# Contents

**Preface** ................................................................. ix
Purpose ........................................................................... ix
Audience ......................................................................... ix
Document Structure ........................................................ x
Where to Find Documentation ........................................... xi
Help Menu Commands ..................................................... xi
Conventions ....................................................................... xii
Additional Support .......................................................... xiii
   Education Services ........................................................ xiii
   Consulting Services ....................................................... xiii
   Technical Support ........................................................ xiii
Documentation Feedback ................................................ xiii

## CHAPTER 1  
**Shared Services User Management** ......................................................... 15
   Benefits of Shared Services User Management ..................... 16
   External Authentication and Single Sign-On ......................... 16
   User Provisioning .......................................................... 16
   Product-Specific Access Control ......................................... 16
   Shared Services User Management System ............................ 17
   System Components ....................................................... 17
      Authentication Directories ............................................. 18
      Projects and Applications ............................................. 19
      Users and Groups ..................................................... 19
      Roles ........................................................................ 20

## CHAPTER 2  
**Implementing Shared Services User Management** .............................. 23
   Process for Setting Up Shared Services User Management .......... 24
   Launching User Management Console ................................ 25
   Navigating in User Management Console .............................. 26

## CHAPTER 3  
**Managing and Provisioning Users and Groups** ................................... 27
   Managing Projects ...................................................... 28
Creating Projects ........................................................................................................... 28
Modifying Project Properties ......................................................................................... 29
Deleting Projects ............................................................................................................ 30
Managing Applications .................................................................................................... 30
Assigning Access Control to Applications ..................................................................... 31
Moving Applications ...................................................................................................... 31
Copying Provisioning Information .................................................................................. 32
Managing User Directories .............................................................................................. 33
Managing Users, Groups, and Roles ................................................................................ 33
Managing Native Shared Services Users ....................................................................... 33
Managing Native Shared Services Groups ....................................................................... 38
Managing Aggregated Roles ............................................................................................ 42
Provisioning Users and Groups ....................................................................................... 44
Provisioning Users .......................................................................................................... 45
Deprovisioning Users ........................................................................................................ 46
Provisioning Groups ......................................................................................................... 46
Deprovisioning Groups ...................................................................................................... 47
Generating Provision Reports ........................................................................................... 48

APPENDIX A Shared Services User Provisioning .......................................................... 49
Shared Services User Roles ............................................................................................... 50
Administrator .................................................................................................................... 50
Directory Manager ............................................................................................................ 50
Project Manager .............................................................................................................. 51
Provisioning Manager ...................................................................................................... 51
Create Integrations ............................................................................................................ 51
Run Integrations ............................................................................................................... 52
User Roles and Tasks .......................................................................................................... 52

APPENDIX B Analytic Services User Provisioning .......................................................... 55
Launching the User Management Console from Analytic Services .................................. 56
Analytic Services User Roles ............................................................................................. 56
Analytic Services User Role and Task Matrix For Shared Services .................................. 57
Analytic Services Projects, Applications, and Databases in Shared Services .................. 59
Analytic Services Users and Groups in Shared Services .................................................... 60
Assigning Database Calculation and Filter Access ............................................................ 60
Setting Application Access Type ...................................................................................... 62
Synchronizing Security Information Between Shared Services and Analytic Services ...... 63
Migrating Analytic Services Users to Shared Services Security ......................................... 63
Backing Up Security Information ...................................................................................... 63

APPENDIX C Analytic High Availability Services User Provisioning .............................. 65
Launching User Management Console from High Availability Services ........................ 66
Analytic High Availability Services User Roles ................................................. 66
Provisioning the Administrator Role in Shared Services ............................... 67
Migrating Analytic High Availability Services Users to Shared Services Security ......................... 68

APPENDIX D Hyperion System 9 BI+ User Provisioning ........................................... 71
Launching User Management Console from Hyperion System 9 ......................... 72
 User Management Console ........................................................................... 72
Hyperion System 9 BI+ Roles ........................................................................ 73
 Basic Roles ........................................................................................................ 74
 Additional Functionality .................................................................................... 75
 Distributing Content ......................................................................................... 76
 Content Creation ............................................................................................... 77
 Content Management ...................................................................................... 78
 Universal Access to Resources and Functionality .............................................. 78
 Internal System Role ........................................................................................ 79
 Aggregated Roles ............................................................................................. 79
 Content Manager Branch .................................................................................. 80
 Scheduler Manager Branch ............................................................................... 81
 Tasks and Roles ............................................................................................... 82
 Role Combinations ......................................................................................... 85
 Custom Roles .................................................................................................. 87
 Default Functionality ....................................................................................... 87
 Assigning Default Hyperion System 9 BI+ Preferences ...................................... 88
 The World Group and Default Roles .................................................................. 89
 Mapping Old Roles to New Roles ..................................................................... 90

APPENDIX E Analytic Services Smart View Provider User Provisioning ................. 93
Analytic Services Smart View Provider User Roles ............................................. 94
 Provisioning the Administrator Role in Shared Services ...................................... 94
 Migrating Analytic Services Smart View Provider Users to Shared Services ............. 95

APPENDIX F Financial Management User Provisioning ..................................... 97
Launching the User Management Console from Financial Management ............... 98
 Shared Services User Roles in Financial Management ........................................ 98
 Financial Management User Roles ................................................................. 100
 Tasks For Default Role .................................................................................... 104
 Assigning Users and Groups to Financial Management Applications ................. 105
 Setting Up Security Classes for Financial Management Applications .................. 106
 Creating Security Classes ................................................................................ 107
 Deleting Security Classes ................................................................................ 107
 Selecting Security Classes ............................................................................... 107
 Assigning User Access to Security Classes ...................................................... 108
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting Up E-mail Alerting</td>
<td>109</td>
</tr>
<tr>
<td>Process Management Alerting</td>
<td>110</td>
</tr>
<tr>
<td>Intercompany Transaction Alerting</td>
<td>111</td>
</tr>
<tr>
<td>Running Security Reports for Financial Management Applications</td>
<td>111</td>
</tr>
<tr>
<td>Migrating Financial Management Users to Shared Services Security</td>
<td>112</td>
</tr>
<tr>
<td>APPENDIX G Planning User Provisioning</td>
<td>113</td>
</tr>
<tr>
<td>About Planning Security</td>
<td>114</td>
</tr>
<tr>
<td>Launching the User Management Console From Planning</td>
<td>114</td>
</tr>
<tr>
<td>Returning to Planning From the User Management Console</td>
<td>114</td>
</tr>
<tr>
<td>Updating Users and Groups in Planning</td>
<td>115</td>
</tr>
<tr>
<td>Updating Users With a Utility</td>
<td>115</td>
</tr>
<tr>
<td>User Roles</td>
<td>117</td>
</tr>
<tr>
<td>Administrator</td>
<td>117</td>
</tr>
<tr>
<td>Interactive User</td>
<td>118</td>
</tr>
<tr>
<td>Planner</td>
<td>119</td>
</tr>
<tr>
<td>View User</td>
<td>119</td>
</tr>
<tr>
<td>User Roles and Tasks</td>
<td>119</td>
</tr>
<tr>
<td>User Roles Between Planning and Business Rules</td>
<td>120</td>
</tr>
<tr>
<td>Access Rights Between Planning and Analytic Services</td>
<td>121</td>
</tr>
<tr>
<td>User Roles in Workforce Planning</td>
<td>121</td>
</tr>
<tr>
<td>About User Roles</td>
<td>121</td>
</tr>
<tr>
<td>Manage Models User Role</td>
<td>123</td>
</tr>
<tr>
<td>About Connection Types and Planning</td>
<td>124</td>
</tr>
<tr>
<td>Migrating Users to Shared Services</td>
<td>124</td>
</tr>
<tr>
<td>APPENDIX H Business Rules User Provisioning</td>
<td>127</td>
</tr>
<tr>
<td>About Business Rules Security</td>
<td>128</td>
</tr>
<tr>
<td>Launching the User Management Console</td>
<td>128</td>
</tr>
<tr>
<td>Business Rules User Roles</td>
<td>128</td>
</tr>
<tr>
<td>Migrating Business Rules Users to Shared Services Security</td>
<td>129</td>
</tr>
<tr>
<td>APPENDIX I Performance Scorecard User Provisioning</td>
<td>131</td>
</tr>
<tr>
<td>Performance Scorecard User Roles</td>
<td>132</td>
</tr>
<tr>
<td>Launching the User Management Console from Performance Scorecard</td>
<td>133</td>
</tr>
<tr>
<td>Managing Permissions in Performance Scorecard</td>
<td>134</td>
</tr>
<tr>
<td>Creating and Provisioning Users and Groups over Shared Services</td>
<td>135</td>
</tr>
<tr>
<td>Access Permissions</td>
<td>135</td>
</tr>
<tr>
<td>Before You Begin</td>
<td>135</td>
</tr>
<tr>
<td>Creating a New User or Group Using Shared Services</td>
<td>136</td>
</tr>
<tr>
<td>Assign Performance Scorecard Properties Individually</td>
<td>136</td>
</tr>
<tr>
<td>Assign Bulk Properties in Performance Scorecard</td>
<td>138</td>
</tr>
</tbody>
</table>
Welcome to the *Hyperion System 9 Shared Services User Management Guide*. This preface discusses the following topics:

- “Purpose” on page ix
- “Audience” on page ix
- “Document Structure” on page x
- “Where to Find Documentation” on page xi
- “Help Menu Commands” on page xi
- “Conventions” on page xii
- “Additional Support” on page xiii
- “Documentation Feedback” on page xiii

**Purpose**

This guide provides information that you need to use Shared Services User Management to manage and provision users for Hyperion products. It explains Shared Services User Management features and options and contains the concepts, processes, procedures, formats, tasks, and examples that you need to use the software.

**Audience**

This guide is for any administrator who uses Shared Services to manage and provision users for Hyperion products.
Document Structure

This document contains the following information:

- **Chapter 1, “Shared Services User Management,”** introduces the concepts of the Shared Services User Management system.
- **Chapter 3, “Managing and Provisioning Users and Groups,”** describes how to perform various user management and user provisioning tasks.
- **Appendix A, “Shared Services User Provisioning,”** lists and describes Shared Services user roles.
- **Appendix E, “Analytic Services Smart View Provider User Provisioning,”** provides information about using Shared Services User Management with Hyperion System 9 Smart View Provider™.
- **Appendix I, “Performance Scorecard User Provisioning,”** provides information about using Shared Services User Management with Hyperion System 9 Performance Scorecard™.
- **Appendix K, “Translation Manager User Provisioning,”** provides information about using Shared Services User Management with Hyperion System 9 Translation Manager.

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

**Index** contains a list of terms and their page references.
Where to Find Documentation

All Shared Services User Management documentation is accessible from the following locations:

- The HTML Information Map is available from the Help menu in User Management Console for all operating systems; for products installed on Microsoft Windows systems, it is also available from the Start menu.
- Online help specific to User Management Console is available from within the console. After you log on to the product, you can access online help by clicking the Help button or selecting Help > Contents from the menu bar.
- The Hyperion Download Center can be accessed from the Hyperion Solutions Web site.

➤ To access documentation from the Hyperion Download Center:

1. Go to the Hyperion Solutions Web site and navigate to Services > WorldWide Support > Download Center.

   Note: Your Login ID for the Hyperion Download Center is your e-mail address. The Login ID and Password required for the Hyperion Download Center are different from the Login ID and Password required for Hyperion Support Online through Hyperion.com. If you are not sure whether you have a Hyperion Download Center account, follow the on-screen instructions.

   2. In the Login ID and Password text boxes, enter your e-mail address and password.

   3. In the Language list box, select the appropriate language and click Login.

   4. If you are a member on multiple Hyperion Solutions Download Center accounts, select the account that you want to use for the current session.

   5. To access documentation online, from the Product List, select the appropriate product and follow the on-screen instructions.

Help Menu Commands

Table I describes the commands that are available from the Help menu in User Management Console.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contents</td>
<td>Launches the User Management Console help.</td>
</tr>
<tr>
<td>Information Map</td>
<td>Launches the Shared Services Information Map, which provides the following assistance:</td>
</tr>
<tr>
<td></td>
<td>- Online help in PDF and HTML format</td>
</tr>
<tr>
<td></td>
<td>- Links to related resources to assist you in using Shared Services</td>
</tr>
<tr>
<td>Technical Support</td>
<td>Launches the Hyperion Technical Support site, where you submit defects and contact Technical Support.</td>
</tr>
</tbody>
</table>
The following table shows the conventions that are used in this document:

<table>
<thead>
<tr>
<th>Item</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arrows</td>
<td>Arrows indicate the beginning of procedures consisting of sequential steps or one-step procedures.</td>
</tr>
<tr>
<td>Brackets [ ]</td>
<td>In examples, brackets indicate that the enclosed elements are optional.</td>
</tr>
<tr>
<td>Bold</td>
<td>Bold in procedural steps highlights user interface elements on which the user must perform actions.</td>
</tr>
<tr>
<td>CAPITAL LETTERS</td>
<td>Capital letters denote commands and various IDs. (Example: CLEARBLOCK command)</td>
</tr>
<tr>
<td>Ctrl+O</td>
<td>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.</td>
</tr>
<tr>
<td>Ctrl+Q, Shift+Q</td>
<td>For consecutive keystroke combinations, a comma indicates that you press the combinations consecutively.</td>
</tr>
<tr>
<td>Example text</td>
<td>Courier font indicates that the example text is code or syntax.</td>
</tr>
<tr>
<td>Courier italics</td>
<td>Courier italic text indicates a variable field in command syntax. Substitute a value in place of the variable shown in Courier italics.</td>
</tr>
<tr>
<td>italic n, x</td>
<td>Italic n stands for a variable number; italic x can stand for a variable number or a letter. These variables are sometimes found in formulas.</td>
</tr>
<tr>
<td>Ellipses (...)</td>
<td>Ellipses points indicate that text has been omitted from an example.</td>
</tr>
</tbody>
</table>
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, click the Services link at the Hyperion Solutions Web site.

Education Services

Hyperion offers instructor-led training, custom training, and e-Learning covering all Hyperion applications and technologies. Training is geared to administrators, end users, and information systems 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 telephone and electronic-based 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. Your opinion on the documentation is of value, so please send your comments by going to http://www.hyperion.com/services/support_programs/doc_survey/index.cfm.
This chapter describes Shared Services User Management and its components.

In This Chapter

- Benefits of Shared Services User Management ............................................. 16
- External Authentication and Single Sign-On .................................................. 16
- User Provisioning ........................................................................................... 16
- Product-Specific Access Control ................................................................. 16
- Shared Services User Management System ............................................... 17
- System Components ....................................................................................... 17
Benefits of Shared Services User Management

Shared Services User Management enables you to manage and provision users of Hyperion products from a centralized location, providing three main benefits:

- Hyperion products use the existing corporate structure of user accounts, thus reducing administrative overhead.
- Single sign-on to Hyperion applications is added, thus enabling users to log on once with one username and password.
- Users, groups, and security for multiple Hyperion products are managed from a centralized interface.

External Authentication and Single Sign-On

To use external authentication for Hyperion products, your organization must have an authentication directory that contains corporate user information. Then you can configure Shared Services to use the directory (or multiple directories) to authenticate Hyperion products users. Each Hyperion product enables external authentication by referencing the Shared Services configuration during the product configuration process.

After external authentication is configured, users can log on once to access multiple Hyperion products (single sign-on).

For instructions on configuring external authentication, see *Shared Services Installation Guide*.

User Provisioning

User provisioning is the process of granting roles and access control to Hyperion product users. Only Shared Services Administrators and Provisioning Managers for an application can provision users. Based on roles assigned, users can perform specific tasks and access content in various applications. Provisioning is managed at the user or group level; that is, a Provisioning Manager selects users or groups and then provisions them with roles for applications, or for Shared Services global roles (see “Roles” on page 20).

Product-Specific Access Control

Product-specific screens within User Management Console™ enable application administrators to perform product-specific provisioning tasks, such as assigning granular access permissions to objects. For example, for Hyperion System 9 BI+™ Analytic Services™ applications, users with the appropriate Analytic Services permissions can assign filter and calculation script access to selected users and groups.

Products that integrate with Shared Services User Management may require that certain security tasks are performed in the product interface itself, not through User Management Console. For example, using Analytic Services, you must create filters and calculation scripts from Analytic Services, and then you can assign specific users or groups access to these objects.
from User Management Console. Likewise, for Hyperion System 9 BI+, you must assign access control on repository content from within that application, not from User Management Console.

For instructions to assign product-specific access control in the User Management Console, see the appropriate product appendix at the end of this guide and also “Assigning Access Control to Applications” on page 31.

**Shared Services User Management System**

The Shared Services User Management system enables you to manage and provision users and groups for Hyperion products from a centralized interface.

Components of Shared Services User Management:

- **The Shared Services server**
  Shared Services user management requires a Shared Services server that is configured for external authentication. See *Shared Services Installation Guide*.

- **One or more authentication directories**
  You can configure the Shared Services server to use one or more corporate authentication directories for external authentication, or you can use the native Shared Services OpenLDAP authentication directory (or a combination of both). The native OpenLDAP directory is installed and configured automatically with Shared Services. See *Shared Services Installation Guide*.

- **User Management Console**
  User Management Console is the centralized user interface for (1) managing projects and applications within projects, (2) provisioning users and groups for applications, and (3) managing the Shared Services native directory. The console software is installed with Shared Services server. See Chapter 2, “Implementing Shared Services User Management.”

- **Hyperion products**
  For Shared Services user management functionality to be implemented for Hyperion products, each product must be registered with the Shared Services server in order to reference its external authentication configuration. See your product installation guide.

  For more information about how individual products integrate with Shared Services User Management, see the appropriate product appendix at the end of this guide.

**System Components**

The Shared Services User Management system consists of these components:

- “Authentication Directories” on page 18
- “Projects and Applications” on page 19
- “Users and Groups” on page 19
- “Roles” on page 20
In User Management Console, you operate on a component by selecting it in the object palette on the left side of the screen, and then right-click to view a context-sensitive menu for the object. The graphic below shows some of the objects contained in the object palette.

![Image of User Management Console]

**Authentication Directories**

You can configure Shared Services to use corporate authentication directories such as Lightweight Directory Access Protocol (LDAP), Windows NT LAN Manager (NTLM), and Microsoft Active Directory (MSAD). You can also use the native Shared Services OpenLDAP authentication directory (or a combination of both). The native OpenLDAP directory is installed and configured automatically with Shared Services. For more information about the OpenLDAP directory, see *Shared Services Installation Guide*.

Any corporate authentication directories that are configured for Shared Services for external authentication are listed in User Management Console under the User Directories node. The native Shared Services directory, which is provided with the Shared Services server, is listed in User Management Console as the Native Directory. When performing user or group management tasks, you select the authentication directory that contains the user or group you want to manage. For information about configuring Shared Services to use corporate directories, see *Shared Services Installation Guide*.

When User Management Console is open, changes made to corporate directories are not reflected immediately in the console. For example, if you add a user to a corporate directory while the User Management Console is open, you must perform another user search in order to display the user in User Management Console.
You cannot use User Management Console to perform certain operations on users and groups whose accounts exist in corporate directories. For example, you cannot rename or delete a user from a corporate directory in User Management Console; likewise, you cannot create users and groups in a corporate directory using User Management Console. You can, however, view and provision users whose accounts exist in corporate directories using User Management Console. For information about managing users and groups in corporate directories, see the respective directory server documentation.

**Projects and Applications**

In User Management Console, Hyperion applications are organized into projects. A project is a container for applications. For example, a project may consist of a Hyperion System 9 BI+ application and a Hyperion System 9 Planning™ application. To provision users to an application, the application must belong to a project. In User Management Console, applications that are registered with Shared Services but do not belong to a project are listed under the Unassigned Applications node.

An application is a reference to one instance of an application against which users and groups are provisioned. An application can belong to only one project. Users and groups can be provisioned with multiple roles for each application.

For instructions on managing projects and applications, see “Managing Projects” on page 28.

**Users and Groups**

In the Shared Services User Management system, users and groups may be maintained in corporate directories or in the native Shared Services directory. When you create users and groups in User Management Console, their information is stored in the native Shared Services directory. You cannot create users or groups in corporate directories from User Management Console.

If you are upgrading Hyperion products from a release that did not support user provisioning, you must migrate users and groups from the products to Shared Services. You can migrate users who were authenticated through native product security or who were authenticated through an external directory in that release. Each product has a migration tool that enables you to migrate user, group, and role information from the product to Shared Services. For migration information, see the appropriate product appendix at the end of this guide.

The Shared Services Administrator is the predefined user in the system. The Administrator performs initial setup tasks and assigns global Shared Services roles as necessary. See “Roles” on page 20.

The World group is the predefined group in the system. At the global level, the World group contains all users who are provisioned with at least one role in the system. At application levels, the World group can be used when an application administrator assigns access control to content within an application. In this context, the membership of the World group becomes application-specific in that it contains only the users provisioned for that application. Having a World group for each application enables administrators to assign access control for all users provisioned for the application at one time.
You can provision users individually or you can combine users into groups and provision the groups. If appropriate for an application, users and groups can be provisioned with multiple roles for the application. For example, a Hyperion System 9 BI+ user might be provisioned with the Cube Navigator and Explorer roles for one application, and a Hyperion System 9 Financial Management™ user might be provisioned with the roles of Generate Recurring and Manage Templates. See “Roles” on page 20.

A native Shared Services group can contain users and groups from the native Shared Services directory as well as users and groups from corporate directories. A group can contain a combination of native and external users and groups. When a group contains other groups, the roles assigned to the parent group are inherited by the child groups.

For instructions on managing users and groups, see “Managing Users, Groups, and Roles” on page 33.

**Roles**

Roles determine the tasks that users can perform within an application or globally within User Management Console. You can grant users a role directly, through membership in a group, or by granting a role that contains another role. Some users may need a combination of roles to perform a comprehensive set of administrative tasks.

- “Global Roles” on page 20
- “Provisioning Manager Role” on page 21
- “Product-Specific Roles” on page 22
- “Aggregated Roles” on page 22
- “Role Assignment Example” on page 22

**Global Roles**

Global roles are Shared Services roles that enable users to perform certain tasks within User Management Console:

- “Administrator” on page 20
- “Directory Manager” on page 21
- “Project Manager” on page 21

**Administrator**

You can configure the system with one Shared Services Administrator. The Administrator can then assign the Administrator role to other users as necessary. The Administrator role is a global role that provides control over all products that integrate with Shared Services User Management. The Shared Services Administrator role is the most powerful role in the user management system and allows more control over security than any previous Hyperion product roles. Administrators can perform all administrative tasks in User Management Console and can provision themselves.
The Administrator role should be assigned sparingly because it grants broad access to all applications registered with Shared Services. The Shared Services Administrator should be the user that sets up access for other administrative users. For example, the Shared Services Administrator assigns other administrative users either the Directory Manager or Provisioning Manager role; in turn, these users are responsible for managing general user access to applications. Therefore, the Shared Services Administrator user should delegate administration to others.

**Note:** The Shared Services role of Provisioning Manager is an application-specific role and must be assigned for individual applications. See “Provisioning Manager Role” on page 21.

**Directory Manager**

Users who are assigned the Directory Manager role can create and manage users and groups within the native Shared Services directory, including managing user and group membership.

The Directory Manager should generally not be assigned the Provisioning Manager role for the same reasons that the Shared Services Administrator role should be rarely assigned. For example, assume that a user is assigned the Provisioning Manager role for Analytic Services Application A, as well as the Directory Manager global role. This user can create a new user, assign the user any role within Analytic Services Application A, and log in as the new user, thereby granting himself/herself access to the Analytic Services application.

The recommended practice is to grant one user the Directory Manager role and grant a second user the Provisioning Manager role. Thus, the user with the Directory Manager role does not have visibility into user and group provisioning privileges.

**Project Manager**

Users who are assigned the Project Manager role can create and manage projects within Shared Services.

**Provisioning Manager Role**

The Shared Services role of Provisioning Manager functions like a product-specific role in that you assign it at the application level. There is no global Provisioning Manager role. Provisioning Managers can provision users and groups to applications but cannot provision themselves. For more information, see Appendix A, “Shared Services User Provisioning.”

**Note:** For guidance about assigning this role in conjunction with other roles, see “Global Roles” on page 20.
If you are migrating users from Hyperion products to Shared Services, be aware that some administrator users are automatically assigned the Provisioning Manager role during migration. For example, users who were Analytic Services Administrators (previously Supervisors) in a previous release are automatically assigned the Provisioning Manager role for the global Analytic Server application during migration. Administrator users that are added to the system after migration are, however, not assigned the Provisioning Manager role. For example, newly added Analytic Services Administrators are not assigned the Provisioning Manager role.

For information about which users are assigned the Provisioning Manager role during migration, see the appropriate product appendix at the end of this guide.

**Product-Specific Roles**

Product-specific roles enable users to perform certain tasks within the product (for example, the Application Administrator in Financial Management and the Planners role in Planning). You assign product-specific roles for individual applications. For a complete list of product-specific roles, see the appropriate product appendix at the end of this guide.

**Aggregated Roles**

Shared Services administrators can create custom roles that aggregate multiple product roles within a product. For example, a Shared Services Administrator or Provisioning Manager can create a role for Planning that combines the Planner and View User roles into a new role. Aggregating roles can simplify the administration of applications that have a large number of granular roles. You cannot create an aggregated role that spans products, and you cannot include global Shared Services roles in aggregated roles. For instructions on creating aggregated roles, see “Creating Aggregated Roles” on page 42.

For instructions on managing roles, see “Managing Users, Groups, and Roles” on page 33.

**Role Assignment Example**

This example illustrates when a user might need a combination of global roles:

For Hyperion System 9 BI+, users who were assigned the Global Administrator role in previous releases would need several roles in this release to perform the same administrative tasks:

- Global Administrator (Hyperion System 9 BI+ role)
- Directory Manager (Shared Services global role)
- Provisioning Manager for the application (Shared Services application-specific role)
Implementing Shared Services User Management

Hyperion recommends that you use Shared Services to manage users and groups outside the context of particular Hyperion products or applications. This chapter helps you implement the Shared Services User Management system and describes the User Management Console interface.

In This Chapter

- Process for Setting Up Shared Services User Management .............................................. 24
- Launching User Management Console ............................................................................. 25
- Navigating in User Management Console ........................................................................ 26
Process for Setting Up Shared Services User Management

Use the following high-level process to set up user management for Hyperion products:

1. Install, configure, and start Hyperion License Server™.
   See Shared Services Installation Guide.

2. Install, configure, and start Shared Services, and configure external authentication for Shared Services.
   See Shared Services Installation Guide.

3. Install Hyperion products.
   See the appropriate product installation guide.

4. Configure installed Hyperion products to reference the Shared Services external authentication configuration.
   See the appropriate product installation guide.

5. If upgrading from previous releases of Hyperion products, migrate existing users from the products to Shared Services.
   See the appropriate product appendix at the end of this guide.

6. Launch User Management Console (either as a stand-alone or from a Hyperion product interface).
   See “Launching User Management Console” on page 25 and the appropriate product appendix at the end of this guide.

7. Shared Services Administrator: Assign global roles to other users as appropriate. For example, provision the appropriate users with the Directory Manager or Project Manager role.
   See “Roles” on page 20 and “Provisioning Users and Groups” on page 44.

8. Shared Services Administrator or Project Managers: Create projects and add applications to projects.
   See “Projects and Applications” on page 19 and “Managing Projects” on page 28.

9. Shared Services Provisioning Managers: Provision users and groups by granting them roles for specific applications.
   See “User Provisioning” on page 16 and “Provisioning Users and Groups” on page 44.

10. Application administrators: Perform product-specific provisioning tasks, such as assigning access control to application objects.
    See “Product-Specific Access Control” on page 16 and the appropriate product appendix at the end of this guide.
Launching User Management Console

You can launch User Management Console directly from a browser or from a Hyperion product interface. For instructions on launching User Management Console from a Hyperion product interface, such as Planning, see the appropriate product appendix at the end of this guide.

**Note:** On Windows, from the Shared Services server computer, you can launch User Management Console from the Start menu (Start > Hyperion System 9 Foundation > Start User Management Console).

➤ To launch User Management Console from a browser:

1. **Open a browser, for example, Internet Explorer.**
2. **In the address bar, type the following URL:**
   
   ```text
   http://SharedServicesServerName:port#/interop
   ```
   
   where `SharedServicesServerName` is the name of the computer where the Shared Services server is installed and `port#` is the Shared Services server port number. The default port number is 58080; if Shared Services server is installed to a non-default port, specify that value.

   For example, using the default port:
   ```text
   http://jdoe:58080/interop/
   ```

   **Note:** As a best practice when accessing User Management Console on the machine where the Shared Services server is running, the URL to access the console should always use an IP address or a fully qualified machine name that includes the domain name. If the IP address is dynamic, use the fully qualified machine name.

3. **On the Logon screen, type the user name and password, and click Log on.**

   **Note:** If pop-up blockers are enabled in the browser, User Management Console may not launch automatically. Place the URL for the User Management Console in the “allowed” URL list, or try changing the pop-up blocker setting from high to medium or low.

   The main screen of the User Management Console is displayed.
Navigating in User Management Console

After you log on to User Management Console, you see the start page, where you work with authentication directories, projects and applications, users and groups, and roles. For more information about these objects, see “System Components” on page 17.

Factors to keep in mind:

- To show or hide the masthead at the top of the screen, select View > Masthead.
- The left part of the screen is called the object palette. Depending on your selections in the top part of the object palette, this pane may be split into two or more parts.
- When performing actions on objects in the object palette, you can select an object and right-click to access a context-sensitive menu. These menu options change dynamically, depending on what is selected. Right-click menu commands are also available on a menu from the menu bar. For example, when a user is selected, the “Provision” menu command is available on the right-click menu and on the Administration menu on the menu bar.
- To view a help topic for a particular screen, click the Help button on the screen. To view the entire help system, select Help > Contents from the menu bar. To view an Information Map to all Shared Services documentation, select Help > Information Map.
- To view users, groups, and roles in User Management Console:
  1. Expand User Directories.
  2. Expand the node for the appropriate authentication directory.
  3. Select Users, Groups, or Roles.
  4. In the lower part of the object palette, specify the text to search for, or click Show All to show all selected items (for example, with Users selected, click Show All to display all users in the selected directory).
  5. To view or perform an action on a user, group, or role, select it in the lower part of the object palette.
- Pop-up blockers may prevent User Management Console from working properly. Either place the URL for the User Management Console in the “allowed” URL list, or try changing the pop-up blocker setting from high to medium or low.
- If you are receiving Java Virtual Machine (JVM) errors in User Management Console using Microsoft Internet Explorer, ensure that your Internet Explorer installation includes Microsoft XML parser (MSXML) version 4.
  MSXML is bundled with Internet Explorer 6.0. To verify that you have the correct MSXML, check that the following file exists:
  \winnt\system32\msxml4.dll
  If you do not see this file, install Internet Explorer 6.0 or higher.
Managing and Provisioning Users and Groups

User Management Console provides a centralized user interface for managing and provisioning Hyperion product users.

In This Chapter

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managing Projects</td>
<td>28</td>
</tr>
<tr>
<td>Managing Applications</td>
<td>30</td>
</tr>
<tr>
<td>Managing User Directories</td>
<td>33</td>
</tr>
<tr>
<td>Managing Users, Groups, and Roles</td>
<td>33</td>
</tr>
<tr>
<td>Provisioning Users and Groups</td>
<td>44</td>
</tr>
</tbody>
</table>
Managing Projects

A project is a container for Hyperion product applications. For example, a project may contain a Planning application and one or more Analytic Services applications. An application can belong to only one project. Applications that are registered with Shared Services but do not yet belong to a project are listed under Unassigned Applications in User Management Console. You can only provision users to assigned applications.

Shared Services User Management enables you to create projects, organize applications within projects, and provision users and groups for applications.

Project management tasks:

- “Creating Projects” on page 28
- “Modifying Project Properties” on page 29
- “Deleting Projects” on page 30

Creating Projects

Project creation includes adding applications to the new project. You must be a Shared Services Administrator or Project Manager to perform this task.

➢ To create a project:

1. From User Management Console, select Projects.

2. Right-click and select New > Project.

   The New Project frame is displayed.

3. For Name, enter the project name.

   Project names are not case-sensitive; the name is displayed exactly as entered. Project names must be fewer than 250 characters and can contain any combination of characters except for a backslash or double quotation mark.

4. Optional: For Description, enter a project description.

5. Add applications to the project:

   a. To display a list of applications in an existing project, select the project from List Applications in Project, and click Update List.

      By selecting an application from a project, the application is moved to the new project along with the application provisioning assignments.

   b. To display a list of unassigned applications, select <Unassigned Applications> from List Applications in Project, and click Update List.

      Unless you are a Shared Services Administrator, only applications for which you are a Provisioning Manager are listed.
c. In Available Applications, select the applications to add to the project, and click Add to move the applications to Assigned Applications.
d. In Assigned Applications, select the applications to add to the project.

6 Click Finish.
A status message is displayed.

**Modifying Project Properties**

You can modify a project to rename it or modify the applications within it. You must be a Shared Services Administrator or Project Manager to perform this task.

**Note:** You can also add applications to projects by moving them from another project or from the Unassigned Applications node. See "Moving Applications" on page 31.

➤ To modify a project:

1 From User Management Console, expand Projects.

2 Select the project.
The Modify Project frame is displayed.

3 **Optional:** For Name, modify the project name.

   Project names are not case-sensitive; the name is displayed exactly as entered. Project names must be fewer than 250 characters and can contain any combination of characters except for a backslash or double quotation mark.

4 **Optional:** For Description, modify the project description.

5 **Optional:** Add or remove applications:

   The applications that belong to the project are listed in the lower part of the frame.

   ● To remove an application from the project:
      i. Select the application.
      ii. Click Remove.

   **Note:** When you remove an application, all provisioning assignments for the application are also removed.

   ● To add an application to the project:
      i. To display a list of applications from an existing project, select the project from List Applications in Project, and click Update List.

      By selecting an application from a project, the application is moved to the new project along with the application provisioning assignments.
ii. To display a list of unassigned applications, select <Unassigned Applications> from List Applications in Project, and click Update List.

Unless you are a Shared Services Administrator, only applications for which you are a Provisioning Manager are listed.

iii. In Available Applications, select the applications to add, and click Add to move the applications to Assigned Applications.

iv. In Assigned Applications, select the applications to add.

6 Click Save.

A status message is displayed.

Deleting Projects

Deleting a project removes the association of applications with the project, removes provisioning assignments from applications within the project, and deletes the project container itself. Applications from deleted projects are moved to the Unassigned Applications node.

You must be a Shared Services Administrator or Project Manager to perform this task.

➤ To delete a project:

1 From User Management Console, expand Projects.

2 Select the project.

3 Right-click and select Delete.

4 At the confirmation prompt, click OK.

A status message is displayed.

Managing Applications

An application is a reference to a single instance of an application against which users and groups are provisioned. User Management Console lists all applications that are registered with Shared Services. Applications that belong to a project are listed under Projects; applications that are registered with Shared Services but do not belong to a project are listed under Unassigned Applications.

Project management tasks:

● “Assigning Access Control to Applications” on page 31

● “Moving Applications” on page 31

● “Copying Provisioning Information” on page 32

For instructions on provisioning, see “Provisioning Users and Groups” on page 44.
Assigning Access Control to Applications

To assign specific security properties for a product, such as access control to application objects or user preferences, you may do so within the application or in User Management Console. Some products require that certain security properties are set only in User Management Console and are not available within the application interface. To assign access control for a product in User Management Console, you must be provisioned with the appropriate product role.

In User Management Console, you select an application and then select the users and groups to which you want to assign product-specific access control. For example, to assign filter permissions for an Analytic Services application, you select the appropriate Analytic Services application and then select the users and groups to which you want to assign specific filter permissions. Likewise, to assign access to dimensions, forms, or task lists for Planning, you select the appropriate Planning application and then select the users and groups to which you want to assign Planning-specific access. Hyperion System 9 BI+ exposes user preferences within User Management Console.

You can assign application-specific access control according to your role for the application.

➤ To assign application-specific access:

1 Ensure that the required server and application are running.

2 From User Management Console, expand Projects.

3 Expand the project.

4 Select the application, right-click, and select the appropriate menu item for that application.

An application-specific frame is displayed.

Note: If the product server is not running, an error message is displayed when the application is selected. You must restart the product server and refresh the object palette by clicking View > Refresh to access the application.

5 Click Help for more information, or see the appropriate product appendix at the end of this guide for instructions on assigning access control for specific products.

Moving Applications

You can move an application from one project to another, and you can move unassigned applications to projects. When you move an application, all user, group, and role information is moved with it. Moving an application from a project removes the association between the application and the project but does not affect provisioning assignments for the application.

You must be a Shared Services Administrator or Project Manager as well as Provisioning Manager for the application being moved to perform this task.
To move an application:
1. From User Management Console, expand Projects.
2. Select the application.
   
   Unless you are a Shared Services Administrator, only the applications for which you are Provisioning Manager are displayed.
3. Right-click and select Move To.
4. On the Move To frame, select the project to which you want the application moved.
5. Click Save.
   
   A status message is displayed.

To move unassigned applications to projects:
1. From User Management Console, expand Unassigned Applications.
2. Select the application.
   
   Unless you are a Shared Services Administrator, only the applications for which you are Provisioning Manager are displayed.
3. Right-click and select Move To.
4. On the Move To frame, select the project to which you want the application moved.
5. Click Save.
   
   A status message is displayed.

**Copying Provisioning Information**

You can copy provisioning information from one application to another; the applications must be from the same product and product version. When you copy provisioning information, all user, group, and role information is copied to the target application. Product-specific access control settings are not copied.

You must be a Shared Services Administrator or Provisioning Manager for both the source and target applications to perform this task.

To copy provisioning information:
1. From User Management Console, expand Projects.
2. Select the application whose provisioning information you want to copy.
3. Right-click and select Copy Provisioning.
4 On the **Copy Provisioning** frame, select the application to which you want to copy provisioning information. Unless you are a Shared Services Administrator, only the applications for which you are Provisioning Manager are displayed.

5 **Click Save.**

A status message is displayed.

---

**Managing User Directories**

You can manage only the native Shared Services directory through User Management Console. You can, however, still provision users and groups that are maintained in other directories.

The native Shared Services directory is an OpenLDAP authentication directory that is installed with Shared Services. For more information about the OpenLDAP directory, see *Shared Services Installation Guide*.

**Note:** If the OpenLDAP directory is restarted, you must also restart the Shared Services server and User Management Console.

For information about configuring and managing users and groups in corporate directories, see *Hyperion Shared Services Installation Guide* and the respective directory server documentation.

---

**Managing Users, Groups, and Roles**

You can assign roles to users and groups that are maintained in corporate directories or in the native Shared Services directory. In User Management Console, you select users and groups and assign roles to them for particular applications.

Some provisioning assignments are application-specific rather than user-based. You assign product-specific access control to application objects at the application level. For instructions, see “Assigning Access Control to Applications” on page 31.

---

**Managing Native Shared Services Users**

Users with Shared Services Administrator and Directory Manager roles can manage native Shared Services users.

User management tasks:

- “Creating Native Shared Services Users” on page 34
- “Modifying Native Shared Services User Properties” on page 35
- “Deleting Native Shared Services Users” on page 36
- “Enabling and Disabling Native Shared Services Users” on page 37
Creating Native Shared Services Users

You can create a user in the native Shared Services directory. You cannot create users in a corporate directory from User Management Console. You must be a Shared Services Administrator or Directory Manager to perform this task.

To create a native Shared Services user:

1. From User Management Console, expand User Directories.
2. Expand Native Directory, and select Users.
3. Right-click and select New > User.
   - The New User frame is displayed.
4. Enter the following user information:
   - User ID
   - First Name
   - Last Name
   - Description (optional)
   - Email Address
   - Password
   - Confirm Password

Guidelines:
- User IDs should follow the naming convention of your organization (for example, first name initial followed by last name, as in jyoung).
- User IDs are not case-sensitive; they are displayed exactly as entered. User IDs can be any length and can contain any combination of characters.
- You cannot create user IDs that are identical except for the number of spaces between parts of the name. For example, you cannot create a user ID as user 1 (with one space between user and 1) and another user ID user 1 (with two spaces between user and 1).
- Passwords are case-sensitive, can be any length, and can contain any combination of characters.

5. If you do not want to add the user to a group, click Finish.
6  **Optional: Add the user to a group:**
   a. Click Next to go to the **Group Membership** frame.
   b. For **Search for Groups**, enter the group to find. Enter * to find all groups.
   c. Click Go to display the groups that match the search criteria.
   d. Select the group, and click **Add**.
   e. In the lower part of the frame, select the group again.

7  **Click Finish.**
   A status message is displayed.

**Modifying Native Shared Services User Properties**

For native Shared Services users, you can modify general user properties and the user’s group membership. You must be a Shared Services Administrator or Directory Manager to perform this task.

➢ To modify user properties:

1  **From User Management Console, expand User Directories.**

2  **Expand Native Directory, and select Users.**

3  **In the bottom part of the object palette:**
   - To view all users in the native directory, click **Show All**.
   - To search for a user in the native directory, enter the text to search for, and click **Search**.
   A list of enabled users is displayed.

4  **Select the user to modify.**
   The Modify User frame is displayed.

5  **On the General tab, modify the user’s information:**
   - User ID
   - First Name
   - Last Name
   - Description (optional)
   - Email Address
   - Password
   - Confirm Password
Guidelines:

- User IDs should follow the naming convention of your organization (for example, first name initial followed by last name, as in jyoung).
- User IDs are not case-sensitive; they are displayed exactly as entered. User IDs can be any length and can contain any combination of characters.
- You cannot create user IDs that are identical except for the number of spaces between parts of the name. For example, you cannot create a user ID as user 1 (with one space between user and 1) and another user ID as user 1 (with two spaces between user and 1).
- Passwords are case-sensitive, can be any length, and can contain any combination of characters.

6 If you do not want to modify the user’s group membership, click Save.

7 Optional: To modify the user’s group membership, click Member Of.

**Note:** Users cannot change their own group membership.

The groups to which the user belongs are listed in the lower part of the frame.

- To remove the user from a group:
  i. Select the group.
  ii. Click Remove.
- To add the user to a group:
  i. For Search for Groups, enter the group to find. Enter * to find all groups.
  ii. Click Go to display the groups that match the search criteria.
  iii. In the lower part of the frame, select the group, and click Add.

8 Click Save.

A status message is displayed.

**Deleting Native Shared Services Users**

Deleting a user removes the user’s associations with groups and roles and also physically removes the user’s information from the native Shared Services directory. You cannot delete users from corporate directories using User Management Console.

You must be a Shared Services Administrator or Directory Manager to perform this task.

➢ To delete a user:

1 From User Management Console, expand User Directories.

2 Expand Native Directory, and select Users.
3 In the bottom part of the object palette:
   ● To view all users in the native directory, click Show All.
   ● To search for a user in the native directory, enter the text to search for, and click Search.
A list of enabled users is displayed.
4 Select the user to delete, right-click, and select Delete.
5 At the confirmation prompt, click OK.
A status message is displayed.

Enabling and Disabling Native Shared Services Users

Users in the native Shared Services directory can be in an enabled or disabled state. An enabled state indicates that the user can currently log in to the appropriate applications. A disabled state indicates that the user cannot access any applications.

Keep in mind this information about users in a disabled state:

   ● Disabled users cannot log on to User Management Console.
   ● The group associations of disabled users are not deleted and remain visible to the Administrator.
   ● Disabled users no longer have role associations.
   ● Disabled users are not displayed on the product-specific access control screens of the items for which access is disabled.
   ● Information about disabled users is not removed. Disabled users are not deleted.
   ● Only native Shared Services users can be disabled. Corporate directory users can be disabled only from within the corporate directory.

Disabling Users

You must be a Shared Services Administrator or Directory Manager to perform this task.

➤ To disable a user:

1 From User Management Console, expand User Directories.
2 Expand Native Directory, and select Users.
3 In the bottom part of the object palette:
   ● To view all users in the native directory, click Show All.
   ● To search for a user in the native directory, enter the text to search for, and click Search.
A list of enabled users is displayed.
4 Select the user to disable, right-click, and select Disable.
A status message is displayed.
Enabling Users

Enabling a user reinstates all associations that existed at the time the user was disabled. If a group that contains the user is deleted while the user is disabled, the user’s associations cannot be reinstated.

You must be a Shared Services Administrator or Directory Manager to perform this task.

To enable a user:

1. From User Management Console, expand User Directories.
2. Expand Native Directory, and select Users.
3. Right-click and select View Disabled Users Only.
   The list of disabled users is displayed.
4. Select the user to enable, right-click, and select Enable.
   A status message is displayed.

Managing Native Shared Services Groups

Users with Shared Services Administrator and Directory Manager roles can manage native Shared Services groups.

Group management tasks:

- “Creating Native Shared Services Groups” on page 38
- “Modifying Native Shared Services Group Properties” on page 39
- “Deleting Native Shared Services Groups” on page 41

Note: For information about provisioning and deprovisioning groups, see “Provisioning Groups” on page 46 and “Deprovisioning Groups” on page 47.

Creating Native Shared Services Groups

You can create a group in the native Shared Services directory that consists of users and groups from the native directory or from corporate directories, or a combination of both.

You cannot create or modify groups that are maintained in a corporate directory using User Management Console. For more information about groups, see “Users and Groups” on page 19.

You must be a Shared Services Administrator or Directory Manager to perform this task.
To create a native Shared Services group:

1. From User Management Console, expand User Directories.
2. Expand Native Directory, and select Groups.
4. In the New Group frame, enter group information:
   - Name—Name of the group
     Group names are not case-sensitive; the name is displayed exactly as entered. Group names can be any length and can contain any combination of characters.
   - Description—Optional description
5. Click Next to go to the Group Membership frame.
6. Optional: Include subgroups in the new group:
   a. For Search for Groups, enter the group to find. Enter * to find all groups.
   b. From Provider, select the authentication directory in which you want to search for the group.
      To search for groups from the native Shared Services directory, select Native Directory.
   c. Click Go to display the groups that match the search criteria.
   d. Select the groups to add, and click Add.
   e. Select the groups again and click Next.
7. Click Next to go to the User Members frame.
8. Optional: Add users to the group:
   a. For Search for Users, enter the user to find. Enter * to find all users.
   b. From Provider, select the authentication directory in which you want to search for the users.
      To search for users in the native Shared Services directory, select Native Directory.
   c. Click Go to display the users that match the search criteria.
   d. Select the users to add, and click Add.
   e. Select the users again.
9. Click Finish.
   A status message is displayed.

Modifying Native Shared Services Group Properties

For native Shared Services groups, you can modify general group properties and group membership. You must be a Shared Services Administrator or Directory Manager to perform this task.
To modify group properties:

1. From User Management Console, expand User Directories.
2. Expand Native Directory, and select Groups.
3. In the bottom part of the object palette:
   - To view all groups in the native directory, click Show All.
   - To search for a group in the native directory, enter the text to search for, and click Search. A list of enabled groups is displayed.
4. In the Modify Group frame, on the General tab, modify group information:
   - Name—Name of the group
     Group names are not case-sensitive; the name is displayed exactly as entered. Group names can be any length and can contain any combination of characters.
   - Description—Optional description
5. Optional: Modify subgroup membership in the group.
   a. Select the Group Members tab.
      The subgroups that are in the group are listed in the lower part of the frame.
   b. To remove a subgroup:
      i. Select the group to remove.
      ii. Click Remove.
   c. To add a subgroup:
      i. For Search for Groups, enter the group to find. Enter * to find all groups.
      ii. From Provider, select the authentication directory in which you want to search for the group.
         To add groups from native Shared Services directory, select Native Directory.
      iii. Click Go to display the groups that match the search criteria.
      iv. Select the groups to add, and click Add.
      v. In the lower part of the frame, select the groups again.
6. Optional: Modify user membership in the group.

   Note: Users cannot change their own group membership.

   a. Select the User Members tab.
      The users that are in the group are listed in the lower part of the frame.
   b. To remove a user:
      i. Select the user.
      ii. Click Remove.
c. To add a user:
   i. For Search for Users, enter the user to find. Enter * to find all users.
   ii. From Provider, select the authentication directory in which you want to search for the user.
      To search for users in the native Shared Services directory, select Native Directory.
   iii. Click Go to display the users that match the search criteria.
   iv. Select the users to add, and click Add.
   v. In the lower part of the frame, select the users again.

7 Click Save.
   A status message is displayed.

Deleting Native Shared Services Groups
Deleting a group removes the group’s associations with users and roles and also physically removes the group’s information from the native Shared Services directory. You cannot delete groups from corporate directories using User Management Console.

You must be a Shared Services Administrator or Directory Manager to perform this task.

➤ To delete a group:

1 From User Management Console, expand User Directories.

2 Expand Native Directory, and select Groups.

3 In the bottom part of the object palette:
   ● To view all groups in the native directory, click Show All.
   ● To search for a group in the native directory, enter the text to search for, and click Search.

   A list of enabled groups is displayed.

4 Select the group, right-click, and select Delete.

5 At the confirmation prompt, click OK.
   A status message is displayed.
Managing Aggregated Roles

Roles define which operations a user may perform. Shared Services Administrators can create custom roles that aggregate multiple roles within a product. You cannot create an aggregated role that spans products, and you cannot include global Shared Services roles in aggregated roles.

Role management tasks:

- “Creating Aggregated Roles” on page 42
- “Modifying Aggregated Roles” on page 43
- “Deleting Aggregated Roles” on page 44

Creating Aggregated Roles

You must be a Shared Services Administrator or Provisioning Manager to perform this task.

To create an aggregated role:

1. From User Management Console, expand User Directories.
2. Expand Native Directory, and select Roles.
3. Right-click and select New > Role.

   The New Aggregated Role frame is displayed.

4. Specify information about the role:
   - **Name**—Name of the role.
     Role names are not case-sensitive; the name is displayed exactly as entered. Role names can be any length and can contain any combination of characters.
   - **Description**—Optional description.
   - **Product Name**—Select the product for which to create the role.
     The list includes all products that are registered with Shared Services.

5. Click Next to go to the Role Members frame.
6. For Search for Roles, enter the role to find. Enter * to find all roles for the selected product.
7. Click Go to display the roles that match the search criteria.
8. Select the roles to add, and click Add.
9. In the lower part of the frame, select the roles again.
10. Click Finish.

   A status message is displayed.
Modifying Aggregated Roles

You can modify aggregated roles. You cannot modify system-defined roles (for example, product-specific roles or Shared Services roles).

You must be a Shared Services Administrator or Provisioning Manager to perform this task.

➤ To modify an aggregated role:

1. From User Management Console, expand User Directories.
2. Expand Native Directory, and select Roles.
3. In the bottom part of the object palette:
   • To view all roles, click Show All.
   • To search for a role, enter the text to search for, and click Search.
     A list of roles is displayed.
4. Select the role to modify.
5. In the Modify Role frame, on the General tab, modify role information:
   • Name—Name of the role.
     Role names are not case-sensitive; the name is displayed exactly as entered. Role names can be any length and can contain any combination of characters.
   • Description—Optional description.

Note: You cannot select a different product when modifying an aggregated role.

6. Select the Role Members tab.
   Roles that are currently part of the aggregated role are listed in the lower part of the frame.
   • To remove a role:
     i. Select the role.
     ii. Click Remove.
   • To add a role:
     i. For Search for Roles, enter the role to find. Enter * to find all roles.
     ii. Click Go to display the roles that match the search criteria.
     iii. Select the roles to add, and click Add.
     iv. In the lower part of the frame, select the roles again.
7. Click Save.
   A status message is displayed.
Deleting Aggregated Roles

Deleting an aggregated role removes the role associations with users, groups, and other roles. You cannot delete system-defined roles (for example, product-specific roles or Shared Services roles). You must be a Shared Services Administrator or Provisioning Manager to perform this task.

➤ To delete an aggregated role:
1. From User Management Console, expand User Directories.
2. Expand Native Directory, and select Roles.
3. In the bottom part of the object palette:
   ● To view all roles, click Show All.
   ● To search for a role, enter the text to search for, and click Search.
   A list of roles is displayed.
4. Select the role.
5. Right-click and select Delete.
6. At the confirmation prompt, click OK.
   A status message is displayed.

Provisioning Users and Groups

Provisioning is the process of granting roles to users of Hyperion applications. Provisioning is managed at the user or group level; a Provisioning Manager selects a user or group and provisions the user or group with one or more roles for one or more applications, or for a Shared Services global role. For conceptual information about user provisioning, see “User Provisioning” on page 16.

Provisioning tasks:

● “Provisioning Users” on page 45
● “Deprovisioning Users” on page 46
● “Provisioning Groups” on page 46
● “Deprovisioning Groups” on page 47
● “Generating Provision Reports” on page 48
Provisioning Users

When you provision a user, you assign the user one or more roles for one or more applications. You cannot provision users to unassigned applications. You must be a Shared Services Administrator or Provisioning Manager to perform this task.

**Note:** Provisioning Managers cannot provision themselves.

➤ To provision users:

1. From User Management Console, expand **User Directories**.
2. Expand the directory that contains the users, and select **Users**.
   
   You can provision users from corporate directories and from the native Shared Services directory.

3. **In the bottom part of the object palette:**
   - To view all users in the selected directory, click **Show All**.
   - To search for a user in the selected directory, enter the text to search for, and click **Search**.
   
   A list of enabled users is displayed.

4. **Select the users to provision, right-click, and select Provision.** To select multiple users, press the **Ctrl** key between selections.
   
   The Provision Users and Groups frame is displayed. All projects that contain applications for which you are Provisioning Manager are displayed.

5. **Expand the appropriate project and application.**

   **Note:** When provisioning a single user, you can click an application name to view the list of roles currently assigned to the user for that application.

6. **Select the roles to assign.**
   
   For information on product-specific roles and Shared Services roles, see the appropriate product appendix at the end of this guide.

7. **Repeat the previous two steps to provision the users for other applications.**

8. **Click Save.**
   
   A status message is displayed.
Deprovisioning Users

Deprovisioning a user removes all roles the user is assigned for all applications to which the Provisioning Manager performing the deprovisioning has access.

You must be a Shared Services Administrator or Provisioning Manager to perform this task.

➤ To deprovision users:
1 From User Management Console, expand User Directories.
2 Expand the directory that contains the user to deprovision, and select Users.
   You can deprovision users from corporate directories and from the native Shared Services directory.
3 In the bottom part of the object palette:
   ● To view all users in the selected directory, click Show All.
   ● To search for a user in the selected directory, enter the text to search for, and click Search.
   A list of enabled users is displayed.
4 Select the users to deprovision, right-click, and select Deprovision. To select multiple users, press the Ctrl key between selections.
5 At the confirmation prompt, click OK.
   A status message is displayed.

Provisioning Groups

When you provision a group, you assign the group one or more roles for one or more applications. You must be a Shared Services Administrator or Provisioning Manager to perform this task.

➤ To provision groups:
1 From User Management Console, expand User Directories.
2 Expand the directory that contains the group to provision, and select Groups.
   You can provision groups from corporate directories and from the native Shared Services directory.
3 In the bottom part of the object palette:
   ● To view all groups in the selected directory, click Show All.
   ● To search for a group in the selected directory, enter the text to search for, and click Search.
   A list of enabled groups is displayed.
4 Select the groups, right-click, and select Provision. To select multiple groups, press the Ctrl key between selections.

The Provision Users and Groups frame is displayed. All projects that contain applications for which you are Provisioning Manager are displayed.

5 Expand the appropriate project and application.

6 Select the roles to assign to the groups.

   For information on product-specific roles and Shared Services roles, see the appropriate product appendix at the end of this guide.

7 Repeat the previous two steps to provision the groups for other applications.

8 Click Save.

   A status message is displayed.

---

## Deprovisioning Groups

Deprovisioning a group removes all roles that the group is assigned for all applications to which the Provisioning Manager performing the deprovisioning has access.

You must be a Shared Services Administrator or Provisioning Manager to perform this task.

➤ To deprovision groups:

1 From User Management Console, expand User Directories.

2 Expand the directory that contains the group to deprovision, and select Groups.

   You can deprovision groups from corporate directories and from the native Shared Services directory.

3 In the bottom part of the object palette:

   ● To view all groups in the selected directory, click Show All.

   ● To search for a group in the selected directory, enter the text to search for, and click Search.

   A list of enabled groups is displayed.

4 Select the groups, right-click, and select Deprovision. To select multiple groups, press the Ctrl key between selections.

5 At the confirmation prompt, click OK.

   A status message is displayed.
Generating Provision Reports

The provision report displays the roles that users are provisioned for selected applications. The report indicates which authentication directory contains each user. You can generate a generic provisioning report for all users, applications, and roles, or you can use filter criteria to generate a customized report.

You must be a Shared Services Administrator or Provisioning Manager to perform this task.

To generate a provision report:

1. In User Management Console, select Administration > View Report.

   **Note:** To restrict the report to specific users, groups, or roles, first select them and then select Administration > View Report.

   The View Report frame is displayed. The default filter selections depend on what is selected in the object palette.

2. Specify filter criteria:

   - **Find all**—Specify whether to filter by users, groups, or roles. The available options depend on what is selected in the object palette. For example, if a role is selected, the list includes only Users and Groups.
     
     If individual users or groups are selected, you can only filter by roles. If individual roles are selected, you can only filter by users or groups.

   - **for user** or **for role**—This label changes depending on what is selected in Find all. If individual users, groups, or roles are selected in the object palette, you cannot edit this field.
     
     - If Roles is selected in Find all, the label is for user. Enter the user name to filter by, or enter * to generate the report for all users. This field is not case-sensitive.
     
     - If Users or Groups is selected in Find all, the label is for role. Enter the role name to filter by, or enter * to generate the report for all roles. This field is not case-sensitive.

   - **show effective roles**—Select this to show only the roles that are obtained from groups that contain the users/groups.

   - **group by**—Specify how to structure the provision report. Your selection determines what is displayed in the left-hand report column.
     
     The options change depending on what is selected in Find all.

     - If Roles is selected in Find all, you can group by Applications or by Users.
     
     - If Users or Groups is selected in Find all, you can group by Applications or by Roles.

   - **in application**—Select the applications to include in the report.

3. Click Create Report.

   A detailed report of provisioned users, groups, and roles is generated and displayed.

4. To print the report, click Print.
This appendix lists the user roles for Shared Services.

In This Appendix

- Shared Services User Roles ................................................................. 50
- User Roles and Tasks ................................................................. 52
Shared Services User Roles

Shared Services supports these user roles, as described in the following topics:

- “Administrator” on page 50
- “Directory Manager” on page 50
- “Project Manager” on page 51
- “Provisioning Manager” on page 51
- “Create Integrations” on page 51
- “Run Integrations” on page 52

Note: For more information, see “Global Roles” on page 20.

Administrator

Users who are assigned the Administrator role have access to all administrative functions within Shared Services.

Note: Hyperion recommends that the Administrator role be assigned sparingly in an organization. The Shared Services Administrator role is the most powerful role in the user management system and allows more control over security than any previous Hyperion product roles.

Directory Manager

Users who are assigned the Directory Manager role can create and manage directory users and groups within Shared Services.

As a Directory Manager user, you can perform these actions in Shared Services:

- Create users
- Modify user details
- Delete users
- Disable and enable user accounts
- Create groups
- Modify group details
- Delete groups
- Disable and enable group accounts

Note: As a best practice for secure systems, Hyperion does not recommend assigning both the Directory Manager role and the Provisioning Manager role to the same user. This is a safeguard against allowing users to provision themselves.
**Project Manager**

Users who are assigned the Project Manager role can create and manage projects within Shared Services.

As a Project Manager user, you can perform these actions in Shared Services:

- Create projects
- Modify project details
- Delete projects

**Provisioning Manager**

Users who are assigned the Provisioning Manager role can provision users and groups to applications. In order to provision a user to an application, the application must belong to a project.

As a Provisioning Manager user, you can perform these actions in Shared Services:

- Provision users
- De-provision users
- Provision groups
- De-provision groups
- Generate the Provision Report

Provisioning Managers cannot provision themselves.

**Note:** As a best practice for secure systems, Hyperion does not recommend assigning both the Directory Manager role and the Provisioning Manager role to the same user. This is a safeguard against allowing users to provision themselves.

**Create Integrations**

Users who are assigned the Create Integrations role can create Shared Services data integrations.

Shared Services enables you to move data between applications, called data integration. A data integration wizard facilitates the process of creating data integrations.

As a Create Integrations user, you can perform these actions on data integrations:

- Assign access to integrations
- Create integrations
- Edit integrations
- Copy integrations
- Delete integrations
- Create data integration groups
● View (including filtering the view of) integrations

**Run Integrations**

Users who are assigned the Run Integrations role can view and run Shared Services data integrations.

As a Run Integrations user, you can perform these actions on data integrations:

- View (including filtering the view of) integrations
- Run, or schedule to run, integrations
- Run, or schedule to run, group integrations

**User Roles and Tasks**

*Table 1  Shared Services User Roles and Tasks Matrix*

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Administrator</th>
<th>Directory Manager</th>
<th>Project Manager</th>
<th>Provisioning Manager</th>
<th>Create Integration s</th>
<th>Run Integrations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create users</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modify user details</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete users</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disable and enable user accounts</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create groups</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modify group details</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete groups</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disable and enable group accounts</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create projects</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modify project details</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete projects</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provision users</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>De-provision users</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Provision groups</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>De-provision groups</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Generate provision reports</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Tasks</td>
<td>Administrator</td>
<td>Directory Manager</td>
<td>Project Manager</td>
<td>Provisioning Manager</td>
<td>Create Integration s</td>
<td>Run Integration s</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------</td>
<td>-------------------</td>
<td>-----------------</td>
<td>----------------------</td>
<td>----------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Assign access to data integrations</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Create data integrations</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Edit data integrations</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Copy data integrations</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Delete data integrations</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Create data integration groups</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View data integrations</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Run, or schedule to run, data integrations</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Run, or schedule to run, data integration groups</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
Analytic Services User Provisioning

This appendix provides information that is specific to Hyperion System 9 BI+ Analytic Services™ and Hyperion Shared Services User Management.

You can use Shared Services to provide security for Analytic Services applications, databases, and objects. To use Shared Services security, you must migrate Analytic Server and any existing Analytic Services users and groups to Shared Services.

For detailed information on Analytic Services security, see the Analytic Services Database Administrator’s Guide and the Administration Services Online Help.

In This Appendix

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Launching the User Management Console from Analytic Services</td>
<td>56</td>
</tr>
<tr>
<td>Analytic Services User Roles</td>
<td>56</td>
</tr>
<tr>
<td>Analytic Services Projects, Applications, and Databases in Shared Services</td>
<td>59</td>
</tr>
<tr>
<td>Analytic Services Users and Groups in Shared Services</td>
<td>60</td>
</tr>
<tr>
<td>Assigning Database Calculation and Filter Access</td>
<td>60</td>
</tr>
<tr>
<td>Setting Application Access Type</td>
<td>62</td>
</tr>
<tr>
<td>Synchronizing Security Information Between Shared Services and Analytic Services</td>
<td>63</td>
</tr>
<tr>
<td>Migrating Analytic Services Users to Shared Services Security</td>
<td>63</td>
</tr>
</tbody>
</table>
Launching the User Management Console from Analytic Services

To manage Analytic Services users in User Management Console, you must log in to User Management Console as a user who is provisioned with the following Shared Services roles:

- Provisioning Manager role for the appropriate Analytic Server or applications.
- Directory Manager role for the appropriate authentication directory.

When you launch User Management Console from Administration Services, you automatically log in to User Management Console as the Analytic Services user that connects the Analytic Server you are accessing.

**Note:** In Shared Services security mode, you must use the same user to log in to Administration Services Console as you use to connect the Analytic Server.

When you launch User Management Console from a browser, you log in as whatever user is appropriate. For example, you must log in as a Shared Services Administrator in order to provision an Analytic Services Administrator with the Directory Manager role, so that he or she can create and delete users.

➢ To launch User Management Console:

1. From Enterprise View, find the appropriate Analytic Server.
2. Under the server node, select the **Security** node.
3. Right-click and select **User Management** from the pop-up menu.
   The User Management Console launch page is opened in a separate browser window.
4. Click **Launch** to open User Management Console.
5. Use the **Help** menu in User Management Console to get assistance with managing and provisioning users and groups.

For information on launching User Management Console from MaxL, see the *Analytic Services Technical Reference*.

**Note:** To ensure that Analytic Services security status and Shared Services security status are synchronized, you may need to refresh security information. For information on refreshing security information, see the *Analytic Services Database Administrator’s Guide*.

**Analytic Services User Roles**

Roles determine the tasks that users can perform. Roles can be grouped as follows:
● Product-specific roles. Examples of Analytic Services roles are Administrator and Database Manager. All Analytic Services roles are specific to a Shared Services application; that is, the permissions granted to the user by the role apply only to the specific application for which the role is assigned, and not to all applications.

● Shared Services roles. Examples of Shared Services roles are Project Manager or Provisioning Manager. Most Shared Services roles are global; that is the role applies to all Shared Services applications. An exception is the Provisioning Manager role, which is specific to an application.

The following Analytic Services roles provide different levels of authority to perform tasks in Analytic Services.

You can provision a user with the following roles for an Analytic Server:

● Administrator
● Create/Delete Application
● Server Access

You can provision a user with the following roles for an application:

● Application Manager
● Database Manager
● Calc
● Write
● Read
● Filter
● Start/Stop Application

In User Management Console, roles that apply to an Analytic Server may have a Product Name prefix of “ESB”; roles that apply to an application may have a Product Name prefix of “ESBAPP.”

**Note:** There is no concept of provisioning an Administration Services Administrator user role through Shared Services. When migrated, an Administration Services Administrator is assigned no roles in Shared Services.

**Analytic Services User Role and Task Matrix For Shared Services**

The following table lists the user roles that are specific to Analytic Services and the Shared Services role of Provisioning Manager, which is application-specific. The table shows the corresponding tasks that each user can perform.
<table>
<thead>
<tr>
<th>User Role</th>
<th>Task Description</th>
</tr>
</thead>
</table>
| Provisioning Manager                            | Provisioning Manager is a Shared Services application-specific role. Users who are assigned the Provisioning Manager role can provision users and groups with roles for applications.  
  **Note:** The Provisioning Manager role is automatically assigned when you migrate Analytic Services Administrators (previously known as Supervisors) and Application Managers. However, when you create an Analytic Services Administrator or Application Manager in User Management Console, you must manually assign the Provisioning Manager role. |
| Administrator (previously Supervisor)           | Full access to administer the server, applications and databases.                                                                                                                                                                                                                |
| Create/Delete Application                       | Ability to create and delete applications and databases within the applications. Includes Application Manager and Database Manager permissions for the applications and databases created by this user.                                                                                   |
| Server Access                                   | Ability to access any application or database that has a minimum access permission other than none.  
  **Note:** When you assign security at the Analytic Services application level, you must also assign the user the Server Access role for the Analytic Server that contains the application (unless the user already has another Analytic Server level role, for example Create/Delete Application). |
| Application Manager (previously Application Designer) | Ability to create, delete and modify databases and application settings within the particular application. Includes Database Manager permissions for databases within the application.  
  **Note:** The Provisioning Manager role is automatically assigned when you migrate Analytic Services Application Managers. However, when you create an Analytic Services Application Manager in User Management Console, you must manually assign the Provisioning Manager role. |
| Database Manager (previously Database Designer)  | Ability to manage the database(s) (for example, to change the database properties or cache settings), database objects, locks and sessions within the assigned application.                                                                                                                                 |
| Calc                                            | Ability to calculate, update, and read data values based on the assigned scope, using any assigned calculations and filter.                                                                                                                                                      |
| Write                                           | Ability to update and read data values based on the assigned scope, using any assigned filter.                                                                                                                                                                                     |
| Read                                            | Ability to read data values.                                                                                                                                                                                                                                                    |
Shared Services and Analytic Services both use the term “application.” Analytic Services uses “application” to refer to a container for databases. Shared Services uses “application” to refer to an object for which you provision users. In this document, “application” refers to a Shared Services application, unless an Analytic Services application is specifically stated. In most cases, an Analytic Services application maps to a Shared Services application and so there is no need to distinguish between the two types of application.

For Analytic Services, migration is done at the Analytic Server level. When you migrate an Analytic Server to Shared Services, a Shared Services project is created for the Analytic Server. The project is named as follows: `Analytic Servers: machineName: AnalyticServer#` where `machineName` is the Analytic Server machine name and `AnalyticServer#` is the sequence number. If you migrate multiple Analytic Servers on the same machine, each Analytic Server migrated gets a different sequence number (`AnalyticServer#`). Also, if you delete the security file and re-migrate an Analytic Server, each successful migration creates a new server project with a new sequence number. You can delete any unwanted projects in User Management Console.

Analytic Services automatically creates the following applications within the project and automatically registers the applications with Shared Services:

- An application with the same name as the Shared Services project. This application allows you to specify security at the Analytic Server level, and is known as the global Analytic Server application.
- A Shared Services application for each Analytic Services application on the Analytic Server. In Shared Services, if an Analytic Services application contains multiple databases, the databases must have the same user security access levels. (However, users can have different calculation script and database filters assigned for databases within the same application. See “Assigning Database Calculation and Filter Access” on page 60).

Once you have migrated to Shared Services, when you create a new application and database in Analytic Services, a corresponding Shared Services application is created within the Analytic Server project and the application is automatically registered with Shared Services.
Analytic Services Users and Groups in Shared Services

When you migrate to Shared Services, all native Analytic Services users and groups that do not already exist in an external authentication directory are converted to native Shared Services users and groups in the native Shared Services user directory and are given equivalent roles. Any externally-authenticated users are registered with Shared Services but are still stored in their original authentication directory. For more information on migrating users and groups, see the Analytic Services Database Administrator’s Guide.

**Note:** Shared Services supports aggregated groups, in which a parent group contains one or more sub-groups. The sub-groups inherit the roles of their parent group. For example, if a parent group is provisioned with the Analytic Services Administrator role, any sub-groups (and users in the groups) inherit the Analytic Services Administrator role.

Once you have migrated to Shared Services, you must create and manage users and groups in User Management Console, or through the external authentication provider. For more information, see the Shared Services User Management Guide.

**Note:** If manual user synchronization is specified, when you provision a user with an Analytic Server role, you must request a refresh of security information to enable the user to log in. For information on manual user synchronization, see the Analytic Services Database Administrator’s Guide.

Assigning Database Calculation and Filter Access

After provisioning users for Analytic Services applications in User Management Console, you can assign more granular access permissions to users and groups for a specific Analytic Services application and database. For example, after assigning a user access to an application and assigning the user’s role for the application, you may want to assign an Analytic Services filter to the user, or assign the user access to a specific calculation script.

When you select an Analytic Services application from User Management Console, a screen is displayed that lists all users and groups who are provisioned to that application. On this screen, you select the users and groups to which you want to assign additional permissions. After clicking Next to go to the next screen, you select the database you want to work with, and then use the appropriate drop-down lists to assign filter and calculation script access to selected users and groups. For descriptive information about these two screens, click the Help button on one of these screens to display a context-sensitive help topic.

When you assign database calculation and filter access, you automatically log in to Administration Services and Analytic Services as User Management Console logged in user. This user must be a valid Analytic Services Administrator, Application Manager, or Database Manager. The user must have the Provisioning Manager role for the appropriate application(s).

You cannot assign database calculation or filter access to an Analytic Services Administrator or Application Manager.
To assign database calculation and filter access:

1. Launch User Management Console.
   
   See “Launching the User Management Console from Analytic Services” on page 56.

2. Expand the Projects node, and select the appropriate Analytic Services application.

3. Right-click and select Assign Access Control.

4. Select the appropriate item from the Available Users and Groups drop-down list to display only users, only groups, or both.

5. Select the users and/or groups that you want to work with for the application. To select multiple users/groups, press the Ctrl key between selections.

6. Click the appropriate arrow button to move your selections to the Selected Users and Groups box. To move all users and groups, click the double arrow button.

7. Click Next to go to the next screen.
   
   This screen lists the users who have access to the application and displays their user roles.

8. From the Database drop-down list, select the database you want to work with.

9. To assign an Analytic Services filter to users and groups:
   
   a. Select the check box next to each user and group you want to assign a filter to.
   
   b. From the Filter drop-down, select the appropriate filter.
      
      The filter list is populated with the filters that exist for the selected database on Analytic Server.

10. To assign users and groups access to an Analytic Services calculation script:
   
    a. Select the check box next to each user and group you want to assign calculation script access to.

    b. From the Calc drop-down, select the appropriate calculation script.
      
      The calculation list is populated with the calculation scripts that exist for the selected database on Analytic Server.

11. If you want to want to assign only calculation access, select No update from the Filter drop-down list.

12. If you want to want to assign only filter access, select No update from the Calc drop-down list.

Note: If you have not yet clicked Save, you can click Reset to revert to the original settings (or to revert to the settings changed since the last save).

13. Click the apply check mark icon next to the Calc drop-down list to apply your selections.

14. Click Save to save the changes.
   
   Status messages are displayed on a new screen. The changes are reflected immediately in Administration Services Console.
To refresh Analytic Services with database calculation and filter access security information for newly provisioned users, click the Refresh button.

Although you can assign access to database filters and calculation scripts through User Management Console, you must create the filters and calculation scripts in Analytic Services. For information on creating database filters, see the Analytic Services Database Administrator’s Guide.

Setting Application Access Type

Analytic Services and Hyperion Planning have the concept of an “application access type” for Analytic Services and Hyperion Planning users. For example, when an Analytic Services user is created using any Analytic Services administration tool, the user is automatically assigned the application access type “Analytic Services”; when a Hyperion Planning user is created using the Planning interface, the user is automatically assigned the application access type “Planning.” A user’s application access type specifies whether the user has access to Analytic Services applications only, to Planning applications only, or to both.

When you select a global Analytic Server application from User Management Console, a screen is displayed that lists all users and groups who are provisioned to that application. On this screen, you select the users and groups for which you want to assign application access type. After clicking Next to go to the next screen, you use the drop-down list to assign application access type to the selected users and groups. For descriptive information about these two screens, click the Help button on one of these screens to display a context-sensitive help topic.

When you assign database calculation and filter access, you automatically log in to Administration Services and Analytic Services as User Management Console logged in user. This user must be a valid Analytic Services Administrator and must have the Provisioning Manager role for the appropriate application(s).

To set application access type for users:

1. Launch User Management Console.
   See “Launching the User Management Console from Analytic Services” on page 56.
2. Expand the Projects node, and select the global Analytic Services application.

Note: An application with the same name as the Shared Services project is created within the project. This global application allows you to specify security at the Analytic Server level.

3. Right-click and select Assign Access Control.
4. The Available Users box lists the users that are provisioned to the global application.
5. Select the users that you want to work with. To select multiple users, press the Ctrl key between selections.
6. Click the appropriate arrow button to move your selections to the Selected Users box. To move all users, click the double arrow button.
Click Next to go to the next screen.

This screen lists the selected users.

Select the check box next to the users whose application access type you want to change.

From the User type drop-down list, select Analytic Services or Planning, as appropriate.

Note: If you have not yet clicked Save, you can click Reset to revert to the original settings (or to revert to the settings changed since the last save).

Click the apply check mark next to the User type drop-down list to apply your selections.

Click Save to save the changes.

Status messages are displayed on a new screen. The changes are reflected immediately in Administration Services Console.

To refresh Analytic Services with application access type information for newly provisioned users, click the Refresh button.

**Synchronizing Security Information Between Shared Services and Analytic Services**

To ensure that Analytic Services security status is synchronized with Shared Services security status, you may need to refresh security information from Shared Services. When the security status is out of synch, the user, group, and application information displayed in Analytic Services may be different from that in Shared Services. For more information on refreshing security information from Shared Services, see the Analytic Services Database Administrator’s Guide and the Administration Services Online Help.

**Migrating Analytic Services Users to Shared Services Security**

Before you can use Shared Services to manage security, you must migrate Analytic Server and any existing Analytic Services users and groups to Shared Services. For detailed information on migrating users and groups to Shared Services, see the Analytic Services Database Administrator’s Guide and the Administration Services Online Help.

**Backing Up Security Information**

For information on backing up security information when Analytic Services is in Shared Services security mode, see the Analytic Services Database Administrator’s Guide.
This appendix provides information specific to using Hyperion System 9 BI+™ Analytic High Availability Services™ with Shared Services User Management Console. The Shared Services User Management Console provides a centralized user interface to perform user management tasks for Hyperion products.

Use Shared Services to provide security for Analytic High Availability Servers, which are administered through Analytic Administration Services. To use Shared Services security, you must migrate Analytic High Availability Servers and any Analytic High Availability Services users and groups to Shared Services.

In This Appendix

- Launching User Management Console from High Availability Services ................................................. 66
- Analytic High Availability Services User Roles .................................................................................. 66
- Provisioning the Administrator Role in Shared Services .................................................................. 67
- Migrating Analytic High Availability Services Users to Shared Services Security ........................... 68
Launching User Management Console from High Availability Services

You administer High Availability Services using Analytic Administration Services Console. You can launch the User Management Console from Administration Services Console to provision users for High Availability Services.

**Note:** You must have registered High Availability Services with Shared Services.

➤ To launch User Management Console:

1. From Enterprise View, select the **High Availability Servers** node.
2. Select a High Availability Server.
3. Right-click and select **Manage users and groups**.

The User Management Console is opened in a browser window. Use the Help menu in the User Management Console to get assistance with managing and provisioning users and groups.

**Analytic High Availability Services User Roles**

Analytic High Availability Services supports one type of user, Administrator, which is categorized under the Power User license type.

If you have licensed the Analytic High Availability Services option of Analytic Services, you can create High Availability Services Administrator users at the Power User license type level.

**Table 3  Analytic High Availability Services User Types and Tasks Matrix**

<table>
<thead>
<tr>
<th>User Type</th>
<th>License Type</th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>Power User</td>
<td>Create, modify, and delete clusters of Analytic Servers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Create, modify, and delete connection pools</td>
</tr>
</tbody>
</table>

Analytic High Availability Services must validate that users being added to a connection pool have been provisioned to Analytic Servers that are in the data source of the connection pool.

If a user is not provisioned for Analytic Server, the administrator is notified. The connection pool can be saved, but not activated on High Availability Server until all users are provisioned.
Provisioning the Administrator Role in Shared Services

In Shared Services mode, the only role that you must assign for High Availability Services is Administrator. Only the Administrator can create Analytic Services clusters and connection pools in High Availability Services. No other roles can be assigned. Non-administrator users can only connect to the clusters and connection pools.

➤ To provision the Administrator role:

1 Log into Shared Services User Management Console at:

2 In Logon, enter the administrator username and password.
   By default, admin and password are the username and password.

3 Click Log on.

4 In the navigation pane, expand Projects and AHAS 9.0.0 Servers.
   Your High Availability Server is listed.

5 To create a new user to provision, follow the proceeding steps:
   a. In the navigation pane, expand User Directories and a directory, such as Native Directory.
   b. Select Users and right-click, then select New > User.
   c. Enter the user information and click Finish.

6 To select an existing user to provision, follow the proceeding steps:
   a. In the navigation pane, expand User Directories and a directory, such as Native Directory.
   b. Select Users.

7 At the bottom of the navigation pane, enter the user ID to and click Search or Show All.

8 From the list, select an existing or new user ID that you want to provision as Administrator, and select Administration > Provision.

9 In the Provision Users or Groups pane, expand AHAS 9.0.0 Servers and expand the name of your High Availability Server.

10 Select Administrator.

11 Click Save.

The user is provisioned as a High Availability Server administrator. Log into Administration Services Console with the administrator user name and password to create and manage Analytic Services clusters and connection pools.
Migrating Analytic High Availability Services Users to Shared Services Security

Using Administration Services Console, migrate existing High Availability Services users to Shared Services. In Shared Services mode, you must create users using the Shared Services User Management Console.

**Note:** Once you migrate your users to Shared Services, the process is irreversible.

➤ To migrate existing users to Shared Services:

1. Log into Administration Services Console using the Shared Services user ID with Administrator privileges for High Availability Services.

**Note:** To migrate users, the user ID must have both Administrator privileges for the High Availability Services and Directory Manager privileges in Shared Services.

2. Under **Enterprise View**, select the **High Availability Servers** node and select a High Availability Server that you have previously added.

**Note:** The default user name “system” and password “password” are not valid in Shared Services mode.

3. Connect to the High Availability Server, then right-click and select **Externalize users and groups**.

A wizard for migrating native users and groups is displayed.

4. In **Select Objects to Externalize**, select one or more of the following objects to externalize:
   - **Users:** Select this check box to migrate users who have not been migrated to Shared Services.
   - **Groups:** Select this check box to migrate groups who have not been migrated to Shared Services. This option is available only for Analytic Servers.

5. Click **Next**.

The **Specify Shared Services Properties** panel displays information about the Shared Services server to which you are migrating the selected objects. This information is retrieved from the Shared Services external authentication configuration file. The fields on this panel are not editable.

6. Click **Next**.
In **Specify Password Information**, specify how passwords for the migrated Shared Services users are to be created. You have the following options:

- **Auto-generate**: Select this option to automatically generate new passwords for the users being migrated to Shared Services. The passwords are generated randomly and are recorded in the text file specified in the text box. You must specify the extension for the file as `.txt`. You can also browse to the location of an existing password file if you want to append new passwords to an existing file.

- **Use native user name as password**: Select this option to assign the native user name as the new password for each user being migrated to Shared Services. During migration, the user name is converted to an all lowercase password; therefore, the password is lowercase in Shared Services. For example, a native user named "Mark" will have "mark" as the password after migration.

- **Password and Confirm password**: Select this option to specify and confirm a new password for the users when they are created in Shared Services. You must specify the same password for all users being migrated.

In **Specify Password Information** under **Logging Details**, specify or browse to the location where you want the migration process to be logged in a text file.

You must specify the extension for the file as `.log`. If you select an existing file, the new log details are appended to the existing file. All information and error messages are written to the specified file. The name of the log file cannot be the same as the name of the password file used in the Auto-generate option.

Click Next.

In **Map Users to External Providers**, select the users to migrate to Shared Services.

The wizard searches authentication providers that were specified when you configured Shared Services for external authentication. This panel displays the results of the search.

Click Next.

In **Externalize Users/Groups**, select one or more objects to migrate:

- **Users**: Select this check box to migrate natively authenticated users.
- **Groups**: Select this check box to migrate groups associated with natively authenticated users (available only for Analytic Server).

Click Start to start the migration process.

Review the status messages and click Finish.

The users have been migrated to Shared Services.

Open a Web browser and log into your Shared Services server. For example, `http://localhost:58080/interop/` using “admin” as the user name and “password” as the password.

Expand **User Directories** and **Native Directory** and select **Users**.

Click Show All.

Verify that the users that you migrated are listed.
This appendix describes Hyperion System 9 BI+™ roles and their use in conjunction with the Shared Services user management system.

<table>
<thead>
<tr>
<th>In This Appendix</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Launching User Management Console from Hyperion System 9.</td>
<td>72</td>
</tr>
<tr>
<td>Hyperion System 9 BI+ Roles.</td>
<td>73</td>
</tr>
<tr>
<td>Universal Access to Resources and Functionality</td>
<td>78</td>
</tr>
<tr>
<td>Tasks and Roles.</td>
<td>82</td>
</tr>
<tr>
<td>Role Combinations</td>
<td>85</td>
</tr>
<tr>
<td>Custom Roles</td>
<td>87</td>
</tr>
<tr>
<td>The World Group and Default Roles</td>
<td>89</td>
</tr>
<tr>
<td>Mapping Old Roles to New Roles</td>
<td>90</td>
</tr>
</tbody>
</table>
**Launching User Management Console from Hyperion System 9**

You have three options for launching User Management Console:

- On the View Pane **Navigate** panel, expand the **Administer** module list and select **User Management**.
- On the menu bar, select **Tools > Administer > User Management**.
- With a Web browser, directly access User Management Console at the following URL:
  
  \[http://Shared_Services_Servername:Port_Number/interop/\]

Each of these methods will display User Management Console in a separate window.

**User Management Console**

User Management Console is a centralized user interface for managing users, user groups, and roles for your Hyperion products. This spares administrators from configuring the same users multiple times for each Hyperion application. User Management Console enables you to complete the following tasks:

- Create native user IDs and groups
- Authenticate external user IDs
- Assign application specific roles to users and groups
- Manage key user preferences for large groups of users

Before you can use User Management Console, you must install and configure Shared Services and external authentication. For more information, see the *Shared Services Installation Guide*.

After users and groups have been authenticated, you must assign Shared Services roles to the users who will administer and provision others.

Shared Services roles:

- **Administrator** - grants administrative access to Shared Services.
- **Directory Manager** - grants ability to create and manage users and groups.
- **Project Manager** - grants ability to create applications and assign Hyperion products.
- **Provisioning Manager** - grants ability to provisions users and groups to applications.
- **Create Integrations** - grants ability to create data integrations
- **Run Integrations** - grants ability to schedule data integrations

You must differentiate these Shared Services roles from internal System 9 BI+ roles described in the next topic.
### Hyperion System 9 BI+ Roles

Each user profile can be assigned multiple roles that control access and behavior in Hyperion System 9 BI+. Specific permissions are associated with each of 28 predefined roles.

<table>
<thead>
<tr>
<th>Roles Group</th>
<th>Role Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic user roles</td>
<td>Viewer</td>
</tr>
<tr>
<td></td>
<td>Explorer</td>
</tr>
<tr>
<td></td>
<td>Personal Page Editor</td>
</tr>
<tr>
<td></td>
<td>Personal Parameter Editor</td>
</tr>
<tr>
<td></td>
<td>Data Editor</td>
</tr>
<tr>
<td></td>
<td>Favorites Distributor</td>
</tr>
<tr>
<td></td>
<td>Metrics Viewer</td>
</tr>
<tr>
<td>Additional functionality</td>
<td>Job Runner</td>
</tr>
<tr>
<td></td>
<td>Scheduler</td>
</tr>
<tr>
<td></td>
<td>Interactive Reporting Viewer</td>
</tr>
<tr>
<td></td>
<td>Dynamic Viewer</td>
</tr>
<tr>
<td></td>
<td>Analyst</td>
</tr>
<tr>
<td></td>
<td>Metrics Analyst</td>
</tr>
<tr>
<td>Distribution</td>
<td>Smart Form Publisher</td>
</tr>
<tr>
<td></td>
<td>Personal Page Publisher</td>
</tr>
<tr>
<td></td>
<td>Manage Models</td>
</tr>
<tr>
<td></td>
<td>Data Source Publisher</td>
</tr>
<tr>
<td></td>
<td>Job Publisher</td>
</tr>
<tr>
<td>Content creation</td>
<td>Content Publisher</td>
</tr>
<tr>
<td></td>
<td>Job Manager</td>
</tr>
<tr>
<td></td>
<td>Report Designer</td>
</tr>
<tr>
<td></td>
<td>Metrics Editor</td>
</tr>
<tr>
<td>Content management</td>
<td>Content Manager</td>
</tr>
<tr>
<td></td>
<td>Schedule Manager</td>
</tr>
<tr>
<td></td>
<td>BI+ Administrator</td>
</tr>
<tr>
<td>Universal access to resources and</td>
<td>BI+ Global Administrator</td>
</tr>
<tr>
<td>functionality</td>
<td></td>
</tr>
<tr>
<td>Internal</td>
<td>Trusted Application</td>
</tr>
</tbody>
</table>

---
**Basic Roles**

The **Viewer** role:
- Reviews content in the Workspace View module. Content is static, and accessible only from your Favorites folder
- Reviews accessible interactive Web Analysis content
- Accesses the Web Analysis Studio
- Accesses and set accessible preferences

The Viewer role provides minimal end user functionality.

**Note:** The Viewer role is assigned when no other role assignment can be made.

The **Explorer** role:
- Accesses the Explore module to list repository content
- Accesses the Web Analysis Studio View Pane Explorer interface
- Subscribes to content and is notified when content changes
- Searches for repository content
- Accesses the Open dialog box, used to list repository content in context

**Note:** Access to the repository does not grant access to individual files and folders. Files and folders are secured by file properties and permissions.

The **Personal Page Editor** role:
- Accesses the Personal Page interface
- Creates, modifies, lays out and customizes Personal Pages
- Copies content from the published Personal Pages of other users

The **Personal Parameter Editor** role enables you to define Web Analysis Point of View (POV) and Personal Variable definitions on database connections to customize the query result set.

The **Data Editor** role enables you to send changed Web Analysis data values back to Analytic Services.

The **Favorites Distributor** role enables you to access the Favorites Manager interface used to distribute content to users’ Favorites folders.

The **Metrics Viewer** role enables you to access Enterprise Metrics content in the Hyperion System 9 BI+ Workspace.
Additional Functionality

The **Job Runner** role:
- Defines personal parameters, to customize data
- Reviews public job parameters
- Runs jobs using customized data
- Accesses configured printers and output devices
- Saves job output to repository

The **Scheduler** role:
- Accesses the Schedule module
- Schedules defined jobs and batches
- Lists and subscribes to repository content
- Reviews public job parameters
- Runs jobs using customized data
- Accesses configured printers and output devices
- Saves job and batch output to repository
- Sets access permissions for the output that you create

**Note:** Schedulers can list and subscribe to repository content because they contain the Explorer role. Schedulers can run jobs and define job parameters because they contain the Job Runner role.

The **Interactive Reporting Viewer** role enables you to review and print static Interactive Reporting content.

The **Dynamic Viewer** role enables you to review, re-query, and print static Interactive Reporting content.

The **Analyst** role:
- Reviews interactive Web Analysis, Financial Reporting, Enterprise Metrics and Interactive Reporting content
- Uses full analytic and reporting functionality
- Edits queries, re-query, and arrange data

The **Metrics Analyst** role enables you to access the Enterprise Metrics Personalize interface.
**Distributing Content**

The **Smart Form Publisher** role enables you to load custom forms for programs. These forms prompt job runners to enter information used to define the job.

**Note:** Job Publisher contains the Smart Form Publisher. In this release, you must have the Job Publisher role to leverage Smart Form Publisher functionality.

The **Personal Page Publisher** role enables you to import personal pages to the repository, where they can be reviewed by other repository users.

**Note:** The Personal Page Publisher contains the Personal Page Editor role.

The **Manage Models** role enables you to import and export Shared Services metadata models. Shared Services provides a database, organized into applications, in which products can store, manage and share application specific data, such as files or strings. There are two kinds of metadata models: dimensional hierarchies and non dimensional objects, such as security files, member lists, rules, scripts and Web forms. The Manage Models role enables you to do the following tasks on Shared Services models:

- Version Tracking
- Access Control
- Synchronize application and Shared Services models
- Edit model content, and the member properties of dimensional models
- Rename and Delete models

**Note:** The Manage Models role user must have Manage permissions for the model. This is set using the Shared Services Model Access window.

The **Job Publisher** role:

- Distributes batches, books, reports and documents to other repository users
- Modifies interactive Web Analysis, and Financial Reporting content (and static Interactive Reporting content)
- Imports and modifies Production Reporting files and Production Reporting output
- Creates, saves, and runs jobs

**Note:** The Job Publisher role is the Content Publisher role with the additional ability to import and modify Production Reporting files and Production Reporting output. It contains the Job Runner and Smart Form Publisher roles.

The **Data Source Publisher** role enables you to distribute data source connectivity files to other users.
Note: The Content Manager role contains the Data Source Publisher role by default.

**Content Creation**

The **Content Publisher** role:

- Distributes batches, books, reports and documents to other repository users
- Modifies interactive Web Analysis and Financial Reporting content (and static Interactive Reporting content)
- Creates Financial Reporting batches and books
- Accesses the Save As dialog box, used to save repository content under a new name or to a new location
- Imports and exports Shared Services metadata models

Note: The Content Publisher contains the Explorer role and the Manage Models role.

The **Job Manager** role:

- Distributes batches, books, reports and documents to other repository users
- Modifies interactive Web Analysis and Financial Reporting content (and static Interactive Reporting content)
- Imports and modifies Production Reporting files and Production Reporting output
- Creates, saves, and runs jobs
- Manages output directories and output printer locations
- Sets public job parameters to customize output

Note: Job Managers are Job Publishers with administrative responsibilities.

The **Report Designer** role:

- Creates and distributes new interactive Web Analysis, Financial Reporting, and Interactive Reporting content
- Creates and distributes custom Web Analysis documents in the Web Analysis Studio Design Documents interface
- Accesses new document creation wizards
- Accesses the Financial Reporting Studio
- Imports and exports Web Analysis and Financial Reporting content

Note: The Report Designer role contains the Content Publisher role.
The Metrics Editor role:

- Creates and distributes Enterprise Metric, and the content used to create Enterprise Metrics (Metrics library)
- Sets data level security for Enterprise Metrics users
- Accesses Enterprise Metrics utilities and technical utilities
- Accesses the Enterprise Metrics Configuration Server
- Accesses the Enterprise Metrics console

**Content Management**

The Schedule Manager role enables you to create and manage events, calendars, time events, public parameters, and physical resources. Schedule Managers can create batches, books, reports, and documents, because they contain both the Scheduler and Content Publisher roles.

*Note:* The Schedule Manager role contains the Job Manager and all of its descendant roles and the Scheduler and all of its descendant roles.

The Content Manager role:

- Manages all published content in the repository
- Executes all tasks enabled by the Analyst, Scheduler, Favorites Distributor, Job Manager, Data Source Publisher, Personal Page Publisher, Metrics Editor, and Report Designer roles

The BI+ Administrator role provides conditional access to all resources (unless the file is locked by “no access.”), but not all functionality. Additional Data Editor, Dynamic Viewer, Interactive Reporting Viewer, and Personal Parameter Editor roles must be assigned for complete functional access. It enables the following tasks:

- Conditionally accesses all resources
- Accesses the Administrate module
- Accesses the Impact Management modules

The Provisioning Manager role is a Shared Services role that enables you to provisions users and groups to applications. It is also required for setting default user preferences for the Hyperion System 9 BI+ application. For more information, see “Assigning Default Hyperion System 9 BI+ Preferences” on page 88.

**Universal Access to Resources and Functionality**

The BI+ Global Administrator role:

- Universally and implicitly accesses all resources and functionality
- Accesses the Administrate module
- Accesses the Impact Management modules
BI+ Global Administrators can never be denied access.

**Internal System Role**

The **Trusted Application** role enables credentialed client-server communication of Open Catalog Extension (OCE) files (that typically encapsulate connectivity, database type, network address, and database username information).

**Aggregated Roles**

Roles are organized into hierarchies, based on the other roles they contain. **Hyperion System 9 BI+ Roles** aggregate into the following **Content Manager Branch** and **Scheduler Manager Branch**: 
Content Manager Branch

Viewer
Personal Parameter Editor
Dynamic Viewer
Interactive Reporting Viewer
Data Editor
BI+ Global Administrator
BI+ Administrator
  Scheduler Manager
  Content Manager
    Report Designer
    Personal Page Publisher
      Personal Page Editor
    Metrics Editor
      Metrics Analyst
        Metrics Viewer
    Data Source Publisher
    Analyst
    Favorites Distributor
    Job Manager
      Job Publisher
        Smart Form Publisher
        Content Publisher
          Explore
            Manage Models
          Job Runner
    Scheduler
      Explore
      Job Runner
Scheduler Manager Branch

The Scheduler Manager role contains all the roles in the Job Manager and Scheduler roles:

- Report Designer
- Dynamic Viewer
- Interactive Reporting Viewer
- Data Editor
- BI+ Global Administrator
- BI+ Administrator
  - Content Manager
- **Scheduler Manager**
  - Job Manager
    - Job Publisher
      - Smart Form Publisher
      - Content Publisher
        - Explore
        - Manage Models
      - Job Runner
  - Scheduler
    - Explore
    - Job Runner
## Tasks and Roles

The following table lists documents, common tasks executed on them, the client interface used, and the corresponding role name.

### Table 5: Task to Role Matrix

<table>
<thead>
<tr>
<th>Content</th>
<th>Task</th>
<th>Client Interface</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal Pages</td>
<td>Access personal pages application to create, modify, layout, copy and customize personal pages</td>
<td>Workspace + Personal Pages interface</td>
<td>Personal Page Editor</td>
</tr>
<tr>
<td></td>
<td>Import personal pages so that other users can review them</td>
<td>Workspace + Personal Pages interface</td>
<td>Personal Page Publisher</td>
</tr>
<tr>
<td></td>
<td>Manages all content, including Personal Pages</td>
<td>Workspace + Personal Pages interface</td>
<td>Content Manager</td>
</tr>
<tr>
<td>Parameters</td>
<td>Create Personal Parameters, Point of View (POV) and Personal Variable definitions</td>
<td>Workspace + User Preferences</td>
<td>Personal Parameter Editor</td>
</tr>
<tr>
<td></td>
<td>Review public job parameters</td>
<td>Workspace + Explore module</td>
<td>Job Runner</td>
</tr>
<tr>
<td></td>
<td>Schedule jobs and batches, save output to the repository and set access permissions</td>
<td>Workspace + Explore module + Schedule module</td>
<td>Scheduler</td>
</tr>
<tr>
<td></td>
<td>Run, modify, and import both jobs and output that use parameters</td>
<td>Workspace + Explore module</td>
<td>Job Publisher</td>
</tr>
<tr>
<td></td>
<td>Create and manage public job parameters</td>
<td>Workspace + Explore module</td>
<td>Job Manager</td>
</tr>
<tr>
<td></td>
<td>Create and manage both public and private job parameters</td>
<td>Workspace + Explore module + Schedule module</td>
<td>Schedule Manager</td>
</tr>
<tr>
<td></td>
<td>Create and manage output that use parameters</td>
<td>Workspace + Explore module + User Preferences</td>
<td>Content Manager</td>
</tr>
<tr>
<td>Jobs and Batches</td>
<td>Run jobs with customized data</td>
<td>Workspace + Explore module</td>
<td>Job Runner</td>
</tr>
<tr>
<td></td>
<td>Schedule jobs and batches, save output to the repository and set access permissions</td>
<td>Workspace + Explore module + Schedule module</td>
<td>Scheduler</td>
</tr>
<tr>
<td></td>
<td>Load programs into custom forms</td>
<td>Smart form Publisher</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Run, modify, and import both jobs and output</td>
<td>Workspace + Explore module</td>
<td>Job Publisher</td>
</tr>
<tr>
<td></td>
<td>Run, modify, and import both jobs and output, as well as create and manage output directories</td>
<td>Workspace + Explore module</td>
<td>Job Manager</td>
</tr>
<tr>
<td></td>
<td>Create and manage output</td>
<td>Workspace + Explore module + User Preferences</td>
<td>Content Manager</td>
</tr>
<tr>
<td>Content</td>
<td>Task</td>
<td>Client Interface</td>
<td>Role</td>
</tr>
<tr>
<td>---------</td>
<td>------</td>
<td>------------------</td>
<td>------</td>
</tr>
<tr>
<td>Task to Role Matrix</td>
<td>Complete Schedule functionality, including the ability to create and manage, events, calendars, time events, and all parameters. Creates batches.</td>
<td>Workspace + Explore module + Schedule module</td>
<td>Schedule Manager</td>
</tr>
<tr>
<td>Interactive Reporting</td>
<td>Review static content</td>
<td>Workspace + View module</td>
<td>Viewer</td>
</tr>
<tr>
<td></td>
<td>List repository content</td>
<td>Workspace + Explore module</td>
<td>Explorer</td>
</tr>
<tr>
<td></td>
<td>Write data values back to Analytic Services</td>
<td>Workspace + Edit Data</td>
<td>Data Editor</td>
</tr>
<tr>
<td></td>
<td>Distribute content to Favorites folders</td>
<td>Workspace + Explore module + Favorites Manager interface</td>
<td>Favorites Distributor</td>
</tr>
<tr>
<td></td>
<td>Review, and print static BQY content</td>
<td>Workspace + View module</td>
<td>Interactive Reporting Viewer</td>
</tr>
<tr>
<td></td>
<td>Review, re-query and print static BQY content</td>
<td>Workspace + View module</td>
<td>Dynamic Viewer</td>
</tr>
<tr>
<td></td>
<td>Modify interactive WA, FR, EM content and static IR, PR content, and save back to the repository</td>
<td>Workspace + View module + Explorer module + Personal Pages + User Preferences + Web Analysis Studio + Save</td>
<td>Content Publisher</td>
</tr>
<tr>
<td></td>
<td>Distribute connectivity files</td>
<td>Workspace + Explore module</td>
<td>Data Source Publisher</td>
</tr>
<tr>
<td></td>
<td>Create and manage all content</td>
<td>Workspace + View module + Web Analysis Studio (New, Custom Document) + Financial Reporting Studio + Interactive Reporting Studio + Enterprise Metrics Studio</td>
<td>Content Manager</td>
</tr>
<tr>
<td></td>
<td>Conditional administrative access and functionality</td>
<td>All clients and all modules</td>
<td>BI+ Administrator</td>
</tr>
<tr>
<td></td>
<td>Unrestricted universal access and functionality</td>
<td>All clients and all modules</td>
<td>BI+ Global Administrator</td>
</tr>
<tr>
<td>Enterprise Metrics</td>
<td>Review Enterprise Metrics content and list repository content</td>
<td>Workspace + View module + Explorer module</td>
<td>Metrics Viewer</td>
</tr>
</tbody>
</table>
Table 5  Task to Role Matrix  (Continued)

<table>
<thead>
<tr>
<th>Content</th>
<th>Task</th>
<th>Client Interface</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personalize Enterprise Metrics</td>
<td></td>
<td>Workspace + View module + Enterprise Metrics Studio (Personalization)</td>
<td>Metrics Analyst</td>
</tr>
<tr>
<td>Create and distribute Enterprise Metrics. Generate the content used to</td>
<td>Create and distribute Enterprise Metrics. Assign Data Security to</td>
<td>Workspace + View module + Enterprise Metrics Studio + Utilities + Technical Utilities + Configuration Server + Console</td>
<td>Metrics Editor</td>
</tr>
<tr>
<td>Enterprise Metrics. Assign Data Security to users</td>
<td>users</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial Reporting</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>List repository content in the workspace</td>
<td></td>
<td>Workspace + Explore module + Open</td>
<td>Explorer</td>
</tr>
<tr>
<td>Review static content</td>
<td></td>
<td>Workspace + View module</td>
<td>Viewer</td>
</tr>
<tr>
<td>Modify interactive WA, FR, EM content and static IR, PR content, and</td>
<td>Modify interactive WA, FR, EM content and static IR, PR content, and</td>
<td>Workspace + View module + Explorer module + Personal Pages + User Preferences + Web Analysis Studio + Save</td>
<td>Content Publisher</td>
</tr>
<tr>
<td>save back to the repository</td>
<td>save back to the repository</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unrestricted universal access and functionality</td>
<td>Unrestricted universal access and functionality</td>
<td>All clients and all modules</td>
<td>BI+ Global Administrator</td>
</tr>
<tr>
<td>Web Analysis</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Review interactive content</td>
<td>Review interactive content</td>
<td>Workspace + View module</td>
<td>Viewer</td>
</tr>
<tr>
<td>List repository content</td>
<td>List repository content</td>
<td>Workspace + Explore module</td>
<td>Explorer</td>
</tr>
<tr>
<td>Write data values back to Analytic Services</td>
<td>Write data values back to Analytic Services</td>
<td>Workspace + Edit Data, Web Analysis Studio Edit Data</td>
<td>Data Editor</td>
</tr>
<tr>
<td>Define Point of View and Personal Variable Definitions</td>
<td>Define Point of View and Personal Variable Definitions</td>
<td>User Preferences Interface for Point of View and Personal Variables. Must be able to access Database Connections.</td>
<td>Personal Parameter Editor</td>
</tr>
<tr>
<td>Distribute content to Favorites folders</td>
<td>Distribute content to Favorites folders</td>
<td>Workspace + Explore module + Favorites Manager interface</td>
<td>Favorites Distributor</td>
</tr>
<tr>
<td>Review full interactive analytical content for Interactive Reporting,</td>
<td>Review full interactive analytical content for Interactive Reporting,</td>
<td>Workspace + View module + Web Analysis Studio (Data Layout) + Financial Reporting Studio + Interactive Reporting Studio</td>
<td>Analyst</td>
</tr>
<tr>
<td>Create, modify and save interactive WA, FR, EM content and static IR,</td>
<td>Create, modify and save interactive WA, FR, EM content and static IR,</td>
<td>Workspace + View module + Explorer module + Personal Pages + User Preferences + Web Analysis Studio + Save</td>
<td>Content Publisher</td>
</tr>
<tr>
<td>PR content, and save back to the repository</td>
<td>save back to the repository</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distribute connectivity files</td>
<td>Distribute connectivity files</td>
<td>Workspace + Explore module</td>
<td>Data Source Publisher</td>
</tr>
</tbody>
</table>
Role Combinations

Provisioning Managers must assign a combination of roles to Hyperion System 9 BI+ users to achieve specific access and functionality. The following table contains examples of common role combinations and their corresponding tasks:

<table>
<thead>
<tr>
<th>Content</th>
<th>Task</th>
<th>Client Interface</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create and manage all content</td>
<td>Workspace + View module + Web Analysis Studio (New, Custom Document) + Financial Reporting Studio + Interactive Reporting Studio + Enterprise Metrics Studio</td>
<td>Content Manager</td>
<td></td>
</tr>
<tr>
<td>Unrestricted universal access and functionality</td>
<td>All clients and all modules</td>
<td>BI+ Global Administrator</td>
<td></td>
</tr>
<tr>
<td><strong>Physical Resources</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Review physical resources.</td>
<td>Workspace + Explore module</td>
<td>Job Runner</td>
<td></td>
</tr>
<tr>
<td>Print static BQY content</td>
<td>Workspace + View module</td>
<td>Interactive Reporting Viewer</td>
<td></td>
</tr>
<tr>
<td>Print updated static BQY content</td>
<td>Workspace + View module</td>
<td>Dynamic Viewer</td>
<td></td>
</tr>
<tr>
<td>Manage output printer locations.</td>
<td>Workspace + Explore module</td>
<td>Job Manager</td>
<td></td>
</tr>
<tr>
<td>Create and manage physical resources</td>
<td>Workspace + Explore module</td>
<td>Schedule Manager</td>
<td></td>
</tr>
</tbody>
</table>

Table 5  Task to Role Matrix  (Continued)
<table>
<thead>
<tr>
<th>Role Combination</th>
<th>Tasks</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Explorer</td>
<td>● Review static content in the Workspace View module</td>
<td>Limits users to reviewing static content, but enables them to access the repository and subscribe to content.</td>
</tr>
<tr>
<td></td>
<td>● List repository content</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Subscribe to content, and be notified when content changes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Search for repository content</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Access the Open dialog box, used to list repository content in context</td>
<td></td>
</tr>
<tr>
<td>Explorer + Favorites</td>
<td>● Review interactive Web Analysis and Financial Reporting content in the Workspace View module</td>
<td>Enables users to share interactive content, without enabling them to modify content or save changes to the repository.</td>
</tr>
<tr>
<td>Distributor + Personal Page</td>
<td>● List and subscribe to repository content</td>
<td></td>
</tr>
<tr>
<td>Editor + Personal Parameter</td>
<td>● Review accessible interactive content in the Web Analysis Studio</td>
<td></td>
</tr>
<tr>
<td>Editor</td>
<td>● Access the Personal Page interface</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Access the Favorites Manager interface</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Define Web Analysis Point of View (POV), Personal Variable definitions, and personal parameter, to customize the query result set</td>
<td></td>
</tr>
<tr>
<td>Metrics Analyst + Analyst</td>
<td>● Review interactive Web Analysis, Financial Reporting, and Interactive Reporting content in the Workspace View module</td>
<td>Enables users to interactively use any document type, to edit queries, re-query and arrange data. Does not enable them to save changes back to the repository.</td>
</tr>
<tr>
<td></td>
<td>● Review accessible interactive content in the Web Analysis Studio</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Edit queries, re-query and arrange data</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Access the Enterprise Metrics Personalize interface</td>
<td></td>
</tr>
<tr>
<td>Explorer + Metrics Analyst</td>
<td>● Review interactive Web Analysis, Financial Reporting, Enterprise Metrics and Interactive Reporting content in the Workspace View module</td>
<td>Enables users to interactively use any document type, to edit queries, re-query, and to save changes back to the repository.</td>
</tr>
<tr>
<td>+ Analyst + Content Publisher</td>
<td>● List and subscribe to repository content</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Review accessible interactive content in the Web Analysis Studio</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Edit queries, re-query and arrange data</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Create Financial Reporting batches and books</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Access the Enterprise Metrics Personalize interface</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Import, modify and Save As dialog box</td>
<td></td>
</tr>
</tbody>
</table>
### Custom Roles

Administrators can also define a custom role by indicating a role name and assigning defined roles to be aggregated into the custom role. You can create as many custom roles as you need.

### Default Functionality

Any provisioned user (a user with at least one role) can log on. By default, provisioned users can access their own Favorites folder and the Preferences interface.

---

**Table 6 Sample Role Combinations (Continued)**

<table>
<thead>
<tr>
<th>Role Combination</th>
<th>Tasks</th>
<th>Notes</th>
</tr>
</thead>
</table>
| **Personal Page Publisher + Metrics Editor + Data Source Publisher + Analyst + Report Designer + Job Manager** | ● Create and distribute new interactive Web Analysis, Financial Reporting, Enterprise Metrics and Interactive Reporting content  
● Create and distribute custom Web Analysis documents in the Web Analysis Studio Design Documents interface  
● Access the Financial Reporting Studio  
● Create and distribute Enterprise Metrics, and the content used to create Enterprise Metrics (Metrics library)  
● Set data level security for Enterprise Metrics users  
● Access the Personal Page interface and distribute content to other repository users  
● Distribute data source connectivity files to other repository users  
● Distribute batches, books, reports and documents to other repository users  
● Import and modify Production Reporting files and Production Reporting output  
● Create, save and run jobs  
● Create and manage output directories | Enables users to access most content creation functionality, without giving them administrator access to resources. |
| **Content Manager + Schedule Manager** | ● Manage all published content in the repository and all content creation functionality  
● Create and manage events, calendars, time events, calendars, public parameters, and physical resources | Enables users to access all content creation and scheduling functionality, without giving them administrator access to resources. |
| **BI+ Administrator + Data Editor** | ● Conditional access to all resources  
● Access the Administrate module  
● Access the Impact Management modules  
● Ability to write edits back to Analytic Services. | Enables users to access most functionality and modules, and conditional access to resources. |
Individual users enjoy the cumulative access granted by their individual role assignments, and the roles assigned to user groups to which they belong (such as the World group). To prevent unwarranted logging on, you must ensure that roles have not been assigned to a user individually and roles have not been assigned to user groups to which the user belongs. In this case it is best to remove the user from user groups.

Assigning Default Hyperion System 9 BI+ Preferences

User Management Console enables users with Provisioning Manager and Explorer roles to set default preferences for specific application users and groups. These defaults are overridden when individual and group preferences take precedence.

Only the following preferences subset can be set through this interface:

- Default Folder—is the folder shown when you initiate the Explore module. Set it to the most frequently accessed folder.
- Desktop—specifies the location of the Desktop folder. The Desktop folder can be used as a scratch pad, or to store items you want to access quickly from the Viewer module. The Desktop interface presents files located in the Desktop folder as icons. The Desktop folder can also be accessed through Explore module.
- New Document—specifies the default location the new document creation wizard searches for supporting files, such as Web Analysis database connections and Interactive Reporting documents.
- Start Page—specifies the Hyperion System 9 BI+ interface that displays at start up. You have 6 options to select from: None, Explore, Document, Desktop, Metrics Builder, and Scorecard.

Note: For default preferences to succeed, users and groups must have the roles and permission to access specified folders and interface elements.

Before you can assign default preferences for an application, the user ID used to access User Management Console and the configuration must be provisioned with the Provisioning Manager and Explorer role.

➤ To assign default preferences for the Hyperion System 9 BI+ application:

1 Log on to User Management Console using a user ID provisioned with Provisioning Manager and Explorer roles.

2 Access the View Pane.

3 Expand the Projects node until a specific instance of the Hyperion System 9 BI+ application is displayed.

4 Right-click the application name and select Assign Preferences from the menu.

In the first step of this three step wizard, you must select the users and groups for whom you will set default preferences. The panel on the left can display either user names or group names for selection.
5 Select either Available Users or Available Groups from the drop down list.
   The left panel will display the corresponding list of users or groups.
6 Select the user names and group names from the left panel, then click the Add button (right arrow).
   You can select a series of names, by holding down the Shift key and selecting the first name in the series, then the last name in the series. You can select multiple names, not necessarily in a series by holding down the CtrI key and selecting names. You can select all of the names using the Add All button.
7 Repeat steps 5 and 6 to select a combination of users and groups.
8 When all user and group names display in the Selected Users and Groups panel, click Next.
   In the second wizard step, you specify the default preferences.
9 To specify the repository location of the Default folder click Select, select a location, then click OK.
10 To specify the repository location of the Desktop folder click Select, select a location, then click OK.
11 To specify the repository location for saving New Documents, click Select, select a location, then click OK.
12 To specify the Start Page, select an interface from the Option list.
13 Optional: If you selected the Explore option or the Document option for the Start Page, you must specify a repository location for the Explore module, or the repository location of a document. Click the corresponding Select button, specify a repository location, then click OK.
14 When all preferences have been specified, click the Next button.
   The Wizard saves the specifications in a preferences file.
15 To proceed from this point, take one of the following options:
   a. To configure options for other applications, select another application in the View Pane at left.
   b. To make changes to the preferences of the currently selected users and groups, click the Back button.
   c. To make specify a new set of users and groups and set their preferences, click the Continue button.

The World Group and Default Roles

All authenticated users are members of the World group, by default. If the World group is provisioned for an application, all users enjoy the specified World group access to the application. Most users are not assigned roles individually, but inherit the roles and privileges assigned to user groups. This enables a wide set of users to be managed collectively and uniformly. Care must be taken however, when provisioning the World group, as this grants the specified access to all authenticated users.
Mapping Old Roles to New Roles

The following table correlates legacy roles to the new Hyperion System 9 BI+ roles. For a complete description of the migration process, see the *Hyperion System 9 Migration Guide*.

<table>
<thead>
<tr>
<th>Old Role Name</th>
<th>New Role Name</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>BI+ Administrator</td>
<td>Also maps to Shared Services Directory Manager and Provisioning Manager.</td>
</tr>
<tr>
<td>Browser</td>
<td>Explorer</td>
<td></td>
</tr>
<tr>
<td>Content Administrator</td>
<td>Content Manager</td>
<td></td>
</tr>
<tr>
<td>Content Publisher</td>
<td>Content Publisher</td>
<td></td>
</tr>
<tr>
<td>Event Services Administrator</td>
<td></td>
<td>Deprecated. Map to Schedule Manager.</td>
</tr>
<tr>
<td>Global Administrator</td>
<td>BI+ Global Administrator</td>
<td>Also maps to Shared Services Directory Manager and Provisioning Manager.</td>
</tr>
<tr>
<td>Group Administrator</td>
<td></td>
<td>Deprecated. Map to Shared Services Directory Manager.</td>
</tr>
<tr>
<td>Group Locator</td>
<td></td>
<td>Deprecated. Map to Explorer.</td>
</tr>
<tr>
<td>iHTML Viewer</td>
<td></td>
<td>Deprecated. Map to Interactive Reporting Viewer.</td>
</tr>
<tr>
<td>Intelligence Analyzer</td>
<td>Analyst</td>
<td></td>
</tr>
<tr>
<td>Intelligence Dynamic Viewer, Quickview</td>
<td></td>
<td>Deprecated. Map to Dynamic Viewer.</td>
</tr>
<tr>
<td>Intelligence Viewer, Freeview</td>
<td></td>
<td>Deprecated. Map to Interactive Reporting Viewer.</td>
</tr>
<tr>
<td>Job Administrator</td>
<td>Job Manager</td>
<td></td>
</tr>
<tr>
<td>Job Publisher</td>
<td>Job Publisher</td>
<td></td>
</tr>
<tr>
<td>Job Runner</td>
<td>Job Runner</td>
<td></td>
</tr>
<tr>
<td>Job Scheduler</td>
<td>Scheduler</td>
<td></td>
</tr>
<tr>
<td>MIME Type Administrator</td>
<td></td>
<td>Deprecated. Map to BI+ Administrator.</td>
</tr>
<tr>
<td>Name Service Administrator</td>
<td></td>
<td>Deprecated. Map to BI+ Administrator.</td>
</tr>
<tr>
<td>OCE Publisher</td>
<td>Data Source Publisher</td>
<td></td>
</tr>
<tr>
<td>Organizational Administrator</td>
<td></td>
<td>Deprecated. Map to Shared Services Directory Manager and Provisioning Manager.</td>
</tr>
<tr>
<td>Personal Page</td>
<td>Personal Page Editor</td>
<td></td>
</tr>
<tr>
<td>Personal Page Publisher</td>
<td>Personal Page Publisher</td>
<td></td>
</tr>
</tbody>
</table>
### Table 7 Old Roles Mapping to New Roles (Continued)

<table>
<thead>
<tr>
<th>Old Role Name</th>
<th>New Role Name</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Resource Administrator</td>
<td></td>
<td>Deprecated. Map to Job Manager.</td>
</tr>
<tr>
<td>Related Content Viewer</td>
<td></td>
<td>Deprecated.</td>
</tr>
<tr>
<td>Role Administrator</td>
<td></td>
<td>Deprecated. Map to Shared Services Provisioning Manager.</td>
</tr>
<tr>
<td>Role Locator</td>
<td></td>
<td>Deprecated. Map to Explorer.</td>
</tr>
<tr>
<td>Schedule Administrator</td>
<td>Schedule Manager</td>
<td></td>
</tr>
<tr>
<td>Session Administrator</td>
<td></td>
<td>Deprecated. Map to BI+ Administrator.</td>
</tr>
<tr>
<td>System Crawler</td>
<td></td>
<td>Deprecated. Map to Trusted Application.</td>
</tr>
<tr>
<td>System Viewer</td>
<td></td>
<td>Deprecated. Map to Explorer.</td>
</tr>
<tr>
<td>Trusted Application</td>
<td>Trusted Application</td>
<td></td>
</tr>
<tr>
<td>User</td>
<td></td>
<td>Deprecated. Map to Explorer and Personal Page Editor.</td>
</tr>
<tr>
<td>User Administrator</td>
<td></td>
<td>Deprecated. Map to Directory Manager.</td>
</tr>
<tr>
<td>User Locator</td>
<td></td>
<td>Deprecated. Map to Explorer.</td>
</tr>
<tr>
<td>View Manager</td>
<td>Viewer</td>
<td></td>
</tr>
<tr>
<td>View Manager Administrator</td>
<td></td>
<td>Deprecated. Map to Viewer.</td>
</tr>
<tr>
<td>View Manager Content Pusher</td>
<td>Favorites Distributor</td>
<td></td>
</tr>
<tr>
<td>Analyzer Administrator</td>
<td></td>
<td>Deprecated. Map to BI+ Global Administrator.</td>
</tr>
<tr>
<td>Analyzer Custom</td>
<td></td>
<td>Custom Aggregated Role. Repurposed.</td>
</tr>
<tr>
<td>Analyzer Power User</td>
<td>Advanced Document Editor</td>
<td></td>
</tr>
<tr>
<td>Analyzer Information Consumer</td>
<td></td>
<td>Deprecated. Map to Information Consumer</td>
</tr>
<tr>
<td>Analyzer Interactive User</td>
<td>Document Editor</td>
<td></td>
</tr>
<tr>
<td>Analyzer Create Reports</td>
<td></td>
<td>Deprecated. Map to Document Editor.</td>
</tr>
<tr>
<td>Analyzer Create POV</td>
<td></td>
<td>Deprecated. Map to Personal Parameters Editor.</td>
</tr>
<tr>
<td>Analyzer Create Links</td>
<td></td>
<td>Deprecated</td>
</tr>
<tr>
<td>Analyzer Design Custom Reports</td>
<td></td>
<td>Deprecated. Map to Advanced Document Editor.</td>
</tr>
<tr>
<td>Analyzer Save Reports</td>
<td></td>
<td>Deprecated. Map to Content Publisher.</td>
</tr>
</tbody>
</table>
### Old Roles Mapping to New Roles (Continued)

<table>
<thead>
<tr>
<th>Old Role Name</th>
<th>New Role Name</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analyzer Edit Data</td>
<td>Data Editor</td>
<td></td>
</tr>
<tr>
<td>Analyzer Administer Users and Groups</td>
<td></td>
<td>Deprecated. Map to BI+ Global Administrator.</td>
</tr>
<tr>
<td>Analyzer Print Reports</td>
<td></td>
<td>Deprecated.</td>
</tr>
<tr>
<td>Analyzer Open User Preferences</td>
<td></td>
<td>Deprecated. Map to Personal Parameter Editor and Data Source Publisher.</td>
</tr>
<tr>
<td>Analyzer Manage Databases</td>
<td></td>
<td>Deprecated. Map to Data Source Publisher.</td>
</tr>
<tr>
<td>Analyzer Cube Navigator</td>
<td>Data Layout</td>
<td>The term Cube Navigator has been removed from the UI. Changing name to Data Layout.</td>
</tr>
<tr>
<td>Analyzer Open Reports</td>
<td></td>
<td>Deprecated. Map to Viewer.</td>
</tr>
<tr>
<td>Analyzer Create Personal Variables</td>
<td>Personal Parameter Editor</td>
<td></td>
</tr>
<tr>
<td>Reports Viewer</td>
<td></td>
<td>Deprecated. Map to Explorer.</td>
</tr>
<tr>
<td>Reports Designer</td>
<td></td>
<td>Deprecated. Facets mapped to Explorer, Content Publisher, and Scheduler.</td>
</tr>
<tr>
<td>Reports System Administrator</td>
<td></td>
<td>Deprecated. Map to BI+ Global Administrator.</td>
</tr>
<tr>
<td>Metrics Builder Administrator</td>
<td></td>
<td>Deprecated. Map to BI+ Administrator.</td>
</tr>
<tr>
<td>Metrics Builder HTML End User</td>
<td>Metrics Viewer</td>
<td></td>
</tr>
<tr>
<td>Smart Form Publisher</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Metrics Builder Editor</td>
<td>Metrics Editor</td>
<td></td>
</tr>
<tr>
<td>Metrics Builder Java End User</td>
<td>Metrics Analyst</td>
<td></td>
</tr>
</tbody>
</table>
This appendix provides information specific to using Hyperion System 9 BI+ Analytic Services Smart View Provider™ with Shared Services User Management Console. Shared Services User Management Console provides a centralized user interface where you can perform user management tasks for Hyperion products.

Use Shared Services to provide security for Analytic Services Smart View Provider, which is administered through Analytic Administration Services. To use Shared Services security, you must register Analytic Services Smart View Provider with Shared Services.

In This Appendix

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analytic Services Smart View Provider User Roles</td>
<td>94</td>
</tr>
<tr>
<td>Provisioning the Administrator Role in Shared Services</td>
<td>94</td>
</tr>
<tr>
<td>Migrating Analytic Services Smart View Provider Users to Shared Services</td>
<td>95</td>
</tr>
</tbody>
</table>
**Analytic Services Smart View Provider User Roles**

Analytic Services Smart View Provider supports one type of user, Administrator, which is categorized under the Power User license type.

<table>
<thead>
<tr>
<th>User Type</th>
<th>License Type</th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>Power User</td>
<td>Create, modify, and delete clusters of Analytic Servers.</td>
</tr>
</tbody>
</table>

**Provisioning the Administrator Role in Shared Services**

In Shared Services mode, the only role that you must assign for Smart View Provider is the Administrator role. Only the Administrator can create Analytic Services clusters in Smart View Provider. No other roles can be assigned. Non-administrator users can only connect to the clusters.

➢ To provision the Administrator role in Shared Services:

2. In Logon, enter the administrator username and password.
   By default, admin and password are the username and password.
3. Click Log on.
4. In the navigation pane, expand Projects and ASVP 9.0.0 Servers.
   Your Smart View Provider is listed.
5. To create a user to provision, follow the proceeding steps:
   a. In the navigation pane, expand User Directories and a directory, such as Native Directory.
   b. Select Users and right-click, then select New > User.
   c. Fill in the user information and click Finish.
6. To select an existing user to provision, follow the proceeding steps:
   a. In the navigation pane, expand User Directories and a directory, such as Native Directory.
   b. Select Users.
7. At the bottom of the navigation pane, enter the user ID to provision and click Search or Show All.
8. From the list, select a user ID and select Administration > Provision.
9. In the Provision Users or Groups pane, expand ASVP 9.0.0 Servers and expand the name of your Smart View Provider.
10. Select Administrator.
11. Click Save.
The user is provisioned as a Smart View Provider administrator. Log into Administration Services Console with the administrator user name and password to create and manage Analytic Services Smart View Provider clusters.

**Migrating Analytic Services Smart View Provider Users to Shared Services**

Because Analytic Services Smart View Provider has no other users, migration to Shared Services is unnecessary.
There are two ways to set up security for Hyperion System 9 Financial Management™ applications:

- Create a file with security information and load it into an application. See “Creating Application Security Files” and “Loading Application Security” in the Hyperion System 9 Financial Management Administrator’s Guide.

- Use the Shared Services User Management Console to set up security. This appendix provides information specific to Financial Management and the Shared Services user management system.
Launching the User Management Console from Financial Management

Before setting up security for Financial Management applications, you must do the following:

3. Provision users by assigning users and groups to applications and assigning roles to users and groups—See “Provisioning Users and Groups” on page 44 and “Financial Management User Roles” on page 100.

You can then use the Shared Services User Management Console to set up security for Financial Management applications. In the console, you can do the following for an application:

- Assign users and groups
- Create and assign security classes
- Assign user permissions to security classes
- Run security reports

To launch the User Management Console from Financial Management:

1. Select Administration > User Management.
   The User Management Console opens in the Financial Management browser window.
2. In Browser View, expand Projects until you can select the application for which to set up security.

Shared Services User Roles in Financial Management

Table 9 lists the Shared Services roles that can be assigned and the tasks that users with that role can perform in Financial Management. You assign users to roles in the Shared Services User Management Console.
Table 9  Shared Services User Roles

<table>
<thead>
<tr>
<th>User Role</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>Perform all administrative functions within Shared Services. The Administrator can assign this role to other users as necessary. It is a global role and provides control over all products that integrate with Shared Services User Management. Therefore it also gives the user access to all aspects of Financial Management applications. A Shared Services Administrator must assign global roles to other users before they can begin performing administrative tasks in the User Management Console. CAUTION! Hyperion recommends that the Administrator role be assigned sparingly in an organization. It is the most powerful role in the user management system and enables more control over security than any other Hyperion role.</td>
</tr>
<tr>
<td>Create Integrations</td>
<td>Perform the following actions on Shared Services integrations:</td>
</tr>
<tr>
<td></td>
<td>● Create, edit, copy, and delete</td>
</tr>
<tr>
<td></td>
<td>● Assign access</td>
</tr>
<tr>
<td></td>
<td>● Create groups</td>
</tr>
<tr>
<td></td>
<td>● View</td>
</tr>
<tr>
<td>Directory Manager</td>
<td>Perform the following actions on Shared Services users and groups:</td>
</tr>
<tr>
<td></td>
<td>● Create</td>
</tr>
<tr>
<td></td>
<td>● Modify details</td>
</tr>
<tr>
<td></td>
<td>● Delete</td>
</tr>
<tr>
<td></td>
<td>● De-activate and reactivate</td>
</tr>
<tr>
<td>Manage Models</td>
<td>Perform the following actions on Shared Services models:</td>
</tr>
<tr>
<td></td>
<td>● Import and export</td>
</tr>
<tr>
<td></td>
<td>● Trace versions</td>
</tr>
<tr>
<td></td>
<td>● Control access</td>
</tr>
<tr>
<td></td>
<td>● Synchronize between product and Shared Services</td>
</tr>
<tr>
<td></td>
<td>● Edit content and set member properties</td>
</tr>
<tr>
<td></td>
<td>● Rename and delete</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This user must have Manage permission for a model via the Shared Services Model Access window to assign permissions to it.</td>
</tr>
<tr>
<td>Project Manager</td>
<td>Create and delete Shared Services projects and modify project details</td>
</tr>
</tbody>
</table>

Shared Services User Roles in Financial Management
Financial Management User Roles

Financial Management user roles determine the tasks that users can perform in an application. Table 10 lists the Financial Management roles that can be assigned and the tasks that users assigned to the role can perform. You assign users to roles in the Shared Services User Management Console.

<table>
<thead>
<tr>
<th>User Role</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provisioning Manager</td>
<td>Perform the following actions within Shared Services:</td>
</tr>
<tr>
<td></td>
<td>● Provision users and groups</td>
</tr>
<tr>
<td></td>
<td>● De-provision users and groups</td>
</tr>
<tr>
<td></td>
<td>● Generate the Provision Report</td>
</tr>
<tr>
<td></td>
<td>In Financial Management, the application creator is assigned to this role when the application is created. Users with this role can load and extract application security, create and delete security classes, and assign access rights to users and groups.</td>
</tr>
<tr>
<td>Run Integrations</td>
<td>Perform the following actions on Shared Services integrations:</td>
</tr>
<tr>
<td></td>
<td>● View integrations</td>
</tr>
<tr>
<td></td>
<td>● Run or schedule integrations or group integrations</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>User Role</th>
<th>Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced User</td>
<td>Use the Browser View and can access Running Tasks</td>
</tr>
<tr>
<td>Application Administrator</td>
<td>Perform all administrative tasks in Financial Management</td>
</tr>
<tr>
<td></td>
<td>Access to this role overrides any other access setting for the user.</td>
</tr>
<tr>
<td></td>
<td>A user who creates an application is automatically assigned this role.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Users with this role only cannot provision users. The user must also have the Shared Services Provisioning Manager role.</td>
</tr>
<tr>
<td>Approve Journals</td>
<td>Approve and reject journals</td>
</tr>
<tr>
<td>Consolidate</td>
<td>Use Consolidate option</td>
</tr>
<tr>
<td>Consolidate All</td>
<td>Use Consolidate All option</td>
</tr>
<tr>
<td>User Role</td>
<td>Tasks</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Consolidate All with Data</td>
<td>Use Consolidate All With Data option</td>
</tr>
<tr>
<td>Create Journals</td>
<td>Create, modify, delete, submit, and unsubmit journals</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Users with this role should also be assigned the Read Journals role.</td>
</tr>
<tr>
<td>Create Unbalanced Journals</td>
<td>Create unbalanced journals</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Users with this role should also be assigned the Create Journals role.</td>
</tr>
<tr>
<td>Data Form Write Back from Excel</td>
<td>Submit data to Financial Management from a data form opened in Smart View</td>
</tr>
<tr>
<td></td>
<td>See the Hyperion System 9 Smart View User’s Guide.</td>
</tr>
<tr>
<td>Database Management</td>
<td>Copy and clear data and delete invalid records</td>
</tr>
<tr>
<td>Default</td>
<td>Perform all default tasks as defined in “Tasks For Default Role” on page 104.</td>
</tr>
<tr>
<td>Enable Write Back in Web Grid</td>
<td>Enter and save data in a Web grid</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Does not apply to Windows Data Explorer users.</td>
</tr>
<tr>
<td>Extended Analytics</td>
<td>Create and execute Extended Analytics queries</td>
</tr>
<tr>
<td>Generate Recurring</td>
<td>Generate recurring journal templates</td>
</tr>
<tr>
<td>Inter-Company Transaction Admin</td>
<td>Open and close periods, lock and unlock entities, manage reason codes, and monitor intercompany transaction process</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Users with this role can perform all intercompany tasks.</td>
</tr>
<tr>
<td>Inter-Company Transaction Auto Match by Account</td>
<td>Auto-match intercompany transactions by account and process intercompany transactions</td>
</tr>
<tr>
<td>User Role</td>
<td>Tasks</td>
</tr>
<tr>
<td>----------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Inter-Company Transaction Auto Match by ID</td>
<td>Auto-match intercompany transactions by ID and process intercompany transactions</td>
</tr>
<tr>
<td>Inter-Company Transaction Manual Match</td>
<td>Manually match intercompany transactions and process intercompany transactions</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If a user has the Manual Match with Tolerance role and the Manual Match role, the Manual Match role takes precedence.</td>
</tr>
<tr>
<td>Inter-Company Transaction Manual Match with Tolerance</td>
<td>Manually match intercompany transactions with a tolerance check and process intercompany transactions</td>
</tr>
<tr>
<td>Inter-Company Transaction Match Template</td>
<td>Manage intercompany matching templates and process intercompany transactions</td>
</tr>
<tr>
<td>Inter-Company Transaction Post/Unpost</td>
<td>Post and unpost intercompany transactions and process intercompany transactions</td>
</tr>
<tr>
<td>Inter-Company Transaction Unmatch</td>
<td>Unmatch intercompany transactions and process intercompany transactions</td>
</tr>
<tr>
<td>Inter-Company Transaction User</td>
<td>Create, edit, delete, load, and extract transactions; run matching reports by account or ID; run transaction reports; drill through from modules; and process intercompany transactions</td>
</tr>
<tr>
<td>Journals Administrator</td>
<td>Perform all tasks involving journals</td>
</tr>
<tr>
<td>Load Excel Data</td>
<td>Load data from Smart View to Financial Management using the Ad Hoc module or Excel functions</td>
</tr>
<tr>
<td>Load System</td>
<td>Load metadata, rules, and member lists</td>
</tr>
<tr>
<td>Lock Data</td>
<td>Lock data</td>
</tr>
<tr>
<td>Manage Custom Documents</td>
<td>Load and extract custom documents</td>
</tr>
<tr>
<td>Manage Data Entry Forms</td>
<td>Manage data forms on the Web</td>
</tr>
<tr>
<td>Manage Ownership</td>
<td>Enter and edit ownership information</td>
</tr>
<tr>
<td>Manage Templates</td>
<td>Manage journal templates</td>
</tr>
<tr>
<td>User Role</td>
<td>Tasks</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Post Journals</td>
<td>Post and unpost journals</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> An entity's security class is checked when a user performs a post or unpost action and when a user reads a posted journal. See “Posting Journals” in the Hyperion System 9 Financial Management User’s Guide.</td>
</tr>
<tr>
<td>Read Journals</td>
<td>Read journals</td>
</tr>
<tr>
<td>Receive E-mail Alerts for IC Transactions</td>
<td>Receive e-mail alerts in the Intercompany Transaction and Intercompany Partner Matching Report modules See “Setting Up E-mail Alerting” in the Hyperion System 9 Financial Management Administrator’s Guide.</td>
</tr>
<tr>
<td>Receive E-mail Alerts for Process Management</td>
<td>Receive e-mail alerts in process management See “Setting Up E-mail Alerting” in the Hyperion System 9 Financial Management Administrator’s Guide.</td>
</tr>
<tr>
<td>Reserved</td>
<td>Not used</td>
</tr>
<tr>
<td>Review Supervisor</td>
<td>Perform the following actions in process management:</td>
</tr>
<tr>
<td></td>
<td>● Start a process unit that enables data input</td>
</tr>
<tr>
<td></td>
<td>● Approve data</td>
</tr>
<tr>
<td></td>
<td>● Publish data</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> A user with this role can see data in the Not Started, First Pass, Submitted, Approved, and Published states, but cannot see data in the Review Level 1 through Review Level 10 states. See “Using Process Management” in the Hyperion System 9 Financial Management User’s Guide.</td>
</tr>
<tr>
<td>Reviewer 1 through Reviewer 10</td>
<td>View and edit data when data is at the user’s designated process management level The privileges associated with these roles also depend on the user’s rights to access entity data. For example, a user assigned to the Reviewer 1 role can view and change data when the data is at Review Level 1. After Reviewer 1 promotes data to Review Level 2, Reviewer 1 can view data but can no longer change it. <strong>Note:</strong> Users with a reviewer role can see data in the First Pass and Published state and their assigned review level state and higher. They cannot see data in the Not Started state or in review level states lower than what they are assigned. See “Using Process Management” in the Hyperion System 9 Financial Management User’s Guide.</td>
</tr>
<tr>
<td>Run Allocation</td>
<td>Run allocations</td>
</tr>
</tbody>
</table>
Tasks For Default Role

All users and groups assigned to the Default role can perform the default tasks in Table 11.

Note: To grant additional access rights, you must assign users and groups to roles.

Table 11  Default Tasks

<table>
<thead>
<tr>
<th>Menu</th>
<th>Default Tasks Available</th>
</tr>
</thead>
<tbody>
<tr>
<td>File</td>
<td>● Open Application</td>
</tr>
<tr>
<td></td>
<td>● Close Application</td>
</tr>
<tr>
<td></td>
<td>● Change Application</td>
</tr>
<tr>
<td></td>
<td>● Set as Default Application</td>
</tr>
<tr>
<td></td>
<td>● Preferences</td>
</tr>
<tr>
<td></td>
<td>● Logoff</td>
</tr>
<tr>
<td></td>
<td>● Exit</td>
</tr>
<tr>
<td></td>
<td>● Create Application</td>
</tr>
</tbody>
</table>

Note: Access is restricted based on the security assigned to the user

| View | ● Masthead |
|      | ● Pane     |
Assigning Users and Groups to Financial Management Applications

Note: Before you can assign users and groups to applications, you must provision users. For information on provisioning users, see “Provisioning Users and Groups” on page 44.

Only a user assigned to the Provisioning Manager role can define users and groups for an application. See “Provisioning Manager” on page 100.

Only the users and groups provisioned for the application are available when you select users and groups.

➤ To select users and groups for an application:

1 From Available Users and Groups, select an option.
2 Select users and groups to assign to the application, and click

**Tip:** Use the Shift and Ctrl keys to select multiple users and groups. Click to add all users and groups in the Available Users and Groups column to the Selected Users column. Use and to remove some or all users and groups from the Selected Users and Groups column.

3 Click Next or Select Classes.

### Setting Up Security Classes for Financial Management Applications

In the Select Classes module, you can perform the following procedures:

- “Creating Security Classes” on page 107
- “Deleting Security Classes” on page 107
- “Selecting Security Classes” on page 107

Security classes determine the access that users have to application elements.

**Note:** Only users assigned to the Provisioning Manager role can define security classes for applications.

After you define security classes for an application, you can assign the security classes to application elements such as accounts and entities.

A user's or group’s ability to access application elements depends on the security classes to which the user or group belongs and on the security class associated with the application elements.
Creating Security Classes

➤ To create a security class:

1 In Class Name, enter a name for the security class.

Note: The name can contain up to 80 characters.

2 Click Add.

Deleting Security Classes

Caution! Before you delete a security class from an application, you must disassociate it from the application elements to which it is assigned.

You can disassociate an entity, account, or scenario from a security class by updating the security class in the metadata file or by modifying the security class attribute in Metadata Manager. See “Managing Metadata” in the *Hyperion System 9 Financial Management Administrator’s Guide.*

You can disassociate a journal from a security class by modifying the journal file or by updating the security class for the journal in the Process Journals module. See “Creating Journal Files” in the *Hyperion System 9 Financial Management Administrator’s Guide.*

➤ To delete security classes:

1 From Available Classes, select the security classes to delete.

Tip: Use the Shift and Ctrl keys to select multiple classes.

2 Click .

3 Click Yes to confirm deletion.

Selecting Security Classes

➤ To select security classes for an application:

1 From Available Classes, select the security classes to assign to the application, and click .
**Tip:** Use the Shift and Ctrl keys to select multiple security classes. Click ![add](image) to add all security classes in the Available Classes column to the Selected Classes column. Use ![remove](image) and ![clear](image) to remove some or all security classes from the Selected Classes column.

<table>
<thead>
<tr>
<th>Available Classes:</th>
<th>Selected Classes:</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCOUNTS</td>
<td>[Default]</td>
</tr>
<tr>
<td>ASIA</td>
<td></td>
</tr>
<tr>
<td>CORPORATE</td>
<td>ACTUAL</td>
</tr>
<tr>
<td>EASTREGION</td>
<td>BUDGET</td>
</tr>
<tr>
<td>EUROPE</td>
<td>FORECAST</td>
</tr>
<tr>
<td>OPERATIONS</td>
<td>SYSTEM</td>
</tr>
<tr>
<td>SALES</td>
<td></td>
</tr>
<tr>
<td>SOUTHAMERICA</td>
<td></td>
</tr>
<tr>
<td>US</td>
<td></td>
</tr>
<tr>
<td>WESTREGION</td>
<td></td>
</tr>
</tbody>
</table>

2 Click **Next** or **Assign Access**.

**Assigning User Access to Security Classes**

After you define users and groups and security classes, you can specify the level of access each user and group has to each security class in the application and set up e-mail alerts.

**Note:** You must select users and classes for the application before you can access the Assign Access module.

<table>
<thead>
<tr>
<th>Table 12</th>
<th>User Access Level</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access Level</strong></td>
<td><strong>User and Group Tasks</strong></td>
</tr>
<tr>
<td>None</td>
<td>No access to elements assigned to the security class.</td>
</tr>
<tr>
<td>Metadata</td>
<td>View a specified member in a list but cannot view or modify data for the member.</td>
</tr>
<tr>
<td>Read</td>
<td>View data for elements assigned to the security class but cannot promote or reject.</td>
</tr>
<tr>
<td>Promote</td>
<td>View data for elements assigned to the security class and can promote or reject.</td>
</tr>
<tr>
<td>All</td>
<td>Modify data for elements assigned to the security class and can promote and reject.</td>
</tr>
</tbody>
</table>
You can use the Pivot Table feature to toggle between two views for assigning access. For example, if you have users and groups on rows and security classes on columns and click Pivot Table, users and groups will be on columns and security classes on rows.

**Note:** A user assigned to the Application Administrator role for an application has access to all information in the application.

To assign user access to security classes:

1. Select cells for which to assign access rights.
2. From Access, select the access level to assign.
3. Click to apply the level to the selected cells.
4. Optional: To add an e-mail alert, select cells in the table and click Add Alert.

---

**Caution!** The alerting process uses the e-mail addresses stored in the external authentication files. To receive e-mail alerts, users must be on Microsoft Active Directory or LDAP. See “Setting Up E-mail Alerting” on page 109.

**Note:** To remove e-mail alerts, select the cell and click Remove Alert.

5. Click Save.

### Setting Up E-mail Alerting

You can use e-mail alerting for intercompany transactions and during the process management review process. E-mail alerts help highlight a key event or data change in the system. For example, you can send an e-mail alert that an intercompany transaction is mismatched and needs to be matched, or that a process unit is ready for the next promotion level.

**Note:** The alerting process uses the e-mail addresses that are stored in the external authentication files. To receive e-mail alerts, users must be on Active Directory or LDAP.
Process Management Alerting

To set up process management e-mail alerts:

1. For the scenario in the process unit, set the SupportsProcessManagement metadata attribute to “A” to allow alerts.
2. Assign the user to the Receive E-mail Alerts for Process Management role.

Note: For information on assigning users to roles, see the Hyperion System 9 Shared Services User Management Guide.

3. Assign the user to Process Management notifiable roles as defined in Table 13.
4. Assign the user ALL or PROMOTE access to the security classes assigned to the scenario and entity in the process unit and add an alert for each security class.

Users who meet all criteria receive e-mail alerts.

Table 13 Process Management User Roles and Alert Notification

<table>
<thead>
<tr>
<th>Process Unit Level Before or After Action</th>
<th>Process Management User Roles Notified</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Pass</td>
<td>Users with ALL or PROMOTE access to the entity are notified.</td>
</tr>
<tr>
<td>Review Level 1</td>
<td>Reviewer 1 and Submitter roles are notified.</td>
</tr>
<tr>
<td>Review Level 2</td>
<td>Reviewer 2 and Submitter roles are notified.</td>
</tr>
<tr>
<td>Review Level 3</td>
<td>Reviewer 3 and Submitter roles are notified.</td>
</tr>
<tr>
<td>Review Level 4</td>
<td>Reviewer 4 and Submitter roles are notified.</td>
</tr>
<tr>
<td>Review Level 5</td>
<td>Reviewer 5 and Submitter roles are notified.</td>
</tr>
<tr>
<td>Review Level 6</td>
<td>Reviewer 6 and Submitter roles are notified.</td>
</tr>
<tr>
<td>Review Level 7</td>
<td>Reviewer 7 and Submitter roles are notified.</td>
</tr>
<tr>
<td>Review Level 8</td>
<td>Reviewer 8 and Submitter roles are notified.</td>
</tr>
<tr>
<td>Review Level 9</td>
<td>Reviewer 9 and Submitter roles are notified.</td>
</tr>
<tr>
<td>Review Level 10</td>
<td>Reviewer 10 and Submitter roles are notified.</td>
</tr>
<tr>
<td>Submitted</td>
<td>Review Supervisor role is notified. Only users with this role can approve the submitted process unit.</td>
</tr>
<tr>
<td>Approved</td>
<td>Reviewer 1 to Reviewer 10 and Submitter roles are notified.</td>
</tr>
<tr>
<td>Published</td>
<td>Users with ALL, READ, or PROMOTE access to the entity are notified.</td>
</tr>
</tbody>
</table>

Note: E-mail alerts are not generated when the process unit is at the Not Started level or for the Sign Off action.
Users with the Application Administrator role do not receive e-mail alerts. For a user with the Application Administrator role to receive e-mail alerts, set up as a separate user and assign the role to receive alerts. The user that performed the action to the process unit is also notified with an e-mail confirmation log stating to whom e-mails were sent. For information on generating e-mail alerts in process management, see the *Hyperion System 9 Financial Management User’s Guide*.

**Intercompany Transaction Alerting**

➤ To set up intercompany transaction e-mail alerts:

1. Assign the user to the Receive E-mail Alerts for IC Transactions role.

*Note:* For information on assigning users to roles, see the *Hyperion System 9 Shared Services User Management Guide*.

2. Assign the user to the Inter-Company Transaction Admin or Inter-Company Transaction User role.

3. Assign the user ALL, READ, or PROMOTE access to the security classes that are assigned to the scenario and entity in the transaction and add an alert for each security class. See “Assigning User Access to Security Classes” on page 108.

Users who meet all criteria receive e-mail alerts from the Intercompany Transactions or Intercompany Partner Matching Report modules.

For information on generating e-mail alerts in intercompany transactions, see the *Hyperion System 9 Financial Management User’s Guide*.

**Running Security Reports for Financial Management Applications**

You can run security reports on the information that you selected while setting up security for the application. You can run reports for classes by user, roles by user, classes and roles by user, and users by group. You can view the report online or you can export it to a CSV file.

➤ To create a security report:

1. Select a report option:
   - Rights and select options:
     - Classes by User
     - Roles by User
   - Users by Group

2. Select an option:
   - Launch Report to open the report in a new window
• Export to File to save the as a CSV file.

**Migrating Financial Management Users to Shared Services Security**

For information on migrating users to Shared Services security, see “Using the Schema Upgrade Utility” in the *Hyperion System 9 Financial Management Installation Guide*.
This appendix provides information that is specific to Hyperion System 9 Planning™, Hyperion System 9 Workforce Planning™, and the Shared Services User Management console.

In This Appendix

About Planning Security ................................................................. 114
Launching the User Management Console From Planning ...................... 114
Returning to Planning From the User Management Console ...................... 114
Updating Users and Groups in Planning ............................................ 115
User Roles .................................................................................. 117
User Roles in Workforce Planning ...................................................... 121
Manage Models User Role ............................................................... 123
About Connection Types and Planning ................................................. 124
Migrating Users to Shared Services ................................................... 124
About Planning Security

You set up users and groups as described in this guide. After users and groups are defined using the User Management console, you assign their appropriate access rights to various application elements. For example, you can assign a user or group access to Entity dimension members, data forms, and task lists. You can assign access for users and groups to Planning application elements from within Planning, or you can invoke that functionality from the User Management console. For more information on assigning access in Planning, see the Hyperion System 9 Planning Administrator’s Guide or help system.

Note: If you are upgrading a Planning application from an earlier release, see “Migrating Users to Shared Services” on page 124.

Launching the User Management Console From Planning

In addition to the other ways you can launch the User Management console, you can also launch the User Management console from within Planning.

➢ To launch the User Management console from within Planning, select Administration > User Management.

The User Management console opens in the same Web browser window as the Planning application. For information on returning to Planning, see “Returning to Planning From the User Management Console” on page 114. For information on using the User Management console, consult the other chapters in this guide.

Returning to Planning From the User Management Console

If you launch the User Management console from within a Planning application, when you are done working with the User Management console, you can return to where you were in the Planning application when you launched the User Management console.

➢ To return to the Planning application from the User Management console:

1 From within the User Management console, select File > Return to Application <application name>.

2 When asked to confirm that you want to navigate from the current page, click:

● OK to return to the current Planning application.
● Cancel to stay on the current page in the User Management console.
Updating Users and Groups in Planning

This section describes how users, groups, and their roles are updated, or synchronized, from the User Management console into Planning. Each time Planning gets the current list of users, groups, and roles from the User Management console, Business Rules also get the same, current list.

A Planning application gets the latest list of users and groups from the User Management console under the following conditions:

- When the application is refreshed on the Planning Desktop, with Security Filters selected.
- When the ProvisionUsers utility is run. (For more information, see “Updating Users With a Utility” on page 115.)
- When you click the Refresh Users and Groups button from within Planning. (For more information, see the steps in this topic on how to ensure that Planning has the latest information on users and groups.)
- When an individual logs into the application, Planning synchronizes that user with the User Management console.

When users and groups are synchronized from the User Management console into Planning, that information is stored in memory and is available for access assignments in Planning. Keep in mind that if other administrators make changes or add users in the User Management console, the information stored in memory becomes outdated. To make sure that you have access to the most current set of users and groups in Planning, you refresh into memory the users, groups, and roles from the User Management console.

To ensure that Planning has the latest information on users and groups:

1. Take one of the following actions:
   - Select Administration > Manage Data Forms and select a form.
   - Select Administration > Dimensions and select a dimension member.
   - Select Administration > Manage Task Lists and select a task list.
2. Click Assign Access.
4. Click Refresh Users and Groups.

Updating Users With a Utility

Planning includes a utility—ProvisionUsers—that enables you, outside of Planning, to synchronize users maintained in the User Management console with Planning applications. A single user or set of users can be synchronized across one or more Planning applications on the server on which the utility is run.

You use the ProvisionUsers utility through a command line interface. Only administrators can run this utility.
To use the ProvisionUsers utility:

1. Launch the `ProvisionUsers.cmd` file from the `Utils` directory, using the following syntax:

   ```provisionusers [/U:user1[;user2;user3]] [/A:app1[;app2;app3]] [/R:n]```

   If you installed Planning in the default location, the `Utils` directory is in the following path:

   `<drive letter>:\Hyperion\HyperionPlanning\Utils`.

   **Note:** The square brackets `[“ and “]` are used to denote the argument as optional. They are not part of the syntax of the command.

### Table 14  ProvisionUsers Utility Syntax

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[/U:user1[;user2;user3]]</td>
<td>This optional argument enables you to specify individual users for synchronization. For example, to synchronize one user, “Planner1”, use <code>/U:Planner1</code>. To synchronize users “Planner1” and “Planner2”, use: <code>/U:Planner1;Planner2</code>. All users are synchronized if this argument is omitted.</td>
</tr>
<tr>
<td>[/A:app1[;app2;app3]]</td>
<td>This optional argument enables you to specify individual Planning applications for synchronization. For example, to synchronize one application, “PlanningApp1”, use <code>/A:PlanningApp1</code>. To synchronize applications “PlanningApp1” and “PlanningApp2”, use: <code>/A:PlanningApp1;PlanningApp2</code>. All applications are synchronized if this argument is omitted.</td>
</tr>
<tr>
<td>[/R:n]</td>
<td>This optional argument enables you to specify an interval, in minutes, in which synchronization is re-run. The “n” denotes an integer value of minutes. For example, to resynchronize applications every 30 minutes, use the argument <code>/R:30</code>. If this argument is omitted, the synchronization is performed just once.</td>
</tr>
<tr>
<td>/?</td>
<td>This argument specified by itself prints out the syntax and options for the <code>ProvisionUsers</code> command.</td>
</tr>
</tbody>
</table>

Following are some examples of using the ProvisionUsers utility.

**Example 1**

If you type:

```
ProvisionUsers
```

This synchronizes all users in all applications on the server on which the utility is run.

**Example 2**

If you type:

```
ProvisionUsers /U:Planner1 /A:PlanningApp1;PlanningApp2 /R:60
```

This synchronizes user “Planner1” in the PlanningApp1 and PlanningApp2 applications every 60 minutes.
Example 3

If you type:

ProvisionUser /?

This prints the following information on using the command:

Usage: ProvisionUsers [/U:user1[;user2;user3]] [/A:app1[;app2;app3]] [/R:30]

Options:

- /U = User name to be synchronized. Multiple users can be separated by semicolon (;). To synchronize all users, use /U:* . By default, all users will be included.
- /A = Application name to be synchronized. Multiple applications can be separated by semi-colon (;). To synchronize all applications, use /A:* . By default, all applications will be included.
- /R = Specifies how often in minutes synchronization should rerun. /R:30 will rerun every 30 minutes.
- /S = Suppresses messages. Errors will still be displayed.

User Roles

Subject to the applicable license for the software and users, Planning supports four user roles, as described in the following topics:

- “Administrator” on page 117
- “Interactive User” on page 118
- “Planner” on page 119
- “View User” on page 119
- “User Roles and Tasks” on page 119

The administrator user role also contains a super-user role called the application owner.

Administrator

Users who are designated as administrators can perform any task in the application and during financial processes, except delete the application or claim ownership of an application. The administrator who is designated as the application owner is the only user who can delete an application. Administrators can perform the following types of tasks:

- Create applications.
- Manage security.
- Maintain metadata.
- Initiate and manage the budget process (for example, start planning units).
- Designate the e-mail server for e-mail notification.
• Create and maintain Web-based data forms.
• Create and manage task lists.
• Create and maintain Smart View worksheets.
• Create and maintain reports using Financial Reporting (if designated with the Designer role).
• Create and launch adapter processes using Hyperion Application Link.
• Create and launch business rules using Business Rules.
• Enter, view, and delete data.

Setting Up Multiple Administrators for an Application with One Owner

Planning allows you to designate more than one administrator for each application. This ability facilitates the delegation of maintenance across large applications. An application owner always exists, because he or she is the only administrator who can delete an application. Other administrators who are assigned to an application can perform all tasks except deleting an application, deleting the application owner, or claiming ownership for themselves or another user. The initial owner of the application is the administrator who created the application. The application owner can later reassign ownership of the application to another user.

When the Manage Database task is in use by an administrator, all other tasks are unavailable to other users, including the application owner. Conversely, when any other task is open, the Manage Database task is unavailable to all users. This maintains consistency between the information in the relational database and the Analytic Services database.

Interactive User

Interactive users can perform the following tasks:
• Enable e-mail notification (for themselves only).
• Create and maintain Web-based data forms.
• Create and manage task lists.
• Create and maintain Smart View worksheets.
• Create and maintain reports using Financial Reporting (if designated with the Designer role).
• Create and launch adapter processes using Hyperion Application Link.
• Create and launch business rules using Business Rules.
• Enter, view, and delete data.
• Submit information and data for approval. They can then control this process, sign off, reject, pass plans to another level, verify the plans with other parts of the organization, and so on. For example a sales director may collect all the planning information for sales managers. Before signing this off, a manufacturing director can review new forecasts based on production capacity.
Interactive users cannot create and maintain applications, dimensions, exchange rates, users or access rights assignments. Examples of interactive users are department heads, sales directors, and business unit managers.

**Planner**

In most cases, planners comprise the majority of users. Planners can perform the following tasks:

- Enable e-mail notification (for themselves only).
- Input, submit, and view data.
- Use reports that have been built by others.
- Run data integration routines designed by others.
- Execute business rules and other processes associated with validating and preparing data.
- View and use task lists.
- Use Smart View.
- Use any data access tools for which they are licensed (for example, Web Analysis).
- Submit information and data for approval. They can then control this process, sign off, reject, pass plans to another level, verify the plans with other parts of the organization, and so on.

Planners are subject to the restrictions placed on interactive users. In addition, planners cannot create and maintain reports, adapter flow diagrams, or business rules.

**View User**

A view user has limited access to view data in a Planning application. Typically, the view user is an executive who wants to see business plans during and at the end of the budget process. View users can use any data access tool for which they are licensed; for example, Planning Web Client, Financial Reporting, Smart View, Web Analysis, and so on.

**User Roles and Tasks**

Subject to the applicable license for the software and users, the following table lists Planning tasks and the corresponding users who can perform the tasks.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Administrator</th>
<th>Interactive User</th>
<th>Planner</th>
<th>View User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create new apps</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modify apps</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Submit plans</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
User Roles Between Planning and Business Rules

The following table shows how user roles in Planning map to user roles in Business Rules:

<table>
<thead>
<tr>
<th>Planning Role</th>
<th>Business Rules Role</th>
<th>Tasks Performed</th>
</tr>
</thead>
</table>
| Administrator | Administrator       | ● Designs business rules  
                             ● Launches business rules for a particular Planning application |
| Interactive user | Interactive user | ● Designs business rules  
                             ● Launches rules that have been assigned Launch privileges by an administrator |
| Planner | Basic user | Launches business rules that have been assigned Launch privileges by an administrator |
| View user | None | None |
Access Rights Between Planning and Analytic Services

After security filters are updated in the Analytic Services database, the type of access a Planning user has in Analytic Services depends on the user type that is used to establish the connection. (For more information on connection types, see “About Connection Types and Planning” on page 124.) The following table describes a user’s rights in Analytic Services.

Table 17  Access Rights Between Planning and Analytic Services

<table>
<thead>
<tr>
<th>User Type for Connection</th>
<th>View User</th>
<th>Planner</th>
<th>Interactive User</th>
<th>Administrator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Named User</td>
<td>Filter Access</td>
<td>Calculate</td>
<td>Calculate</td>
<td>Database Designer¹</td>
</tr>
</tbody>
</table>

¹ Not reflected in Essbase Administration Services for Essbase 7/Analytic Administration Services for Analytic Services 9.

User Roles in Workforce Planning

Subject to the applicable license for the software and users, this section discusses the user roles in Workforce Planning.

About User Roles

Workforce Planning supports the same user roles as Planning. Access to Workforce Planning tasks is determined by user role; users see only functionality to which their user role has access. This topic describes which user roles can perform which tasks. Administrators further refine access by specifying which planners can access which cost center accounts, employees, and data forms.

Administrator Tasks

Administrators establish the worldwide structure for Workforce Planning and run the routine processes for preparing and consolidating the budget. The administrator has the highest level of permissions in Workforce Planning. For an overview to the typical tasks an administrator performs, see “User Roles and Tasks in Workforce Planning” on page 122.

Interactive User Tasks

Interactive users can perform such tasks as modify the predefined data forms. For more information on specific tasks that an interactive user can perform in Workforce Planning, see “User Roles and Tasks in Workforce Planning” on page 122.
Planner Tasks

Working with management, planners are responsible for inputting data and reviewing the budget. They can enter summary-level expenses (for example, department expenses) for top-down planning, and can work with individual employee salaries and bonuses to which they have access. Planners can also view reports. For more information on specific tasks that a planner can perform in Workforce Planning, see “User Roles and Tasks in Workforce Planning” on page 122.

Note that in Planning, planner users cannot view or change a dimension’s outline. In Workforce Planning, planners affect the Entity dimension’s outline by adding an employee.

User Roles and Tasks in Workforce Planning

The following table lists Workforce Planning tasks and the corresponding users who can perform the tasks. For information on other Planning tasks that each user role can perform, see “User Roles” on page 117.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Administrator</th>
<th>Interactive User</th>
<th>Planner</th>
<th>View User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create new Workforce Planning applications</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Load information by creating Hyperion Application Link flow diagrams</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Run Hyperion Application Link flow diagrams</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Modify the predefined employee attribute values or accounts</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create new employee attributes</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add custom attribute values</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete predefined attributes and accounts</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add, edit, and terminate employees</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong>: Users must have access</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adjust expenses accounts (for example, salary, bonus, and so on)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong>: Users must have access</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Manage Models User Role

Users who are assigned the Manage Models role can export and import Shared Services models. (For information on the Project Manager role, see the Shared Services User Roles appendix of this guide.)

Shared Services provides a database, organized into applications, in which products can store, manage, and share metadata models. A model is a container of application-specific data, such as a file or string. There are two types of models: dimensional hierarchies such as entities and accounts, and nondimensional objects such as security files, member lists, rules, scripts, and Web forms.

The process of copying a model from a local application to Shared Services is known as exporting. The process of copying a model from Shared Services to a local application is known as importing.

As a Manage Models user, you can perform the following actions on Shared Services models:

- Track versions
- Control access
- Synchronize models in the product and corresponding models in Shared Services
- Edit model content and set member properties of dimensional models
- Rename and delete models

<table>
<thead>
<tr>
<th>Table 18</th>
<th>User Roles and Tasks in Workforce Planning (Continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tasks</td>
<td>Administrator</td>
</tr>
<tr>
<td>Modify the predefined data forms</td>
<td>X</td>
</tr>
<tr>
<td>Associate a custom data form with a view</td>
<td>X</td>
</tr>
<tr>
<td>Set the context of the data forms</td>
<td>X</td>
</tr>
<tr>
<td>Add accounts with specific subaccount settings</td>
<td>X</td>
</tr>
<tr>
<td>Create and update business rules in Business Rules</td>
<td>X</td>
</tr>
<tr>
<td>View data through views</td>
<td>X</td>
</tr>
<tr>
<td>Enter data into budgets</td>
<td>X</td>
</tr>
<tr>
<td>Submit data</td>
<td>X</td>
</tr>
<tr>
<td>View data through Financial Reporting</td>
<td>X</td>
</tr>
</tbody>
</table>
Note: The Manage Models user must have Manage permission for a model through the Shared Services Model Access window in order to assign permissions to it.

### Table 19  Manage Models User Role and Tasks

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Manage Models</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version tracking</td>
<td>X</td>
</tr>
<tr>
<td>Access control</td>
<td>X</td>
</tr>
<tr>
<td>Synchronize models in the application and corresponding models in Shared Services</td>
<td>X</td>
</tr>
<tr>
<td>Edit model content and set member properties of dimensional models</td>
<td>X</td>
</tr>
<tr>
<td>Rename and delete models</td>
<td>X</td>
</tr>
</tbody>
</table>

### About Connection Types and Planning

Planning connects to the Analytic Services database using the appropriate user type to establish a connection. The possible connection types are listed in the following table:

### Table 20  Connection Types and Planning

<table>
<thead>
<tr>
<th>Program Used to Log on to Planning Application</th>
<th>Analytic Services Connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Planning Web and Smart View client through the Planning provider</td>
<td>Pool of supervisor user connections</td>
</tr>
<tr>
<td>Planning Windows Desktop</td>
<td>A single supervisor connection</td>
</tr>
<tr>
<td>Financial Reporting, Business Rules, and third-party tools</td>
<td>Named user</td>
</tr>
</tbody>
</table>

### Migrating Users to Shared Services

If you are upgrading a Planning application from an earlier release of Planning, follow the instructions in the Hyperion System 9 Planning Installation Guide. Also, before any users can log on to the new release of Planning, you must migrate the upgraded application’s users and groups to the User Management console, following the instructions in this topic.
To migrate existing users and groups for a Planning application:

1 Log on to the application and, if you have not done so already, register the application with Shared Services:
   a. A message is displayed on the Planning **System Settings** tab, prompting you to register the application with Shared Services.
   b. In the **Shared Services Server URL** text box, type the URL to the Shared Services server in the following format: http://<host>:58080.
      For more information on registering a Planning application with Shared Services, see the Hyperion System 9 Planning Administrator’s Guide or help system.
   c. Click **Register Shared Services**.
   d. To enable you to assign the current application to a Shared Services project, a dialog box is displayed. Select one of the following:
      - **New Project**—to create a new Shared Services Project and assign the current application to the new Project. Enter the new project name in the text box.
      - **Existing Projects**—to add the application to an existing project by selecting it from a drop-down list.
      - **Unassigned Project**—to leave the application unassigned.
   e. Click **Submit**.
      The application is now registered with Shared Services.

2 Migrate the application’s existing users and groups to the User Management console:
   a. A message is displayed, prompting you to migrate the existing users and groups, and a **Migrate Users and Groups** button is displayed.
   b. Click **Migrate Users and Groups** to migrate existing users and groups to the User Management console.
   c. If the migration is successful, the application is populated with all the existing user and group role assignments and the Migrate Users and Groups button is no longer displayed. All Planning groups are added to the Native Directory in the User Management console. Any Planning administrator that is migrated to the User Management console is automatically assigned the Provisioning Manager role as well. If the migration is not successful, a window displays the users and groups that failed to migrate. Take one of the following actions:
      - Click **OK** to ignore the errors and complete the migration.
      - Click **Cancel** to cancel the migration and resolve the errors. Until you have completed the migration process, Planning presents the Migrate Users and Groups button each time you log on.

For more information about working with users and groups, refer to this guide.
This appendix provides information that is specific to Hyperion System 9 Business Rules™ and the User Management Console within Shared Services. The User Management Console provides a centralized user interface where you can perform user management tasks for Hyperion products.

In This Appendix

- About Business Rules Security ................................................................. 128
- Launching the User Management Console ............................................. 128
- Business Rules User Roles ................................................................. 128
- Migrating Business Rules Users to Shared Services Security .................. 129
About Business Rules Security

When you migrate your Analytic Administration Services and Business Rules users, groups, and roles to Shared Services, the users and groups are automatically provisioned for use in Business Rules and other Hyperion products. For more information on managing users and groups in Shared Services, see Chapter 3 of this guide.

After users and groups are migrated to Shared Services, you assign Business Rules roles to them. Business Rules has three predefined roles that you can assign to users and groups: administrator, interactive user, and basic user. These roles determine what tasks users and groups can perform on Business Rules repository objects such as business rules, sequences, macros, variables, and projects. For more information on Business Rules roles, see “Business Rules User Roles” on page 128. For more information on assigning Business Rules roles to users and groups, see Chapter 3 of this guide.

After you assign roles to users and groups, you can assign them access privileges to various repository objects in Business Rules. You assign access privileges for users and groups to specific repository objects from within the Business Rules node in Analytic Administration Services. For example, you might want to assign a user access privileges to edit all of the business rules in a particular Business Rules project. For more information on assigning access privileges for users and groups, see the Hyperion System 9 Business Rules Administrator’s Guide or the Hyperion System 9 Business Rules Administrator’s Online Help.

Launching the User Management Console

➢ To launch the User Management Console, from the Windows Start menu:


The User Management Console is displayed in a separate browser window.

2. Use the Help menu in the User Management Console to get assistance with managing users and groups and assigning roles to them.

Business Rules User Roles

Subject to the applicable license for the software and users, Business Rules supports three predefined user roles. For information about assigning Business Rules roles to users and groups, see Chapter 4 of this guide.

Note: You cannot edit Business Rules roles.

- Administrator: A user or group who has the role of administrator can do any of the following tasks:
  - Create, launch, edit, validate, and manage business rules, sequences, macros, variables, and projects
- Assign access privileges to business rules, sequences, macros, variables, and projects
- Create and edit users and groups

**Note:** You create and edit users and groups in the User Management Console. You cannot create users and groups in Business Rules.

- Set up the repository and log file

**Note:** You set up the repository and log file using the Configuration Utility in Shared Services.

- Interactive User: A user or group who has the role of *interactive user* can do any of the following tasks (as long as they are assigned by an administrator):
  - Create business rules, sequences, macros, variables, and projects
  - Assign access privileges to business rules, sequences, macros, variables, and projects
- Basic User: A user or group who has the role of *basic user* can do any of the following tasks (as long as they are assigned by an administrator):
  - Launch business rules and sequences to which the user has access
  - View business rules and sequences to which the user has access
  - View all variables and macros
  - Edit specific business rules, sequences, macros, variables, and projects for which the user was granted editing privileges

---

**Migrating Business Rules Users to Shared Services Security**

In order to migrate native Analytic Administration Services and Business Rules users to Shared Services, you need to run the Externalize Users utility in Analytic Administration Services. When you run this utility, all native Analytic Administration Services and Business Rules users from the previous release are copied from the Analytic Administration Services/Business Rules repository into the Shared Services repository. (For more information on the Externalize Users utility, see the *Hyperion System 9 Analytic Administration Services Installation Guide*.)

After you run the Externalize Users utility, you migrate your Business Rules repository from the previous release to this release of Business Rules using the migration utility in Business Rules. When you migrate the repository to this release, the repository is also migrated automatically to Shared Services. (For more information on migrating the Business Rules repository, see the *Hyperion System 9 Business Rules Administrator’s Guide*.)

During migration, any Business Rules roles assigned to users are migrated and assigned equivalent roles in Shared Services. In addition, any Business Rules groups are migrated to Shared Services. If the groups have roles assigned to them, these roles are also migrated and assigned equivalent roles in Shared Services. If a Business Rules group does not exist in Shared Services, it is created.
When you migrate your Business Rules repository, all Business Rules repository objects including rules, sequences, variables, macros, and projects, as well as any database locations and access privileges assigned to them, are migrated to Shared Services. Now you are ready to use Shared Services to manage security for Business Rules.
You can provision users for Hyperion System 9 Performance Scorecard™ using Shared Services. This feature enables you to use existing user information for a number of Hyperion applications, or to provision multiple users at one time.

To provision users through Shared Services, you need to select this as an option after installation, when you run the Configuration Utility, as outlined in the Hyperion System 9 Performance Scorecard Installation Guide. The Shared Services Administrator must also be provisioned to the Performance Scorecard application.

The provisioning process requires you to have both Shared Services and Performance Scorecard configured and running. External authentication ensures that the applications can communicate seamlessly to provision users easily and accurately.

The information in this Appendix provides instructions for the Performance Scorecard portion of user provisioning only. For detailed instructions on using Shared Services, refer to the Hyperion System 9 Shared Services User Management Guide.

<table>
<thead>
<tr>
<th>In This Appendix</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance Scorecard User Roles</td>
<td>132</td>
</tr>
<tr>
<td>Launching the User Management Console from Performance Scorecard</td>
<td>133</td>
</tr>
<tr>
<td>Creating and Provisioning Users and Groups over Shared Services</td>
<td>135</td>
</tr>
<tr>
<td>Migrating Performance Scorecard Users and Groups to Shared Services Security</td>
<td>139</td>
</tr>
</tbody>
</table>
Performance Scorecard User Roles

In Performance Scorecard, each user ID that is created is attached to an employee. The user must also be assigned one of three default security roles, as follows:

- Administrator
- Designer
- User

The security role assigned to each Performance Scorecard user determines the actions and access available to that user. Access for a group of users grants similar security access to all its members.

Depending on the access requirements for a particular user, the assigned security may be modified to attach a wider or narrower access. Custom security roles can also be created, as outlined in the *Hyperion System 9 Performance Scorecard Administrator’s Guide*.

Refer to Table 21, “Default Performance Scorecard Security Roles,” for a list of default Performance Scorecard security roles, and a description of their associated access.

Table 21  Default Performance Scorecard Security Roles

<table>
<thead>
<tr>
<th>Security Role</th>
<th>Shared Services Role</th>
<th>Access Description</th>
</tr>
</thead>
</table>
| admin         | Power Manager        | Enables administrative users (admins) to perform tasks such as:  
                          ● Create and manage user accounts, including security roles, permissions and restrictions  
                          ● Track changes and monitor locks applied to business objects in use.  
                          ● Generate Star Schema and Analytic Services databases of application data  
                          ● Configure Performance Scorecard for Shared Services.  
                          ● Migrate application data to another environment using promotion.  
                          ● Configure the Alerter, enabling users to send and receive alert notifications.  
                          ● Create, modify or delete domains  
                          ● Edit or delete annotations |
| user          | Basic                | Enables end users to perform tasks such as:  
                          ● Use the Map work area to view maps and drill down into map elements  
                          ● Use the Report work area to access data about business objects to which they have access and use notes  
                          ● Create and subscribe to alerts  
                          ● Create, edit or delete annotations |

*Note:* This role restricts access to measures and scorecards unless the user meets certain criteria. Do not apply this role to the accounts of employees who need to define frameworks, build maps, create measures, and set up scorecards.
Launching the User Management Console from Performance Scorecard

This section describes how to launch User Management Console from within Performance Scorecard.

To launch User Management Console:

1 Log on to Performance Scorecard.
2 Ensure the Shared Services server is running.
3 From Performance Scorecard, select Administration > User Management.

The User Management Console on Shared Services is displayed.

From the Shared Services User Management Console, you can perform the following tasks:

- Add and provision new users
- Modify or delete existing users
- Perform bulk provisioning of multiple users

For detailed instructions on using the Shared Services User Management console, refer to the Hyperion System 9 Shared Services User Management Guide.

<table>
<thead>
<tr>
<th>Security Role</th>
<th>Shared Services Role</th>
<th>Access Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>designer</td>
<td>Interactive</td>
<td>Enables designers to build scorecards and applications, including the following tasks:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Create frameworks and employees</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Define measures and dimensional outlines</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Build Strategy, Accountability, and Cause and Effect maps</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Enter employee and scorecard data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Create alerts and subscriptions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Create, access and reply to notes attached to application business objects to which they have access.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Assign annotation creators to a business object</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Access Performance Scorecard reports, and enter data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● View and drill down into the components of the Strategy, Accountability, and Cause and Effect maps to which they have access</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Create and subscribe to alerts, including creating public alerts and subscribing others to alerts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Run data integrations and publish data to Shared Services for use in other supported Hyperion product applications</td>
</tr>
</tbody>
</table>
Managing Permissions in Performance Scorecard

User provisioning through Shared Services requires configuration on both the Shared Services server and Performance Scorecard application. You can provision users and groups individually, or migrate existing users on Performance Scorecard to perform user provisioning on multiple users.

When you configure the application in the Configuration Utility after installing Performance Scorecard, you must use the Shared Services server, which automatically points to the Shared Services CSS.xml file for external authentication. This step enables Performance Scorecard and the Shared Services server to communicate seamlessly when provisioning users.

Note: The Shared Services Administrator must also be provisioned to the Performance Scorecard application.

You can access Shared Services through Performance Scorecard or directly, using the appropriate URL. The URL to User Management Console is in the following format:

http://<server name>.hyperion.com:<port number>/interop

An overview of the process is presented in the following table:

<table>
<thead>
<tr>
<th>Environment</th>
<th>Tasks</th>
<th>Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Configuration Utility</td>
<td>● Select Shared Services, to automatically point to the Shared Services CSS.xml file for external authentication  &lt;br&gt;● Select user provisioning through Shared Services</td>
<td>Refer to the Hyperion System 9 Performance Scorecard Installation Guide</td>
</tr>
<tr>
<td>2. Shared Services Server</td>
<td>● Create the project for Performance Scorecard and assign the application to the project.  &lt;br&gt;● Provision the users and groups on the Shared Services server and assign the appropriate security roles for the application. You can add individual users and groups, or you can migrate existing users from Performance Scorecard for bulk provisioning.</td>
<td>Refer to the Hyperion System 9 Shared Services User Management Guide</td>
</tr>
<tr>
<td>3. Performance Scorecard</td>
<td>● Synchronize Performance Scorecard users with users and groups created on Shared Services.  &lt;br&gt;● Migrate multiple users from Performance Scorecard to Shared Services server</td>
<td>&quot;Creating and Provisioning Users and Groups over Shared Services&quot; on page 135 &lt;br&gt;&quot;Migrating Performance Scorecard Users and Groups to Shared Services Security&quot; on page 139</td>
</tr>
</tbody>
</table>
Creating and Provisioning Users and Groups over Shared Services

You can provision users and groups for Performance Scorecard using Shared Services. This feature enables you to use existing user information for a number of Hyperion applications, or to provision multiple users at one time.

In order to provision users for Performance Scorecard from existing users in Shared Services, you need to select this as an option after installation, when you run the Configuration Utility, as outlined in the Hyperion System 9 Performance Scorecard Installation Guide. The Shared Services Administrator must also be provisioned to the Performance Scorecard application.

The provisioning process requires you to have both the Shared Services server and Performance Scorecard configured and running. External authentication ensures that the applications can communicate seamlessly to provision users easily and accurately. Refer to the following sections for detailed instructions:

Access Permissions

User provisioning through Shared Services requires configuration on both the Shared Services server and Performance Scorecard applications. You can provision users and groups individually, or migrate existing users on Performance Scorecard to perform user provisioning on multiple users.

When you configure the application in the Configuration Utility after installing Performance Scorecard, you must use the Shared Services server, which automatically points to the Shared Services CSS.xml file for external authentication. This step enables Performance Scorecard and the Shared Services server to communicate seamlessly when provisioning users.

Note: The Shared Services Administrator is automatically provisioned to the Performance Scorecard application.

Before You Begin

Before you create and provision users using Shared Services, ensure the following conditions have been completed:

- Performance Scorecard has been configured to use Shared Services-based provisioning, and to obtain directory definition file from Shared Services (css.xml).
- The Performance Scorecard application has been registered on Shared Services. Registration is managed through the Hyperion® Configuration Utility™, and may be performed during installation or later. For instructions on configuring and registering Performance Scorecard applications with Shared Services, refer to the Hyperion System 9 Performance Scorecard Installation Guide.
- Shared Services is running
- Performance Scorecard is running
Creating a New User or Group Using Shared Services

You can create users for Performance Scorecard through Shared Services.

To create and provision a new user from Performance Scorecard:

1. Ensure the Shared Services server is running.
2. Log on to Performance Scorecard as an Administrator.
3. From Performance Scorecard, select Administration > User Management.

   The Shared Services User Management Console is displayed.
4. From the Shared Services User Management Console, create and provision the users and groups as outlined in the Hyperion System 9 Shared Services User Management Guide.
5. After the users and groups are provisioned, from Performance Scorecard, assign Performance Scorecard user and group properties using one of the following options:
   - Assign properties individually, as outlined in “Assign Performance Scorecard Properties Individually” on page 136.
   - Assign bulk properties for all provisioned users at one time, as outlined in “Assign Bulk Properties in Performance Scorecard” on page 138.

Assign Performance Scorecard Properties Individually

After a user or group has been created and provisioned, all active directly and indirectly provisioned users and groups must be assigned Performance Scorecard-specific attributes or properties. If the users or groups are not assigned the Performance Scorecard permissions, the user logon is rejected by Performance Scorecard as an unknown user.

Individual user or group properties are created each time the properties are edited and saved on User Management Console. If this step is skipped, user logon will be rejected by Performance Scorecard due to unknown user.

To assign Performance Scorecard permissions individually:

1. Log on to Performance Scorecard as an Administrator.
2. From the View pane, select Projects, and expand the tree to select the project and application to which the newly provisioned user has been assigned.

   The Available Users and Groups list for the selected project is displayed.
3 Select the name of the newly provisioned user from the list, and click **Next**.

4 On the **Manage Properties** tab, click **Select** to select the employee.

   The Select Employee dialog box is displayed.

   5 From the Select Employee dialog box, select the name of the Performance Scorecard employee record that is to be associated with the selected user ID.

6 Optional: From the **Primary Domain** drop-down list on the **Manage Properties** tab, select a Primary Domain for the user.
7 Under the Security Roles pane, select the Performance Scorecard security role that you want to assign to the user.

For detailed information on Performance Scorecard security roles, refer to the *Hyperion System 9 Performance Scorecard Administrator’s Guide*.

8 Click Finish to complete the provisioning of the user for both Shared Services and Performance Scorecard.

**Assign Bulk Properties in Performance Scorecard**

As an alternative to assigning Performance Scorecard permissions individually, you can assign permissions to all newly provisioned users and groups at one time. The Synchronize with Shared Services button is provided on the User Account List and Group Account List page which updates Performance Scorecard with newly provisioned users or groups in Shared Services.

When you synchronize users, the following actions are initiated:

- Group synchronization is implicitly launched to ensure that associated user groups become available for the user.
- All active directly and indirectly provisioned users are pulled from Shared Services.
- The Shared Services list is compared to the Performance Scorecard User Account, matched by Logon Name (user id).
- Any missing user accounts are automatically created. The appropriate default security role is set based on directly and indirectly provisioned role (Performance Scorecard Power Manager > admin, Performance Scorecard Interactive > designer, Performance Scorecard Basic > user).
- An employee record is created and associated with each created user. The first name, last name, and e-mail ID are obtained from directory user information.
- All user accounts that are no longer provisioned in Shared Services are listed for optional deletion. The list excludes the default admin, designer, and user User Accounts.

When you synchronize groups, the following actions are initiated:

- All active directly and indirectly provisioned groups are pulled from Shared Services.
- The Shared Services list is compared to the Performance Scorecard Group Account, matched by Group Name.
- Any missing group accounts are automatically created. The appropriate default security role is set based on the directly and indirectly provisioned roles (Performance Scorecard Power Manager > admin, Performance Scorecard Interactive > designer, Performance Scorecard Basic > user).
- All group accounts that are no longer provisioned in Shared Services are listed for optional deletion.
To assign bulk Performance Scorecard permissions:

1. Log on to Performance Scorecard as an Administrator.
2. From the Object View tab, select **Security > User Account List**. The list displays all existing Performance Scorecard users and provisioned Shared Services users. For Groups, select **Security > Group Account List**.
3. On the Account List, click **Synchronize with Shared Services** to update user or group account information in Performance Scorecard with the provisioned users and groups in Shared Services. A confirmation message is displayed.
4. Click **Yes** to confirm you want to synchronize all Performance Scorecard users with users on the Shared Services server. The users and groups are synchronized, and the results are displayed on the Synchronized with Shared Services Results window. The results show the names of all users and groups that were newly provisioned, and the names of any users and groups who are no longer provisioned on Shared Services.
5. Select any users or groups that you want to delete, and complete the synchronization.

**Migrating Performance Scorecard Users and Groups to Shared Services Security**

When you have a large number of users and groups to provision through Shared Services, you can perform a one-time migration. For example, you can provision all existing members at once with the same security access. Subsequently, you can assign the properties to individual users or groups who require particular access after the main transfer.

**Caution!**
The Migration option is only available once. After you have migrated the bulk of your users and groups in this one-time operation, the option is disabled and cannot be used again.

Before performing a migration, the following tasks must be performed:

- Ensure that the Performance Scorecard Administrator exists in Shared Services, and has been assigned the security role of Provisioning Manager.
- Ensure that the Performance Scorecard application has been registered and assigned to a project in Shared Services.
- Ensure that all employee e-mail addresses are in a valid and correct format, such as `<user>@<provider>.com`. Any users with incorrect e-mail addresses will not be migrated correctly.

Refer to the **Hyperion System 9 Shared Services User Management Guide** for detailed instructions.
To migrate users and groups to Shared Services from Performance Scorecard:

1. Ensure the Shared Services server is running.
2. Log on to Performance Scorecard as an Administrator.
3. From Performance Scorecard, select **Administration > User Provisioning Migration**.
   The Shared Services Administrator For Migration page is displayed.
4. On the Shared Services Administrator for Migration page, enter the **User ID** and **Password** for the Administrator. The migration administrator must exist in Shared Services, and have been assigned as the Provisioning Manager.
5. Click **Next** to display the Pre-Migration Check page.
6. Click **Perform Pre-Migration Check** to verify existing data, and create the database tables for the migration. As the verification progresses, appropriate status messages are displayed. A message is shown when the pre-migration progress check is complete. Click **OK** to dismiss the message and continue.
7. Click **Next** to display the Externalize Users page. The page shows a list of all users in the model, their details and service provider. The Migration Action status is displayed as Migrate.
8. For each user that you DO NOT WANT to include in the migration, click Edit. The Migration dialog box is displayed.

9. From the Migration Action drop-down list, select Do Not Migrate for the selected user, then click Save. This user will not be included in the one-time migration. In future, if the user needs to be added to the Shared Services list, you must add the user individually, as outlined in “Creating and Provisioning Users and Groups over Shared Services” on page 135.
Caution! Because the Migration option is only available once, Hyperion recommends that you include as many users in the migration as possible. After you have migrated the bulk of your users in this one-time operation, the option is disabled and cannot be used again.

10 Repeat Step 9 for each user that you want to exclude from the migration.

11 **Optional:** When the list of users is complete, select the **Externalize Groups** tab to select the groups that you want to migrate. The page shows a list of all groups in the model, the details and service provider. The Migration Action status is displayed as Migrate.

12 For each group that you DO NOT WANT to include in the migration, click **Edit**. The Migration dialog box is displayed.
From the Migration Action drop-down list, select **Do Not Migrate** for the selected group, then click **Save**. This group will not be included in the one-time migration. In future, if the group needs to be added to the Shared Services list, you must add the group individually, as outlined in “Creating and Provisioning Users and Groups over Shared Services” on page 135.

**Caution!** Because the Migration option is only available once, Hyperion recommends that you include as many users in the migration as possible. After you have migrated the bulk of your users in this one-time operation, the option is disabled and cannot be used again.

Repeat Step 13 for each group that you want to exclude from the migration.

When the list of groups is complete, click **Next** to display the Migration to Shared Services page.
16 From the Migration to Shared Services page, click Test migration. A confirmation is displayed when the test migration process has been successfully completed. Click OK to dismiss the message. If a problem is indicated in the migration status messages, correct any errors and try again.

17 Click Migrate to begin the migration process. The progress of the migration is indicated by the Migration status messages. A message is displayed to advise the migration has been successfully completed.

All migrated users and groups are displayed, and have the inherited Performance Scorecard attributes for their security roles.
This appendix lists the user groups and roles for Hyperion System 9 Strategic Finance™.
User Roles

Hyperion Strategic Finance user types are described in the following topics:

- “User Types” on page 146
- “User Types and Tasks” on page 146

User Types

In Hyperion Strategic Finance, a user type determines what actions a user can perform. There are four access types in Hyperion Strategic Finance that determine the type of user and the actions that the user can perform:

- Power Manager
- Interactive User
- Basic User
- View User

User Types and Tasks

The following table describes the user types the actions that can be performed by a user of each type in Hyperion Strategic Finance:

<table>
<thead>
<tr>
<th>Access Type</th>
<th>Privileges</th>
<th>Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Manager</td>
<td>Unrestricted</td>
<td>● Add and maintain servers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Add and maintain databases</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Add and maintain users</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Add and maintain user groups</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Create and maintain entities</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Design and view reports</td>
</tr>
<tr>
<td>Interactive User</td>
<td>Restricted</td>
<td>● Create and maintain entities</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Enter data into entities</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Add scenarios</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Add subaccounts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Add dimensions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Design and view reports</td>
</tr>
<tr>
<td>Basic User</td>
<td>Restricted</td>
<td>● Enter data into entities</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Add scenarios</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Add subaccounts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● View reports</td>
</tr>
<tr>
<td>View User</td>
<td>Restricted</td>
<td>● View entities</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● View reports</td>
</tr>
</tbody>
</table>
This appendix lists the user groups and roles for Hyperion Translation Manager™.
User Roles

Hyperion Translation Manager supports two types of users, as described in the following topics:

- “Hyperion Translation Manager Administrator” on page 148
- “Hyperion Translation Manager User” on page 148

Hyperion Translation Manager Administrator

A user of the Administrator type can perform user maintenance using the Administration functionality. Administrators can perform user maintenance tasks such as adding, editing or removing users from the system. They can also manage table access rights and change ownership of tables.

Hyperion Translation Manager User

Hyperion Translation Manager users who are assigned the User role can create and publish tables of translation rules, and they can modify tables that they own. Users can also run validation data sets against the rules they have entered in tables, and they can import and export rules in the tables.
This appendix provides information that is specific to Hyperion Business Modeling™ and Shared Services User Management.

**Business Modeling User Roles**

In Hyperion Business Modeling, there are three types of users, as follows:

- “Administrator” on page 149
- “Builder” on page 150
- “End User” on page 150

The security role assigned to each Hyperion Business Modeling user determines the actions and access available to that user. Access for a group of users grants similar security access to all its members.

**Administrator**

The administrator’s role is to manage the users, security and databases for the application, both on the desktop and the Web.

On the desktop component of the application, the administrator is responsible for the following tasks:

- Setup and maintenance of databases and containers
- Creation and dropping of database tables
- Installation and configuration of the application and associated properties
- Setup and modification of authentication settings
- Setup of new users and user groups
- Maintenance of existing users and user groups
- Assignment of permissions for users to specific models and model data
- Assignment of owners to models and scenarios, if required
- Conversion of models
For the Web component of the application, the administrator is responsible for the following tasks for the Web component of the application:

- Configuration of the application and Web servers

The *Hyperion Business Modeling Installation Guide* and the *Hyperion Business Modeling Installation Checklist* describe how to install and configure the applications.

In some instances, the tasks assigned to the administrator and model builder may overlap. The *Hyperion Business Modeling Model Builder’s Guide* provides additional detail and explanation in cases where the administrator requires more information about the application.

If you are planning to import and export metadata and data between authorized Hyperion applications through Hyperion Shared Services, the administrator is also responsible to register products, set up and manage models over the Hub, and create data integrations.

### Builder

The builder or model builder is the user who actually creates the original model or enterprise model by defining all elements of the model, such as boxes, links, variables and financial values, and attaching financial data.

The builder can perform the following tasks:

- Build and update models
- Calculate models and save results to Hyperion Essbase or a relational database
- Assign permissions for users to specific models and model data
- Designate which portions of a model are available for sharing over the Web
- Play scenarios in the application and over the Web
- Generate reports in the application and over the Web
- Create integrations for the Hyperion Business Modeling Adapter.

For detailed information on building a model, refer to the *Hyperion Business Modeling Model Builder’s Guide*.

### End User

The end user’s role is an integral part of updating model periods and playing with scenarios that is available through Hyperion Business Modeling. Using business and operational knowledge to adjust parameters for the original model, the end user can experiment with the workings of the scenario over the Web to search for process improvements, time or money savings, or unexpected bottlenecks or benefits.
Based on security set by the model builder, the end user can perform the following tasks:

- Update model period data
- Modify available data to play scenarios over the Web
- Generate reports over the Web
- Compare multiple scenarios
- Save changes to forward to the model owner
- Save changes as a new scenario to be shared with other users.
Glossary

application  A reference to a single instance of an application against which users and groups are provisioned.

authentication repository/authentication directory  A centralized, corporate store of user and group information. May also be referred to as directory or provider. The security platform provides built-in support for the following providers: Lightweight Directory Access Protocol (LDAP) Directory, Windows NT LAN Manager (NTLM), and Microsoft Active Directory (MSAD).

configuration file  The security platform relies on an XML document to be configured by the product administrator or installer of the software. The XML document must be modified to indicate meaningful values for properties, specifying locations and attributes pertaining to the corporate authentication scenario.

external authentication  The process of authenticating a user ID and password on an authentication server, such as an LDAP or NTLM server, instead of authenticating with the current server or application.

identity  A unique identification of one valid user or group existing on an external authentication repository.

managed server  An application server process running in its own Java Virtual Machine (JVM).

object palette  The left-hand pane in the User Management console. Most operations are performed on objects that you select in the object palette.

project  An instance of Hyperion products that are grouped together to comprise an implementation. For example, a Planning project may consist of a Planning application, an Analytic Services application, and a Financial Reporting Server instance.

role  Determines the tasks that users can perform within an application or globally within the User Management console.

security agent  A Web access management solutions provider employed by companies to protect Web resources. It is also known as a Web security agent. The Netegrity product, SiteMinder, is an example of a security agent.

security platform  A framework providing the ability for Hyperion applications to use external authentication and single sign-on.

single sign-on  The ability of an externally-authenticated user to access multiple, linked Hyperion applications after logging on to the first application. The user can launch other applications from the first application, and from other linked Hyperion applications, without logging on again. The user's ID and password are already authenticated.

token  An encrypted identification of one valid user or group existing on an external authentication system.

user provisioning  User provisioning enables centralized management of user role assignment and accessibility to applications created under various projects of different products.

World group  The predefined group in the system. At the global level, the World group contains all users who are provisioned with at least one role in the system.
Index

A
access control
    introduction, 16
Administrator role, Shared Services, 20
aggregated roles
    creating, 42
    deleting, 44
    modifying, 43
    naming guidelines, 42
    overview, 22
    renaming, 43
Analytic High Availability Services, 65
    administrator role, 66
    migrating users, 68
    user provisioning, 67
    user role, 66
Analytic Services
    application access type, 62
    backing up security information, 63
    calculation and filter access, 60
    global Analytic Server application, 59
    launching the User Management console, 56
    migrating to Shared Services, 63
    projects, applications, and databases, 59
    synchronizing and refreshing security information from Shared Services, 63
    user management and security, 55
    user provisioning, 55
    user roles and tasks, 56
    users and groups, 60
Analytic Services Smart View Provider, 93
    administrator role, 94
    user provisioning, 94
    user roles, 94
application-level access, 31
applications
    adding to existing projects, 29
    adding to new projects, 28
    copying provisioning between, 32
    moving, 31
    overview, 19
    removing from projects, 29
    security for, 16
assigning access control, 31
audience for this guide, ix
auditing provisioning assignments, 48
authentication directories
    defined, 153
    introduction, 18
    managing, 33

B
browser problems, 25 to 26
Business, 124
Business Rules
    launching the User Management console, 128
    migrating users to Shared Services, 129
    roles, described, 128
    security for, 128
Business Modeling
    user provisioning information, 149

C
commands, Help menu, xi
configuration file, defined, 153
consulting services, xiii
context-sensitive menus, 26
copying provisioning information, 32
corporate authentication directories, 18
deleting
  aggregated roles, 44
  applications from project, 29
  native groups, 41
  native users, 36
  projects, 30
deprovisioning
  groups, 47
  users, 46
Directory Manager user role, 21
disabling
  native users, 37
  users, 37
documentation, 26
documents, accessing
  Hyperion Download Center, xi
  Hyperion Solutions Web site, xi
  Information Map, xi
  online help, xi
documentation, accessing
  Hyperion Download Center, xi
  Hyperion Solutions Web site, xi
  Information Map, xi
  online help, xi
deleting security classes, 107
launching user management console, 98
migrating users, 112
running security reports, 111
selecting security classes, 107
setting up security classes, 106
Shared Services user roles in, 98
user roles, 100
global Administrator role, 20
groups
  creating native, 38
  deleting native, 41
deprovisioning, 47
  introduction, 19
  modifying native, 39
  naming guidelines, 39
  provisioning, 46
  renaming native, 39
Help menu commands, xi
help, getting, 26
Hyperion Consulting Services, xiii
Hyperion Download Center
  accessing documents, xi
Hyperion Education Services, xiii
Hyperion Planning. See Planning
Hyperion product information, xiii
Hyperion support, xiii
Hyperion System 9 BI+
  assigning default preferences for application users and groups, 88
default functionality, 87
launching the User Management console, 72
old role mappings to new roles, 90
Provisioning Manager Shared Services role, 78
role aggregation, 78
role combinations, 85
roles, 73
  Analyst, 75
  BI+ Administrator, 78
  BI+ Global Administrator, 78
Education services, xiii
enabling
  native users, 37
tools, xii
Content Manager, 78
Content Publisher, 77
Data Editor, 74
Data Source Publisher, 76
Dynamic Reporting Viewer, 75
Explorer, 74
Favorites Distributor, 74
Interactive Reporting Viewer, 75
Job Manager, 77
Job Publisher, 76
Job Runner, 75
Manage Models, 76
Metrics Analyst, 75
Metrics Editor, 78
Metrics Viewer, 74
Personal Page Editor, 74
Personal Page Publisher, 76
Personal Parameter Editor, 74
Report Designer, 77
Schedule Manager, 78
Scheduler, 75
Smart Form Publisher, 76
Trusted Application, 79
Viewer, 74
Shared Services roles used, 72
task to role matrix, 82
User Management console tasks, 72
World Group, 89
Hyperion Technical Support, xiii
Hyperion Workforce Planning. See Workforce Planning

I
identity, defined, 153
inherited roles, 20

J
JVM errors, 26

L
LDAP, 18

M
managed server, defined, 153
managing
applications, 30
groups, 38
projects, 28
roles, 42
user directories, 33
users, 33
masthead
expanding and collapsing, 26
menus
context-sensitive, 26
migrating users to Shared Services, 19, 22
modifying
aggregated roles, 43
native groups, 39
native users, 35
projects, 29
moving applications, 31
MSAD, 18

N
naming guidelines
aggregated roles, 42
groups, 39
projects, 28
users, 34, 36
native Shared Services directory, 18
NTLM, 18

O
object palette, 26
object-level security, 31
open LDAP native directory, 18, 33

P
Performance Scorecard
access permissions, 134 to 135
assign permissions
bulk, 138
individually, 136
launching the User Management Console, 133
migrating, 139
security roles, 132
user roles, 132
users and groups, 135
Planning
access rights with Analytic Services, 121
administrator role, 117
and connection types with Analytic Services, 124
and Hyperion Application Link tasks, 118
assigning a migrated application to a Shared Services project, 125
interactive user role, 118
launching the User Management Console, 114
Manage Models user role, 123
migrating users, 124
planner user role, 119
ProvisionUsers utility, 115
registering with Shared Services, 125
returning to Planning from User Management, 114
roles and permissions, 113
security overview, 114
setting up multiple administrators, 118
synchronizing users and groups with a utility, 115
synchronizing with the User Management Console, 115
user roles, 117
user roles and tasks, 119
user roles with Business Rules, 120
view user role, 119
pop-up blockers, 25 to 26
prerequisites for using this guide, ix
product-specific access, 31
projects
adding applications to new projects, 28
creating, 28
deleting, 30
naming guidelines, 28
overview, 19
renaming, 29
provisioning
generating report on, 48
groups, 46
users, 45
Provisioning Manager user role, 21
provisioning. See user provisioning

native groups, 39
native users, 35
projects, 29
reporting
provisioning information, 48
right-click menus, 26
roles
aggregating, 42
assigning to groups, 46
assigning to users, 45
global Shared Services roles, 20
introduction, 20

S
security
product-specific, 31
security agent, defined, 153
security platform, defined, 153
Shared Services
Administrator user role, 20, 50
Create Integrations user role, 51
Directory Manager role, 21
Directory Manager user role, 50
Project Manager user role, 51
Provisioning Manager role, 21
Provisioning Manager user role, 51
roles overview, 20
Run Integrations user role, 52
user roles, 49
user tasks, 52
single sign-on, 16
Smart View Provider. See Analytic Services Smart View Provider
Strategic Finance
user provisioning information, 145

T
technical support, xiii
token, defined, 153
Translation Manager
user provisioning information, 147

U
unassigned applications, 28
user management
  system components, 17

User Management console
  described, 26

user provisioning
  copying to another application, 32
  introduction, 16
  role required, 21
  system components, 17

users
  creating native, 34
  deleting native, 36
  deprovisioning, 46
  disabling native, 37
  enabling native, 37
  introduction, 19
  migrating to Shared Services, 19, 22
  modifying native, 35
  naming guidelines, 34, 36
  provisioning, 45
  renaming native, 35

W

Workforce Planning
  user roles, 121
  user roles and tasks, 122
  user roles overview, 121

World group, 19