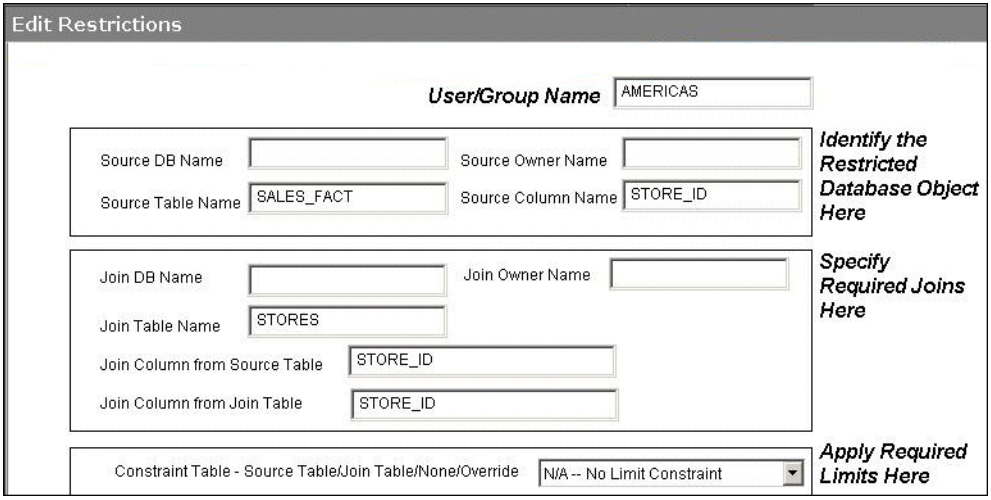


Figure A-6 Join to STORES Table

Now, the join to the Regions table is added, with the appropriate constraining value, as shown in Figure A-7.

Edit Restrictions

User/Group Name: AMERICAS

Identify the Restricted Database Object Here

Source DB Name:
Source Owner Name:
Source Table Name: STORES
Source Column Name: REGION_ID

Specify Required Joins Here

Join DB Name:
Join Owner Name:
Join Table Name: REGIONS
Join Column from Source Table: REGION_ID
Join Column from Join Table: REGION_ID

Apply Required Limits Here

Constraint Table - Source Table/Join Table/None/Override: J -- Limit on Join Table
Constraint Column to which limit is applied: REGION
Constraint Operator: =
Constraint Values: 'Americas'

Delete
Update
Cancel Change
Copy to Add
Return to Menu

Figure A-7 Join to Regions Table

The only remaining part of the example is letting user BRIO, also a member of the AMERICAS group, see the data in an unrestricted way. Handling this case is left as an exercise for the reader.

Other Important Facts

This section contains miscellaneous information about the implementation of row-level security.

Custom SQL

Custom SQL is used to provide special SQL syntax that the software does not generate. In the absence of row-level security, users with proper permissions on the document can modify custom SQL to produce ad hoc results.

When row-level security is in place, Custom SQL is affected in two ways:

- If the published document contains an open Custom SQL window, it is used as is when the user processes a query. No restrictions are applied to the SQL. However, the user cannot modify the SQL. While this can be a handy feature, care should be taken when publishing documents that require custom SQL that they don't compromise the security requirements.
- If the user chooses the Reset button on the Custom SQL window, the SQL shown includes the data restrictions, and the original intent of the Custom SQL is lost and the user will not be able to get it back except by requesting the document from the server again.

Similar issues apply to the use of imported SQL.

Limits

The row-level security feature affects limits three ways:

First, if a user is restricted from accessing the content of certain columns, and the user attempts to show values when setting a limit on the restricted column, the restrictions will be applied to the SQL used to get the show values list. That way, the user cannot see and specify a value they would not otherwise be permitted to access.

Second, setting limits can result in some perhaps unexpected behavior when coupled with row-level security restrictions. This is best explained by example. In order to read the amount of sales, the user is restricted to a join on the STORE_ID column back to the stores table and in addition, the user can only see information for the STORE_ID when the state is Ohio. This user tries to set a limit on the unrestricted column STATE, and chooses something other than Ohio, thinking this a way to subvert the data restrictions. Unfortunately for that user, no sales amount information will be returned at all in this case. The SQL will specify "where state = 'user selected value' AND state = 'OH'". Obviously, the state cannot be two different values at the same time, so no data will be returned.

Of course, a user may try to set a limit on the CITY column instead of the STATE column, thinking the city name might exist in multiple states. As long as the need exists to access the amount of SALES column in the SALES table with identifying store information, though, the state limit will still be applied, and no data the user should not be able to see will be accessible to that user. It just will not prevent a user from getting a list of stores when sales data is not part of that list. Generally speaking, restricting access to facts based on the foreign key in the fact table(s) works best. If it is necessary to restrict the user's access to a list of stores, these dimension restrictions work best when applied to all columns in the dimension table with a limit on the source table.

For example, using the requirements described above to restrict the amount of sales information in Ohio only, with the same restriction on the dimension-only queries, do not apply any limit on access of the amount sales information except that it must be joined back to the STORES table on STORE_ID. Then, add a restriction for all columns in the STORES table, limiting it to only stores in Ohio. This limits access to both fact and dimension data.

Third, when setting a limit using Show Values, it has already been noted that any restrictions on the column to be limited are applied to the SQL that generates the show values list. For example, using the restrictions described in the previous paragraph, attempting to show the values list for the CITY column would be constrained to those cities in Ohio. Now, consider the following scenario.

The SALES FACT table also has a TRANSACTION DATE and PRODUCT_ID column. The transaction date column is tied back to a PERIODS table, where dates are broken down into quarters, fiscal years, months, and so on. In this somewhat contrived example, a restriction is placed on the PERIODS table, where values there are joined back to the SALES TRANSACTION table and restricted by PRODUCT_ID values in a certain range. The user sets a limit on fiscal year in the PERIODS table and invokes show values in the Limit dialog box to pick the range. Because of the restrictions in place, only one fiscal year is available, and the user picks it. Now, the user builds a query that does not request the FISCAL YEAR column itself but does reference the PRODUCT_ID field and processes it. This query returns, for the sake of argument, 100 rows. Now the user decides there is a need to see the fiscal year value and adds it to the Request line. Reprocessing the query only returns 50 rows.

Why? In the first case, PRODUCT_ID values outside of the range allowed when querying the FISCAL YEAR column will appear in the results. In the second case, the query will cause the restriction on PRODUCT_ID range to be included. Restrictions are only applied when a user requests to see data. There was no request to see the FISCAL YEAR column in the first case, except while setting the limit. There is no restriction on seeing PRODUCT_ID values. This example is contrived because restricting access to a dimension based on data in a fact table would be extremely unusual. Nevertheless, it illustrates a behavior that should be kept in mind when implementing restrictions.

Naming

Another way to set the restrictions described above is by a subquery. Instead of directly setting the limit on the STATE column, limit the values in the STORE_ID column in the STORES table. The constraint operator would be IN, and the constraint values field might look something like this:

```
(SELECT S.STORE_ID FROM STORES S WHERE S.STATE = 'OH')
```

Now, no matter what limit the user sets in the STORES table, they will always be constrained to the set of store IDs that are allowed based on their group memberships and their own user name. Even if a city outside of the allowed state is chosen, such as a city that exists in more than one state, any stores that other city has will not show up in the results.

Using a subquery can be useful when incorporating existing security systems into the row-level security feature of Hyperion Intelligence Client and Hyperion Intelligence iServer clients. When constructing constraints of this type, it is especially important to know SQL. For example, to specify a subquery, it helps to know that a subquery is always enclosed in parentheses. It is also important to know how Hyperion Performance Suite generates SQL and to follow its naming conventions to make sure the syntax generated is appropriate.

Table and Column Names

For the most part, simple security constraints reference directly the actual object names in the database. Case sensitivity in names should be observed when and where required. For subqueries and other SQL constructs used to specify the constraint values, it is sometimes useful to refer to objects already used by the software's SQL generation process. To do this:

- For table references in the FROM clause, use `From.tablename`, where *tablename* is the display name seen in the Intelligence document's data model as the display name. If the display name contains a space, use the underscore to represent the space.
- For column names, use `tablename.columnname`, following the same rule as above, except that the `From.` should *not* be used.

Alias Names

By default, when processing user queries, table references in the SQL are always given alias names. Alias names are convenient shorthand for long table references, and they are required when trying to build correlated subqueries. These alias names take the form "ALn", when the 'n' is replaced by an arbitrary number. These numbers are usually based on the topic priority properties of the data model and can easily change based on several factors. For example, a user with the proper permissions can rearrange the topics, thus giving them different priorities. Because these numbers are dynamic, constraint specifications should never rely on them. Instead, by using the naming scheme above, the appropriate alias will be added to the constraints. So, if the requirement is a correlated subquery, the appropriate name will be given to the column in the outer query when referenced by the correlated subquery.

In the example above, using a subquery to restrict STORE_ID values to those in a specific state, it was neither necessary nor desirable to use the Hyperion naming conventions. There, the set of values was to be derived in a subquery that operated independently of the main query. Consequently, the 'From.' was not used in the FROM clause of the subquery, and the alias names were given in a way to not conflict with the alias names generated automatically by the software.

To use a correlated subquery, then, consider syntax like the following:

```
…FROM STORES S WHERE S.STORE_ID = Stores.Store_Id
```

The reference to the right of the equal sign will pick up the alias name from the outer query and thus provide the correct correlation requirements.

B Process Monitor Implementation

This appendix provides specific instructions for implementing and configuring process monitors for starting and stopping the Intelligence service and the Data Access service.

About Process Monitors

Process monitors allow you to periodically restart services that might have deteriorated in performance over time. Use a process monitor to start and stop a service that needs to be monitored and controlled. Each service has its own process monitor.

A process monitor gracefully shuts down a service while starting another one to take its place. Currently process monitors are available to start and stop the Intelligence service and the Data Access service. The process monitor insures that there is only one registered Intelligence service and one registered Data Access service in the system at a time with the same instance ID processing incoming requests.

In the `server.xml` file you can choose the event and the event threshold you want to use to restart the service. For Intelligence service, you can choose from the following events: maximum number of documents retrieved, maximum number of jobs run, maximum amount of time running the service, or simply state a specific time. For the Data Access service, you can choose from the following events: maximum number of database requests, maximum number of other database requests, maximum amount of time running the service, or simply state a specific time.

Using Process Monitors

Use a process monitor to startup the Intelligence service and the Data Access service. The process monitor automatically starts, stops, and restarts the service so you have less down time.

To configure and start a process monitor to monitor a service:

1. **Configure process monitor properties in the `BIprocessmonitor.properties` file or the `DASprocessmonitor.properties` file.**

   See "Configuring a Process Monitor" on page B-4 for details.

2. **Configure the event trigger threshold you want to use in the `server.xml` file for the services you are starting with a process monitor.**

   See "Intelligence Service Process Monitor Event Thresholds" on page B-5 and "Data Access Service Process Monitor Event Thresholds" on page B-5 for details.

3. **Start the BI service or DAS service using a process monitor script.**

   See "Starting a Service Using a Process Monitor" on page B-6 for details.

4. **Use the process monitor log files to monitor the service.**

Configuring a Process Monitor

Configure the process monitor properties in the `server.xml` file and the `BIprocessmonotor.properties` file or `DASprocessmonitor.properties` file located in the `Install_Home\BrioPlatform\etc` directory. The `server.xml` file stores event threshold information, while the properties files store configurable properties for either BI process monitors or DAS process monitors. The following three tables describe the fields in each file. The properties in the following table are in the properties files.

Set the process monitor log level in `remoteServiceLog4jConfig.xml`. For more information on configuring log levels, see "Configuring Log Files for Troubleshooting" on page 14-9.

Table B-1 Process Monitor Properties

MONITOR_THREAD_INTERVAL	Interval for polling the internal status of the service in seconds. Minimum and default = 30, maximum=300.
MONITOR_THREAD_TIMEOUT	Number of seconds the service is stopped if the polling is not working. Minimum and default = 300, maximum=600.
HARD_SHUTDOWN_TIMEOUT	Number of seconds the process continues before a hard shutdown. Maximum and default = 30, no minimum.
GRACEFUL_SHUTDOWN_TIMEOUT	Number of seconds the process continues during a graceful shutdown. This allows a service to continue processing in the background. Default=14400(4 hours), minimum=3600 (1 hour), maximum= 86400 (1 day).
IOR-FILE_NAME	The path to the services generated data file. Default is C:\\IOR.txt
SERVICES_STDOUT_FILE_PATH	The path to the services standard output file location. Default is C:\\DAS_stdout.txt.
SERVICE_STDERR_FILE_PATH	The path to the services standard error file location. Default is C:\\DAS_stderr.txt.

Intelligence Service Process Monitor Event Thresholds

Set threshold events, listed in the following table, to trigger the process monitor to stop and restart the service. The threshold events for BI service are in the `server.xml` file in a property list called BQ_EVENT_MONITOR_PROPERTY_LIST. Set the first property, EVENT_MONITORING, to ON to enable threshold event usage. Comment out or delete the thresholds not in use.

Table B-2 Intelligence Service Process Monitor Event Threshold

EVENT_MONITORING	Set to ON to use one of the following events.
MAXIMUM_DOCUMENTS_THRESHOLD	Number of BQY documents retrieved.
MAXIMUM_JOBS_THRESHOLD	Number of BQY jobs run.
MAXIMUM_UP_TIME_THRESHOLD	Total time the service has been running since its first request.
SPECIFIC_SHUTDOWN_THRESHOLD	Specific time of day the service is not available in minutes after midnight. For example, 150 means 2:30 AM.

Data Access Service Process Monitor Event Thresholds

Set threshold events, listed in the following table, to trigger the process monitor to stop and restart the service. The threshold events for DAS service are in the `server.xml` file in a property list called DAS_EVENT_MONITOR_PROPERTY_LIST. Set the first property, EVENT_MONITORING, to ON to enable threshold event usage. Comment out or delete the thresholds not in use.

Table B-3 Data Access Service Process Monitor Event Thresholds

EVENT_MONITORING	Set to ON to use one of the following events.
MAXIMUM_RELATIONAL_PROCESS_THRESHOLD	Number of relational database process requests including Oracle, SQL Server, Sybase, DB2, etc.
MAXIMUM_MDD_PROCESS_THRESHOLD	Number of MDD database process requests including Essbase, MSOLAP, SAP, etc.

Table B-3 Data Access Service Process Monitor Event Thresholds *(Continued)*

MAXIMUM_RELATIONAL_OTHER_THRESHOLD	Number of all other relational database requests including requests like stored procedure calls, get function lists, etc.
MAXIMUM_MDD_OTHER_THRESHOLD	Number of all other MDD database requests including requests like build outline, get members, show values, etc.
MAXIMUM_UP_TIME_THRESHOLD	Total time the service has been running since its first request.
SPECIFIC_SHUTDOWN_THRESHOLD	Specific time of day the service is not available in minutes after midnight. For example, 150 means 2:30 AM.

Starting a Service Using a Process Monitor

Use the process monitor scripts located in the *Install_Home*/BrioPlatform/bin directory. Each startup script is either an executable Bourne shell script file with the extension .sh (UNIX), or a batch file with the extension .bat (Windows).

Each startup script name is composed of an abbreviation for the service type, a number uniquely identifying the particular service, and the string *start*, followed by the extension .sh or .bat. Typical startup script names are, for example:

- BI1_apollo_start.bat – Intelligence Service
- DAS1_apollo_start.sh – DAS

Use the same startup script if using a process monitor or if not using a process monitor. To start the service with a process monitor do not pass a command line parameter. To start the service without a process monitor pass any command line parameter (such as nopm).

For Windows, you can also start the BI and DAS service with a process monitor in the Windows Services tool. In the Windows Services tool, in addition to the BrioPlatform Server, there is a Windows service for the Intelligence Service and one for the DAS that uses the process monitor. A typical Windows service name is, for example, BrioPlatform_BI1_apollo_12345 (for the Intelligence Service).

Glossary

access control A security mechanism that manages a user's privileges—such as viewing, modifying, publishing—to a system's resources.

access privileges The level of access—for example, view, modify, run, full control—that the publisher of an item grants to others; also, at what level other users or groups can access a user or group as well as what a user and members of a group can do.

actions Execution of a BQY job is defined in terms of a series of actions. Actions define the job output format.

active group A group that is currently entitled to access the system.

active service A service whose *Run Type* is set to Start rather than Hold.

active user *A* user who is currently entitled to access the system.

adaptive states BQY level of permission. There are six levels of permission: view only, view and process. analyze, analyze and process, query and process, and datamodel and analyze.

administrator A predefined user who generally is granted roles that grant administrative capabilities, but is not exempt from access privilege checking.

appender Log4j term for destination.

application A program running within a system, such as SQR.

Authentication Service A Core service that manages one authentication system.

Authentication Service repository (ASR) A Database that contains a complete model of users/groups in external system.

authentication system A security measure designed to validate and manage users and groups.

bookmark A link to a Hyperion Performance Suite item or a web site, displayed on a Personal Page of a user. The two types of bookmarks are My Bookmarks and image bookmarks.

bounding rectangle The perimeter that encapsulates the BQY content when embedding BQY sections in a Personal Page. It is required by the Intelligence iServer to generate HTML and is specified in pixels for height and width or row per page.

BQY files or jobs Files created by the Hyperion's Intelligence products and published into the Repository as files or as jobs. Files and jobs have different capabilities.

BQY sections Divisions of a BQY file used to display and analyze information in different formats (such as Chart Section and Pivot Section).

BrioPlatform Server A Windows service that starts all the active Foundation services of Hyperion Performance Suite. Its default name is: `BrioPlatform_`*`LocalHost_GSMHost_GSMPort.`*

connection file See Open Catalog Extension Files (OCE) Files

content Information stored in the Hyperion Foundation Repository. It includes report programs (jobs), report output, documents such as spreadsheets or word processing documents, images, HTML pages, files of any type, multiple versions of files, or URLs.

cookie A small piece of information placed on your computer by a web site.

custom calendar Any calendar created by an administrator.

cycle Used when scheduled BQY jobs need to process and produce different job output with one job run. Cycles are among the BQY job parameters.

default folder A user's home folder.

embedded section Sections from the Hyperion Intelligence Products (Results, Tables, Pivots, Charts, and OLAP Results) can be embedded into a Personal Page. All embedded sections maintain live data content and formatting from the original section.

exception A condition or result (such as a threshold being reached) generated by an automated process, which requires some intervention or oversight. It can cause (a) the corresponding indicator on a subscribing user's Exceptions Dashboard to change, or (b) a notification to be sent to a user who has subscribed to it.

Exceptions Dashboard An optional content window used to monitor exceptions on Personal Pages. Add exception indicators to this dashboard. Each indicator represents one exception-capable report.

external authentication system An authentication system that uses an external driver to access an external system, from which it retrieves user and group information.

externally triggered events Non-time-based events that are used to schedule job runs.

folders Items are organized into folders. Folders are similar to the directories or folders of your operating system, and are arranged in a hierarchical structure. A folder can contain subfolders, items, or both.

generic jobs Jobs that are neither SQR nor BQY jobs.

global administrator A predefined user who has control of all Hyperion Performance Suite resources and is not subject to access privilege checking by the system.

group A construct that allows the assignment of users that have similar system access requirements.

host A server on which a Hyperion Performance Suite service is installed.

host properties Properties pertaining to a host, or if the host has multiple Install_Homes, to a Install_Home. The host properties are configured from the LSC.

Hypertext Markup Language (HTML) A programming language used to create World Wide Web pages, with hyperlinks and tags that explain to a browser how to format the information on the screen.

image bookmarks Graphic links to web pages or Hyperion Performance Suite items.

inactive group A group that cannot access the system because an administrator has inactivated it. Only in the authentication system that manages a group can a particular group be deleted.

inactive service A service that has been placed on hold or excluded from the list of services to be started.

inactive user *A* user who cannot access the system because an administrator has inactivated the user account. Only in the authentication system that manages a user can a particular user be deleted.

Intelligence iServer A thin-client product used to interactively view BQY documents with a browser.

Intelligence Products A fully integrated business intelligence solution that provides powerful query, analysis, and reporting functionality across both client/server and web environments.

Install_Home The directory under which a Hyperion Performance Suite client or server is installed. *Install_Home* is a variable; its path and name were specified during installation. *See also next definition.*

Install_Home A single set of Hyperion Performance Suite servlets or services, which run in a single process space and are installed in the same *Install_Home* directory (see definition above). The term "Install_Home" is used in this way to indicate a single client or server even when *n* clients or servers, in *n* Install_Home directories, are installed on the same machine.

item A piece of content. An item can be a report program (job), report output, a document created in a spreadsheet or word processing application, an image, an HTML page, a file of any type, a set of versions of a file, or a URL. Every item possesses properties, which store extra information about the item.

JSP Java Server Page(s).

jobs Executable objects; typically reports, programs, or scripts.

job output Files or reports produced from running a job.

job parameters The compile time and run time values necessary to run a job.

logger Log4j term for where the logging message originates. The class or component of the system in which a log message originated.

LSC services The services that are configured with the Local Service Configurator. They include: Global Services Manager (GSM), Local Services Manager (LSM), Session Manager, Authentication Service, Authorization Service, and Publisher Service (all of the Foundation), and in some contexts, Data Access Service (DAS) and Intelligence Service (outside the Foundation).

metadata Data about data; properties and options pertaining to particular content items or other resources (such as users).

MIME Type Multipurpose Internet Mail Extension. Describes the format of data in an item (for example, an Excel spreadsheet or an SQR program) so that the system knows which application to launch to open the object.

native authentication server An authentication server for which Hyperion Performance Suite manages all the user and group information in its own database, the Authentication Service repository (ASR). It does not use an authentication driver.

null value A value that is absent of data.

OCE See *Open Catalog Extension Files (OCE) Files*

Open Catalog Extension Files (OCE) Files Files that encapsulate and store connection information used to connect Hyperion Intelligence applications to a database. OCE files specify the database API (ODBC, SQL*Net, etc.), database software, the network address of the database server, and your database user name. Administrators create and publish OCE files.

personal job parameters Reusable, named job parameters that are accessible only to the user who created them.

Personal Pages Your personal window to information in Hyperion Performance Suite. You select what information to display, as well as its layout and colors.

personal recurring time events Reusable time events that are accessible only to the user who created them.

properties Information about a file or other resource. For example, the Name or MIME Type of a file, or the User ID and Password of a user. (Also called *metadata.*)

proxy server A server that acts as an intermediary between a workstation user and the Internet to ensure security.

public job parameters Reusable, named job parameters created by a Hyperion Foundation administrator and accessible to users who have the requisite access privileges.

public recurring time events Reusable time events created by an administrator and accessible through the access control system.

publish To enter a file into the Hyperion Foundation Repository. The publisher uploads the file and sets its access control and other properties.

RSC services The services that are configured with the Remote Service Configurator. They include: Repository Service, Service Broker, Name Service, Event Service, and Job Service.

reconfigure URL URL to enter new servlet settings when one is logged in.

recurring time event An event that specifies a starting point and the frequency to run a job.

register *See* publish

Repository The file system and database where Hyperion Performance Suite content and metadata are stored.

resources Objects or services that the system manages. Examples of a resource include a role, user, group, file, job, Publisher Service, and so on.

role A construct that defines the access privileges granted in order to perform a business function; for example, the job publisher role grants the privilege to run or publish a job.

schedules Specify the job you want to run, as well as the event schedule and job parameter list for running the job.

security platform A framework providing the ability for Hyperion applications to use external authentication and single sign-on using the security platform driver.

services Resources that provides the ability to retrieve, modify, add, or delete business items. Some Hyperion Foundation services are: Authorization, Authentication, Global Service Manager (GSM).

servlet A piece of compiled code executable by a web server. In Hyperion Foundation, the servlets are Browse, Personal Pages, Job Manager, View Manager, Administration, Data Access, and iHTML.

Servlet Configurator A software utility for configuring all of the locally installed servlets.

shortcut A link to an item elsewhere in Hyperion Foundation. Create a shortcut when, for example, you want an item to appear in folder A, though it is stored in folder B.

single sign-on The ability of an externally authenticated user to access multiple, linked Hyperion applications after logging on only to the first application.

SmartCut A link to an item in Hyperion Foundation, in the form of a special URL.

SPF files Printer-independent files created by the SQR server that contains a representation of the actual formatted report output, including fonts, spacing, headers, footers, and so on.

SQR A specialized programming language for data access, data manipulation, and reporting.

subscribe To register an interest in an item or folder, in order to receive automatic notification whenever the item or folder is updated.

super service A special service used by the startCommonServices script to start the RSC services.

time events Triggers for execution of jobs.

token An encrypted identification of one valid user or group existing on an external authentication system.

transparent login A mechanism that allows users who have been previously authenticated by external security criteria to log in to Hyperion Performance Suite, bypassing the login screen.

trusted password A password that allows users who have been previously authenticated in another system to have access to other applications without entering a password.

trusted user A user authenticated by some mechanism in the environment.

URL An address used by a web browser to find web pages.

user A Hyperion Performance Suite account owner identified by a user ID, user name, and password. A user is created in, and managed by, an authentication system.

variable A value that can be modified when you run a report.

web client Intelligence plug-in product that enables users to create queries, analyze data, and create reports through a browser.

web server Software or hardware hosting intranet or Internet web pages or web applications. In the *Foundation User's Guide*, this term often refers to the Hyperion Performance Suite servlets' host, because in many installations, the servlets and the web server software reside on a common host. This configuration is not required, however; the servlets and the web server software may reside on different hosts.

ws.conf A configuration file for Windows platforms.

wsconf_*platform* A configuration file for UNIX platforms.

Zero Administration A software tool that identifies the version number of the most up-to-date plug-in on the server.

Index

A

access control
  default
    on business items, 3-7
    on business items (figure), 3-7
  introduced, 1-9
  setting for documents you publish, 4-16
  users and groups, 4-3
access privileges
  checking
    examples, 3-22 – 3-24
    for access to business items, 3-18
    for access to services, 3-20
  defined, 3-4
  group and role, 3-11
  “modify” privilege
    granted to user, 3-16
  modifying, 4-11
  “no access”, 3-21
  other items, 3-10
  physical resources, 3-8
  printer and output directory, 3-8
  public events, 3-9
  settings for publishing, 4-16
  shortcuts, 3-10
  users, 3-10
  users imported from external authentication system, 10-13
account names, 10-36
activating or inactivating
  services, 10-7, 10-21, 10-24
activating or inactivating. *See* users, groups, items, MIME types
Active Directory Provider, 6-12
adaptive states
  vs. Intelligence Client roles, 3-8
  vs. Intelligence Client roles (table), 3-25
adding
  groups, 4-14
  roles, 4-14
  See also object or resource types, 4-14
  users, 4-9, 4-12 – 4-13
administering
  public job parameters, 8-16
Administration module
  common tasks, 2-19, 2-21
  introduced, 2-2
  Preferences options, 2-2
administrator
  compared to global administrator, 3-12
  create mini-administrators, 4-14 – 4-15
  password, 9-51
  predefined user, 4-2
Apache, 14-2
APIs
  custom login, 5-16
  custom services, 1-25
  described, 1-28

exceptions, 1-49
external authentication system, 10-16
group synchronization, 5-5
trigger an event, 8-15
user synchronization, 5-5
appenders, 14-2
applications
command strings, 9-36 – 9-37
enterprise-reporting applications, 9-42
running jobs against enterprise applications, 9-43
specifying executable file, 9-39
URL property, 11-23
Applications properties (of servlets), 11-23
architecture, desktop applications, 1-8
archives. *See* backing up
ASMTP, 10-36
associations
group, 4-10
modifying, 4-9
roles, 4-10
attachments
enabling, 10-36
maximum size, 10-36
audience for this guide, xvi
authentication
Active Directory Provider, 6-12
automatic importing of users, 10-16
LDAP, 6-12
levels, 10-18
manual importing of users, 10-16
method, 10-18
NT LAN Manager support, 6-5
process explained, 1-30
sample deployment scenarios, 6-22
security platform driver, 6-2
single sign-on, 6-2
SiteMinder, 6-3, 6-21
authentication driver
custom, 10-19
external, 10-6 – 10-7, 10-9
properties of external authentication system, 10-13
Authentication Service, 1-22
See also services
authentication systems
adding, 10-18 – 10-19
default
for servlet, 5-8
where configured, 5-8
deleting of user and groups, 4-3
described, 4-2
importing users or groups from external, 10-16
listing, 10-8
native, 10-9
owner, 10-13
Service-Managed, 10-8
specifying at login, 5-9
synchronization, 5-5
synchronizing, 10-16
System, 5-8
types of, 5-2 – 5-5
Authorization Service, 1-22
See also services
automatic login, URLs, 5-13 – 5-15

B

backing up
clients, 12-8
overview, 12-2
procedures, 12-2
Repository database, 12-8
restoring data, 12-2
scripts, 12-7
servlet configuration files, 12-8
servlets, 12-8
batch files
and application command strings, 9-37

batch utilities
synchronizing user lists, 5-19
bookmarks
automatic logins, 5-13
generated Personal Pages, 7-7
setting up graphics for, 7-11
BQY
documents, publishing as files, 1-35
jobs
defined, 9-40
publishing, 1-37
managing OCE files, 8-16
BrioPlatform....dat file, 2-10
Broadcast Messages
changing default Personal Pages and, 7-9
generated Personal Pages and, 7-7 – 7-8
overview, 7-9
push content, 7-9
renaming folder, 7-10, 10-35
specifying categories for, 10-35
subfolders, 7-8
understanding, 7-9
Browse servlet
name, 10-37
Personal Page preconfiguration, 7-6 – 7-8
web application deployment name, 10-38
Browser properties, 11-21

C

Cache properties group
Browser subgroup, 11-21
described, 11-19
Notification subgroup, 11-21
Objects subgroup, 11-19
System subgroup, 11-20
caches
of content listings, 10-31
for services, 10-21
of user interface elements, 10-31
calendars
creating, 8-4
default name, 10-43
deleting, 8-4
end dates, 8-9
managing, 8-2
modifying, 8-5
non-working days, 8-8
periods and years, 8-7
properties of, 8-6
user-defined weeks, 8-6
week start, 8-6
classpath, 9-15, 9-28, 10-32
clients. *See* servlets
Color properties
described, 11-11
General, 11-11
Navigation Frame, 11-13
Text, 11-12
color schemes
customizing on Personal Pages, 7-16
properties, 11-16
command strings for applications
described, 9-36 – 9-37
example, 9-37
config.dat file
distributing services and, 9-49
editing, 9-2, 9-51
encryption and, 9-50
services startup and, 9-49
startup process, 2-18
sync host properties, 10-33
ConfigFile... utility, 9-50 – 9-51
ConfigFile.sh. *See* ConfigFile... utility
ConfigFileAdmin.bat. *See* ConfigFile... utility
configuration, 6-9
See also Local Service Configurator, Remote Service Configurator, Servlet Configurator, ConfigFile... utility
components for, 1-18

ConfigFile... utility, 9-51
information in startup process, 2-18
configuration files
See also notification.properties, services.properties, output.properties, config.dat file
backing up, 12-8
server.xml, 10-33
ws.conf or wsconf_platform, 11-2
connections pool, 10-27
connectivity
type, 10-26
connectivity, defining for a database server, 9-19
consulting services, xxii
content windows, headings, 7-16
content, providing optional Personal Page to users, 7-10
content-browsing solution, components, 1-14
copying
See also object or resource types
existing users, 4-12
Personal Pages, 7-15
core services
See also individual service names
in diagrams, 1-33
listed, 1-20
requirements for, 1-5
custom login implementation, 11-5

D

DAS response timeout, 11-24
.dat files. *See* BrioPlatform....dat
Data Access Service (DAS)
adding OLE DB connection, 10-28
data sources
adding, 10-27
described, 1-26
OCE properties, 10-27
starting with process monitor, B-1
data sources
connectivity type, 10-26
listing, 10-25
maximum connections, 10-26
name, 10-26, 10-42
properties of DAS, 10-25
database
authentication driver, 5-3
changing password, 9-12
properties (of host or Install_Home), 10-32
database properties (of host or Install_Home), 10-32 – 10-33
database servers
adding, 9-16
associating with a Job Service, 9-18 – 9-20
changing driver, 9-12
DDO, 9-44 – 9-49
deleting, 9-21
environmental variables for SQR, 9-20
managing, 9-16
properties, 9-17
databases
connectivity, 10-42
type, 10-26, 10-42
DDO, configuring a Job Service for, 9-44 – 9-49
default Personal Pages, changing, 7-9
deleting
MIME types, 7-5
denying access, 3-21
diagnostics properties, 11-22
directories. *See* output directories
directory server, 10-17
displayable items. *See* file content windows
displaying
HTML file on a Personal Page, 7-10
documents
conventions used, xxi
feedback, xxiii
ordering print documents, xxi

structure of, xvi
documents, accessing
Hyperion Download Center, xx
Hyperion Solutions Web site, xx
Information Map, xx
online help, xx
drivers
See also authentication
authentication, 10-13
database, 9-14, 9-28, 10-32
external authentication, 10-14

E

education services, xxii
encoding
of URLs, 10-38
UTF-8, 10-38
Event Service
described, 1-25
event log, 10-35
service type in BrioPlatform....dat file, 2-11
events
creating externally triggered event, 8-13
time events, managing, 8-12
triggering, 8-15
exception icon, on job output, 1-45
exceptions
configuring, 7-11
described, 1-49
reporting, 7-11
reporting on Personal Pages, 7-11
Exceptions Dashboard
described, 1-49
generated Personal Pages and, 7-7
expiration times, 10-36
exporting, registry keys, 12-2
external authentication
about, 5-3
externally triggered events
creating, 8-13
polling for, 10-43

F

file content window, 7-10
file size
of attachments, 10-36
file systems
backing up, 12-2, 12-7
restoring data, 12-2
files
adding to folders, 7-14
in email attachments, 10-36
publishing, 1-34
publishing BQY, 1-35
“Flag as an exception” field, 1-44
flags in startCommonServices script, 2-8
folders
administrator-only System folder, 7-2
Broadcast Messages, 10-35
organizing, 7-2
pre-configured, 7-13
publishing items in, 7-14
user’s default, 4-8
Foundation of Hyperion Performance Suite, 1-1, 1-4
FTP
report output directory, 8-22
functional services
described, 1-5
listed, 1-25

G

General properties (of groups and roles), 4-8
Generated Personal Page properties (of servlets), 11-15
generic files, access privileges, 3-10

Global Service Manager (GSM), 1-21, 2-9 – 2-10, 10-30 – 10-31, 10-35
globaladministrator
  compared to administrator, 3-12
  predefined user, 4-2
graphics. *See* images
groups
  access control, 4-3
  active and inactive, 4-3
  adding, 4-14
  adding users to, 4-9
  associating users with groups, 4-10
  associating with a role, 4-10
  deleting, 4-3
  general properties, 4-8
  synchronizing between authentication systems, 5-5
  users and, 4-2

H

headings (within Personal Pages), 7-16
Hold. *See* Run Type property
hosts
  adding, 9-7
  deleting, 9-11
  and Install_Homes, 10-2
  list of, 9-10
  managing, 9-7 – 9-11
  modifying, 9-10
  properties of, 10-29
HTML files
  and customizing generated Personal Page, 7-8
  displaying on Personal Pages, 7-10
HTTP protocol, Smartcut for email notification, 10-37
HTTPS protocol, 10-37
Hub, 6-37, 10-40
Hyperion Consulting Services, xxii
Hyperion Download Center
  accessing documents, xx
Hyperion Education Services, xxii
Hyperion Intelligence Clients
  load testing, 11-29
  zero administration, 11-27
Hyperion product information, xxii
Hyperion Product Integration
  Hyperion Hub, 6-37
  related content, 6-37
Hyperion Solutions Web Site
  accessing documents, xx
Hyperion support, xxii
Hyperion Technical Support, xxiii

I

icons
  See also toolbars
  DBCS, 7-11
  exception, 1-45
  exception, on job output, 1-45
  files, 7-2
  for access privileges on BQY, 3-25
  for HTML output of SQR, 11-11
  Local Service Configurator, 10-3
  logo in servlets window, 11-7
  on Exceptions Dashboard, 1-49, 7-2
  on LSC toolbar, 10-4
  on RSC toolbar, 9-5
  Remote Service Configurator, 9-2
  in Servlet Configurator, 11-3
  on Servlet Configurator toolbar, 11-3
  Show host properties, 10-4
  Show item properties (Local Service Configurator), 10-4
  system, 10-34, 10-40 – 10-41
  View Job Execution Log Entries, 8-9
images

for bookmarks, setting up, 7-11
inactivating
MIME types, 7-4
users and groups, 4-6
inactive or active users and groups, 4-3
Install_Home
See also hosts
and physical, 10-2
defined, 10-2
described, 2-4
directory, 2-4
users in, 5-3
Install_Home directory, 10-29, 12-3 – 12-4
installation
See also Install_Home
backing up immediately after, 12-3 – 12-4, 12-8
config.dat file, 9-52
Install_Home, 2-4
installed services, 2-5
installed servlets, 11-2, 12-8
installed system, 10-35
location of components, 10-26, 11-2
location of installed files, 10-42
modular, 1-4
multiple Install_Homes, 10-2
new host, 9-7
Servlet Configurator, 11-2
of Zero Administration, 11-28
of zero administration, 11-28
installation directory, 10-31
installation program, 2-21, 5-3, 9-2, 9-22
installed services
deleting a host with, 9-11
Install_Home, 10-2, 10-29
Intelligence and DAS services, 2-12
LSC displays, 10-4
recommendation for Job Service, 9-42
replicate job service, 9-42
RSC services, 9-22
RSC toolbar, 9-4
installed servlets, 9-53
Intelligence Client roles
assigning, 3-26
Intelligence iServer solution, 1-12
Intelligence products' servlets, listed, 1-27
Intelligence roles, 3-25
vs. adaptive states, 3-8
assigning, 3-26
vs adaptive states, 3-25
Intelligence Server solution, components of, 1-13
Intelligence Service
See also services
described, 1-26
printers and, 8-20
starting with process monitor, B-1
Internal properties (in Servlet Configurator)
Job subgroup, 11-18
Redirect subgroup, 11-17
Transfer subgroup, 11-17
Upload subgroup, 11-18
IP ports. *See* ports
items
and generated Personal Page, 7-7
headings on, 7-16
organizing in folders, 7-2, 7-14
retrieval of, 1-33

J

JDBC driver, 9-15, 9-28, 10-32
JDBC URL, 9-14, 9-28, 10-32
job execution
job process explained, 9-43
Job Log
columns in, 8-10
dates, 8-9
deleting entries, 8-11
marking entries for deletion, 8-11

sorting, 8-10
start dates and times, 8-9
user displays for, 8-9
job log file, suppress, 8-12
job output property, 11-10
job parameters, administering, 8-16
Job Service
application, 9-33, 9-35
applications
configuring, 9-33 – 9-34
managing, 9-34
described, 1-25
executable of application, 9-35
overview, 9-40
properties
Application, 9-33 – 9-34
Database, 9-30
Executable, 9-38 – 9-39
SQR, 9-32
running jobs against enterprise applications, 9-43
SAP configuration, 9-49
service type in BrioPlatform....dat file, 2-11
shutting down, 2-17
specifying executable file for application, 9-39
user name for running SQR jobs, 10-42
Job Utilities, 1-27
jobs
ad hoc execution vs. scheduled execution, 1-40
automatic login and job execution, 5-15
BQY, publishing, 1-37
email output attachments, 10-36
Job Log, 8-9
SQR, publishing, 1-38
jobs property, 11-18

K

kill commands, 2-17

L

LDAP, 6-12, 10-17
licenses, trial product, 1-3
listing
user, role, or group, 4-5
load balancing, 1-30
Local Service Configurator (LSC)
See also LSC services
described, 2-4
list of services, 10-2
modify host properties, 10-29
server.xml file, 10-2, 10-33
starting, 10-3
Local Service Manager (LSM), 1-21, 10-30 – 10-31
localization properties, 11-8
located, 2-10
log files
analyzing, 14-17
for BQY output, 10-43
configuration, 14-9
configuration log, 14-8
file formats, 14-8
location, 14-4
naming convention, 14-6
notification log, 10-36
log levels, 14-11
Log Management Helper, 14-3
log4j, 14-2
loggers, 14-2
logging events, 8-9
logging in
described, 5-8 – 5-18
Logging Service
configuration, 14-9
usage, 14-3
login
authentication of user during, 1-30

bypassing, 5-10
Login properties (servlets), 11-5
login *See* authentication, crawlers
Logo icon properties, 11-7
logout, disabling, 5-12
LSC services
introduced, 1-10
list of, 1-10

M

macros
$NONE$, 5-13
for transparent macros, 5-16 – 5-17
magnifying glass icon, 11-3
mail server host names, 10-36
manage time events, 8-12
management services
defined, 1-5
management tasks, Organization tab, 4-4
managing OCE files, 8-16
Message property of job output, 1-44
metadata, retrieving, 1-32
Microsoft Windows. *See* Windows
MIME types
creating, 7-3
deleting, 7-5
inactivating or re-activating a, 7-4
modifying, 7-3
working with, 7-2
mini-administrators, create, 4-14 – 4-15

N

Name Service
config.dat file and, 9-49
described, 1-23
service type in BrioPlatform....dat file, 2-11
in startup process, 9-51 – 9-52
startup process, 2-18
$NONE$ macro, 5-13
notification properties, LSC, 10-35
notification property, servlets, 11-21
notifications
See also subscriptions
ASMTP, 10-36
attachments, 10-36
email
account for sending, 10-36
enabling attachments, 10-36
server host name, 10-36
events that trigger, 1-48
other, 1-47
subscriptions and, 1-47
types of, 1-49
NT LAN Manager support, 6-5
nts, 12-8

O

object administrator, 3-12
objects properties, 11-19
OCE files
explicit access property, 8-16
managing, 8-16
Oracle Reports, command string example, 9-37
Organization tab
accessing, 4-4, 13-4
Organization, management tasks, 4-4
organizing items and folders, 7-2
output directories
adding, 8-18
deleting, 8-19
modifying, 8-18
properties
FTP, 8-22
General, 8-22
purpose, 8-21

output.properties, 1-44, 1-49

P

parameters, job administering public, 8-16
pass-through
  configuring, 10-11
  credentials, 5-6, 8-17
  definition, 5-6, 8-17
  properties, 10-12
passwords
  Administrator, changing, 1-9
  automatic login properties and macros, 5-16 – 5-17
  automatic login with URLs, 5-13 – 5-15
  Config.file, changing, 1-9
  database, changing, 9-12
  default and trusted, for authentication systems, 10-12
  directory server manager, 10-18
  encrypted, 9-50
  Global Administrator, changing, 1-9
  of Job Service, for running SQR jobs, 10-42
  modifying required minimum characters, 4-8
  modifying service, 9-51 – 9-52
  of services, 9-50
  RDBMS password, 9-52
  Repository Service, 9-12
  of services for database access, 9-28, 10-32
  ServletUser, changing, 1-9
  system, 9-50
  transparent login, 5-13 – 5-18
  trusted, 5-15
  trusted passwords, 5-19
Personal Pages
  Broadcast Messages on, 7-9
  configuration tool, 7-16
  customized graphics, 7-11
  default Personal Pages, 7-9
  example of setting up content, 7-12
  generated
    customizing, 7-7
    properties, 11-15
    setting up, 7-6
  graphic files on, 7-11
  multiple, 7-9
  optional content to users, 7-10
  optional content, providing to users, 7-10
  properties, configuring, 7-16
  publishing, 7-15
  publishing other pages, 7-15
  setting up items in folders, 7-14
  viewing new user's, 7-15
Personal Pages properties
  Color Scheme, 11-16
  General, 11-14
  Publish, 11-14
physical resources
  See also printers, output directories
  access control on, 8-19
  adding, 8-18
  deleting, 8-19
  modifying, 8-18
pinging a service, 9-6
portal.properties, 10-42 – 10-43
ports, Browse servlet, 10-38
pre-configured folders, setting up, 7-13
preconfigured roles, 3-15
predefined users, 4-2
prerequisites for using this guide, xvi
printers
  adding, 8-18
  deleting, 8-19
  modifying, 8-18
  properties of, 8-20
  purpose of, 8-20
priority setting in administration module, 10-35
privileges, modifying access, 4-11
process monitors, B-2

programs, running jobs against enterprise applications, 9-43
properties
confidential, 10-19
configuring Personal Pages, 7-16
for external authentication drivers, 10-6 – 10-7, 10-9
for LDAP, 6-12
for NTLM, 6-19
general
groups and roles, 4-8
users, 4-7
general (of Authentication Service), 10-8
generated Personal Page, 7-8
Job Service, 9-29 – 9-39
Navigation properties of servlets, 11-7
pass-through, 10-12
Servlet Configurator, 11-5
standard, of LSC service, 10-6
system properties, 10-34
viewing in the Servlet Configurator, 11-3
properties files
modifying, 6-9
protocols for Smartcuts, 10-38
publish properties, 11-14
Publisher Service
described, 1-21
publishing BQY files and, 1-36
publishing
BQY documents as files, 1-35
BQY documents as jobs, 1-37
files, 1-34
SQR programs, 1-38
publishing Personal Pages, 7-15
push content
Broadcast Messages, 7-9
pushed content, 7-5
pushing content. *See* Broadcast Messages

Q

queries
maximum cells in results, 10-24
maximum rows in results, 10-24

R

RDBMS
passwords, 9-52
starting, 2-6
re-activating
MIME types, 7-4
users/groups/roles, 4-6
rebooting machines, 2-17
recovering data, 12-2
Redirect properties, 11-17
registry keys, 12-2
related content, 6-37
Relational Database Management System. *See* RDBMS
Remote Service Configurator (RSC)
See also RSC services
config.dat file and, 9-50
database password, 9-12
described, 2-3
pinging a service, 9-6
Storage tab, 9-12
toolbar icons, 9-5
what it does, 9-2
REMOTE_USER property, 5-18
renaming Broadcast Messages folders, 7-10
replicating services, 1-7
replicating servlets, 11-4
report registry keys, 12-2
Reports iServer solution, components of, 1-15
Repository database, backing up, 12-8
Repository Service
described, 1-21
service type in BrioPlatform....dat file, 2-11

stopping, 2-17
restoring data, 12-2
role and group access privileges, 3-11
role containment example, 3-3
roles
access privileges, 3-11
adding, 4-14
assigning Intelligence Client roles, 3-26
associating users/groups with a role, 4-10
general properties, 4-8
Intelligence, 3-25
preconfigured, 3-15
roles and groups, general properties, 4-8
root directories, 10-38
root group, 3-16
row-level security, 10-41
RSC services
configuring, 10-1
introduced, 1-10
list of, 1-10
setting properties, 10-33
super service, 10-6
Run Type property, 10-7 – 10-8, 10-21, 10-24
Run Type property of services, 2-10

S

SAP, 9-44 – 9-49
schedules, running scheduled jobs, 1-46
scripts
extension, 2-14
start_Common Services, 2-7
stop scripts, 2-17
SDK *See* APIs
security
row-level, properties, 10-42
transparent logins and, 5-10
security Platform Driver, 5-4
security platform driver, 5-1, 6-1 – 6-2
server, overview, 1-5
server.xml file, 1-18, 1-23, 10-33
servers, mail, 10-36
server-side software components. *See* services
Service Broker
described, 1-23
service type in BrioPlatform....dat file, 2-11
services
See also specific service names
adding, 10-2
BP_host.dat file, 2-10
common tasks, 2-19, 2-21
deleting, 9-6
deleting message during deletion, 9-2
modifying properties, 9-22
names in BrioPlatform....dat, 2-11
pinging, 9-6
properties
Advanced, 9-26
General, 9-24 – 9-25
removing one or more, 10-2
replicating, 1-7
Run type property, 2-10
running as separate processes, 2-17
starting individually, 2-12 – 2-16
starting Intelligence and DAS services with process monitor, B-2
starting subset of, 2-10
starting under UNIX, 2-7
starting under Windows, 2-7
stopping, with scripts, 2-17
types of, 2-11
user name for database access, 9-28, 10-32
viewing properties, 9-22
servlet
default authentication system for, 5-8
Servlet Configurator
configuring default authentication system, 5-8

defined, 11-2
described, 2-4
making new settings effective, 11-4
starting, 11-2
toolbar, 11-3
Servlet Engine
session timeout value, 11-17
servlets
backing up, 12-8
configuring, 2-4
listed, 1-27
replicating, 11-4
Session Manager, 1-22
session object, 1-30
session time-out value, 11-17
shell scripts. *See* scripts
shortcuts, access privileges, 3-10
shutting down. *See* services
single sign-on
about, 6-2
prerequisites, 6-4
SiteMinder
authentication, 6-3
configuration, 6-21
SmartCuts
email notifications, 10-37
in notifications, 1-49
servlet property, 11-11
system properties, 10-37
Software Development Kit (SDK) *See* APIs
Solaris (Sun), 12-7
See also UNIX systems
SQR Developer solution, components of, 1-16
SQR files
See also SPF files
publishing (figure), 1-17
SQR jobs
data sources, 9-31
defined, 9-40
exceptions, 1-44
publishing (figure), 1-16
SQR servers, properties of, 9-32
SQR, environment variables for, 9-20
SQR/DDO. *See* DDO
start scripts, 2-7, 10-33
Start. *See* Run Type property
startCommonServices script, 2-7, 10-33
starting RDBMS, 2-6
starting system or components
administrative tools
Local Service Configurator, 10-3
Remote Service Configurator, 9-2
Servlet Configurator, 11-2
services
config.dat file and, 9-49
RSC services, 10-6
run type, 10-8
starting individually, 2-12 – 2-16
starting subset of, 2-10
starting under UNIX, 2-7
starting under Windows, 2-7
servlets, 2-19
starting under UNIX, 2-7
stylesheets, 11-11
Subscribe page, 1-49
subscription property, 11-10
subscriptions, 1-47, 10-35
See also notifications
Sun ONE servlet engine, 10-38
super service, 10-6
system configuration. *See* configuration
System folder
described, 7-2
system properties, 10-34
in Administration servlet, 10-39
described, 11-20

system properties, modifying, 10-34
system usage, 13-1

T

technical support, xxiii
time events, managing, 8-12
times
  notification expiration times, 10-36
titles on items, 7-16
toolbars
  Local Service Configurator, 10-4
  Service Configurator, 9-2
  Servlet Configurator, 11-3
transfer property, 11-17
transparent login
  automatic login properties and macros, 5-16 – 5-17
  types of integration, 5-10
transparent macros, macros for, 5-16 – 5-17
trial license, 1-3
triggering an event, 8-15
troubleshooting, 14-1
trusted password
  configuring, 5-19, 10-11, 11-6
  macro for, 5-17
trusted passwords
  configuring, 5-19
  transparent login, 5-15
types of, 1-5, 2-11
types of authentication systems, 5-3 – 5-5

U

UNIX systems
  backing up the clients, 12-8
  backup procedure, 12-2
  kill command shutdowns, 2-17
  maximum number of file descriptors, 9-26
  start Servlet Configurator, 11-2
  startCommonServices method, 2-7
  system backup procedures, 12-2
  terminate the Job Service, 2-17
  using kill command, 2-17
unknown file type message, 7-5
upload property, 11-18
URL properties, 11-23
URLs
  transparent login, 5-12
Usage Service
  configuration, 13-3
  defined, 13-2
  events, 13-3
  managing, 13-4
  properties, 13-3 – 13-4
  reports, 13-7
user authentication. *See* authentication
user names
  automatic login properties and macros, 5-16
  automatic login with URLs, 5-13
  transparent login, 5-13 – 5-16
user role, 3-17
UserPassword property, 5-18
users
  access control, 4-3
  access privileges, 3-10
  active and inactive, 4-3
  adding to groups, 4-9
  associating with a role, 4-10
  common tasks, 2-19, 2-21
  copying, 4-12
  creating
    by copying, 4-12
    new, 4-13
  default folders, 4-8
  deleting, 4-3
  general properties, 4-7
  and groups, 4-2
  identifiers, 10-18

implicit modify access privilege, 3-16
Job Log displays for, 8-9
predefined, 4-2
UTF-8 encoding, 10-38

V

View Manager
pushed content, 7-5
virus protection, 7-2

W

web modules. *See* servlets
WebSphere, 10-38
Windows (Microsoft)
backup procedure, 12-2
exporting Registry key, 12-2
plugins, 11-28
Task Manager shutdowns, 2-17
terminating a process, 2-17
Windows 2000, 12-6
world group, 3-16
ws.conf file, 11-2, 11-4
wsconf_platform file, 11-2

Z

Zero Administration
client processing, 11-28
server processing, 11-27
starting download of, 11-27