# Contents

**Documentation Accessibility** .......................................................... 11

**Documentation Feedback** ............................................................ 13

**Chapter 1. About Shared Services** .................................................. 15
  What Is Shared Services? ................................................................. 15
  Launching Shared Services Console ................................................. 15
  Overview of Shared Services Console ............................................. 16
  Searching for Users, Groups, Roles, and Delegated Lists ..................... 17

**Chapter 2. EPM System Security Concepts** ..................................... 19
  Security Components ........................................................................ 19
  User Authentication Components ...................................................... 19
    Native Directory ........................................................................... 20
    User Directories ........................................................................... 20
  Provisioning (Role-based Authorization) .......................................... 20
    Roles .............................................................................................. 21
      Global Roles ............................................................................... 21
      Predefined Roles ......................................................................... 21
      Aggregated Roles ........................................................................ 21
    Users .............................................................................................. 22
      Default EPM System Administrator ............................................ 22
      System Administrator .................................................................. 22
      Functional Administrators ......................................................... 22
      Groups ......................................................................................... 22

**Chapter 3. Working with Application Groups and Applications** .......... 23
  Overview .......................................................................................... 23
  Working with Application Groups ..................................................... 23
    Creating Application Groups ......................................................... 24
    Modifying Application Group Properties ....................................... 24
    Deleting Application Groups ......................................................... 25
  Managing Applications ....................................................................... 25
Chapter 4. Delegated User Management

About Delegated User Management

Hierarchy of Administrators
   System Administrator
   Functional Administrators
   Delegated Administrators

Enabling Delegated User Management Mode

Creating Delegated Administrators

Planning Steps
   User Accounts for Delegated Administrators
   Create a Delegation Plan

Provisioning Delegated Administrators

Creating Delegated Lists

Modifying Delegated Lists

Deleting Delegated Lists

Viewing Delegated Reports

Chapter 5. Managing Native Directory

About Native Directory

Default Native Directory Users and Groups

Managing Native Directory Users
   Creating Users
   Viewing and Modifying User Accounts
   Deactivating User Accounts
   Activating Inactive User Accounts
   Deleting User Accounts
   Changing Native Directory User Password

Managing Native Directory Groups
   Nested Groups
   Creating Groups
   Modifying Groups
   Deleting Groups
   Managing Roles
## Chapter 6. Managing Provisioning

- About Provisioning .................................................... 51
- Before Starting Provisioning .......................................... 51
- Overview of Provisioning Steps ........................................ 52
  - Provisioning Administrative Users ................................... 52
  - Provisioning EPM System Users .................................... 52
- Provisioning Groups ................................................... 53
  - Deprovisioning Groups ................................................. 54
- Auditing Security Activities and Lifecycle Management Artifacts ........................................ 55
- Manually Purging Audit Data ............................................ 55
- Selecting Objects for Application and Application Group-Level Audits ............................... 56
- Changing Purge Interval ................................................ 56
- Generating Reports .................................................... 57
  - Generating Provisioning Reports ..................................... 57
  - Generating Audit Reports ............................................. 58
  - Generating Migration Status Report ................................ 59
- Importing and Exporting Native Directory Data ...................................................... 60

## Chapter 7. Managing Taskflows

- About Taskflows ...................................................... 61
- Taskflow Components ................................................. 61
  - Stages ........................................................................ 61
  - Links ........................................................................ 62
  - Variables .................................................................... 63
- Prerequisites for Working with Taskflows ...................................................... 63
- Creating and Managing Taskflows ........................................ 63
  - Accessing the Manage Taskflow Screen ...................... 63
  - Creating Taskflows .................................................. 63
  - Editing Taskflows ................................................... 65
- Viewing Taskflow Information ........................................... 66
- Scheduling Taskflows .................................................. 66
- Manually Running Taskflows ........................................... 66
- Viewing Taskflow Status and Execution Details ........................................ 67
- Taskflow Scripts Location ............................................... 67
Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.
In This Chapter

What Is Shared Services? ................................................................................. 15
Launching Shared Services Console ................................................................. 15
Overview of Shared Services Console ............................................................... 16
Searching for Users, Groups, Roles, and Delegated Lists .............................. 17

What Is Shared Services?

Oracle Hyperion Shared Services, an Oracle Hyperion Foundation Services component, helps establish a secure environment for Oracle Enterprise Performance Management System products. Using Shared Services, users define and manage security for EPM System deployments. Users interact with Shared Services through Oracle Hyperion Shared Services Console.

All EPM System components depend on Shared Services to define how users are authenticated and how they are authorized to use product resources.

Launching Shared Services Console

You use a menu option in Oracle Hyperion Enterprise Performance Management Workspace to Access Shared Services Console.

▷ To launch the Shared Services Console:

1. Go to:

   http://web_server_name:port_number/workspace

   In the URL, web_server_name indicates the name of the computer where the web server used by Foundation Services is running, and port_number indicates the web server port; for example, http://myWebserver:19000/workspace.

   Note: If you are accessing EPM Workspace in secure environments, use https (not http) as the protocol and the secure web server port number. For example, use a URL such as: https://myserver:19043/workspace.

2. Click Launch Application.
Note: Pop-up blockers may prevent EPM Workspace from opening.

3 In Logon, enter your user name and password.

Initially, the only user who can access Shared Services Console is the EPM System Administrator whose user name and password were specified during the deployment process.

4 Click Log On.

5 Select Navigate, then Administer, and then Shared Services Console.

Overview of Shared Services Console

Shared Services Console comprises a View pane, also known as the Application Management pane, and task tabs. When you initially Access Shared Services Console, it displays the View pane and a Browse tab.

The View pane is a navigation frame where you can choose objects (such as Native Directory and application groups). Typically, details of the current selection in the View pane are displayed on the Browse tab. Additional task tabs open as needed, depending on the task that you perform; for example, a Report tab opens when you generate or view a report.

Depending on the current configuration, Shared Services Console lists your existing objects in the View pane. You can expand these object listings to view details. For example, you may select the User Directories node to view a list of configured user directories.

A shortcut menu, accessible by right-clicking an object, is associated with some objects in the View pane.

Shortcut menus associated with objects in the View pane provide the quickest method to perform operations on the objects. Options in shortcut menus change dynamically, depending on what you select. These options are available also on a menu in the menu bar. Buttons representing enabled menu options are displayed on the toolbar.

Note: Because Native Directory is administered from Shared Services Console, some menu options available in the shortcut menu for Native Directory are not available for other user directories.

The following features are available through Shared Services Console:

- User directory configurations
- Single sign-on configuration
- Native Directory management
- Role-based access control management of users
- Audit configuration and report management
- Access to Oracle Hyperion Enterprise Performance Management System Lifecycle Management and product artifact exploration
Searching for Users, Groups, Roles, and Delegated Lists

Shared Services Console enables searching for users and groups from configured user directories, and for application roles registered with Shared Services.

When searching for users, the search parameters that you can specify depend on the type of user directory you select. For example, in Native Directory, you can search for all users, active users, and inactive users.

Search boxes displayed on the Browse tab reflect the search context based on the selection in the View pane.

To search for users, groups, roles, or delegated lists:

1. In the View pane, expand User Directories.

2. From the user directory that you want to search, select one of the following:
   - Users
   - Groups
   - Roles
   - Delegated List

   **Note:** Roles and Delegated List are available only in Native Directory searches.

   Delegated List is available only if Shared Services is in Delegated Administration mode. See Chapter 4, “Delegated User Management” for detailed information.

   Available search fields are displayed on the Browse tab.

3. **To search for users:**
   a. In User Property, select a user property to search.

      The user properties that you can select depend on the type of the user directory you selected. For example, you can search user name, first name, last name, description, and email address. In Native Directory, you can search for all users, active users, or inactive users, an option that is not available while searching for users in other user directories. Except in searches using the wildcard (asterisk), records for which this property value is not set are not searched.

      Searchable user properties:
      - **LDAP-based user directories:** User name, first name, last name, description, and email address
      - **Database providers:** User name

   b. **Optional:** In User Filter, specify a filter for identifying specific users. Use an asterisk (*) as the wildcard in pattern searches.
c. Optional: In **Group(s)**, specify groups in which the search is to be performed. Use an asterisk (*) as the wildcard in pattern searches. To search multiple groups, use a semicolon to separate group names.

d. Native Directory only: From **View**, select a search context (**All**, **Active**, or **Inactive**).

e. In **Page Size**, select the number of records to display in a search result page.

f. Click **Search**.

4 To search for groups:

a. In **Group Property** select a property to search.

   **Note:** Shared Services considers Oracle and SQL Server roles as equivalent to groups in user directories. Shared Services considers each role in a nested Oracle database role as a separate group that can be provisioned individually. Shared Services does not honor relationships between nested database roles.

b. Optional: In **Group Filter**, enter a filter to limit the search. Use an asterisk (*) as the wildcard in pattern searches.

c. Click **Search**.

5 To search for roles:

Role search is supported only for Native Directory.

a. In **Role Property**, select the property to search. Records for which this property value is not set in Native Directory are not searched except in a search using the wildcard (asterisk).

b. Optional: In **Role Filter**, enter a filter to limit the search. Use an asterisk (*) as the wildcard in pattern searches.

c. Click **Search**.

6 To search for delegated lists:

a. In **List Name**, enter a search string. Use an asterisk (*) as the wildcard in pattern searches.

b. Click **Search**.
In This Chapter

Security Components ................................................................. 19
User Authentication Components .............................................. 19
Provisioning (Role-based Authorization) .................................... 20

Security Components

EPM System security comprises two complementary layers that control user access and permissions:

- “User Authentication Components” on page 19
- “Provisioning (Role-based Authorization)” on page 20

User Authentication Components

EPM System users must be authenticated before their provisioning data is checked to determine the EPM System components that they can access. By default, users enter a user name and password into a login screen to gain single sign-on (SSO) access to all EPM System components for which they are provisioned.

SSO is a session and user-authentication process that enables EPM System product users to enter credentials only once, at the beginning of a session, to access multiple products. SSO eliminates the need to log in separately to each product to which the user has access.

To enhance security, EPM System components may be protected using security agents that can pass preauthenticated users to EPM System. Additionally, EPM System security can be enhanced by using other mechanisms such as client certificate authentication, custom Java authentication, and Kerberos. For detailed information on establishing a secure infrastructure for EPM System, see the Oracle Enterprise Performance Management System Security Configuration Guide.

EPM System components check authenticated user credentials against configured user directories. User authentication, along with component-specific provisioning, grants the user access to EPM System components. Provisioning Managers grant users access to artifacts belonging to EPM System components.

The following sections describe the components that support SSO:
Native Directory

Native Directory refers to the relational database that Shared Services uses to support provisioning and to store seed data such as default user account, and additional users and groups that you create.

Native Directory functions:
- Maintains and manages the native user accounts
- Maintains and manages the native group accounts
- Central storage for all EPM System provisioning information; it stores the relationships among groups, roles, and applications

An administrator account, with the default name admin, is created during the deployment process to create a System Administrator who manages EPM System security. This is the most powerful EPM System account. The user name and password of this account is set during Foundation Services deployment.

Directory Managers access and manage Native Directory using the Shared Services Console. See Chapter 5, “Managing Native Directory”.

User Directories

User directories refer to any corporate user and identity management system that is compatible with EPM System components.

EPM System components are supported on several user directories, including LDAP-based user directories, and Relational databases. User directories other than Native Directory are referred to as external user directories throughout this document. Only Administrators are permitted to manage external user directories.

Provisioning (Role-based Authorization)

EPM System security determines user access to applications using the concept of roles. Roles are permissions that determine user access to functions within EPM System components. Some EPM System components enforce object-level ACLs to further refine user access to their artifacts such as reports and members.

Each EPM System component provides several default roles tailored to various business needs. Applications belonging to an EPM System component inherits these roles. Predefined roles from the applications registered with Shared Services are displayed in the Shared Services Console.
To facilitate provisioning, you may create custom Native Directory roles that aggregate the default roles to suit specific requirements. The process of granting roles and object ACLs belonging to EPM System applications to users and groups is called provisioning.

Native Directory and configured user directories are sources for user and group information for provisioning.

After a user is authenticated, the EPM System component that the user attempted to access determines the user's groups. It then retrieves the user's provisioning data to determine the EPM System application roles that are applicable to the user. Additional data or object access security may be handled through finer permissions defined within the application.

Role-based provisioning of EPM System products uses these concepts.

**Roles**

A role is a construct that defines the authorizations to use an EPM System component feature. It is different from an access control list, which generally specifies access permissions for a specific resource or object of the application.

Access to EPM System application resources is restricted; users can access them only after a role that provides access is assigned to the user or to the group to which the user belongs.

Access restrictions based on roles enable functional administrators to control and manage application access. See Appendix A, “EPM System Roles.”

**Global Roles**

Global roles, Shared Services roles that span multiple components, enable users to perform certain tasks across products. These roles, managed by Shared Services, cannot be deleted. See “Foundation Services Roles” on page 137 for a list of global roles.

**Predefined Roles**

Predefined roles are built-in roles in EPM System components; you cannot delete them. Each application instance of an EPM System component inherits all the predefined product roles. These roles, for each application, are registered with Shared Services when you create and register the application. See Appendix A, “EPM System Roles”, for a list of predefined roles.

**Aggregated Roles**

Aggregated roles, also known as custom roles, aggregate multiple predefined application roles. An aggregated role can contain other aggregated roles. For example, a Provisioning Manager of an Oracle Hyperion Planning application can create an aggregated role that combines the Planner and View User roles of that application. Aggregating roles can simplify the administration of applications that have several granular roles. Global Shared Services roles can be included in aggregated roles. You cannot create an aggregated role that spans applications or EPM System components.
Users

User directories—Native Directory and corporate user directories—are the source for users who can access EPM System components. The authentication and the authorization processes utilize user information.

You can create and manage Native Directory users only from Shared Services Console. Users from all configured user directories are visible from Shared Services Console. Although users can be individually provisioned to grant access rights on the EPM System applications registered with Shared Services, Oracle does not recommend provisioning individual users.

Default EPM System Administrator

An administrator account, with the default name admin, is created in Native Directory during the deployment process. This is the most powerful EPM System account and should be used only to set up a System Administrator, who is the Information Technology expert tasked with managing EPM System security and environment.

System Administrator

The System Administrator, typically a corporate Information Technology expert, is responsible for setting up and maintaining a secure environment for EPM System.

Functional Administrators

The Functional Administrator is a corporate user who is an EPM System expert. Typically, this user is defined in the corporate directory that is configured in Shared Services as an external user directory.

The System Administrator creates EPM System Functional Administrators who perform EPM System administration tasks such as creating other functional administrators, setting up delegated administration, and creating and provisioning applications and artifacts.

Groups

Groups are containers for users or other groups. You can create and manage Native Directory groups from Shared Services Console. Groups and users from configured user directories can be assigned as members of Native Directory groups. You can provision these groups to grant permissions for EPM System products registered with Shared Services.
Overview

Application groups and applications are important EPM System concepts. An application is a reference to one instance of an EPM System component that is registered with Shared Services. Provisioning activities are performed against an application. Generally, applications are grouped into application groups.

Working with Application Groups

Generally, EPM System places a deployed application instance in an existing application group of your choice or into the default application group.

An application group is a container for EPM System applications. For example, an application group may contain a Planning application and Oracle Hyperion Reporting and Analysis applications. While an application can belong to only one application group, an application group can contain multiple applications.

Generally, EPM System components place their applications into their own application groups. If an EPM System component does not create its own application group, the user registering the application can select an application group; for example, Default Application Group, to organize the applications. Applications that are registered with Shared Services but are not yet added to an application group are listed under the Default Application Group node in the View pane. Provisioning Managers can provision users and groups with roles from applications listed in the Default Application Group node.

Topics detailing application group management tasks:

- “Creating Application Groups” on page 24
- “Modifying Application Group Properties” on page 24
- “Deleting Application Groups” on page 25
Creating Application Groups

During application group creation, you can also assign applications to the new application group.

To create an application group:

1. Access Shared Services Console as a Functional Administrator.
   
   See “Launching Shared Services Console” on page 15.

2. In the View pane, right-click **Application Groups**, and then select **New Application Group**.

3. In Name, enter a unique application group name, and then, in Description, enter an optional description.

   Application group names are case-sensitive. For example, **Test_1**, **TEst_1**, and **test_1** are unique group names.

4. To assign applications to this application group:
   
   a. From **List Applications in Application Group**, select an application group that contains the application that you want to assign.
   
   b. Click **Update List**. The Available Applications list displays the applications that you can assign to the application group.
   
   c. From **Available Applications**, select the applications to assign to the application group, and then click ➤.
   
   d. To remove an assigned application, from **Assigned Applications**, select the application to remove, and then click ✖.

5. Click **Finish**.

6. Click **Create Another** to create another application group, or click **OK** to close the status screen.

Modifying Application Group Properties

You can modify all properties and settings of an application group, including application assignments.

Note: Functional Administrators can also add applications to application groups by moving them from another application group. See “Moving Applications” on page 26.

To modify an application group:

1. Access Shared Services Console as a Functional Administrator.
   
   See “Launching Shared Services Console” on page 15.
2 In the View pane, right-click an application group, and then select Open.

3 Modify the application group properties as needed. See step 4 on page 24 for information on assigning or removing applications.

   **Note:** Applications that you remove from a group are automatically reassigned to the Default Application Group.

4 Click Save.

### Deleting Application Groups

Deleting an application group removes the association of applications with the application group and deletes the application group but does not remove provisioning assignments from applications.

You cannot delete the following application groups:

- Default Application Group
- Foundation
- File System

To delete an application group:

1 Access Shared Services Console as Functional Administrator.
   
   See “Launching Shared Services Console” on page 15.

2 In the View pane, right-click the application group, and then select Delete.

   **Note:** Applications that are assigned to the application group are automatically reassigned to the Default Application Group.

3 Click Yes.

4 Click OK.

### Managing Applications

Shared Services tracks registered EPM System applications.

Generally, application instances are registered with Shared Services during the deployment process.

Registration of some applications creates application groups and assigns applications to them. If registration does not create an application group, then the application is listed under Default Application Group. Provisioning Managers can provision these applications. When a Functional Administrator moves applications from Default Application Group to another application group, Shared Services retains the provisioning information.

Topics addressing application management tasks:
Moving Applications

Functional Administrators can move applications from one application group to another without losing provisioning data. Moving an application from an application group removes the association between the application and the application group.

Note: Shared Services and Deployment Metadata application cannot be moved from the Foundation application group.

To move an application:

1. Access Shared Services Console as Functional Administrator.
   See “Launching Shared Services Console” on page 15.
2. Expand the node of the application group that contains the application that you want to move.
3. Right-click the application and select Move To.
4. On Move To, select the application group to which you want to move the application.
5. Click Save.

Copying Provisioning Information Across Applications

Functional Administrators can copy provisioning information across EPM System application instances; for example, from one Planning application to another. When Provisioning Managers copy provisioning information, all user, group, and role information is copied to the target application. Artifact provisioning information cannot be copied across applications.

To copy provisioning information across applications:

1. Access Shared Services Console as Provisioning Manager or Functional Administrator.
   See “Launching Shared Services Console” on page 15.
2. In the View pane, expand the node of the application group that contains the application from which you want to copy provisioning information.
3. Right-click the application from which you want to copy provisioning information, and then select Copy Provisioning.

   Copy Provisioning opens. This tab lists the target application to which you can copy provisioning information.
4. Select the destination application.
Deleting Multiple Applications

When Functional Administrators delete applications, the provisioning information also is deleted.

To delete applications:
1. Access Shared Services Console as Functional Administrator.
   See “Launching Shared Services Console” on page 15.
2. In the View pane, right-click Application Groups and then select Delete.
3. Select the applications to delete. To delete all applications within an application group, select the application group.

   Note: You cannot delete application groups from this screen. See “Deleting Application Groups” on page 25.
4. Click Delete.
5. Click OK.

Deleting an Application

Functional Administrators can delete applications from application groups. When you delete an application from an application group, all provisioning information for that application is removed.

To delete an application:
1. Access Shared Services Console as Functional Administrator.
   See “Launching Shared Services Console” on page 15.
2. In the View pane, expand the node of the application group that contains the application that you want to delete.
3. Right-click the application, and then select Delete.
4. Click OK.

 Provisioning Essbase Application Artifacts

EPM System enforces application- and artifact-level provisioning to ensure application and data security. Access to each EPM System application is restricted by provisioning users and groups with application roles. Typically, a Provisioning Manager uses the Shared Services Console to provision users and groups to EPM System applications.
Some EPM System applications create their own artifacts; for example, reports and calculation scripts that belong only to the application. In most cases, access to application artifacts can be controlled by provisioning application users and groups. For example, a user creates filters and calculation scripts for an Oracle Essbase application using the Oracle Essbase Administration Services Console or MaxL. A Provisioning Manager for the Essbase application can use the Shared Services Console to provision these filters and calculation scripts.

Provisioning Managers can provision groups with roles from the applications for which they are defined as provisioning manager. Generally, the owner of the application (the user of who created and registered the application with Foundation Services) is automatically granted the Provisioning Manager role of the application.

Before starting this procedure, ensure that the required servers and applications are running.

1. Access Shared Services Console as Provisioning Manager.
   See “Launching Shared Services Console” on page 15.

2. In the View pane, expand the application group that contains the application for which you want to assign access permissions.

3. Right-click the application and select Assign Access Control. This option is available only for applications for which access permissions can be set.

   Note: If the application is not running, an error message is displayed when you select the application. Start the application and refresh the View pane by clicking View, and then Refresh to access the application.

4. Assign access permissions. See Appendix A, “EPM System Roles” for a list of product roles.

Exploring Applications

The Lifecycle Management interface in Shared Services Console enables you to view, search, export, and import application artifacts. The artifacts are sorted into categories so that they are exposed in an organized manner. See the Oracle Enterprise Performance Management System Lifecycle Management Guide.
Delegated User Management

In This Chapter

- About Delegated User Management ................................................................. 29
- Hierarchy of Administrators ............................................................................. 29
- Enabling Delegated User Management Mode .................................................. 30
- Creating Delegated Administrators ................................................................. 31

About Delegated User Management

Delegated user management enables creating a hierarchy of administrators for EPM System products. This feature allows the Shared Services Administrator to delegate the responsibility of managing users and groups to other administrators who are granted restricted access to manage users and groups for which they are responsible.

Only users with the Shared Services Administrator role can view all EPM System products users and groups. Delegated Administrators can view and administer only the users and groups for which they are responsible. Also, Delegated Administrators can perform only the administrative tasks permitted by their assigned roles.

Hierarchy of Administrators

Three tiers of administrators—System Administrator, Functional Administrators, and Delegated Administrators—exist in delegated administration mode.

System Administrator

System Administrators are Information technology experts who are tasked with managing EPM System security and system environment.

Functional Administrators

The System Administrator creates Functional Administrators by provisioning a corporate user with the LCM Administrator role of Foundation Services and the Administrator role of each deployed EPM System component. This Functional Administrator can perform all provisioning activities across applications.
The Functional Administrator can create other Functional Administrators with more limited access within EPM System. For example, to administer Planning application PlanApp1, the Functional Administrator may provision a user with the LCM Administrator role of Foundation Services and the Administrator role of the Planning application PlanApp1.

**Delegated Administrators**

Delegated Administrators have limited administrator-level access to EPM System components. They can access only the users and groups for which they are granted Administrator access, dividing user and group management tasks across multiple administrators.

The scope of actions that Delegated Administrators can perform on EPM System components is controlled by the access rights that the Functional Administrator granted them through provisioning. For example, assume that a Delegated Administrator is granted the Directory Manager global role in Shared Services, enabling the user to create users and groups in Native Directory. Without additional roles, this Delegated Administrator cannot view a list of users and groups that other administrators created. Further, Delegated Administrators require additional roles to view the users that they create.

**Enabling Delegated User Management Mode**

The default Shared Services deployment does not support delegated administration. You must enable Delegated User Management mode for Shared Services before you can create Delegated Administrators. Additional screens and menu options become available after you switch to Delegated User Management mode.

In Delegated User Management mode, the scope of the roles assigned to Delegated Administrators is restricted to the users and groups in their delegated list. Reverting to the default mode removes the restrictions and restores the original scope of the role. For example, assume that user del_admin1, who is assigned the Essbase Provisioning Manager role, is the delegated administrator for Esb_group1 and Esb_group2. Reverting to the default mode makes del_admin1 an Essbase Provisioning Manager for all users and groups.

To enable Delegated User Management mode:

1. Access Shared Services Console as the Functional Administrator. See “Launching Shared Services Console” on page 15.
2. From Administration, select Configure User Directories.
3. Select Security Options, and then Show Advanced Options.
5. Click OK.
6. Click OK.
7. Restart Foundation Services and other EPM System components.
Creating Delegated Administrators

- “Planning Steps” on page 31
- “Provisioning Delegated Administrators” on page 31
- “Creating Delegated Lists” on page 32
- “Viewing Delegated Reports” on page 35

Planning Steps

- “User Accounts for Delegated Administrators” on page 31
- “Create a Delegation Plan” on page 31

User Accounts for Delegated Administrators

The Functional Administrator creates Delegated Administrators from user accounts in the user directories configured in Shared Services. Unlike in provisioning, delegated administration capabilities cannot be assigned to groups. Before starting the process of delegating Shared Services administration, verify that Delegated Administrators are created as users in a configured user directory.

Create a Delegation Plan

The delegation plan should identify the Delegated Administrators needed to effectively administer EPM System components and the tasks that they should be allowed to perform. The plan should identify these users, groups, and roles:

- Users and groups that each Delegated Administrator should manage. This list can be used while creating Delegated Lists. See “Creating Delegated Lists” on page 32.
- Shared Services and EPM System product roles that each Delegated Administrator should be granted

Provisioning Delegated Administrators

The Functional Administrator provisions Delegated Administrators by granting them roles based on the delegation plan, which defines the activities they should perform. See “Foundation Services Roles” on page 137.

Delegated Administrators can be granted roles from EPM System products; for example, Provisioning Manager from Planning, to allow them to perform administrative tasks in EPM System products.
Creating Delegated Lists

Delegated lists identify the users and groups that a Delegated Administrator can manage. Each list is assigned to one or more Delegated Administrators, who can perform the following tasks:

- View only the users and groups assigned to them through delegated lists. All other users and groups remain hidden from them.
- Create delegated lists for other users that they manage.
- Search and retrieve only the users and groups that are included in their delegated lists.

**Note:** Shared Services displays the Delegated List node only if the current user is assigned to manage delegated lists.

The users and groups that a Delegated Administrator creates are not automatically assigned to the administrator who created them. The Functional Administrator must add these users and groups to delegated lists before Delegated Administrators can access them. Delegated Administrators, however, can assign these users and groups to the delegated lists that they create.

To create delegated lists:

1. Access Shared Services Console. See "Launching Shared Services Console" on page 15.
2. Under Native Directory in View pane, right-click Delegated List, and then select New Delegated.
3. On General, enter a unique delegated list name and an optional description.
4. **Optional:** To add groups that the Delegated Administrator assigned to this list can administer, click Next.
   - **Group Members** is displayed.
     a. In Directory, select the user directory from which groups are to be displayed. If you are a Delegated Administrator, only groups assigned to you can be searched.
     b. Select a group attribute (group name or description) that you want to search in the drop-down list, and enter a search filter.
     c. Click Search.
     d. From Available Groups, select groups.
     e. Click ➡️.

   **Note:** Shared Services considers Oracle and SQL Server database roles the equivalents of groups in user directories.
   - Oracle database roles can be hierarchical.
   - SQL Server database roles cannot be nested.

5. **Optional:** From Assigned Groups, select a group, and then click ✗ to unassign a group.
6. **Optional:** Click Next to add users that the Delegated Administrator of this list can administer.
**User Members** is displayed.

a. In **Directory**, select the user directory from which users are to be displayed. If you are a Delegated Administrator, the search lists only the users assigned to you.

b. Select a user attribute that you want to search in the drop-down list, and enter a search filter.

c. Click **Search**.

d. From **Available Users**, select users.

e. Click ➤

The selected users are listed in **Assigned Users**.

f. **Optional:** From **Assigned Users**, select a user, and then click to unassign a user.

**Note:** The Delegated Administrator of the list is automatically added as a user.

6 **Optional:** Click **Next** to assign Delegated Administrators for this list.

**Managed By** is displayed.

a. In **Directory**, select the user directory from which users are to be displayed.

b. Select a user attribute that you want to search in the drop-down list, and enter a search filter.

c. Click **Search**.

d. From **Available Users**, select users.

e. Click ➤

The selected users are listed in **Assigned Users**.

f. **Optional:** From **Assigned Users**, select a user, and then click to unassign a user.

**Note:** The user who creates the list is automatically added as a Delegated Administrator of the list.

7 Click **Finish**.

8 Click **Create Another** to define another list, or **OK** to close the **Create Delegated List** screen.

**Modifying Delegated Lists**

Delegated Administrators can modify only the lists assigned to them. Functional Administrators can modify all delegated lists.

- To modify delegated lists:

  1. **Access Shared Services Console.** See “Launching Shared Services Console” on page 15.

  2. **Select Delegated Lists** from the **Native Directory** node in the View pane.
3. **Search for the delegated list to modify.**

   See “Searching for Users, Groups, Roles, and Delegated Lists” on page 17.

   Delegated lists that meet the search criterion are listed on the Browse tab.

4. **Right-click the delegated list, and then select Properties.**

5. **Optional:** On General, modify the list name and description.

6. **Optional:** Click Group Members to modify group assignments.

   a. In **Directory**, select the user directory from which groups are to be displayed. If you are a Delegated Administrator, only groups assigned to you can be searched.

   b. Select a group attribute (group name or description) that you want to search in the drop-down list, and enter a search filter.

   c. Click **Search**.

   d. From **Available Groups**, select groups.

   e. Click **>`**

   **Note:** Shared Services considers Oracle and SQL Server database roles the equivalents of groups in user directories.

   Oracle database roles can be hierarchical.

   SQL Server database roles cannot be nested.

   f. **Optional:** From **Assigned Groups**, select a group, and then click **>`** to unassign a group.

7. **Optional:** Click User Members to modify user assignments.

   a. In **Directory**, select the user directory from which users are to be displayed. If you are a Delegated Administrator, the search lists only the users assigned to you.

   b. Select a user attribute that you want to search in the drop-down list, and enter a search filter.

   c. Click **Search**.

   d. From **Available Users**, select users.

   e. Click **>`**

   The selected users are listed in **Assigned Users**.

   f. **Optional:** From **Assigned Users**, select a user, and then click **>`** to unassign a user.

8. **Optional:** Click Managed By to modify Delegated Administrator assignment.

   a. In **Directory**, select the user directory from which users are to be displayed.

   b. Select a user attribute that you want to search in the drop-down list, and enter a search filter.

   c. Click **Search**.

   d. From **Available Users**, select users.
e. Click ➡️.

The selected users are listed in Assigned Users.

f. Optional: From Assigned Users, select a user, and then click ❌ to unassign a user.

9 Click OK.

10 Click OK.

Deleting Delegated Lists

To delete delegated lists:

1 Access Shared Services Console. See “Launching Shared Services Console” on page 15.

2 Select Delegated Lists from the Native Directory node in the View pane.

3 Search for the delegated list to modify.

   See “Searching for Users, Groups, Roles, and Delegated Lists” on page 17.

   Delegated lists that meet the search criterion are listed on the Browse tab.

4 Right-click the delegated list, and then select Delete.

5 Click Yes.

6 Click OK.

Viewing Delegated Reports

Delegated reports contain information about the users and groups assigned to the selected delegated lists and the delegated administrators to whom the list is assigned.

Functional Administrators can generate and view delegated reports on all delegated lists. Delegated Administrators can generate reports on the delegated lists that they created and on the delegated lists assigned to them.

To view delegated reports:

1 Access Shared Services Console. See “Launching Shared Services Console” on page 15.

2 In Native Directory node in the View pane, right-click Delegated List, and then select View Delegated Report.

3 In Delegated List Name, enter the name of the list for which the report is to be generated. Use * as wildcard for pattern searches.

4 In Managed By, enter the user ID of the Delegated Administrator whose assignments in the specified list are to be reported. Use * as the wildcard for pattern searches.

5 Click Create.

6 Click OK to close the report or Print Preview to preview the report.

   If you preview the report:
a. Click **Print** to print the report.

b. Click **Close** to close the View Report window.
About Native Directory

Native Directory is a relational database that stores user provisioning data and product registration data.

Shared Services Console is the administrative interface for Native Directory. Shared Services Console displays a list of EPM System users and groups derived from configured user directory, including Native Directory. These users and groups are used in provisioning.

Caution! You can create and provision Native Directory users to support your development and testing efforts. EPM System does not support password policies for Native Directory users. Because the use of Native Directory users with weak passwords in a production environment may pose a security risk, such users must be used for development and testing purposes only. Native Directory users should be disabled or deleted in production environments.

Default Native Directory Users and Groups

Native Directory, by default, contains the default administrator account (suggested default user name is admin). This account is used to create a System Administrator who is responsible for maintaining EPM System security and system environment.

The System Administrator creates Functional Administrators who perform all Native Directory and Shared Services administration tasks.

All EPM System users, whether defined in Native Directory or in an external user directory, belong to the WORLD group, the only default Native Directory group. WORLD is a logical group. All Shared Services users inherit the roles assigned to this group. A user gets the sum of
all permissions assigned directly to that user as well as those assigned to the user’s groups (including the WORLD group).

If Shared Services is deployed in delegated mode, the WORLD group contains groups as well as users. If the delegated list of a user contains the WORLD group, then the user can retrieve all users and groups during searches.

Managing Native Directory Users

Functional Administrators or Directory Managers can perform some of the following tasks to manage Native Directory user accounts:

- “Creating Users” on page 38
- “Viewing and Modifying User Accounts” on page 39
- “Deactivating User Accounts” on page 40
- “Deleting User Accounts ” on page 41
- “Provisioning Groups” on page 53
- “Deprovisioning Groups” on page 54
- “Generating Provisioning Reports” on page 57

Note: Users in external user directories cannot be managed from Shared Services Console.

Creating Users

To create users:

1. Access Shared Services Console as a Functional Administrator or Directory Manager. See “Launching Shared Services Console” on page 15.
2. In the Native Directory node in the View pane, right-click Users, and then select New User.
3. In Create User, enter the required information.

<table>
<thead>
<tr>
<th>Table 1</th>
<th>Create User Screen</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Label</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>User Name</strong></td>
<td>A unique user identifier (maximum 256 characters) that follows the naming conventions of your organization (for example, first_name initial followed by the last name, as in jyoung)</td>
</tr>
<tr>
<td></td>
<td>User names can contain any number or combination of characters.</td>
</tr>
<tr>
<td></td>
<td>You cannot create identical user names, including names that are differentiated only by number of spaces. For example, you cannot create user names user 1 (with one space between user and 1) and user 1 (with two spaces between user and 1).</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Passwords are case-sensitive and can contain any combination of characters.</td>
</tr>
<tr>
<td><strong>Confirm Password</strong></td>
<td>Re-enter password.</td>
</tr>
<tr>
<td>Label</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>First Name</td>
<td>User's first name (optional)</td>
</tr>
<tr>
<td>Last Name</td>
<td>User's last name (optional)</td>
</tr>
<tr>
<td>Description</td>
<td>User's description (optional)</td>
</tr>
<tr>
<td>Email Address</td>
<td>User's email address (optional). The email server domain extension; for example, .com, .org, and .gov, cannot contain more than four characters.</td>
</tr>
</tbody>
</table>

4 **Optional:** To assign the user to Native Directory groups, click **Next**.
   
a. Using the fields above the **Available Groups** list, search for groups.
   
i. From the drop-down list, select **Group Name** to search based on group names. Select **Description** to search based on group descriptions.
   
   ii. Enter the criterion for retrieving groups. Use * (asterisk) as the wildcard to retrieve all available groups.
   
   iii. Click **Search**.
   
      Groups that match the search criterion are listed under **Available Groups**.
   
b. From **Available Groups**, select groups.
   
c. Click [ ]
   
   The selected groups are listed under **Assigned Groups** list.
   
d. **Optional:** To retrieve and assign additional groups, repeat step 4.a.
   
   Using the fields above the **Assigned Groups** list, you can search assigned groups to identify the groups that you want to remove. For instructions on searching within assigned groups, see step 4.a.
   
   To remove assigned groups, from **Assigned Groups**, select the groups to remove, and then click [ ].

5 Click **Finish**.

6 Click **Create Another** to create another user or **Finish** to close Create User.

**Viewing and Modifying User Accounts**

Functional Administrators and Directory Managers can view and modify any property of Native Directory user accounts, including the user name of the System Administrator account that you created while deploying EPM System.

Native Directory users who are not administrators can view their information but cannot modify it.

➢ To view and modify user information:

1 **Access Shared Services Console as a Functional Administrator or Directory Manager.** See “Launching Shared Services Console” on page 15.
2 From the Native Directory node in the View pane, select Users.

3 Search for the user account. See “Searching for Users, Groups, Roles, and Delegated Lists” on page 17.

4 Right-click the user account to modify and select Properties.

   **Note:** User Properties displays the **Delegated List** if Shared Services is deployed in Delegated Administration mode.

5 On General, modify user properties.

   See Table 1 for descriptions of the properties that you can modify.

6 **Optional:** Modify the user's associations with Native Directory groups.

   a. Click **Member Of**.

   b. Using the fields above **Available Groups**, search for groups.

      i. From the drop-down list, select **Group Name** to search based on group names. Select **Description** to search based on group descriptions.

      ii. Enter the criterion for retrieving groups. Use * (asterisk) as the wildcard to retrieve all available groups.

      iii. Click **Search**.

         Groups that match the search criterion are listed under **Available Groups**.

   c. From **Available Groups**, select groups.

   d. Click **»**.

      The selected groups are listed under **Assigned Groups**.

   e. **Optional:** To retrieve and assign additional groups, repeat step 6.b.

      Using the fields above the **Assigned Groups** list, you can search assigned groups to identify the groups that you want to remove. For instructions on searching within assigned groups, see step 6.b.

      To remove assigned groups, from **Assigned Groups**, select the groups to remove, and then click **X**.

7 **Optional:** Click **Delegated List** to view the user's delegated list assignment.

8 Click **Finish**.

**Deactivating User Accounts**

You can deactivate Native Directory user accounts that should not have access to EPM System applications. Account deactivations are, typically, temporary suspensions that the Shared Services administrator intends to reactivate.

- Inactive user accounts cannot be used to log on to EPM System applications, including Shared Services Console.
Group associations of inactive accounts are maintained and remain visible to Functional Administrators.

Role associations of inactive accounts are maintained.

Inactive user accounts are not displayed on the product-specific access-control screens.

Inactive user accounts are not deleted from Native Directory.

**Note:** A user who is provisioned with the LCM Administrator role can deactivate other administrators, including the System Administrator.

To deactivate user accounts:

1. Access Shared Services Console as a Functional Administrator or Directory Manager. See “Launching Shared Services Console” on page 15.
2. Search for Native Directory users to deactivate. See “Searching for Users, Groups, Roles, and Delegated Lists” on page 17.
3. Right-click the user account, and then select Deactivate.
4. Click OK.

**Activating Inactive User Accounts**

Activating inactive Native Directory user accounts reinstates associations that existed before the accounts were deactivated. If a group of which the inactive user account was a member was deleted, the roles granted through the deleted group are not reinstated.

**Note:** Deactivated System Administrator and Functional Administrator accounts can be activated only by another administrator.

To activate deactivated user accounts:

1. Access Shared Services Console as a Functional Administrator or Directory Manager. See “Launching Shared Services Console” on page 15.
2. Search for Native Directory users to reactivate. See “Searching for Users, Groups, Roles, and Delegated Lists” on page 17.
3. Right-click the user account and select Activate.
4. Click OK.

**Deleting User Accounts**

Deleting a user account removes the user’s associations with Native Directory groups, the role assignments of the user, and the user account from Native Directory.
Note: The System Administrator account (by default, admin) cannot be deleted.

To delete user accounts:

1 Access Shared Services Console as a Functional Administrator or Directory Manager. See “Launching Shared Services Console” on page 15.

2 Search for Native Directory users to delete. See “Searching for Users, Groups, Roles, and Delegated Lists” on page 17.

3 Right-click the user account, and then select Delete.

4 Click Yes.

5 Click OK.

Changing Native Directory User Password

Because Native Directory account is segregated from the user accounts created to support other corporate applications, password changes affect only EPM System products.

To change Native Directory password of the current user:

1 Launch EPM Workspace. See “Launching Shared Services Console” on page 15.

2 Select Tools, and then Change Password.

3 In Current Password, enter your password.

4 In New Password and Confirm Password, enter the new password.

5 Click Save.

Managing Native Directory Groups

Native Directory users can be grouped based on common characteristics. For example, users can be categorized into groups such as staff, managers, and sales based on function, and Sales_West and Managers_HQ based on location. A user can belong to many groups.

Native Directory groups can contain other groups and users from user directories configured on Shared Services.

Group affiliations of a user are important considerations in the authorization process. Typically groups, rather than individual user accounts, are used to facilitate provisioning.

Tasks performed by Functional Administrators and Directory Managers:

- “Creating Groups” on page 43
- “Modifying Groups” on page 45
- “Deleting Groups” on page 46
- “Provisioning Groups” on page 53
- “Deprovisioning Groups” on page 54
Note: Groups on external user directories cannot be managed from Shared Services Console.

Nested Groups

Nested groups are groups that are members of other groups (parent groups). You use nested groups to facilitate provisioning. Group members inherit the roles assigned to the parent group. You can create nested groups in Native Directory using groups from any configured user directory. Using very complex nested groups is not recommended. The illustrated concept:

In addition to the roles assigned directly to it, each component group (for example, Group2) inherits all the roles assigned to the parent group (Role8 and Role9 in the illustration). For example, the role assignment of Group1 in the illustration is Role1, Role8, and Role9. The parent group does not inherit the roles assigned to member groups.

Creating Groups

A Native Directory group can contain users and groups from the user directories configured in Shared Services, including Native Directory.

When a group from an external user directory is added to a Native Directory group, Shared Services creates a reference in the database to establish the relationship.

To create Native Directory groups:

1. Access Shared Services Console as a Functional Administrator or Directory Manager.
   See “Launching Shared Services Console” on page 15.
2. In the View pane, expand Native Directory.
3. Right-click Groups, and then select New Group.
4. In Name, enter a unique group name (maximum 256 characters).
   Group names are not case-sensitive.
5. Optional: Enter a group description.
6 Perform an action:
   - Click Finish to create the group without adding groups or users, and go to step 11.
   - Click Next to create a nested group or assign users to the group.

7 Create a nested group. To skip this step, click Next.
   a. Using the fields above Available Groups, search for the groups that you want to add as group members.
      i. In Directory, select the user directory from which you want to add the child group. Select All to search for groups in all configured user directories.
      ii. From the drop-down list, select Group Name to search based on group names. Select Description to search based on group descriptions.
      iii. Enter the criterion for retrieving groups. Use * (asterisk) as the wildcard to retrieve all available groups.
      iv. Click Search.

         Groups that match the search criterion are listed under Available Groups.
   b. From Available Groups, select the member groups for the new group.
   c. Click ➔.

      The selected groups are listed under Assigned Groups list.
   d. Optional: To retrieve and assign additional groups, repeat step 7.a–step 7.c.

      Using the fields above the Assigned Groups list, you can search assigned groups to identify the groups that you want to remove. For instructions on searching within assigned groups, see step 7.a–step 7.c.

      To remove assigned groups, from Assigned Groups, select the group to remove, and then click ✖.

8 Perform an action:
   - Click Finish to create the group without adding users, and then go to step 11.
   - Click Next to assign users to the group.

9 To assign users to the group:
   a. Using the fields above the Available Users list, search for the users that you want to add as group members.
      i. In Directory, select the user directory from which you want to add user members. Select All to search for users in all configured user directories.
      ii. From the drop-down list, select User Name to search based on user names. Select Description to search based on user descriptions.
      iii. Enter the criterion for retrieving users. Use * (asterisk) as the wildcard to retrieve all available users.
      iv. Click Search.

         Users that match the search criterion are listed under Available Users.
b. From Available Users, select the users to add to the group.

c. Click to move the selected user accounts to Assigned Users.


Using the fields above Assigned Users, you can search assigned users to identify users that you want to remove.

To remove assigned users, from Assigned Users, select the users to remove, and then click .

10 Click Finish.

11 Select Create Another to create another group or Finish.

Modifying Groups

You can modify the properties of all Native Directory groups except the WORLD group. If you remove a subgroup from a nested group, the role inheritance of the subgroup is updated. Similarly, if you remove a user from a group, the role inheritance of the user is updated.

To modify groups:

1 Access Shared Services Console as a Functional Administrator or Directory Manager.

See “Launching Shared Services Console” on page 15.

2 Search for a group. See “Searching for Users, Groups, Roles, and Delegated Lists” on page 17.

3 Right-click a group, and then select Properties.

Note: The Group Properties screen displays the Delegated List tab if Shared Services is deployed in Delegated Administration mode.

4 On the General tab, edit the name and description to modify the general properties of the group.

5 Open the Group Members tab and perform the actions from either step 5.a, step 5.b, or from both, to modify group assignments:

a. To add groups to the group:

   • In Directory, select the user directory from which you want to add the nested group. Select All to search for groups in all configured directories.

   • Select Group Name to search based on group names. Select Description to search based on group descriptions.

   • Enter the criterion for retrieving groups. Use * (asterisk) as the wildcard to retrieve all available groups.

   • Click Search.

   • From Available Groups, select groups and click .

     Selected groups are listed in the Assigned Groups list. From Assigned Groups, choose the group, and then click to remove a selected group.
Optional: Repeat this procedure to retrieve and assign groups from other user directories.

b. To remove assigned groups:
   - From **Assigned Groups**, select the group to remove.
     
     Shared Services enables you to search the assigned groups to identify the groups to remove. Use the fields above the **Assigned Groups** list to define the search criteria for searching within the assigned groups list.
   - Click \[button\].

6 Select the **User Members** tab, and then perform actions from either step 6.a, step 6.b, or from both, to modify user assignments:

   a. To add users to group:
      - In **Directory**, select the user directory from which you want to add users. Select **All** to search for users in all configured directories.
      - Select the user property (**User Name**, **First Name**, **Last Name**, **Email Address**, or **Description**) to search.
      - Enter the criterion for retrieving users. Use * (asterisk) as the wildcard to retrieve all available users.
      - Click **Search**.
      - From **Available Users**, select users to assign to the group.
      - Click \[button\].
      
      The selected users are listed in **Assigned Users** list.
      - Optional: Repeat this procedure to retrieve and assign users from other user directories.

   b. To remove users from the group:
      - From **Assigned Users**, select the users to remove.
        
        Shared Services enables you to search the assigned users list to identify the users to remove. Use the fields above the **Assigned Users** list to define the search criteria.
      - Click \[button\].

7 Select **Delegated List** (available only if Shared Services is deployed in Delegated Administration mode) to view the delegated administrators assigned to the group.

8 Click **OK**.

**Deleting Groups**

Deleting a group removes the group’s associations with users and roles and removes the group’s information from Native Directory but does not delete the users or subgroups assigned to the deleted group.
To delete groups:

1. Access Shared Services Console as a Functional Administrator or Directory Manager.
   See “Launching Shared Services Console” on page 15.
2. From the View pane, select Groups.
3. Search for the group to delete. See “Searching for Users, Groups, Roles, and Delegated Lists” on page 17.
4. Right-click the group, and then select Delete.
5. Click Yes to confirm the delete operation.
6. Click OK.

Managing Roles

Roles define the tasks that users can perform in EPM System applications. Roles from all registered EPM System applications can be viewed but cannot be updated or deleted from Shared Services Console. Functional Administrators and Provisioning Managers can perform these tasks:

- “Creating Aggregated Roles” on page 47
- “Modifying Aggregated Roles” on page 48
- “Deleting Aggregated Roles” on page 49
- “Generating Provisioning Reports” on page 57

Note: You can provision newly created users and groups. However, the roles provisioned to the new users and groups become effective only after Shared Services refreshes its cache. By default, the cache refresh interval is 60 minutes, which you can modify by updating the value of Shared Services Security Cache Refresh Interval. Setting this value to a shorter interval, for example, 30 minutes, may cause performance degradation.

Creating Aggregated Roles

To facilitate administration and provisioning, Functional Administrators and Provisioning Managers can create aggregated roles that associate multiple application-specific roles into a custom Shared Services role. Users with the Shared Services Provisioning Manager role can create aggregated roles for the applications for which they are Provisioning Managers. Functional Administrators can create aggregated roles for all EPM System applications.

For information on aggregated roles, see “Aggregated Roles” on page 21.

Note: You can create roles only after at least one EPM System application is registered with Shared Services.
To create aggregated roles:

1. Access Shared Services Console as a Functional Administrator or Provisioning Manager.
   
   See “Launching Shared Services Console” on page 15.

2. In the View pane, expand Native Directory.

3. Right-click Roles, and then select New Role.

4. For Name, enter a role name (maximum 256 characters).

   Role names should not contain special characters and should not start or end with a \ (backslash).

5. Optional: For Description, enter a role description.

6. From Product Name, select the application for which you want to create the role.

7. Click Next.

8. On the Role Members tab, find the roles to add.

   - Click Search to retrieve all roles from the selected application.
   
   - Enter the role name in Role Name, and then click Search to search for a specific role. Use * (asterisk) as the wildcard in pattern searches.

9. From Available Roles, select the application roles to assign.

10. Click ".

    The selected roles are listed in Assigned Roles.

    From Assigned Roles, select the role, and then click to remove a selected role.

11. Click Finish.

12. Click OK to return the Browse tab or Create Another to create another custom role.

Modifying Aggregated Roles

You can modify only aggregated roles; default application-specific roles cannot be modified from Shared Services. You may change any role property except the product name.

To modify aggregated roles:

1. Access Shared Services Console as a Functional Administrator or Provisioning Manager.

   See “Launching Shared Services Console” on page 15.

2. In the View pane, expand Native Directory.

3. Select Roles.

4. Retrieve an aggregated role. See “Searching for Users, Groups, Roles, and Delegated Lists” on page 17.

5. Right-click the role, and then select Properties.

6. On the General tab, edit the name and description to modify general properties of the role.
To modify role member assignments, on Role Members, perform actions from step 7.a, step 7.b, or both:

a. To add role members:
   - Retrieve the roles to add.
     - Click **Search** to retrieve all roles.
     - Enter the role name in **Role Name** and click **Search** to retrieve a specific role. Use * (asterisk) as the wildcard in pattern searches.
   - From **Available Roles**, select one or more.
   - Click **Add**. The selected roles are listed under **Assigned Roles**.
   - From **Assigned Roles**, select roles, and then click **Remove** to remove the selected role.

b. To remove role assignments:
   - From **Assigned Roles**, select roles to remove.
   - Click **Remove**.

8 Click **OK**.

**Deleting Aggregated Roles**

You can delete aggregated roles that are created from Shared Services. You cannot delete application-specific roles.

To delete aggregated roles:

1 Access Shared Services Console as a Functional Administrator or Provisioning Manager.
   See “Launching Shared Services Console” on page 15.

2 In the View pane, expand **Native Directory**.

3 Select **Roles**.

4 Retrieve an aggregated role.
   See “Searching for Users, Groups, Roles, and Delegated Lists” on page 17.

5 Right-click a role, and then select **Delete**.

6 Click **Yes**.

7 Click **OK**.

**Backing Up Native Directory**

Native Directory is a part of the Shared Services database. Using database backup tools, you must regularly back up the Shared Services database to recover from loss of data due to media failures, user errors, and unforeseen circumstances.
About Provisioning

Each organization has unique provisioning requirements. This section presents a typical flow for provisioning users and groups with Shared Services roles.

Provisioning users and groups with Shared Services roles is designed primarily to create administrative level users who can manage applications and provision them. EPM System product users and the groups need not be provisioned with Shared Services roles; they require roles only from the EPM System products and applications that they need to access.

Before Starting Provisioning

Before starting provisioning, ensure that the following activities are complete.

- Plan how to provision EPM System products:
  - Understand the available roles. See “Foundation Services Roles” on page 137 for a list of EPM System product roles.
  - Understand available artifact-level access permissions. Many EPM System applications enforce artifact-level provisioning using Access Control Lists (ACL) to restrict access to artifacts. For example, an account is a Planning artifact for which access rights can be set.
  - Identify the users and groups to provision. These users and groups can belong to Native Directory or to an external user directory.
Determine the provisioning mode: centralized (default) or Delegated Administration mode. The scope of the roles assigned to Delegated Administrators is limited to the delegated lists assigned to them. For example, if user Admin1 is assigned the Essbase Provisioning Manager role for DelegatedList1, Admin1 can provision only the users from DelegatedList1. See Chapter 4, “Delegated User Management.”

Overview of Provisioning Steps

All Shared Services provisioning activities must be performed by a Functional Administrator or Provisioning Manager.

Provisioning users and groups should follow a provisioning plan tailored for your organization. Typically, you should create Functional Administrators and application-specific provisioning managers to provision EPM System users and groups. Depending on the needs of your organization, you could also create other power users; for example, LCM Administrators, by assigning Shared Services roles. See “Foundation Services Roles” on page 137 for a discussion of available roles and their access privileges.

EPM System products can have two types of users: administrators and end users. Generally, administrators support EPM System products by performing administrative actions such as managing user directories, creating applications, provisioning users and groups, and migrating applications and artifacts. End users utilize the functionalities of the applications; for example, to create plans using a Planning application.

Typically, administrative users cannot perform EPM System product functions. For example, without functional role assignments, a Planning Provisioning Manager cannot create or manage plans using a Planning application.

Provisioning Administrative Users

Provisioning administrative users and groups involves using Shared Services Console to assign the required EPM System product administrator roles. For example, the Planning Provisioning Manager role enables the recipient to provision users and groups with Planning roles. Other EPM System products have similar administrative roles. A Functional Administrator must assign these administrative roles to users and groups using the Shared Services Console.

You can combine roles to assign additional access privileges to a user or group or to provide administrative access across EPM System components. Oracle does not recommend combining Provisioning Manager and Directory Manager roles.

Provisioning EPM System Users

You must provision users with application roles to allow them to access EPM System applications. Functional Administrators and Provisioning Managers perform the following steps to provision users and groups:

1. From the Shared Services Console, identify and select the users (or the groups to which they belong) who need access to the EPM System. See “Searching for Users, Groups, Roles, and Delegated Lists” on page 17.
2. Assign roles that allow users to access EPM System components. For example, all Essbase users should have the Server Access role for the Essbase Cluster (by default, EssbaseCluster-1). See “Provisioning Groups” on page 53.

EPM System roles are described in Appendix A, “EPM System Roles.”

3. Assign application-specific roles that grant access to the functions of EPM System applications. For instance, Essbase application Esb_App1 provides the Calc role, which can be assigned to users who must work with Calc scripts of Esb_App1.

These roles are assigned on a per-application basis. For example, roles from Essbase application Esb_App1 allows users to access functionalities in Esb_App1 only.

4. Using a product administration screen, assign access to the artifacts managed by the EPM System application.

You can launch the administration screen of some applications from Shared Services Console using these steps:

Artifact-level access control allows administrators to fine-tune access to application objects. Because these access privileges are by design more granular than application roles, you can use them to restrict the access rights that were granted using roles.

a. In the View pane of Shared Services Console, expand Application Groups.

b. Expand the application group node that contains the application.

c. Right-click the application to provision.

d. Select Assign Access Control. A product administration screen, which is not a part of Shared Services Console, opens.

e. Provision users.

Artifact-level access control is explained in the Administration Guide of the EPM System product.

**Provisioning Groups**

Provisioning is the process of granting EPM System roles to users and groups. Provisioning is performed by Provisioning Managers or Functional Administrators by assigning EPM System application roles to a group. See “Provisioning (Role-based Authorization)” on page 20.

**Note:** Provisioning managers cannot modify their own provisioning data.

**Tip:** To facilitate administration, Oracle recommends that you provision groups rather than users, and that you use aggregated roles.

➢ To provision users or groups:

1. **Access Shared Services Console as a Functional Administrator or Provisioning Manager.**
2 Find and select groups to provision.

   See “Searching for Users, Groups, Roles, and Delegated Lists” on page 17.

3 Select Administration and then Provision.

4 Optional: Select a view.

   Roles can be displayed in a hierarchy (tree) or a list. You must drill down the hierarchy to display available roles. The list view lists available roles but does not show their hierarchy.

5 Select roles, and then click  

6 Click OK.

### Deprovisioning Groups

Deprovisioning removes the application roles that are assigned to the group. Functional Administrators can deprovision roles from one or more applications. Provisioning managers of applications can deprovision roles from their applications. For example, assume that the group Sales_West is provisioned with roles from Planning and Oracle Hyperion Financial Management. If this group is deprovisioned by a Planning Provisioning Manager, only the roles from Planning are removed.

**Note:** Functional administrators can deprovision their own accounts. Because Shared Services require at least one System Administrator (a user who is provisioned with the Shared Services Administrator role) in Native Directory, administrators must verify the existence of such an account before deprovisioning themselves.

idineprovision groups:

1 Access Shared Services Console as a Functional Administrator or Provisioning Manager.

   See “Launching Shared Services Console” on page 15.

2 Find the group to deprovision.

   See “Searching for Users, Groups, Roles, and Delegated Lists” on page 17.

3 Right-click the group, and then select Deprovision.

4 Perform an action:

   ● To remove role assignments from specific applications, make selections.

   ● To remove all provisioned roles, select Check All.

5 Click OK.

6 In the confirmation dialog box, click Yes.

7 In the Deprovision Summary screen, click OK.
Auditing Security Activities and Lifecycle Management Artifacts

Shared Services allows the auditing of provisioning and lifecycle management activities to track changes to security objects and the artifacts that are exported or imported using Lifecycle Management functionality.

Auditing can be configured at three levels: global, application group, and application.

At the global level, you can audit security and artifacts handled by Shared Services. Application group-level and application-level auditing allows you to audit security activities related to an application group or application performed through Shared Services. Application group and application security activities that are performed outside Shared Services; for example, assigning calculation scripts in Essbase, cannot be audited.

By default, auditing is disabled. Only Functional Administrators can enable auditing or change the list of objects and artifacts that are audited at the global level. You must restart all EPM System products for audit configuration changes to take effect.

To change the auditing configuration:

2. Select Administration and then Configure Auditing.
3. On the Audit Configuration screen, perform the following actions:
   a. Select Enable Auditing to activate auditing. If this option is not selected, Shared Services does not support auditing at any level. By default, auditing is disabled.
   b. Select Allow Global Settings Override to disable application group and application-level auditing. If this option is selected, application group and application-level task selections are discarded in favor of the global selections.
   c. Optional: To remove old audit data from the system, in Purge Data Older than, set the number of days for which audit data is to be retained. Older audit data is marked for removal when you click OK.
   d. From Select Tasks, select the tasks for which audit data is to be preserved. Tasks are categorized based on the applications registered with Shared Services.
   e. Click OK.
4. Restart EPM System products including Shared Services.

Manually Purging Audit Data

EPM System automatically removes audit data from the Shared Services database based on the purge settings specified in Oracle Hyperion Shared Services Registry. Use this procedure to manually purge audit data.
Caution! Functional Administrators must purge the data based on your company’s audit data retention policies. Before purging data, back up the Shared Services database.

To purge audit data:

2. Select Administration and then Configure Auditing.
3. In Purge Data Older than, set the number of days for which audit data is to be retained.
4. Click OK.

Selecting Objects for Application and Application Group-Level Audits

Only Functional Administrators can select objects for auditing at application and application group levels.

To select objects for auditing:

2. In the View pane, right-click one of the following, and then select Configure Auditing:
   - An application group to enable auditing for all the applications in the application group
   - An application to enable auditing for the application

   Note: If Allow Global Settings Override is selected on the Audit configuration screen, Configure Auditing is not enabled at the application group and application levels. See “Auditing Security Activities and Lifecycle Management Artifacts” on page 55.
3. From Select Tasks, select the tasks for which audit data is to be preserved. Tasks are categorized based on the applications registered with Shared Services.
4. Click OK.

Changing Purge Interval

By default, a background thread removes audit data that is older than 25 days. You can modify the AUDIT.PURGE.EARLIERTO.DAYS Shared Services Registry setting to change the purge interval.
To modify the purge interval:

1. Start a command prompt on the Foundation Services server host machine, and navigate to $EPM_ORACLE_HOME/bin$ on a Windows server.

2. Use the following command to view the current purge interval:
   
   ```
   epmsys_registry.bat view SHARED_SERVICES_PRODUCT/@AUDIT.PURGE.EARLIERTO.DAYS
   ```

3. Use the following command to update the purge interval:
   
   ```
   epmsys_registry.bat update SHARED_SERVICES_PRODUCT/@AUDIT.PURGE.EARLIERTO.DAYS NEW_PURGE_INTERVAL
   ```

   In the preceding command, replace `NEW_PURGE_INTERVAL` with the number of days for which the audit data is to be stored. For example, to keep audit data for 6 months, use the following command:

   ```
   epmsys_registry.bat update SHARED_SERVICES_PRODUCT/@AUDIT.PURGE.EARLIERTO.DAYS 180
   ```

4. Repeat step 2 to verify that the purge interval has been updated.

---

### Generating Reports

Shared Services can generate three report types: provisioning reports, audit reports, and migration status report. See:

- “Generating Provisioning Reports” on page 57
- “Generating Audit Reports” on page 58
- “Generating Migration Status Report” on page 59

### Generating Provisioning Reports

Functional Administrators and Provisioning Managers can use the reporting capabilities of the Shared Services Console to review the provisioning data of users and roles. Provisioning reports can contain information on users assigned to roles from selected applications, and roles from selected applications assigned to users. The report also contains inheritance information that shows the sequence of inheritance starting with the original group or role that was responsible for granting the provisioned role to the user.

Provisioning reports enable Functional Administrators and Provisioning Managers to review the access rights and permissions granted to users across EPM System applications, which helps track user access for compliance reporting.

If the WORLD group of Native Directory is provisioned, roles inherited from the WORLD group are included in provisioning report only if the report is generated for users or groups.

To generate provisioning reports:

1. Access Shared Services Console as a Functional Administrator or Provisioning Manager.

   See “Launching Shared Services Console” on page 15.
2 Select a role.

See “Searching for Users, Groups, Roles, and Delegated Lists” on page 17.

3 Select Administration and then View Report.

4 Enter report generation parameters.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Find All</td>
<td>Select the object type (user, group, or role) for which the report is to be generated.</td>
</tr>
<tr>
<td>For Users or For Roles</td>
<td>The label of this changes depending on what is selected in Find All.</td>
</tr>
<tr>
<td>Filter By</td>
<td>The criterion to use to filter the report data.</td>
</tr>
<tr>
<td>Show Effective Roles</td>
<td>Select Yes to report on all effective roles (inherited as well as directly assigned). Inherited roles (as opposed to directly assigned roles) are assigned to groups to which the user or group belongs. Select No to report only on directly assigned roles.</td>
</tr>
<tr>
<td>Group By</td>
<td>Select how to group the data in the report. Available grouping criteria depend on the selection in Find All.</td>
</tr>
<tr>
<td>Results Per Page</td>
<td>Number of report results to display in a page. Default is 500.</td>
</tr>
<tr>
<td>In Application</td>
<td>Select the applications from which provisioning data is to be reported, or select Select All to report on all applications. Note: You can report only on the applications belonging to an application group.</td>
</tr>
</tbody>
</table>

5 Select Create Report.

6 Optional: To print the report:
   a. Click Print Preview.
   b. Click Print.
   c. Select a printer and then click Print.
   d. Click Close.

7 Optional: Click Export to CSV to export the report into a Comma Separated Value (CSV) file.

8 Click OK.

Generating Audit Reports

Three audit reports—Security Reports, Artifact Reports, and Config Report—can be generated. The Security Report displays audit information related to the security tasks for which auditing is configured. Artifact Report presents information on the artifacts that were imported or exported using Lifecycle Management.

Functional Administrators can generate and view audit reports to track historical changes to the security data.
To generate audit reports:

1. Access Shared Services Console as a Functional Administrator.
2. Select Administration, and then Audit Reports.
3. Select an option:
   - Security Reports to generate Security Audit report
   - Artifact Reports to generate a report on the artifacts that were migrated using Lifecycle Management
   - Config Reports to generate security audit report on the configuration tasks that were performed

   Note: These reports are automatically generated to show the data for users for the last 30 days.
4. To regenerate the report, select parameters:
   a. In Performed By, select the users for which the report is to be generated.
   b. In Performed During, select the period for which the report is to be generated. You can set the period as number of days or as a date range.
   c. Optional: Select Detailed View to group the report data based on the attribute that was modified and the new attribute value.
   d. Optional: In Per Page, select the number of rows of data to display in a report page.
   e. Click View Report.
5. To create a CSV file containing the report data, click Export.
   a. Select Save as CSV.
   b. Click OK.
   c. Click Open to open the file or Save to save the file to the file system. By default, the Security Report file is named auditsecurityreport.csv, the Artifact Report is named AuditArtifactReport.csv, and the Config Report is named AuditConfigReport.csv.
6. Click Close.

Generating Migration Status Report

The Migration Status Report contains information on the artifact migrations performed using the Lifecycle Management functionality. For each migration, this report presents information such as the user who performed the migration, source, destination, start time, completed time, duration, and status.
For failed migrations, you can view the information such as the source and destination applications, artifact path, artifact name, and error that cause the migration to fail.

To generate Migration Status Report:

1. Access Shared Services Console as a Functional Administrator.
2. Select Administration, and then Migration Status Report.
   
   This report is automatically generated to show all migrations performed in the last 30 days.
3. To regenerate the report, click Refresh.
4. To close the report, click Cancel.

**Importing and Exporting Native Directory Data**

Use Lifecycle Management to perform the following tasks:

- Move provisioning data across environments
- Bulk provision users and groups
- Manage users and groups in Native Directory

See the *Oracle Enterprise Performance Management System Lifecycle Management Guide*. 
About Taskflows

Taskflows automate some or all of a business process. Tasks are passed from one taskflow participant to another based on a set of procedural rules. Taskflows can automate product tasks in EPM System components such as Financial Management, Oracle Hyperion Profitability and Cost Management, and Oracle Hyperion EPM Architect.

Two types of taskflow actions—automatic and manual—are supported. Automatic taskflow actions are started by the workflow engine and executed by an EPM System component without any user interaction. Manual taskflow actions are started by workflow engine but are executed manually by users.

Taskflow Components

Generally, taskflows are designed to utilize a number of variables, stages, and links.

Stages

A stage describes a step in a taskflow usually performed by one individual. Each stage has one application action or event in the taskflow. Actions can have parameters for which values are supplied at runtime.
Many default actions are available for each EPM System component that uses taskflows. These actions are defined and managed by taskflow-enabled EPM System components. Shared Services default actions are described in Table 3. See the following information sources for description of actions available for other EPM System components:


### Table 3  Default Stage Actions and Parameters: Shared Services

<table>
<thead>
<tr>
<th>Action</th>
<th>Parameters</th>
</tr>
</thead>
</table>
| Email   | This action automatically sends an email message. Complete these parameters for the email action:  
- To: Enter the recipient's email address  
- Subject: Enter a subject for the e-mail  
- Message: Select a variable (by double-clicking a variable from the variables list) to display success or failure  
- Variables: Lists the available variables for the email action |
| Execute | This action runs an external program from a command line. Complete these parameters for the execute action:  
- Command: Enter a command to run an external program.  
  - The external program can be a valid command line script (such as a .bat script on Windows or a .sh script on UNIX) and any valid program execution command. Ensure that your script file does not resolve the path dynamically; if the file uses any variables to resolve the path, it will not work.  
  - For example, to launch Internet Explorer, enter: IEXPLORE.EXE. See “Taskflow Scripts Location” on page 67. |

1SMTP mail configuration must be available in Foundation Services for this action to execute successfully.

## Links

Links connect taskflow stages. Links can be unconditional where the completion of a stage leads to the start of the next stage, or conditional where the results of the operations of a stage determines how the taskflow proceeds.

Links specify the action that the taskflow should take next. Every stage needs a link. Generally, most stages have two links: success and failure. For the success link, you specify the next processing stage (receiving stage) based on the results of the current stage. For the failure link, you specify the action to take if the taskflow action in the stage fails.

For example, you can set a success link so that if Data_Synchronization action in a Performance Management Architect taskflow stage succeeds, Performance Management Architect proceeds to the Redeploying_Consolidation stage. You can also set a failure link so that if the Data_Synchronization action fails, Performance Management Architect stops the process and terminates the taskflow.

The last stage in each taskflow must have a final link with “End” as the target to complete the taskflow.
Variables

Taskflows use variables as global contexts that can be referenced throughout their runtime lifecycles. Variables created within a taskflow can be used to pass values from one stage to another within a taskflow.

Prerequisites for Working with Taskflows

EPM System provides the following global taskflow roles. Users who are assigned these roles can work with taskflows from any EPM System component.

- Mange Taskflow: this role allows users to create, edit, schedule, assign ACLs, and run taskflows across EPM System components.
- Run Taskflow: this role permits users to run and schedule taskflows across EPM System components. Users who are assigned only this role cannot create or edit taskflows.

Creating and Managing Taskflows

You can use the Manage Task Flow screen of EPM Workspace or a product-specific screen to work with taskflows. To access the taskflow screen from an EPM System component, in addition to taskflow roles (see “Prerequisites for Working with Taskflows” on page 63), you must have application roles that grant you access to these EPM System components.

Accessing the Manage Taskflow Screen

Typically, you use the Manage Task Flow screen of EPM Workspace to work with taskflows. This screen is accessible to all EPM System users who have the Manage Taskflow role.

To access Manage Task Flows screen:
1. Log into EPM Workspace.
2. Select Navigate, and then Application Library.
3. Select Administration, and then Manage Taskflows.

Creating Taskflows

To create taskflows:
1. Open the Manage Task Flows screen. See “Accessing the Manage Taskflow Screen” on page 63.
3. In Name, enter a unique taskflow name.
4. In Application, enter the name of the application to which this taskflow belongs.
The application name is used to categorize applications in the Manage Taskflows screen.

5 For **Description**, enter a taskflow description.

6 Click **Submit**.

The taskflow editor, which allows you to add stages and links, is displayed.

7 **Add stages to the taskflow:**
   a. On **General**, enter the following information:
      - **Name**: Enter a stage name.
      - **UserName**: Enter the EPM System user whose account will be used to initiate the taskflow stage.
      - **Password**: Enter the password of the user identified in the **UserName** field.
   b. On **Processing**, enter the following information:
      i. In **Application**, select an application from which to run the task.
      ii. In **Action**, select an action to perform and then enter the required information.
         Actions available in **Actions** list reflect the selected application. For a list of actions for each EPM System component, see the following topics:
         - See Table 3, “Default Stage Actions and Parameters: Shared Services,” on page 62 for a list of available Shared Services actions.
         - See the *Oracle Hyperion Enterprise Performance Management Architect Administrator’s Guide* for a list of Performance Management Architect actions.
   c. On **Starting Event**, enter the following information to schedule an event:
      i. In **Starting Event**, select **Scheduled Event**.
      ii. In **Start Date**, enter the date on which the task is to be run.
      iii. In **Start Time**, select a time at which the task should start.
      iv. If this task is to be repeated, select the **Recurrence**, and in **Recurrence Pattern**, select the task frequency.
      v. Select an option for the task end date and time:
         - **No End Date**
         - **End After occurrences**, and enter the number of occurrences.
         - **End Date**, enter an end date, and then select an **End Time**.
   d. **Optional**: add more stages to the taskflow.

8 **Add links to taskflow stages:**
   a. Select the stage for which link is to be added, and then click **Add Link**.
   b. In **General**, enter a unique link name and an optional description.
c. In **Receiving Stage** select the next stage in the taskflow.

d. **Optional**: Set link conditions if needed.

9 **Click Save.**

## Editing Taskflows

To edit taskflows:

1. Open the Manage Task Flows screen. See “Accessing the Manage Taskflow Screen” on page 63.

2. From Taskflow Listing Summary, select a taskflow, and then click **Edit**.

   The first stage of the task flow is selected by default.

3. **In Password**, enter the password of the EPM System user whose account is used to initiate the taskflow stage.

4. Edit the current stage, if required, or select another stage by clicking the stage name.
   a. In General, complete these steps.
      i. **Optional**: Change the stage name and the EPM System user whose account is used to initiate the taskflow.
      ii. **In Password**, enter the password of the EPM System user whose account is used to initiate the current taskflow stage.

   b. In Processing, modify the following stage processing information. You can change the values in any field on this tab.
      
      * See Table 3, “Default Stage Actions and Parameters: Shared Services,” on page 62 for a list of available Shared Services actions.
      * See the *Oracle Hyperion Enterprise Performance Management Architect Administrator’s Guide* for a list of Performance Management Architect actions.
      * See the *Oracle Hyperion Financial Management User’s Guide* for a list of Financial Management actions.

   c. In Starting Event, modify schedule for starting the stage.

   d. **Optional**: Modify links, if needed.

   **Note:** Before you can edit links, you must, at a minimum, enter the password of the EPM System user whose account is used to initiate the current taskflow stage.

   i. Click the name of the link that you want to edit.
   ii. In General, edit link details, such as name, description, and receiving stage. You cannot modify the sending stage of the link.
   iii. **Optional**: Modify link conditions if needed.

5 **Click Save.**
Viewing Taskflow Information

The Taskflow Listing Summary on Manage Taskflows lists all defined taskflows.

To view taskflow information:
1. Open the Manage Task Flows screen. See “Accessing the Manage Taskflow Screen” on page 63.
2. Select the taskflow that you want to view.
3. Click Edit.

Scheduling Taskflows

You can schedule taskflow execution from the Manage Taskflows screen.

To schedule an existing taskflow:
1. Open the Manage Task Flows screen. See “Accessing the Manage Taskflow Screen” on page 63.
2. Select the taskflow that you want to schedule.
3. Click Schedule Taskflow.
4. In Starting Event, select Scheduled Event.
5. In Start Date, select the date on which the taskflow should be run.
6. In Start Time, use the drop-down lists to select the time at which the taskflow execution should start.
7. Optional: To schedule jobs to run on a recurring basis:
   a. Select Recurrence.
   b. In Recurrence Pattern, select a recurring pattern, such as Monthly or Weekly.
   c. Schedule frequency for the selected recurrence pattern.
8. Optional: To schedule the taskflow to run until it is manually cancelled or deleted, select No End Date.
9. Optional: To schedule the taskflow to run a specified number of times, select End After x Occurrences. In the text box, enter the number of times the job is to be run.
10. Optional: To run the taskflow until a specified date, select End Date, and then select the date and time of the final run.
11. Click Save.

Manually Running Taskflows

To run a taskflow:
1. Open the Manage Taskflows screen. See “Accessing the Manage Taskflow Screen” on page 63.
2. Select the taskflow that you want to run.
Viewing Taskflow Status and Execution Details

Use the Taskflow Status Summary screen to monitor taskflow status.

To view taskflow status:

1. Log into EPM Workspace.
2. Select Navigate, and then Application Library.
3. Select Administration, and then View Taskflow Status.
4. In Manage Taskflows, select the search criteria to locate the taskflow that you want to monitor.
   - To search for taskflows in a specific execution status, in Status, select a taskflow status. Select All to search for taskflows in any status.
   - To search for taskflows belonging to a specific application, in Application, select the application to which the taskflow belongs.
   - To search for a specific taskflow, in Taskflow, select taskflow name.
5. To limit the search to a specific time period, set start and end values in values Initiated Between.
6. Click Search.
7. Optional: Click Refresh to update status information.
8. Optional: To end a running taskflow, select the taskflow, and then click Stop.
   The taskflow stops when the application returns the results of the selected step. The results for previous steps are not discarded; however, if the taskflow is rerun, it begins at the first step.
9. To view detailed taskflow execution details, click the taskflow ID.
   The Taskflow Participant Summary is displayed, showing details of the task and its status.
10. Click Cancel to return to Taskflow Status Summary.

Taskflow Scripts Location

All scripts that are to be executed during a taskflow stage must be stored in a dedicated directory. The default location for the directory containing such scripts is EPM_ORACLE_HOME/common/utilities.

If you want to store taskflow scripts in directory other than the default directory, you must update a Shared Services Registry property by running one of the following commands at a command prompt. In this command, replace SCRIPT_LOCATION with the absolute path of the directory where taskflow scripts are stored:

- epmsys_registry.bat updateproperty SHARED_SERVICES_PRODUCT/@workflowEngine.ces.location SCRIPT_LOCATION (Windows)
epmsys_registry.sh updateproperty SHAREDSERVICESPRODUCT/
  @workflowEngine.ces.location SCRIPT_LOCATION(UNIX/LINUX)

For example, you may run the following command for a Windows deployment:
epmsys_registry.bat updateproperty
  SHAREDSERVICESPRODUCT/@workflowEngine.ces.location C:\taskflowscripts

You must secure the SCRIPT_LOCATION directory from unauthorized access. Further, to enhance security, run services and processes using a secure user account.

Restart EPM System after updating Oracle Hyperion Shared Services Registry.
Essbase Security Model

Essbase enforces two levels of roles: Essbase Server roles and Essbase application roles. These roles are granted and maintained through Shared Services Console.

In addition to roles, Essbase enforces access control (for example, read and write) on artifacts such as dimension members, filters, and calculation scripts. Filters are also security constructs that limit access.

Provisioning information on Essbase application roles is stored in the Shared Services repository. Access control information on Essbase artifacts is stored in `essbase.sec`, the Essbase security file, which is stored on the same server as Essbase.

Prerequisites

Subtopics

- Foundation Services
- Web Server
- Essbase Server
- Administration Services
- Performance Management Architect (Optional)
- Essbase Studio Server (Optional)

Foundation Services

Foundation Services must be running. Starting Foundation Services starts these components:

- Shared Services
- EPM Workspace
Web Server

The EPM System web server must be running.

Essbase Server

- Essbase is deployed in Shared Services mode (the default deployment option). See the Oracle Hyperion Enterprise Performance Management System Installation and Configuration Guide.

  If Essbase is not deployed in Shared Services mode, Consult Administration Services Online Help for instructions on how to convert a stand-alone Essbase server to Shared Services mode.

- Essbase Server is running. See the Oracle Enterprise Performance Management System Installation and Configuration Guide.

Administration Services

- Administration Services is running. See the Oracle Hyperion Enterprise Performance Management System Installation and Configuration Guide.

  The admin user of Administration Services is automatically externalized to Shared Services if Essbase is deployed in Shared Services mode using the Oracle Hyperion Enterprise Performance Management System Configurator.

  If you convert a stand-alone Essbase instance to Shared Services mode, you must externalize the admin user from Administration Services. See Administration Services Online Help for instructions.

  Essbase sample applications, for example, Demo and Sample, are added to the server, if they have been installed. You can use these applications to become familiar with the provisioning process if you do not want to create an application.

Performance Management Architect (Optional)

Performance Management Architect is required to create Essbase applications using the Application Library. Performance Management Architect components such as Application Library and Dimension Library are accessed through EPM Workspace.

- Performance Management Architect Server is running.

- Performance Management Architect is running.

  See the Oracle Enterprise Performance Management System Installation and Configuration Guide.

- Performance Management Architect web server is running.
Essbase Studio Server (Optional)

Oracle Essbase Studio Server is required to deploy Essbase applications from Performance Management Architect.

Accessing EPM System Products

You must access EPM System components such as Shared Services, EPM Workspace, and Administration Services during provisioning. See the following topics:

- “Launching Shared Services Console” on page 15
- “Accessing EPM Workspace” on page 161
- “Accessing Administration Services Console” on page 162

Provisioning Process

You can use three interfaces to create Essbase applications: Administration Services Console, Essbase Studio, and the Application Library. Access Application Library through EPM Workspace.

Essbase applications created through Administration Services Console and Essbase Studio are known as Classic Essbase applications. Classic applications are stand-alone applications that do not share dimensions and members with other applications. Essbase applications created using the Application Library of Performance Management Architect are known as Performance Management Architect Essbase applications. These applications can share dimensions and members with each other.

Behavior of Essbase applications is identical regardless of the interface that is used to create them.

Classic Essbase Applications

The following illustration shows the steps involved in provisioning a classic Essbase application.

![Diagram showing steps of Classic Essbase Applications]

* Accesses Essbase Application
Performance Management Architect Essbase Applications

The following illustration shows the steps involved in provisioning Performance Management Architect Essbase applications.

Provisioning Users and Groups with Essbase Server Roles

All EPM System users can log in to Administration Services Console. The activities that users can perform in Administration Services Console, and by extension on the Essbase Server, are defined by the user’s Essbase Server role assignments.

If Essbase is deployed in Shared Services mode, a Functional Administrator account is used initially to administer Essbase Server and applications.

➢ To provision users with Essbase server roles:

1. Log in to Shared Services Console as a Functional Administrator. See “Launching Shared Services Console” on page 15.

2. From a configured user directory, find the user or group to provision. See “Searching for Users, Groups, Roles, and Delegated Lists” on page 17.

3. Provision the user or group with an Essbase Server role.
   a. Right-click the user or group, and then select **Provision**.
   b. Optional: Select a view.
      Roles can be displayed in a hierarchy (tree) or a list. You must drill down the hierarchy to display available roles. The list view lists available roles but does not show their hierarchy.
   c. In Available Roles, expand the Essbase node; for example, **EssbaseCluster-1**.
   d. In the Essbase node, expand the node that represents the Essbase Server; for example, **EssbaseCluster-1**.
   e. Select Essbase Server roles and click **Table 4** describes Essbase Server roles.
Table 4  Essbase Server Roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
</table>
| Administrator         | Full access to administer Essbase Server, applications, and databases  
                        | **Note:** The Provisioning Manager role is automatically assigned when you migrate Essbase Administrators; however, when you create an Essbase Administrator in Shared Services Console, you must manually assign the Provisioning Manager role. |
| Create/Delete Application | Creates and deletes applications and databases. Includes Application Manager and Database Manager permissions for the applications and databases created by this user. |
| Server Access         | Accesses any application or database belonging to this Essbase Server. This level is the minimum access permission a user must have to access applications and databases. |
| Provisioning Manager  | Provisions users with roles of this Essbase server                                                                                            |

f. Click OK.

g. Click OK to close the confirmation screen.

Creating Essbase Server Connection

Before you can perform tasks from Administration Services Console, you must connect to an Essbase Server installation. Initially, the Functional Administrator is the only user who can create a server connection.

After you create an Essbase Server connection from the Administration Services Console, the Enterprise View displays a node that represents the Essbase Server connection. Nodes, such as Applications and Security, appear within the node that represents the Essbase Server connection.

You can install seven Essbase sample applications (ASOsamp, Demo, DMDemo, Sampeast, Sample, Sample_U, and Samppart). If installed, these applications are registered with Shared Services, and are listed under the Application node.

Sample Essbase applications are owned by the Functional Administrator. They can be used to practice Essbase application provisioning.

To create an Essbase Server connection:

1. Log in to Administration Services Console as a Functional Administrator. See “Accessing Administration Services Console” on page 162.
2. Right-click Essbase Servers, and then select Add Essbase Server.
3. Enter required information. Consult online help for assistance.

Creating Classic Essbase Applications

Each Essbase server can support multiple applications, each with its own database. The Essbase application that you create is automatically registered with Shared Services. Essbase Server users must be provisioned separately to each application and its artifacts. See the Oracle Essbase
To create Essbase applications and artifacts:

1. **Log in to Administration Services Console as a Functional Administrator.**

   **Note:** Users provisioned with Essbase Server Administrator or Create/Delete Application role also can create Essbase applications. These users do not require a Shared Services role (for example, Essbase Application Creator) to create Essbase applications from Administration Services Console.

2. **Create an Essbase application.**

   **Note:** EPM System automatically assigns Provisioning Manager and Application Manager roles to the user who creates the Essbase application.

   a. Under **Essbase Servers**, right-click **Applications**.
   b. Select **Create application**, and then either **Using aggregate storage** or **Using block storage**.
   c. Enter required information. Consult online help for assistance.

3. **Add a database for the application.**

   a. Right-click the application that you created, and then select **Create database**.
   b. Enter the required information. Consult online help for assistance.

4. **Add dimensions and members to the outline.**

   a. Expand the node representing the application database you created.
   b. Right-click **Outline**, and then select **Edit**.
   c. On the Outline tab, right-click **Outline**, and then select **Add child**.
   d. Enter member name. Click **Help** for assistance.
   e. Click **Verify** to validate the outline.
   f. Add additional members by repeating step 4.c–step 4.e.
   g. Click **Save**.
   h. Click **Close**.

---

**Creating Performance Management Architect Essbase Applications**

**Note:** If you are using Administration Services Console to create Essbase applications, skip this section.
Each Essbase server can support multiple applications, each with its own databases. The Essbase application that you create is automatically registered with Shared Services. Essbase Server users must be provisioned separately to each application and its artifacts.

Performance Management Architect Essbase applications are created from the Application Library.

The applications that you deploy become a part of the Application Library. Essbase applications are listed also in Shared Services Console and Administration Services Console.

To create an application:

2. Select Navigate, then Administer, and then Application Library.
3. Select File, then New, and then Application.

The Application Creation Wizard is displayed.

4. In Name, enter an application name (maximum eight characters). Application names should not contain special characters; for example, a space or an asterisk.
5. In Type, select Essbase (ASO) or Essbase (BSO) depending on the type of storage to use for the application.
6. Enter a database name.
7. Select Unicode if you want the database to be a unicode database.
8. Click Next.

9. Select application dimensions. You must select at least one dimension. Consult online help for assistance.
10. Click Next to create the application in the Application Library.
11. Click Validate. Correct reported errors. You can find detailed validation information in the Library Job Console. To open the Library Job Console, select Navigate, then Administer, and then Library Job Console.
12. Click Finish.

The Dimension Library opens. From the Dimension Library, you can add members for your application dimensions. An icon for the application is displayed in the Application Library.

13. Deploy the application:
   a. In Application Library, right-click your Essbase application.
   b. Select Deploy.

      Performance Management Architect validates the application. If no errors are found, the Deploy window opens.
   c. Enter or select the required information. Consult online help for assistance.
   d. Click Deploy.
The deployment process takes awhile to finish. Performance Management Architect displays a deployment job ID that can be used to track deployment progress and reported errors.

**Creating Essbase Artifacts**

Subtopics

- Creating Security Filters
- Creating Calculation Scripts

You must create filters and calculation scripts in the Essbase application database before artifact access controls can be imposed. Essbase uses filters to accommodate the security needs of specific parts of a database and to control security access to data values or cells by restricting access to database cells. Essbase Server stores filters in `essbase.sec`.

Calculation scripts are commands that define how a database is consolidated or aggregated. Calculation scripts may also contain commands that specify allocation and other calculation rules separate from the consolidation process.

You can use the Administration Services Console or MaxL to create filters and calculation scripts. For information on creating and managing filters and calculation scripts, see the Oracle Essbase Administration Services Online Help or the Oracle Essbase Database Administrator's Guide.

**Creating Security Filters**

Security filters control access to data values or cells in the Essbase database. Filters are the most granular form of Essbase security access. While creating a filter, you designate restrictions on a database cell. Filter information is stored in `essbase.sec` on the Essbase server.

Filters can be assigned to Essbase users and groups.

➢ To create a filter:

1. Log in to Administration Services Console as a Functional Administrator or as a user provisioned with the Essbase Administrator role. See “Accessing Administration Services Console” on page 162.

2. Under Essbase Servers, expand Applications.

3. Expand the node representing the Essbase application for which you want to define security filters.

4. Right-click the database for which you want to define security filters, select Create, and then Filters.

5. Create the filter. Consult online help for assistance.

**Creating Calculation Scripts**

Calculation scripts specify how databases are calculated. They override the calculations defined by the database outline. You construct calculation scripts using the Calculation Script Editor.

Calculation scripts can be assigned to Essbase users and groups.
To create a calculation script:

1. Log in to Administration Services Console as a Functional Administrator or as a user provisioned with Essbase Administrator role.
2. Under Essbase Servers, expand Applications.
3. Expand the node representing the Essbase application for which you want to define calculation scripts.
4. Select the database for which you want to define calculation scripts.
5. Select File, then Editors, and then Calculation Script Editor.
6. Create the calculation script. Consult online help for assistance.

**Provisioning Users with Essbase Application Roles**

Each Essbase server can have multiple Essbase applications, each with its own databases. Essbase server users must be provisioned separately to each application and its databases.

To provision users with Essbase application roles:

1. Log in to Shared Services Console as a Functional Administrator. See “Launching Shared Services Console” on page 15.

   **Note:** Users provisioned with Provisioning Manager role of an Essbase application can provision other users with roles from the application.

2. Find a user or group to provision.
   
   See “Searching for Users, Groups, Roles, and Delegated Lists” on page 17.

3. Select Administration and then Provision.
4. Optional: Select a view.
   
   Roles can be displayed in a hierarchy (tree) or a list. Drill down the hierarchy to display available roles. The list view lists available roles but does not show their hierarchy.

5. Expand the node that represents your Essbase Server; for example, EssbaseCluster-1.

6. Under the Essbase Server node, expand the node representing the Essbase application that you created in the preceding section.

7. Select Essbase application roles, and click Table 5 describes Essbase application roles and their embedded permissions.
<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Manager</td>
<td>Creates, deletes, and modifies databases and application settings within the assigned application. Includes Database Manager permissions for databases within the application. An Application Managers can delete only those applications and databases that he created.</td>
</tr>
<tr>
<td>Note:</td>
<td>The Provisioning Manager role is automatically assigned to you when you migrate Essbase Application Managers; however, when you create an Essbase Application Manager in Shared Services Console, you must manually assign to yourself the Provisioning Manager role.</td>
</tr>
<tr>
<td>Database Manager</td>
<td>Manages the databases, database artifacts, and locks within the assigned application</td>
</tr>
<tr>
<td>Calc</td>
<td>Calculates, updates, and reads data values based on assigned scope, using any assigned calculations and filter</td>
</tr>
<tr>
<td>Write</td>
<td>Updates and reads data values based on assigned scope, using any assigned filter</td>
</tr>
<tr>
<td>Read</td>
<td>Reads data values</td>
</tr>
<tr>
<td>Filter</td>
<td>Accesses specific data and metadata according to filter restrictions</td>
</tr>
<tr>
<td>Start/Stop Application</td>
<td>Starts and stops applications or databases</td>
</tr>
<tr>
<td>Provisioning Manager</td>
<td>Provisions Essbase users with roles from this application</td>
</tr>
</tbody>
</table>

8 Click **OK**.

9 Click **OK**.

10 **Optional**: Repeat step 2—step 8 to provision other users with roles from this Essbase application.

11 **Optional**: Repeat step 6—step 9 to provision the selected user with roles from other Essbase applications belonging to this Essbase Server.

### Defining Access Controls

Essbase application roles grant wide-ranging access to the artifacts stored in the application’s database. You can set limits to artifact access by defining access controls. Essbase artifacts include filters and calculation scripts.

To grant access to Essbase artifacts:

1 Log in to Shared Services Console as a Functional Administrator. See “Launching Shared Services Console” on page 15.

2 In the View Pane, expand Application Groups, and then expand the Essbase server node; for example, EssbaseCluster-1.

3 Right-click the Essbase application for which artifact access permissions are to be set, and then select Assign Access Control.

The Application tab opens. By default, this tab lists the users who are provisioned with roles belonging to this Essbase application. You can list all users and groups or only available groups.
4 Select the users and groups for which artifact access controls are to be set and move them to the selected list.

5 Click Next.

6 Select the users who should receive access to artifacts.

7 From Filter, select the database security filter to which the users should be granted access.

8 From Calc, select the calculation script that the selected users can access.

9 Select the check mark next to Calc.

10 Repeat step 7–step 9 to assign access to more filters and calculation scripts.

11 Click OK.
Planning Security Model

Planning enforces two types of roles: Planning global roles and Planning application roles. Planning global roles (Dimension Editor and Planning Application Creator) are used to provision users who create Planning applications using Performance Management Architect. These are granted through the Shared Services Console. Planning application roles are also granted using Shared Services Console.

Planning artifacts such as Web Forms and dimensions/members are maintained and defined from a Planning user interface. Security on these artifacts is defined from within the Planning application. Planning artifacts are stored in the Planning relational repository.

Prerequisites

Subtopics

- Foundation Services
- Web Server
- Essbase Server
- Administration Services (Optional)
- Performance Management Architect (Optional)
- Relational Database

Foundation Services

- Foundation Services is running. Starting Foundation Services starts these components:
  - Shared Services
  - Performance Management Architect
• **Optional:** The external user directories that are the source for user and group information for Planning are configured in Shared Services.

**Web Server**

The EPM System web server must be running.

**Essbase Server**

• Essbase is deployed in Shared Services mode by default. See the *Oracle Enterprise Performance Management System Installation and Configuration Guide*.

  If Essbase is not deployed in Shared Services mode, see *Administration Services Online Help* for instructions to convert a stand-alone Essbase Server to Shared Services mode.

• Essbase Server is running.

  See the *Oracle Enterprise Performance Management System Installation and Configuration Guide*.

**Administration Services (Optional)**

Administration Services, the administration console for Essbase, is required only if you want to verify the creation of Planning applications, databases, and members in Essbase.

• Administration Services is running.

  See the *Oracle Enterprise Performance Management System Installation and Configuration Guide*.

**Performance Management Architect (Optional)**

Performance Management Architect is required to create Performance Management Architect Planning applications that can share dimensions across applications. Performance Management Architect components such as Application Library and Dimension Library are accessed through EPM Workspace.

• Performance Management Architect Server is running.

• Performance Management Architect is running.

  See the *Oracle Enterprise Performance Management System Installation and Configuration Guide*.

• Performance Management Architect web server is running.
Relational Database

A relational database account with sufficient privileges must be available to store Planning application data.

See the *Oracle Enterprise Performance Management System Installation Start Here* for supported database platforms and required privileges.

Accessing EPM System Products

You must access EPM System products such as Shared Services and EPM Workspace during provisioning. See the following topics:

- “Launching Shared Services Console” on page 15
- “Accessing EPM Workspace” on page 161
- “Accessing Administration Services Console” on page 162

Planning Provisioning Process

There are two types of Planning applications: Classic and Performance Management Architect. Classic Planning applications are stand-alone applications that do not share dimensions and members with other Planning applications. Classic Planning applications are created using the Classic Application Wizard.

Planning applications created using Performance Management Architect are referred to as Performance Management Architect Planning applications throughout this document. Performance Management Architect Planning applications can share dimensions and members.

Provisioning users and groups to work with Planning applications is a process.

Process Overview

Subtopics

- Classic Planning
- Performance Management Architect Planning

Classic Planning

The steps involved in provisioning Classic Planning applications are depicted in the following illustration.
Performance Management Architect Planning

The steps involved in provisioning Performance Management Architect Planning applications are depicted in the following illustration.

Creating Planning Data Source

Each Planning application requires a unique data source, which comprises connection information for a Planning application database and an Essbase Server. Because a Planning application database can store information from only one Planning application, each data source requires a unique database. Many data sources can use an Essbase Server.

**Note:** The data sources that you create using this process can be used for classic and Performance Management Architect Planning applications.

To create a data source:

2. **Select Navigate, then Administrator, and then Planning Administration.**
3. **In Planning Administration, click Manage Data Source.**
4. **From Actions in Manage Data Source, select Create.**
5. **In Data Source Name, enter a name.**
6 From Database, select the database type for the Planning application database.

7 Enter connection information for Application Database and Essbase Server. Ensure that you enter information for an Essbase Server administrator (or Functional Administrator) in Essbase Server settings. Consult online help for assistance.

8 Click Validate to validate the Application Database Connection and the Essbase Server Connection.

9 Click Save to create the data source.

Creating Classic Planning Applications with Dimensions and Members

A Planning installation can support multiple Planning applications. The application that you create is automatically registered with Shared Services.

Creating a classic Planning application with dimensions and members involves the following steps:

- “Creating Classic Planning Application” on page 85
- “Accessing Planning Applications” on page 86
- “Creating Dimensions and Members in Classic Planning Applications” on page 86

Creating Classic Planning Application

To create an application:

1 Access EPM Workspace as a Functional Administrator. See “Accessing EPM Workspace” on page 161.

2 Select Navigate, then Administer, and then Planning Administration.

3 In Planning Administration, click Manage Applications.

4 From Actions in Manage Applications, select Create.

5 In Data Source, select a data source.

6 In Application, enter an application name (maximum eight characters). Application names should not contain special characters (for example, a space or an asterisk).

7 In Application Type, select the type of application to create.

   Select Sample to use sample Planning application settings. You cannot select information for Calendar, Currencies, and Plan Types for sample applications.

8 In Shared Services Project, select an application group to which the Planning application should be added.

   EPM System does not create a default Planning application group. You can create it as a custom group in Shared Services Console if needed. See “Creating Application Groups” on page 24.

9 Click Next.
10 If you are not creating a sample application, enter or select information on Calendar, Currencies, and Plan Types. Click Next after entering information on a screen. Consult online help for assistance.

11 Click Create to create the Classic Planning application.

**Note:** The Planning application that you created is listed in the **Essbase Servers** node of Administration Services and in Shared Services Console under the node representing the application group that you selected in step 8.

### Accessing Planning Applications

To open your Planning application:

2. Select File, then Open, then Applications, and then Planning.
3. Select the Planning application that you created.

### Creating Dimensions and Members in Classic Planning Applications

When you create a Planning application, default dimensions are populated in the application database. At this stage, you can perform these actions:

- Add custom dimensions to the application
- Add members to dimensions

To add dimensions and dimension members:

1. Open the Planning application. See “Accessing Planning Applications” on page 86.
2. Select Administration, then Manage, and then Dimensions.
3. Optional: Add a custom dimension.
   a. On Dimensions, click [ ].
   b. Enter a dimension name and other required values. Consult online help for assistance.

**Note:** You must select the Apply Security check box if you plan to define security access for the custom dimension.

   c. Click Save.

Custom dimensions that you create in Planning are not automatically written to the Essbase database. See “Working with Essbase Database” on page 97.

4. Add dimension members.

   All dimensions other than Currency, Period, and Year are secure dimensions. You can enforce security only on members (children) of secure dimensions.

   a. From Dimensions, select the dimension for which you want to define members.
b. Click **Add Child**

c. Enter a member name and other required values. Consult online help for assistance.

d. Click **Save**.

e. Repeat step 4.b–step 4.d to add members (children and siblings).

5 Update the Essbase database with custom dimensions and members data. See “Working with Essbase Database” on page 97 for instructions.

**Creating and Deploying Performance Management Architect Planning Applications**

**Note:** If you are using classic Planning, skip this section.

Performance Management Architect Planning applications are created from the Application Library.

Each Performance Management Architect Planning application requires a unique data source. A data source comprises connection information for a Planning application database and an Essbase Server. Because a Planning application database can store information from only one Planning application, each data source requires a unique database. Many data sources can point to an Essbase Server. See “Creating Planning Data Source” on page 84.

**Note:** The Performance Management Architect Planning application creation process allows you to create a data source before deploying your application. However, Oracle recommends that you create the data source as the first step in creating the application.

The applications that you deploy become a part of the Application Library. Planning applications are listed also in Shared Services Console and Administration Services Console.

➤ To create an application:


2. Select **Navigate**, then **Administer**, and then **Application Library**.

3. Select **File**, then **New**, and then **Application**.

4. In **Name**, enter an application name (maximum eight characters). Application names should not contain special characters (for example, a space or an asterisk).

5. In **Type**, select **Planning**.

**Note:** You can create an empty application, into which you can drag dimensions from the Dimension Library. To create an empty application, select Create Blank Application and click Finish.

6. **Optional:** Enter or select information in the **Planning** area.
a. To use multiple currencies, select **Use Multiple Currencies**.

b. To create an Oracle Hyperion Workforce Planning, data cube in Essbase, select **Workforce** and enter a name.

c. To create an Oracle Hyperion Capital Asset Planning, data cube in Essbase, select **Capital Asset** and enter a name.

7 In Calendar area, perform these actions:

a. Select **Create New Local Period Dimension** and enter a period name.

b. Select **Create New Local Year Dimension** and enter information:
   - Year Name
   - Fiscal Start Year
   - Total Years

8 Click **Next**.

9 On Dimension Selection, choose the dimensions for the application. You must create the required default dimensions—Entity, Version, Scenario, Account, Year, Period, Alias, and Currency—and custom dimensions, if needed, as local dimensions. The required dimensions are in bold type.

a. Click in the Dimension column, and then select **Create New Dimension**.

b. Enter a dimension name.

c. Click **OK**.

10 Click **Next** to seed the dimensions that you created.

Security access for custom dimensions can be defined only after you apply security to the dimension and its members.

To apply security to custom dimensions:

a. On Application Settings, expand the node representing your application.

b. Select the custom dimension for which the apply security property is to be defined.

c. In Properties, select **Apply Security**.

11 Click **Validate**. Correct reported errors. You can find detailed validation information in the Library Job Console. To open the Library Job Console, select **Navigate**, then **Administer**, and then **Library Job Console**.

12 Click **Finish**.

From the Dimension Library, you can add members for your application dimensions. At this stage, an icon for the application is displayed in the Application Library.

13 Create dimension members. Dimension members are the highest level at which access control can be defined. To create dimension members:

**Note:** Application dimensions can be protected by defining the users and groups that can access them. Access control can be defined for members of secure dimensions (default dimensions other than Currency, Period, and Year) from the Dimension Library.
a. Right-click the application dimension for which you want to define a member.
b. Select Create Member, and then As Child.

   **Note:** If you selected an existing dimension member, you can create a member as the child or sibling of the current member.
c. In the New Member dialog box, enter a name for the member.
d. Click OK.

14 Optional: Specify plan type performance settings. To specify plan type performance settings:
a. Right-click the application.
b. Select Performance Settings.
c. In Plan Type Performance Settings window, select a plan type (for example, Plan1, Plan2, or Plan3).
d. To change the performance setting for a dimension, double-click in the Density column.
e. Select a setting (Dense or Sparse).

15 Deploy the application:
a. In Application Library, right-click your Planning application.
b. Select Deploy, and then Application.

   Performance Management Architect validates the application. If no errors are found, the Deploy window opens.
c. Enter or select the required information. Consult online help for assistance.

   **Note:** You should select a data source for the application. See “Creating Planning Data Source” on page 84 for instructions to create data sources using classic Planning. You can also create data source by clicking the Create Datasource button next to the Data Source drop-down list.

   Ensure that you select an appropriate application group from Shared Services Project list.
d. Click Deploy.

   The deployment process takes awhile to finish. Performance Management Architect displays a deployment job ID that can be used to track deployment progress and reported errors.

### Provisioning Users and Groups with Planning Application Roles

Each Planning deployment can support multiple Planning applications. You must provision Planning users separately to each application.
Functional Administrator and Planning Provisioning Managers can provision Planning application users using the Shared Services Console.

To provision users or groups with Planning application roles:

1. Access Shared Services Console as a Functional Administrator or as a Provisioning Manager role of the Planning application that you want to provision. See: “Launching Shared Services Console” on page 15.

2. Provision users and groups to Planning application:
   a. Find a user or group to provision. See “Searching for Users, Groups, Roles, and Delegated Lists” on page 17.
   b. Right-click the user or group, and then select Provision.
   c. Optional: Select a view. Roles can be displayed in a hierarchy (tree) or a list. You must drill down the hierarchy to display available roles. The list view lists available roles but does not show their hierarchy.
   d. In Available Roles, expand the application group (for example, Planning) that contains your Planning application.
   e. Expand the node that represents your application.
   f. Select roles and click Add.

The selected roles are displayed in Selected Roles list. See Table 6 for a list of Planning application roles and the tasks to which they provide access.

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power Roles</strong></td>
<td></td>
</tr>
<tr>
<td>Administrator</td>
<td>Performs all application tasks except those reserved for the Application Owner and Mass Allocate roles. Creates and manages applications, manages access permissions, initiates the budget process, and designates the e-mail server for notifications. Can use the Copy Data function.</td>
</tr>
<tr>
<td>Provisioning Manager</td>
<td>Provisions users to the Planning application</td>
</tr>
<tr>
<td>Mass Allocation</td>
<td>Accesses the Mass Allocate feature to spread data multidimensionally down a hierarchy, even to cells not visible in the data form and to which the user does not have access. Any user type can be assigned this role, but it should be assigned sparingly.</td>
</tr>
<tr>
<td>Essbase Write Access</td>
<td>For planners and interactive users: Grants users access to Planning data in Essbase equivalent to their Planning access permissions. If security filters that limit access to year and period dimensions are not created, this role grants write access to all periods and years. Enables users having write access to change Planning data directly in Essbase using another product such as Oracle Hyperion Financial Reporting or a third-party tool.</td>
</tr>
<tr>
<td>Role</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Approvals Administrator      | Approvals Administrators are typically business users in charge of a region in an organization who need to control the Approvals process for their region but do not need to be granted the Planning Administrator role. Users with Approvals Administrator role can resolve any approval issue by manually taking ownership of the process. They can perform these tasks:  
  - Control approvals process  
  - Perform actions on Planning units to which they have write access  
  - Assign owners and reviewers for the organization under their charge  
  - Change the secondary dimension or update validation rules |
| Approvals Administrator role | consists of the following roles:  
  - Approvals Ownership Assigner  
  - Approvals Process Designer  
  - Approvals Supervisor |
| Approvals Ownership Assigner | Performs tasks assigned to Planner role. Approvals Ownership Assigners perform the following tasks for any member of the planning unit hierarchy to which they have write access:  
  - Assign owners  
  - Assign reviewers  
  - Specify users to be notified |
| Approvals Process Designer   | Performs tasks assigned to Planner and Approvals Ownership Assigner roles. Approvals process designers perform the following tasks for any member of the planning unit hierarchy to which they have write access:  
  - Change secondary dimensions and members of entities to which they have write access  
  - Change the scenario and version assignment for a planning unit hierarchy  
  - Edit data validation rules of data forms to which they have access |
| Approvals Supervisor         | Perform the following tasks for any member of the planning unit hierarchy to which they have write access even if they do not own the planning unit:  
  - Stop and start a planning unit  
  - Take any action on a planning unit  
  **Note:** Approval Supervisors cannot change data in planning units that they do not own. |
| Ad Hoc Grid Creator          | Creates and saves Smart Slices in addition to performing the tasks that an Ad Hoc User can perform |
| Ad Hoc User                  | Analyzes data forms using ad hoc features. |
| Task List Access Manager     | Not applicable to this release; reserved for future use. |

### Planner Roles

<p>| Planner | Enters and submits plans for approval and adapter processes. Uses reports that others have created, views and uses task lists, enables e-mail notification for themselves, and creates data using Oracle Smart View for Office. |</p>
<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interactive Roles</strong></td>
<td></td>
</tr>
<tr>
<td>Interactive User</td>
<td>Creates and maintains data forms, Smart View worksheets, business rules, task lists, Financial Reporting reports, and adapter processes. Manages the budget process. Can create Smart Slices in Smart View, use the Clear Cell Details function, and perform all Planner tasks. Interactive users are typically department heads and business unit managers.</td>
</tr>
<tr>
<td><strong>View Roles</strong></td>
<td></td>
</tr>
<tr>
<td>View User</td>
<td>Views and analyzes data through Planning data forms and any data access tools for which they are licensed (for example, Financial Reporting, Oracle Hyperion Web Analysis, and Smart View). Typical View users are executives who want to see business plans during and at the end of the budget process.</td>
</tr>
</tbody>
</table>

g. Click **Save**.  
h. Click **OK**.

3 Repeat the preceding step for each Planning application that you want to provision.

### Adding Users and Groups into Planning Database

After provisioning users and groups in Shared Services, you must add them to the Planning database to make the newly provisioned users and groups available to Planning applications.

**Note:** The following procedures presents one of the many methods you can use to add users and groups into the Planning database. For additional methods, see *Oracle Hyperion Planning User’s Guide*.

To populate users and groups in the Planning database:

2. Open the Planning application. See “Accessing Planning Applications” on page 86.
3. Select **Administration**, then **Application**, and then **Refresh Database**.
4. Select **Security Filters**.
5. Optionally select other database refresh options. See the *Oracle Hyperion Planning Administrator’s Guide*.
6. Click **Refresh**.
7. Click **Finish**.

### Assigning Access for Dimension Members

Application dimensions can be protected by defining the users and groups that can access them. Access control can be defined for members of secure dimensions (default dimensions other than Currency, Period, and Year).
Only the custom dimensions that were created with the **Apply Security** option support the assigning of access control to members.

To define access control:

2. **Open the Planning application.** See “Accessing Planning Applications” on page 86.
3. **Select Administration,** then Manage, and then **Dimensions.**

   **Note:** Classic Planning applications allow you to create members from this screen, but Performance Management Architect Planning applications do not. If you need to add dimensions or members to a Performance Management Architect Planning application, use the Dimension Library. You must validate and redeploy your Performance Management Architect Planning application if you change dimensions or members.

4. **Select the secure dimension for which security is to be assigned.**
5. **Right-click the dimension and select Expand to display dimension members and their children.**
6. **Select a dimension member.**
7. **From Actions, select Assign Access.**
8. **In Assign Access window, click** ![add](image)

   **Note:** Only the users and groups provisioned to the current application are listed on the Add Access window.

9. **Select the users or groups who should be granted access to the selected member.**
10. **From Type of Access, select the access to grant on the member.**
11. **From the list, select access relationship.** For example, select **Children** to assign access to the children of the selected member.
12. **Select Add.**
13. **Select Close to return to the Assign Access window.**
14. **Repeat step 6—step 13 to assign access to additional members.**

**Working with Data Forms**

Data forms are grids for entering data. You can create many data forms to meet users' needs.

**Creating Data Form Folders**

To create data form folders:

2 Open a Planning application. See “Accessing Planning Applications” on page 86.
3 Select Administration, then Manage, and then Forms and Ad Hoc Grids.
4 Expand a folder in Form Folders, and then click [+] .
5 Enter a folder name.
6 Click OK.

Creating Data Forms

Because composite data forms are comprised on simple data forms, you must create simple data forms before creating composite data forms. Composite data forms display many data forms simultaneously, including those associated with different plan types. Users can enter data and see results aggregated to an upper-level intersection, such as Total Revenue. Some tasks for creating composite data forms are the same as for regular data forms.

To create data forms:
1 Access EPM Workspace. See “Accessing EPM Workspace” on page 161.
2 Open a Planning application. See “Accessing Planning Applications” on page 86.
3 Select Administration, then Manage, and then Forms and Ad Hoc Grids.
4 To create a data form, select an option from Actions:
   - Select Create simple form to create a simple data form.
   - Select Create composite form to create a composite data form.
5 Define form properties, layout and business rules. Consult online help for assistance.

Granting Access to Data Form Folders

Only planners, interactive users, and administrators can be granted access to folders.

To grant access to data form folders:
1 Access EPM Workspace. See “Accessing EPM Workspace” on page 161.
2 Open a Planning application. See “Accessing Planning Applications” on page 86.
3 Select Administration, then Manage, and then Forms and Ad Hoc Grids.
4 Select a folder.
5 Click [ ] .
6 Click [ ] .
7 Select the users and groups that are to be granted access to the folder.

Note: Only the users and groups provisioned to the current application, but have not been granted access to folder, are listed on the Add Access screen.
Select the type of access (Read, Write, or None) to grant.

Click Add.

Click OK.

In the Add Access window, click Close.

In the Assign Access window, click Close.

Granting Access to Data Forms

Planners can view or enter data only into data forms to which they have access (and can work only with members to which they have access). Administrators and interactive users have write access to all data forms for design modifications.

Only planners and interactive users can be granted access to data forms.

To grant access to data forms:

1. Open a Planning application. See “Accessing Planning Applications” on page 86.
2. Select Administration, then Manage, and then Forms and Ad Hoc Grids.
3. Select the folder that contains the form to which access is to be granted.
4. In Forms and Ad Hoc Grid Management, select a form.
5. Click (image)

6. In Assign Access window, click (image)

7. Select the users or groups that are to be granted access to the form.

Note: Only the users and groups provisioned to the current application, but not assigned access to the form, are listed on the Add Access window.

8. Select the type of access (Read, Write, or None) to grant.
9. Click Add. Consult online help for assistance.
10. In the Add Access window, select Close.
11. In the Assign Access window, select Close.

Working with Task Lists

Task lists guide users through the planning process by listing tasks, instructions, and due dates. Administrators and interactive users create and manage tasks and task lists. Users who are granted the Task List Access Manager role can assign access to task lists and tasks.
Creating Task List Folders

1. Open a Planning application. See “Accessing Planning Applications” on page 86.
2. Select Administration, then Manage, and then Task Lists.
3. In Manage Task Lists, select a task list folder, and then click.
4. Enter a folder name.
5. Click OK.

Creating Task Lists

Task lists help organize tasks. Administrators and interactive users create and manage tasks and task lists.

1. Open a Planning application. See “Accessing Planning Applications” on page 86.
2. Select Administration, then Manage, and then Task Lists.
3. From Manage Task Lists, select a folder in which to store the task list.
4. In Task List, click.
5. Enter a task list name, and click OK.

Creating Tasks

1. Open a Planning application. See “Accessing Planning Applications” on page 86.
2. Select Administration, then Manage, and then Task Lists.
3. From Manage Task Lists, select the folder containing the task list to which you want to add the task.
4. From Task List, select a task list.
5. Click.
6. In the Edit Task List window, click.
7. Create task by entering information. Consult online help for assistance.
8. Click Save.
Granting Access to Task Lists

To grant access to task lists:

1. Open a Planning application. See “Accessing Planning Applications” on page 86.
2. Select Administration, then Manage, and then Task Lists.
3. From Manage Task Lists, select a task list folder.
4. Select a task list.
5. Click Add.
6. In the Assign Access window, click Add.
7. Select the users or groups that are to be granted access to the task list.

Note: Only the users and groups provisioned to the current application, but do not have access to the task list, are listed on the Add Access window.
8. Select the type of access (Assign, Manage, Manage and Assign, or None) to grant. Consult online help for assistance.
9. Click Add.

Working with Essbase Database

Planning applications require an Essbase database to store outlines, dimensions and their members, data forms, and filters. Because this database is not automatically created during the Planning application creation process, you must create it.

Data about custom dimensions and members and data forms are not automatically written into the Essbase database. If you create custom dimensions after creating the database, you must refresh the database to write the information into it.

To work with the Essbase database:

1. Open the Planning application. See “Accessing Planning Applications” on page 86.
2. Select Administration, then Application, and then Create Database.
   Existing dimension, dimension member, and access permission data is automatically written into the database.

   Note: In Administration Services, the database that you created is listed under your Planning application node within the Essbase Server node.
4. Click Create.
Setting Applications in Production Mode

By default, newly created Planning applications are placed in maintenance mode, which permits only Planning administrators to access them.

**Note:** You must be a Planning administrator to perform this task.

To put Planning applications in production mode:

1. Open the Planning application. See “Accessing Planning Applications” on page 86.
2. Select Administration, then Application, and then Settings.
3. In **Enable Use of application for**, select **All Users**. This field is in the Application Maintenance Mode section on the System Settings tab.
4. Click **Save**.

Generating Access Control Report for Planning Applications

From Shared Services Console, you can view current access permissions and print reports.

To generate access control report:

1. Access Shared Services Console as a user who is provisioned as Planning Administrator. See “Accessing Shared Services” on page 161.
2. In **View Pane**, expand **Application Groups**.
3. Expand the application group (for example, Planning) that contains your Planning application.
4. Right-click your application, and then select **Access Control Report**.
5. Select the following for which the report is to be generated:
   - Users or groups
   - Application objects
7. Click **Finish**.
Financial Management Security Model

Financial Management roles are assigned to users from the Shared Services Console. Data security can be specified on dimensions such as Entities, Scenarios, Customs. Security is defined for each dimension independently in what is called a Financial Management security class, which defines access rights (Modify, View, and so on) on a specific set of members of one dimension. Usually, security classes are assigned to groups of users. Artifacts (Journals, Web Forms, Web Grids, and Task Lists) also are assigned security classes.

**Note:** Security cannot be defined on an intersection of members from different dimensions.

Financial Management uses its own native interface to define data security. It maintains its own repository of data security information. Assigning data security to user and groups is performed using the Shared Services Console.

Prerequisites

Subtopics

- Foundation Services
- Foundation Services Web Server
- Performance Management Architect (Optional)
- Relational Database

Foundation Services

- Foundation Services is running. Starting Foundation Services starts these components:
Optional: The external user directories that are the sources for user and group information for Financial Management are configured in Shared Services.

Foundation Services Web Server
Foundation Services web server must be running.

Performance Management Architect (Optional)
Performance Management Architect is required to create Financial Management applications using the Application Library. Performance Management Architect components such as Application Library and Dimension Library are accessed through EPM Workspace.

- Performance Management Architect Server is running.
- Performance Management Architect is running.
  
  See the *Oracle Enterprise Performance Management System Installation and Configuration Guide*.

- Performance Management Architect web server is running.

Relational Database
A relational database account with sufficient privileges must be available to store Financial Management application data.

See the *Oracle Enterprise Performance Management System Installation Start Here* for supported database platforms and required privileges.

Accessing EPM System Products
You must access EPM System Products such as Shared Services and EPM Workspace during provisioning. See the following topics:

- “Launching Shared Services Console” on page 15
- “Accessing EPM Workspace” on page 161
- “Accessing Administration Services Console” on page 162
You can use Classic Application Administration, the Application Library, and the Financial Management Desktop to create Financial Management applications. Of these, Classic Application Administration and the Application Library interfaces are accessed through EPM Workspace.

Financial Management applications created through Classic Application Administration and Financial Management Desktop are Classic Financial Management applications. Classic applications are stand-alone applications with their own profiles that define their calendar and the languages. A classic application has its own metadata file that defines its dimensions. Classic applications do not share dimensions and members with other Financial Management applications. Financial Management applications created using the Application Library of Performance Management Architect can share dimensions and members with each other and with Planning applications.

Classic and Performance Management Architect applications require that you create a security class before you can load or deploy metadata using that security class. For Performance Management Architect applications, security classes and metadata deployment can occur simultaneously. For Classic applications, security classes must already be available before you can load metadata into the application.

A major difference between classic and Performance Management Architect Financial Management applications is the way in which artifact-level security is defined. Classic Financial Management applications allow you to create or load security classes after you create the application while Performance Management Architect Financial Management applications do not permit it. You must define security class members and assign them to securable dimension members while creating the application.

The behavior of Financial Management applications is identical regardless of how you created them.

**Process Overview**

The steps involved in creating and provisioning Financial Management applications using the Classic Application Administration menu option in EPM Workspace are depicted in the following illustration.
Creating Classic Applications

Creating classic Financial Management applications involves these steps:

- “Creating Application Profiles” on page 102
- “Creating Classic Financial Management Applications” on page 103

Creating Application Profiles

An application profile contains language, calendar, frequency, and period information for an application. You must specify a profile for each application that you create; you can use a profile for multiple applications.

Note: You create application profiles using the Financial Management Client, which can be downloaded from EPM Workspace.
To create application profiles:

1. In Financial Management Client, select **Define Application Profile**.
2. Select **Create a New Application Profile**.
3. Click **Next**.
4. Enter settings for the following:
   - Application Languages
   - Calendars
   - Frequencies
   - Periods

See the *Oracle Hyperion Financial Management Administrator’s Guide* for detailed information on entering these settings.

5. In Save Profile screen, enter a profile name, and click **Finish**.

By default, application profiles are stored in `EPM_ORACLE_HOME/products/FinancialManagement` with the `.per` file extension; for example, `C:/Oracle/Middleware/EPMSystem11R1/products/FinancialManagement/Sample Apps \APP_NAME/Profileprofile2.per`.

---

**Creating Classic Financial Management Applications**

Classic Financial Management applications are created using the Classic Application Administration menu option in EPM Workspace.

To create classic Financial Management applications:

2. Select **Navigate**, then **Administer**, and then **Consolidation Administration**.
3. From Consolidation Administration, select **Administration**, and then **Applications**.
4. From Applications, select **Actions**, and then **Create**.
5. In **Application Name**, enter an application name. Maximum 10 alphanumeric characters or 12 bytes. The application name cannot start with a number or contain spaces or special characters; for example, ampersand (&) or asterisk (*).
6. In **Application Profile**, select the profile that you want to use for this application. See “Creating Application Profiles” on page 102.
7. In **User Management Project**, select an existing Shared Services application group to which the application should be added.
   You can create a custom application group in Shared Services if needed.
9. Click **Create**.
Note: The Financial Management application that you created is listed in Shared Services Console under the node representing the application group that you selected in step 7.

Creating Performance Management Architect Financial Management Applications

Performance Management Architect Financial Management applications are created using the Application Library, which is accessed from EPM Workspace.

To create Performance Management Architect Financial Management applications

2. Select Navigate, then Administer, and then Application Library.
3. In the Application Library, select File, then New, and then Application.
4. In Name, enter an application name (maximum eight characters). Application names should not contain special characters (for example, a space or an asterisk).
5. In Type, select Consolidation or Tax Provisioning.

Additional fields are displayed on the screen.

Note: You can create an empty application, into which you can drag dimensions from the Dimension Library. To create an empty application, select Create Blank Application, and then click Finish.

6. Optional: Select Auto Create Local Dimensions to automatically create the dimensions required in the application.

The dimension name for each new dimension is identical to the dimension type with (New) in parentheses. Automatically creating local dimensions saves time because it populates the required dimensions to create the application.

7. In Application Type select the type of application (Standard Consolidation or Tax Provisioning) that you want to create.
8. Click Next.
9. On Dimension Selection, choose the dimensions for the application. You must create the required default dimensions—Entity, Account, Scenario, Year, Period, ICP, View, Value, Alias, Currency, Consolidation Method, and Security Class, To Custom, and From Custom—as local dimensions.

Note: Be sure to create security classes as members of Security Class dimension. Associate members of Security Class dimension with members of the Account dimension to define the security class for Account dimension members.

a. Click in the Dimension column, and then select Create New Dimension.
In the Add New Dimension window, enter a dimension name and an optional description.

- Click **OK**.

10 **Click Next** to seed the dimensions that you created.

11 **Click Validate** to validate the application. Correct reported errors. You can find detailed validation information in the Library Job Console. To open the Library Job Console, select **Navigate**, then **Administer**, and then **Library Job Console**.

12 **Click Finish**.

From the Dimension Library, you can add members for your application dimensions. An icon for the application is displayed in the Application Library.

13 **Deploy the application**:
   
a. In Application Library, right-click your Financial Management application.

b. Select **Deploy**, and then **Application**.

   Performance Management Architect validates the application. If no errors are found, the Deploy window opens.

c. Enter or select the required information. Consult online help for assistance.

d. Click **Deploy**.

   The deployment process takes awhile to finish. Performance Management Architect displays a deployment job ID that can be used to track deployment progress and reported errors.

---

**Provisioning Groups with Financial Management Application Roles**

Each Financial Management instance (deployment) can support multiple applications. You must provision Financial Management users separately to each application.

Shared Services Administrators and Financial Management Provisioning Managers can provision Financial Management application users using Shared Services Console.

To provision users or groups with Financial Management application roles:

1. **Access Shared Services Console** as a Functional Administrator or as a user provisioned with the Provisioning Manager role for the Financial Management application that you want to provision. See “Accessing Shared Services” on page 161.

2. **Provision users or groups to the Financial Management application**.
   
a. Find a user or group to provision.

b. Right-click the user or group, and then select **Provision**.

c. **Optional**: Select a view.
Roles can be displayed in a hierarchy (tree) or a list. You must drill down the hierarchy to display available roles. The list view lists available roles but does not show their hierarchy.

d. In **Available Roles**, expand the application group (for example, Financial Management) that contains your Financial Management application.

e. Expand the node that represents your application.

f. Select the roles that you want to assign to the users or groups, and click [ ].

See Table 7 for a list of Financial Management roles and the tasks to which they provide access.

**Table 7  Financial Management Roles**

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power Roles</strong></td>
<td></td>
</tr>
<tr>
<td>Application Administrator</td>
<td>Performs all Financial Management tasks. Access to this role overrides any other access setting for the user.</td>
</tr>
<tr>
<td>Load System</td>
<td>Loads rules and member lists</td>
</tr>
<tr>
<td>Inter-Company Transaction Admin</td>
<td>Opens and closes periods, locks and unlocks entities, and manages reason codes. Users with the role can also perform all intercompany tasks.</td>
</tr>
<tr>
<td><strong>Interactive Roles</strong></td>
<td></td>
</tr>
<tr>
<td>Rules Administrator</td>
<td>Performs any Oracle Hyperion Calculation Manager tasks for the specific application</td>
</tr>
<tr>
<td>Rules Designer</td>
<td>Creates new rules objects and modifies or deletes rules objects</td>
</tr>
<tr>
<td>Approve Journals</td>
<td>Approves or rejects journals</td>
</tr>
<tr>
<td>Create Journals</td>
<td>Creates, modifies, deletes, submits, and unsubmits journals</td>
</tr>
<tr>
<td>Create Unbalanced Journals</td>
<td>Creates unbalanced journals</td>
</tr>
<tr>
<td>Default</td>
<td>Opens and closes applications; manages documents and favorites; manages Smart View; and accesses running tasks, data tasks, and load and extract tasks. Cannot extract metadata or rules.</td>
</tr>
<tr>
<td>Journals Administrator</td>
<td>Performs all tasks related to journals</td>
</tr>
<tr>
<td>Post Journals</td>
<td>Posts and unpasts journals</td>
</tr>
<tr>
<td>Manage Templates</td>
<td>Grants access to the journals templates for managing journals</td>
</tr>
<tr>
<td>Generate Recurring</td>
<td>Grants access to the generate recurring task for managing journals</td>
</tr>
<tr>
<td>Review Supervisor</td>
<td>Starts process management units and approves and publishes process management data. Can promote or reject process units, depending on process level.</td>
</tr>
<tr>
<td>Role</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Reviewer 1 through Reviewer 10</td>
<td>Views and edits a block of data when that data is at the user's designated process management level</td>
</tr>
<tr>
<td>Submitter</td>
<td>Submits a block of data for final approval</td>
</tr>
<tr>
<td>Lock Data</td>
<td>Locks data in Data Explorer</td>
</tr>
<tr>
<td>Unlock Data</td>
<td>Unlocks data in Data Explorer</td>
</tr>
<tr>
<td>Consolidate All</td>
<td>Runs consolidate all</td>
</tr>
<tr>
<td>Consolidate</td>
<td>Runs consolidate</td>
</tr>
<tr>
<td>Consolidate All with Data</td>
<td>Runs consolidate with all data</td>
</tr>
<tr>
<td>Run Allocation</td>
<td>Runs allocations</td>
</tr>
<tr>
<td>Manage Data Entry Forms</td>
<td>Manages data entry forms on the web</td>
</tr>
<tr>
<td>Save System Report On Server</td>
<td>Saves system reports on server</td>
</tr>
<tr>
<td>Load Excel Data</td>
<td>Loads data from Smart View</td>
</tr>
<tr>
<td>Inter-Company Transaction User</td>
<td>Creates, edits, deletes, loads, and extracts transactions. Runs matching report by account or ID, runs transaction report, and drills through from modules.</td>
</tr>
<tr>
<td>Inter-Company Transaction Match Template</td>
<td>Manages intercompany matching templates</td>
</tr>
<tr>
<td>Inter-Company Transaction Auto Match by Account</td>
<td>Automatically matches intercompany transactions by account</td>
</tr>
<tr>
<td>Inter-Company Transaction Auto Match by ID</td>
<td>Automatically matches intercompany transactions by ID</td>
</tr>
<tr>
<td>Inter-Company Transaction Manual Match with Tolerance</td>
<td>Manually matches intercompany transactions with tolerance check</td>
</tr>
<tr>
<td>Inter-Company Transaction Manual Match</td>
<td>Manually matches intercompany transactions</td>
</tr>
<tr>
<td>Inter-Company Transaction Unmatch</td>
<td>Unmatches intercompany transactions</td>
</tr>
<tr>
<td>Inter-Company Transaction Post/Unpost</td>
<td>Posts and unposts intercompany transactions</td>
</tr>
<tr>
<td>Enable write back in Web Grid</td>
<td>Enters and saves data directly to a Web Grid</td>
</tr>
<tr>
<td>Database Management</td>
<td>Copies and clears data and deletes invalid records</td>
</tr>
<tr>
<td>Manage Ownership</td>
<td>Enters and edits ownership information</td>
</tr>
<tr>
<td>Manage Custom Documents</td>
<td>Loads and extracts custom documents to and from the server</td>
</tr>
<tr>
<td>Extended Analytics</td>
<td>Exports data to a database</td>
</tr>
<tr>
<td>Data Form Write Back from Excel</td>
<td>Submits data from Smart View while using a Web Data Entry Form</td>
</tr>
<tr>
<td><strong>View Roles</strong></td>
<td></td>
</tr>
<tr>
<td>Advanced User</td>
<td>Uses the Browser View and can access Running Tasks</td>
</tr>
<tr>
<td>Role</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td>Rules Viewer</td>
<td>Views rules objects</td>
</tr>
<tr>
<td>Read Journals</td>
<td>Reads journals</td>
</tr>
<tr>
<td>Receive Email Alerts for Process Control</td>
<td>Receives e-mails</td>
</tr>
<tr>
<td>Receive Email Alerts for Intercompany</td>
<td>Receives e-mails</td>
</tr>
<tr>
<td>Reserved</td>
<td>Not currently used</td>
</tr>
<tr>
<td>View Data Audit</td>
<td>View and export data audit information</td>
</tr>
<tr>
<td>View Task Audit</td>
<td>View and export task audit information</td>
</tr>
</tbody>
</table>

3. Repeat step 2 for each Financial Management application that you want to provision.

### Creating Security Classes

Security classes are usually groupings of metadata elements or application artifacts (Web Forms, Web Grids, and so on) that determine the access that users have to application elements. A security class is assigned to metadata elements or artifacts. Users and groups are assigned permissions on security classes.

#### Classic Applications

You can create security classes anytime. Only Provisioning Managers and Shared Services Administrators can define security classes for applications.


#### Performance Management Architect Applications

For Performance Management Architect Financial Management applications, security classes are created as members of the Security Class dimension. Members of the Security Class dimension are then assigned to members of Account dimension to define the security class that controls access to the Account dimension member.

### Creating Financial Management Artifacts

Financial Management security is defined for each dimension independently in what is called a security class, which defines access rights on a set of members of a dimension. Usually, security
classes are assigned to groups of users and to Financial Management artifacts (Journals, Web Forms, Web Grids, and Task Lists). You should create Financial Management artifacts and assign security classes to them to control access.

Access to journals, data forms, and data grids are controlled by the security class assigned to each artifact. Users and groups that are provisioned with the security class assigned to an artifact gain access to the artifact in the Financial Management application.

**Loading Journals**

Many external general ledger systems can generate ASCII text files containing journal information that you can load into a Financial Management application. If necessary, you can edit the file before loading it into your Financial Management application.

Sample journal (.jlf) files that you can use to model your journal file are in the `EPM_ORACLE_HOME/products/FinancialManagement/SampleApps` directory.

Journals are loaded using the Replace mode, which clears all data for a journal label before loading the new journal data. Financial Management administrators can load working, rejected, submitted, approved, and posted journals as well as standard and recurring journal templates.

**Note:** Before you can load journals, you must open the periods to which to load journals. See “Managing Periods” in the *Oracle Hyperion Financial Management User’s Guide*.

You can only replace working and submitted journals. You cannot overwrite approved or posted journals.

To load journals:

1. Open a Financial Management application.
2. Expand Application Tasks, and then select Load, and then Journals.
3. In Journal File, enter the file name to load, or click Browse and find the file to load.
4. In Delimiter Character, specify the character that is used to separate information in the file.
5. Specify other settings as needed. Consult online help for assistance.
6. Click Load.

**Creating Data Forms**

A data form is generally used to enable Financial Management users to enter data into the database from an interface such as a web browser, and to view and analyze data or related text. Two methods are available for creating data forms:

- Using a script
- Using the Form Builder
See the *Oracle Hyperion Financial Management Administrator’s Guide* for the data form script syntax.

You must be a Financial Management administrator or a user with Manage Data Entry Forms role to create data forms.

➢ To create data forms using the Form Builder:

1. Open a Financial Management application.
2. In Document Manager, select **New**, and then **Data Form**.
3. Select **Administration**, then **Manage Documents**, and then **Data Forms**.
4. Click **New**.
5. Enter POV information, Row and Column information, and optionally, Form Details. Consult Online Help for assistance.
   - To scan the form for proper syntax, select **Scan**.
   - To reset the form values, select **Reset**.
6. Select **Actions**, and then **Save**.
7. Specify the data form name and the directory in which to store it.

   **Note:** Financial Management saves the data form only if it does not contain errors.

### Creating Data Grids

Data grids allow users to manually enter or edit Financial Management application data.

➢ To create data grids:

1. Open a Financial Management application.
2. In Document Manager, select **New**, and then **Data Grids**.
3. Click **New Data Grid**.
4. Enter POV information, Row and Column information, and grid display options. Consult Online Help for assistance.
5. Select **Actions**, and then **Save**.
6. Specify the data grid name, description, security class and location, and the directory in which to store it.

   **Note:** Financial Management saves the data grid only if it does not contain errors.

### Provisioning Security Classes

Security classes determine the access that users have to Financial Management applications. You assign 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 is granted access.

Access to journals, data forms, and data grids is controlled by the security class assigned to each artifact. Users and groups that are provisioned with the security class assigned to an artifact gain access to the artifact in the Financial Management application.

To grant access to security classes:

1. **Access Shared Services Console as Shared Services Administrator or as the Application Administrator of the Financial Management application for which you want to define access control.** See “Accessing Shared Services” on page 161.

2. **In the View Pane, perform these steps:**
   a. Expand **Application Groups**.
   b. Expand the application group that contains your Financial Management application.
   c. Right-click the Financial Management application for which security roles access is to be set, and then select **Assign Access Control**.

   Users and groups that are provisioned with roles from the selected application, along with their current security class assignments, are listed on **Applications**. Security classes can be assigned to these users and groups only.

3. **Optional: Add security classes for classic applications.**
   a. From **Actions**, select **Add Security Classes**.
   b. In **Class Name**, enter a name for the new security class.
   c. Click **OK**.

4. **On Application**, set the access right each user or group has to each security class. By default, no access right is granted to rely provisioned application users and groups. Consult online help for assistance.
   - To change all the security class access assignment of one user or group, right-click the user or group name and then select an access level.
   - To set the same all the security class access assignment levels for many users and groups, while holding down the control key, right-click the user or group names and then select an access level.
   - To change the access level for one security class, right-click the cell that lists the access level and then select a level.

Available access levels are explained in Table 8.

<table>
<thead>
<tr>
<th>Access Level</th>
<th>Permitted Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>No access to elements assigned to the security class.</td>
</tr>
<tr>
<td>Metadata</td>
<td>User can view a specified member in a list but cannot view or modify data for the member.</td>
</tr>
<tr>
<td>Read</td>
<td>User can view data for elements assigned to the security class but cannot promote or reject.</td>
</tr>
<tr>
<td>Access Level</td>
<td>Permitted Tasks</td>
</tr>
<tr>
<td>--------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Promote</td>
<td>User can view data for elements assigned to the security class and promote or reject.</td>
</tr>
<tr>
<td>All</td>
<td>User can modify data for elements assigned to the security class and promote and reject.</td>
</tr>
</tbody>
</table>

5 **From Actions**, select **Save**.

6 **Optional**: Select **Actions** and then Security Reports to generate a Security Report to verify that the security classes are properly assigned to provisioned users and groups.
Reporting and Analysis Security Model

Reporting and Analysis roles are assigned to users from the Shared Services Console. In addition to global roles, access preferences can be specified on Reporting and Analysis artifacts such as folders and documents (reports, charts, dashboards, and so on). Usually, access privileges on these artifacts are assigned to groups of users.

Reporting and Analysis products such as Financial Reporting, Oracle Hyperion Interactive Reporting, and Web Analysis require you to access data from a data source (for example, Essbase and Financial Management) to create meaningful reports and dashboards. Because the data that Reporting and Analysis products access is owned by the data source, a provisioning interdependency exists between the data source and Reporting and Analysis. For example, assume that user J Doe is provisioned with Reporting and Analysis roles but is not provisioned for Essbase application Esb_Demo1. In this scenario, J Doe cannot use Web Analysis to analyze data from Esb_Demo1 if the user logs into Essbase as j Doe. This user may, however, log into Essbase as a different user who is provisioned for Essbase application.
Prerequisites

Subtopics
- Foundation Services
- Foundation Services Web Server
- Reporting and Analysis Agent Services
- Reporting and Analysis Components
- Access to Data Source

Foundation Services
- Foundation Services is running. Starting Foundation Services starts these components:
  - Shared Services
  - EPM Workspace
- Optional: The external user directories that are the sources user and group information for Reporting and Analysis are configured in Shared Services.

Foundation Services Web Server
Foundation Services web server must be running.

Reporting and Analysis Agent Services
Reporting and Analysis Agent Services must be running.

Reporting and Analysis Components
The Reporting and Analysis component for which you want to provision users and groups, and their tools, should be running. Reporting and Analysis components and tools:
- Financial Reporting
- Interactive Reporting
- Oracle Hyperion SQR Production Reporting
- Web Analysis
- Financial Reporting Studio
- Interactive Reporting Studio
- Production Reporting Studio
- Oracle Hyperion Web Analysis Studio
Access to Data Source

Reporting and Analysis users and groups must be provisioned with data source roles that allow them to access data. Reporting and Analysis data sources include Essbase, Planning, and Financial Management applications. Products such as Interactive Reporting and Web Analysis can access relational data sources as well.

Essbase (Optional)

If you are using an Essbase application as the data source for Reporting and Analysis, ensure that the following are running:

- Essbase Server
- Essbase application that is used as the data source. You can start Essbase applications from Administration Services or using a MaxL command.

  See the Oracle Enterprise Performance Management System Installation and Configuration Guide.

Planning (Optional)

If you are using a Planning application as the data source for Reporting and Analysis, ensure that the following are running:

- Essbase Server
- Planning Server
- Planning application that is used as the data source

  See the Oracle Enterprise Performance Management System Installation and Configuration Guide.

Financial Management (Optional)

If you are using a Financial Management application as the data source for Reporting and Analysis, ensure that the following are running:

- Financial Management
- Financial Management application that is used as the data source

  See the Oracle Enterprise Performance Management System Installation and Configuration Guide.

Accessing EPM System Products

You must access EPM System products such as Shared Services and EPM Workspace during provisioning. See the following topics:

- “Launching Shared Services Console” on page 15
Reporting and Analysis Provisioning Process

The following Reporting and Analysis roles must be granted to the Functional Administrator to facilitate provisioning:

- Provisioning Manager
- Reporting and Analysis Administrator
- Reporting and Analysis Global Administrator

Process Overview

The steps involved in provisioning Reporting and Analysis users and groups are depicted in the following illustration.

* Data sources include Financial Management, Planning, Essbase applications, and relational databases
** Reporting and Analysis artifacts are created using tools such as Financial Reporting Studio, Production Reporting Studio, Interactive Reporting Studio, and Web Analysis
Provisioning Steps

Subtopics

- Provisioning the Data Source
- Provisioning Users and Groups with Reporting and Analysis Roles
- Creating Reporting and Analysis Artifacts
- Controlling Access to Reporting and Analysis Artifacts

Provisioning the Data Source

Data sources for Reporting and Analysis includes Essbase, Planning, and Financial Management applications. Reporting and Analysis users and groups must be provisioned with roles from the data source from which data is to be retrieved for analysis or presentation. Generally, this step is completed when you provision Essbase, Planning, or Financial Management applications. For detailed provisioning steps, see:

- Chapter 8, “Provisioning Essbase”
- Chapter 9, “Provisioning Planning”
- Chapter 10, “Provisioning Financial Management”

Provisioning Users and Groups with Reporting and Analysis Roles

Reporting and Analysis roles allow users to access tools such as Financial Reporting and Web Analysis. The data that users can view and analyze using these tools is controlled by the roles that they have in the data source. Users can view Financial Management application data in Financial Reporting if they have a Financial Management application role that allows them to view data.

To provision users or groups with Reporting and Analysis roles:

1. Access Shared Services Console as Functional Administrator or as a user provisioned with Reporting and Analysis Provisioning Manager role. See “Accessing Shared Services” on page 161.

2. Provision users or groups.
   a. Find users or groups to provision.
      See “Searching for Users, Groups, Roles, and Delegated Lists” on page 17.
   b. Right-click the user or group, and select Provision.
   c. Optional: Select a view.
      Roles can be displayed in a hierarchy (tree) or a list. You must drill down the hierarchy to display available roles. The list view lists available roles but does not show their hierarchy.
   d. In Available Roles, expand the Reporting and Analysis application group.
   e. Select the roles that you want to assign to the users or groups, and click Add.
See Table 9 for a list of Reporting and Analysis roles and Table 10 for useful role combinations.

**Table 9  Reporting and Analysis Roles**

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power Roles</strong></td>
<td></td>
</tr>
<tr>
<td>Reporting and Analysis Administrator</td>
<td>Conditionally accesses all resources (unless the file is locked by “no access”), but not all functionality; accesses the Administer and Impact Manager modules. Applies to Financial Reporting, Interactive Reporting, Production Reporting, and Web Analysis.</td>
</tr>
<tr>
<td>Reporting and Analysis Global Administrator</td>
<td>Universally and implicitly accesses all resources and functionality; accesses the Administer and Impact Manager modules. <strong>Note:</strong> Reporting and Analysis Global Administrators can never be denied access. Applies to Financial Reporting, Interactive Reporting, Production Reporting, and Web Analysis.</td>
</tr>
<tr>
<td>Content Manager</td>
<td>Manages imported repository content and execute tasks, with implicit access to all resources (unless the file is locked by “no access”); contains the Data Source Publisher role. Applies to Financial Reporting, Interactive Reporting, Production Reporting, and Web Analysis.</td>
</tr>
<tr>
<td>Data Source Publisher</td>
<td>Imports data source connectivity files. Applies to Interactive Reporting and Web Analysis.</td>
</tr>
<tr>
<td>Favorites Distributor</td>
<td>Pushes content to users' Favorites folders using the Favorites Manager. Applies to Financial Reporting, Interactive Reporting, Production Reporting, and Web Analysis.</td>
</tr>
<tr>
<td>Job Manager</td>
<td>Creates and manages public job parameters, output directories, and output printer locations. Applies to Interactive Reporting and Production Reporting. <strong>Note:</strong> This role does not apply to, and should not be assigned to Financial Management and Planning users who access Financial Reporting or Web Analysis through EPM Workspace.</td>
</tr>
<tr>
<td>Schedule Manager</td>
<td>Creates and manages events, calendars, time events, public parameters, and physical resources; creates batches; contains the Scheduler and Job Manager roles. Applies to Financial Reporting, Interactive Reporting, and Production Reporting.</td>
</tr>
<tr>
<td>Provisioning Manager</td>
<td>Provisions Reporting and Analysis users.</td>
</tr>
<tr>
<td><strong>Interactive Roles</strong></td>
<td></td>
</tr>
<tr>
<td>Analyst</td>
<td>Accesses interactive content using full analytic and reporting functionality. Applies to Interactive Reporting and Web Analysis.</td>
</tr>
<tr>
<td>Content Publisher</td>
<td>Imports, saves, and modifies batches, books, reports, and documents; creates and modifies shortcuts and folders. Deletes data sources and database connections in Financial Reporting through EPM Workspace. Applies to Financial Reporting, Interactive Reporting, Production Reporting, and Web Analysis.</td>
</tr>
<tr>
<td>Data Editor</td>
<td>Pushes Web Analysis data to Essbase.</td>
</tr>
<tr>
<td>Role</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Job Publisher*</td>
<td>Imports and modifies documents, jobs, and job output; runs jobs; contains the Smart Form Publisher role. Applies to Interactive Reporting and Production Reporting.</td>
</tr>
<tr>
<td>Personal Page Publisher*</td>
<td>Publishes Personal Pages to the repository, where they can be viewed by other repository users; contains the Personal Page Editor role. Applies to Interactive Reporting and Production Reporting.</td>
</tr>
<tr>
<td>Scheduler</td>
<td>Schedules jobs and batches using the Schedule module; navigates the repository and assigns access control; contains the Explorer and Job Runner roles. Applies to Financial Reporting, Interactive Reporting, and Production Reporting.</td>
</tr>
<tr>
<td>Smart Form Publisher*</td>
<td>Loads custom forms for programs (forms prompt job runners to enter information used to define jobs). Applies to Production Reporting. Note: You must have the Job Publisher role to leverage Smart Form Publisher functionality.</td>
</tr>
<tr>
<td>Personal Page Editor*</td>
<td>Creates, modifies, and customizes Personal Pages; copies content from other users' published Personal Pages. Applies to Interactive Reporting and Production Reporting.</td>
</tr>
</tbody>
</table>

**View Roles**

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic Viewer*</td>
<td>Views, reprocesses, and prints Interactive Reporting documents</td>
</tr>
<tr>
<td>Explorer</td>
<td>Lists repository content in the Explore module and in context using the Open dialog box; searches, views, and subscribes to content. Note: Access to the repository does not grant access to individual files and folders, which are secured by file properties and permissions. Applies to Financial Reporting, Interactive Reporting, Production Reporting, and Web Analysis.</td>
</tr>
<tr>
<td>Interactive Reporting Viewer*</td>
<td>Reviews and prints static Interactive Reporting documents</td>
</tr>
<tr>
<td>IR HTML Viewer</td>
<td>Uses the HTML Viewer to browse BQY documents. This role is not automatically assigned to users who were migrated from a previous version.</td>
</tr>
<tr>
<td>IR WebClient Viewer</td>
<td>Uses Interactive Reporting plug-in to browse BQY documents. This role is not automatically assigned to users that were migrated from a previous version.</td>
</tr>
<tr>
<td>Job Runner*</td>
<td>Runs jobs and views public job parameters and physical resources. Applies to Interactive Reporting and Production Reporting.</td>
</tr>
<tr>
<td>Personal Page Editor*</td>
<td>Creates, modifies, and customizes Personal Pages; copies content from other users' published Personal Pages. Applies to Interactive Reporting and Production Reporting.</td>
</tr>
<tr>
<td>Role</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Personal Parameter Editor</td>
<td>Defines points of view and personal parameters on database connections to customize query result sets. Applies to Interactive Reporting, Production Reporting, and Web Analysis.</td>
</tr>
<tr>
<td>Viewer</td>
<td>Reviews EPM Workspace content. The content is static and accessible only from the Favorites folder. <strong>Note:</strong> This role provides minimal user functionality; use it only when no other role assignments are possible. Applies to Financial Reporting, Interactive Reporting, Production Reporting, and Web Analysis.</td>
</tr>
</tbody>
</table>

**System Roles**

| Trusted Application         | Enables credentialed client-server communication of Interactive Reporting database connection files (*oce* extension) that encapsulate connectivity, database type, network address, and database user name information. |

This Reporting and Analysis role should not be assigned to Financial Management and Planning users who access Financial Reporting or Web Analysis through EPM Workspace.

**Table 10  Reporting and Analysis Role Combinations**

<table>
<thead>
<tr>
<th>Combined Role</th>
<th>Tasks</th>
<th>Access Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Explorer + Favorites</td>
<td>* Review interactive Web Analysis and Financial Reporting content in EPM Workspace</td>
<td>Share interactive content without modifying content or saving changes to the repository</td>
</tr>
<tr>
<td>Distributor + Personal Page Editor + Personal Parameter Editor</td>
<td>* List and subscribe to repository content</td>
<td></td>
</tr>
<tr>
<td>Parameter Editor</td>
<td>* Review accessible interactive content in Web Analysis Studio</td>
<td></td>
</tr>
<tr>
<td></td>
<td>* Access Personal Page</td>
<td></td>
</tr>
<tr>
<td></td>
<td>* Access Favorites Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td>* Define Web Analysis points of view, personal variables, and personal parameters, to customize the query result set</td>
<td></td>
</tr>
<tr>
<td>Explorer + Analyst + Content Publisher</td>
<td>* Review interactive Web Analysis, Financial Reporting, and Interactive Reporting content in the EPM Workspace</td>
<td>Interactively use document types to edit queries, rerun queries, and save changes back to the repository</td>
</tr>
<tr>
<td></td>
<td>* List and subscribe to repository content</td>
<td></td>
</tr>
<tr>
<td></td>
<td>* Review accessible interactive content in Web Analysis Studio</td>
<td></td>
</tr>
<tr>
<td></td>
<td>* Edit queries, rerun queries, 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>* Import and modify content</td>
<td></td>
</tr>
<tr>
<td>Combined Role</td>
<td>Tasks</td>
<td>Access Permissions</td>
</tr>
<tr>
<td>---------------</td>
<td>-------</td>
<td>--------------------</td>
</tr>
</tbody>
</table>
| Personal Page Publisher Data Source Publisher + Analyst + Report Designer + Job Manager | ● Create and distribute new interactive Web Analysis, Financial Reporting, and Interactive Reporting content  
● Create and distribute custom Web Analysis documents in Web Analysis Studio Design Documents interface  
● Access Oracle Hyperion Financial Reporting Studio  
● Access Personal Pages and distribute content to repository users  
● Distribute data source connectivity files to repository users  
● Distribute batches, books, reports, and documents to repository users  
● Import and modify Production Reporting files and Production Reporting output  
● Create, save, and run jobs  
● Create and manage output directories | Access most content creation functionality, but not 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 | Access all content creation and scheduling functionality but cannot administrator access to resources |
| Reporting and Analysis Administrator + Data Editor | ● Conditional access to all resources  
● Access the Administer module  
● Access the Impact Manager module  
● Ability to write edits back to Essbase | Access most functionality and modules, with conditional access to resources |

f. Click **Save**.

g. Click **OK**.

**Creating Reporting and Analysis Artifacts**

Reporting and Analysis artifacts include documents (reports and dashboards) and the directories that store them. Each Reporting and Analysis artifact can be separately provisioned. Use the following tools to create Reporting and Analysis artifacts:

● Financial Reporting Studio  
● Interactive Reporting Studio  
● Production Reporting Studio  
● Oracle Hyperion Web Analysis Studio

See the following sources for instructions to create Reporting and Analysis artifacts using these tools:

● *Oracle Hyperion Financial Reporting Studio User’s Guide*  
● *Production Reporting User’s Guide*  
● *Oracle Hyperion Interactive Reporting User’s Guide*
Controlling Access to Reporting and Analysis Artifacts

Reporting and Analysis artifacts are available to users after they are granted access to the artifacts by an administrator or a provisioning manager.

To set access control:
1. Access EPM Workspace as Reporting and Analysis Administrator or Provisioning Manager. See “Accessing EPM Workspace” on page 161.
2. Select Navigate, and then Explore.
3. From Folders, select the folder where Reporting and Analysis artifacts are stored.
4. Select the artifacts for which you want to specify access control.
5. Select Edit, and then Edit Permissions.
6. In Permissions, specify preferences to assign to the selected users and groups:
   a. Find the users, groups, and roles for which you want to specify access control and move them to the Selected Users, Groups and Roles list.
   b. Set access control.
      - The level and type of access that you can set change depending on the selected artifact. Access levels include Inherit, No Access, View, Modify, Full Control, Run, and Job Output Only. Access types include Access to Folder, Access to File, Access to Job, Access to Job Output, Adaptive State, and Favorite. Consult online help for assistance.
   c. Click OK.
Standard Profitability and Cost Management Security Model

Profitability and Cost Management roles are assigned to users from the Shared Services Console. Data security can be specified on Profitability and Cost Management dimensions.

Profitability and Cost Management applications are created and deployed using Performance Management Architect.

Prerequisites

Subtopics

- Foundation Services
- Foundation Services Web Server
- Performance Management Architect
- Essbase Server for Standard Profitability Only
- Administration Services
- Relational Databases for Detailed Profitability

Foundation Services

Foundation Services is running. Starting Foundation Services starts these components:

- Shared Services
- EPM Workspace
Foundation Services Web Server

Foundation Services web server must be running.

Performance Management Architect

Performance Management Architect components such as Application Library and Dimension Library are accessed through EPM Workspace.

- Performance Management Architect Server is running.
- Performance Management Architect is running.

See the Oracle Enterprise Performance Management System Installation and Configuration Guide.

- Performance Management Architect web server is running.

Essbase Server for Standard Profitability Only

Standard Profitability and Cost Management applications are deployed to Essbase. The financial and other data required for allocation in Standard Profitability and Cost Management are imported into an Essbase multidimensional database.

- Essbase is deployed in Shared Services mode by default. See the Oracle Enterprise Performance Management System Installation and Configuration Guide.

  If Essbase is not deployed in Shared Services mode, see Administration Services Online Help for instructions to convert a stand-alone Essbase Server to Shared Services mode.

- Essbase Server is running.

  See the Oracle Enterprise Performance Management System Installation and Configuration Guide.

Administration Services

Administration Services, the administration console for Essbase, is used to verify the creation of Standard Profitability and Cost Management cubes and to optimize cube outlines.

Ensure that Administration Services is running. See the Oracle Enterprise Performance Management System Installation and Configuration Guide.

Relational Databases for Detailed Profitability

For Detailed Profitability applications, dimensional data and model definition are stored in the same relational database schema that is used to store dimensional data and model definitions for Standard Profitability applications. This schema, referred to as the Product Schema, is created when Profitability and Cost Management is installed. Dimensional data is populated in the
Product Schema when you deploy your application from Performance Management Architect. Model definitions are stored in this schema as you build your model.

For Detailed Profitability applications, the business data upon which allocations are performed is also stored in the relational database (not in Essbase as is the case for Standard Profitability applications). This data resides in a separate database schema called the Model Data Schema. The Model Data Schema is user-defined and must reside in the same database instance as the Product Schema. Only Oracle and MS SQL Server databases are supported.

**Accessing EPM System Products**

You must access EPM System products such as Shared Services and EPM Workspace during provisioning. See the following topics:

- “Launching Shared Services Console” on page 15
- “Accessing EPM Workspace” on page 161
- “Accessing Administration Services Console” on page 162

**Profitability and Cost Management Provisioning Process**

You create Profitability and Cost Management applications from the Performance Management Architect Application Library, accessed through EPM Workspace. Profitability and Cost Management applications created using the Application Library can share dimensions and members.

**Process Overview**

This illustration shows the steps involved in creating and provisioning Profitability and Cost Management applications.

* Accessed through EPM Workspace
Creating and Deploying Profitability and Cost Management Applications

Profitability and Cost Management applications are created using the Application Library, accessed from EPM Workspace. You can create two types of Profitability and Cost Management applications—Standard and Detailed. For information on these application types, see the Oracle Hyperion Profitability and Cost Management User’s Guide.

You must be a Shared Services Administrator or a user with Profitability Application Creator role to create Profitability and Cost Management applications.

Creating and Deploying Standard Profitability Applications

Standard Profitability and Cost Management must abide by these conditions:

- At least one dimension has been set to POV (Point of View) type. Up to four dimensions may be marked as POV dimensions.
- The application should contain at least one Business dimension.
- The application must contain one each of these dimensions.
  - Measures
  - Allocation Type
- Dimension Sort Order is set for the model.

To create Standard Profitability and Cost Management applications:

2. Select Navigate, then Administer, and then Application Library.
3. In the Application Library, select File, then New, and then Application.
4. In Name, enter an application name (maximum seven characters). Application names should not contain special characters (for example, a space or an asterisk).
5. In Type, select Profitability.

Note: You can create an empty application, into which you can drag dimensions from the Dimension Library. To create an empty application, select Create Blank Application, and then click Finish.

Optional: Select Auto Create Local Dimensions to automatically create dimensions that are required in the application.

The dimension name for each new dimension is the dimension type with (New) in parentheses. Automatically creating local dimensions save time because it populates the required application dimensions.

6. Click Next.
Profitability and Cost Management uses dimensions and members created in Performance Management Architect to represent many structural elements of the business model in the Essbase outline.

8. In the Dimension Selection window, choose the dimensions for the application. You must select the required default dimensions as local dimensions:
   - Measures
   - AllocationType
   - POV (At least one and up to four POV dimensions may be included)
   - At least one Business dimension
   - Alias (optional)
   - Attribute (optional)

To create the dimensions for the application:
   a. Click in the Dimension column, and then select Create New Dimension.
   b. Enter a dimension name and an optional description.
   c. Click OK.

9. Click Next to create the application.

10. In Application Settings window, do the following tasks. See the Oracle Hyperion Profitability and Cost Management Administrator’s Guide.
   a. Ensure that Dimension Sort Order is set correctly for each dimension (Measure 1, Allocation Type 2, POV 3, Business Dimension 4).
   b. Ensure that each Business Dimension in the application has at least two members, including NoMember, and that NoMemer is the last member in the hierarchy.
   c. Select Deploy when finished. This selection launches the Deploy window when you click Finish.

11. Click Validate and correct reported errors. You can find detailed validation information in the Library Job Console. To open the Library Job Console, select Navigate, then Administer, and then Library Job Console. See the Oracle Hyperion Profitability and Cost Management Administrator’s Guide for a list of validations.

12. Click Finish.

13. Deploy the application. The deployment process registers the application with Shared Services and deploys it to the application server.
   a. Select Instance Name, Application Server, and Shared Services Project for the Profitability and Cost Management application. Consult online help for assistance.
   b. Select Deploy.

   The deployment process takes awhile to finish. Performance Management Architect displays a deployment job ID that you can use to track deployment progress and errors.
Creating and Deploying Detailed Profitability Applications

Detailed Profitability and Cost Management must abide by these conditions:

- At least one EPMA POV dimension is required.
- At least one Business dimension is required.
- MeasuresDetailed dimension is required.
- Dimension Sort Order is set for the model.

To create Detailed Profitability and Cost Management applications:

1. Populate the new shared library in Performance Management Architect using a flat file import or a Performance Management Architect interface table import.

   Caution! Add business dimensions to be included in the application, for example, Generic, Account, Entity, Time, or Country, to the Dimension Library before creating the application; otherwise, the dimensions will not be available for the Application Wizard to select.


3. Select Navigate, then Administer, and then Application Library.

4. In the Application Library, select File, then New, and then Application.

5. In Name, enter an application name (maximum seven characters). Application names should not contain special characters (for example, a space or an asterisk).

6. In Type, select Profitability.

   Note: You can create an empty application, into which you can drag dimensions from the Dimension Library. To create an empty application, select Create Blank Application, and then click Finish.

7. Optional: Under Description, enter a description.

8. Optional: Select Auto Create Local Dimensions to automatically create dimensions that are required in the application.

   The dimension name for each new dimension is the dimension type with (New) in parentheses. Automatically creating local dimensions save time because it populates the required application dimensions.

9. Under Profitability, click Create as Detailed Application.

10. Click Next.

    Profitability and Cost Management uses dimensions and members created in Performance Management Architect to represent many structural elements of the business model in the Essbase outline.

11. In the Dimension Selection window, choose the dimensions for the application. You must select the required default dimensions as local dimensions:

    - MeasuresDetailed (Required)
- At least one EPMA POV dimension (Required)
- At least one Business Dimension (Required)
- Alias Dimension (Optional)
- Attribute Dimensions (Optional)

To create the dimensions for the application:

a. Click in the Dimension column, and then select Create New Dimension.
b. Enter a dimension name and an optional description.
c. Click OK.

12 Click Next to create the application.

13 In Application Settings window, do the following tasks as outlined in the Oracle Hyperion Profitability and Cost Management Administrator's Guide.

a. Set the Dimension Sort Order for all model dimensions.
b. Reorder the NoMember to display this member as the last generation 2 member on the list.
c. Set the Properties for POV Dimensions, and the POV Display Order for multiple POV dimensions, if required.
d. Select Deploy when finished. This selection launches the Deploy window when you click Finish.

14 Click Validate and correct reported errors. You can find detailed validation information in the Library Job Console. To open the Library Job Console, select Navigate, then Administer, and then Library Job Console. See the Oracle Hyperion Profitability and Cost Management Administrator's Guide for a list of validations.

15 Click Finish.

16 Deploy the application. The deployment process registers the application with Shared Services and deploys it to the application server.

a. Select Instance Name, Application Server, and Shared Services Project for the Profitability and Cost Management application. Consult online help for assistance.
b. Select Deploy.

The deployment process takes awhile to finish. Performance Management Architect displays a deployment job ID that you can use to track deployment progress and errors.

**Deploying Standard Profitability and Cost Management Applications to Essbase**

You must do the following tasks before you can deploy Standard Profitability and Cost Management application to Essbase. When you deploy Standard Profitability to Essbase, you use the model information from the application to create an Essbase database that can be fine-tuned for profitability and cost analysis without needing to understand a scripting language.
Standard Profitability and Cost Management model design contains the information needed to generate Essbase outline and the calculation script required by the Essbase component of the model. Each model requires access to the following databases:

- A relational database to store the model design, including the dimension metadata deployed from Performance Management Architect
- An Essbase database that includes a Calculation database (BSO) and a Reporting database (ASO).

**Note:** Multiple models can be stored in a database.

Deploying Standard Profitability and Cost Management applications to Essbase involves these tasks:

- “Adding Stages to the Application” on page 130
- “Adding POV to the Application” on page 131

After completing these tasks, you must deploy the applications to Essbase.

**Adding Stages to the Application**

Standard Profitability and Cost Management uses model stages to reflect each major business process or activity. You assign dimensions to each stage to define the intersections where data for the stage is stored.

Newly deployed applications do not contain stages. You must add at least one model stage before you can deploy the application to Essbase.

**Note:** You can import model stage data into Standard Profitability and Cost Management. See the *Oracle Hyperion Profitability and Cost Management Administrator’s Guide*.

To add stages:

1. Open a Standard Profitability and Cost Management application.
   b. From EPM Workspace, select **File**, then **Open**, then **Applications**, and then **Profitability**.
   c. Select the Standard Profitability and Cost Management application that you created.
2. From **Manage Model** in the **View pane**, select **Stages**.
3. Click the Add icon above the Stage list.
4. Enter required stage information. Consult online help for assistance.
5. Click **OK**.
Adding POV to the Application

POVs are used to create various versions of a model; for example, to hold budget versus actual figures, or to play scenarios to measure the impact of various changes on the bottom line. You add a POV to view information and calculation for a model for the select year, period, scenario, or status. Newly deployed applications do not contain POV manager definitions.

**Note:** You can import model stage data into Standard Profitability and Cost Management. See the *Oracle Hyperion Profitability and Cost Management Administrator’s Guide*.

To add POV managers:

1. **Open the Standard Profitability and Cost Management application.**
   b. From EPM Workspace, select **File**, then **Open**, then **Applications**, and then **Profitability**.
   c. Select the Standard Profitability and Cost Management application that you created.

2. **From Manage Model in the View pane, select POV Manager.**

3. **Click Add.**

4. **Enter required POV information. Consult online help for assistance.**

5. **Click OK.**

Provisioning Users and Groups with Profitability and Cost Management Roles

Each Standard Profitability and Cost Management instance (deployment) can support multiple applications. You must provision Standard Profitability and Cost Management users separately to each application.


To provision users or groups with Standard Profitability and Cost Management application roles:

1. **Access Shared Services Console as a Functional Administrator or as a user provisioned with the Provisioning Manager role of the Profitability and Cost Management application that you want to provision.** See “Accessing Shared Services” on page 161.

2. **Provision users or groups to the Profitability and Cost Management application.**
   a. Find users or groups to provision.
      
      See “Searching for Users, Groups, Roles, and Delegated Lists” on page 17.
   b. Right-click the user or group, and select **Provision**.
   c. **Optional:** Select a view.
d. In **Available Roles**, expand the application group (for example, Financial Management) that contains your Standard Profitability and Cost Management application.

e. Expand the node that represents your application.

f. **Optional:** For Standard Profitability applications, select roles that you want to assign to the users or groups, and click **Add**.

See Table 11 for a list of Standard Profitability and Cost Management roles and the tasks to which they provide access.

<table>
<thead>
<tr>
<th>Table 11 Standard Profitability and Cost Management Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security Role</strong></td>
</tr>
<tr>
<td><strong>Power Roles</strong></td>
</tr>
</tbody>
</table>
| Administrator | - Create and maintain user accounts and security roles, and provision users, using Shared Services  
- Generate Essbase databases  
- Set up and maintain application preferences  
- Build the model database using Performance Management Architect to select the common dimensions and members  
- Create and maintain elements within the model, such as stages, drivers, POVs, driver selections, assignments, and application preferences  
- Perform POV Copy, calculation, validation, data entry, and trace allocations  
- Deploy to Essbase and generate calculation scripts  
- Import and export data  
- Use the Lifecycle Management Utility to promote data from one environment, such as development or testing, to another environment, such as production.  
- Back up and restore Profitability and Cost Management model components.  
- Monitor changes made to business objects.  
- Access Profitability Application Home screen to create, maintain, register, duplicate and update Profitability and Cost Management applications using Application Loader for Exalytics.  
- Create, edit, copy, delete, and launch queries from Smart View Connections screen |

**Note:** The Power User does not necessarily require specific security roles to perform tasks. For example, if a Power User runs a calculation from the Calculate screen, this action creates and executes a taskflow behind the scenes. The Power User does not require the Manage Taskflow role to perform this task, unless the Power User wants to access this task directly from the Manage Taskflows task.

| Power User | - Create and maintain elements within the model, such as stages, drivers, POVs, driver selections, assignments, and application preferences.  
- Perform POV Copy, calculation, validation, data entry and trace allocations.  
- Deploy to Essbase and generate calculation scripts.  
- Import and export data  
- Access Profitability Application Home screen to create, maintain, register, duplicate and update Profitability and Cost Management applications using Application Loader for Exalytics.  
- Create, edit, copy, delete, and launch queries from Smart View Connections screen |
### Security Role | Description
--- | ---
**Interactive Roles**

Interactive User | ● View all modelling screens  
| | ● View and modify data in the Data Entry screen  
| | ● View Trace Allocations  
| | ● Launch queries from Smart View Connections screen

View User | View only access for these functions:  
| | ● Trace Allocations  
| | ● Application Preferences  
| | ● Model Stages, Drivers and POVs

**Shared Services Roles**

Manage Taskflows | Required to create and edit taskflows.

Run Taskflows | Required to enable users to only run and view taskflows. Users with this role cannot create or edit taskflows.

g. **Optional:** For Detailed Profitability applications, select roles that you want to assign to the users or groups, and then click **Add**. See Table 12, “Detailed Profitability and Cost Management Roles” for a list of Detailed Profitability roles and tasks to which they provide access.
### Table 12  Detailed Profitability and Cost Management Roles

<table>
<thead>
<tr>
<th>Security Role</th>
<th>Description</th>
</tr>
</thead>
</table>
| Administrator | • Set up and maintain application preferences  
|               | • Build the model database using Performance Management Architect to select the common dimensions and members  
|               | • Create and deploy reporting views to the relational database  
|               | • Create, Read (View), Update and Delete the following functions:  
|               |   ◦ Stages  
|               |   ◦ Drivers  
|               |   ◦ POVs  
|               |   ◦ Driver Associations  
|               |   ◦ Assignments  
|               |   ◦ Application Preferences  
|               |   ◦ Calculation Rules  
|               |   ◦ Calculation Process Administration  
|               |   ◦ Jobs Library and Status  
|               |   ◦ Table Registration  
|               | • Perform the following tasks:  
|               |   ◦ POV Copy  
|               |   ◦ Validate  
|               |   ◦ Deploy  
|               |   ◦ Calculate  
|               |   ◦ Stop Jobs  
|               | • Use the Lifecycle Management Utility to promote data from one environment, such as development or testing, to another environment, such as production.  
|               | • Import and export data  
|               | • Back up and restore Profitability and Cost Management model components.  
|               | • Monitor changes made to business objects.  
|               | • Create, edit, copy, delete, and launch queries from Smart View Connections screen  
<p>|               | • Access Profitability Application Home screen to create, maintain, register, duplicate and update Profitability and Cost Management applications using Application Loader for Exalytics. |</p>
<table>
<thead>
<tr>
<th>Security Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power Roles</strong></td>
<td></td>
</tr>
</tbody>
</table>
| **Power User** | - Create and maintain user accounts and security roles, and provision users, using Shared Services  
- Create and deploy reporting views to the relational database  
- Access Profitability Application Home screen to create, maintain, register, duplicate and update Profitability and Cost Management applications using Application Loader for Exalytics.  
- Create, edit, copy, delete, and launch queries from Smart View Connections screen  
- Create, Read (View), Update and Delete the following functions:  
  - Stages  
  - Drivers  
  - POVs  
  - Driver Associations  
  - Assignments  
  - Application Preferences  
  - Calculation Rules  
  - Calculation Process Administration  
  - Jobs Library and Status  
  - Table Registration  
- Perform the following tasks:  
  - POV Copy  
  - Validate  
  - Deploy  
  - Calculate  
  - Stop Jobs  

*Note:* The Power User does not necessarily require specific security roles to perform tasks. For example, is a Power User runs a calculation from the Calculate screen, this action creates and executes a taskflow behind the scenes. The Power User does not require the manage Taskflow role to perform this task, unless the Power User wants to access this task directly from Manage Taskflows task. |
| **Interactive Roles** | |
| **Interactive User** | - View (Read) the following functions:  
  - Stages  
  - Drivers  
  - POVs  
  - Driver Association  
  - Assignments  
  - Application Preferences  
  - Calculation Rules  
  - Calculation Process Administration  
  - Jobs Library and Status  
  - Table Registration  
- Launch queries from Smart View Connections screen |
<table>
<thead>
<tr>
<th>Security Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View User</td>
<td>View (Read) the following functions:</td>
</tr>
<tr>
<td></td>
<td>- Stages</td>
</tr>
<tr>
<td></td>
<td>- Drivers</td>
</tr>
<tr>
<td></td>
<td>- POVs</td>
</tr>
<tr>
<td></td>
<td>- Driver Association</td>
</tr>
<tr>
<td></td>
<td>- Assignments</td>
</tr>
<tr>
<td></td>
<td>- Application Preferences</td>
</tr>
<tr>
<td></td>
<td>- Calculation Rules</td>
</tr>
<tr>
<td></td>
<td>- Calculation Process Administration</td>
</tr>
<tr>
<td></td>
<td>- Jobs Library and Status</td>
</tr>
<tr>
<td></td>
<td>- Table Registration</td>
</tr>
</tbody>
</table>

**Shared Services Role**

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage Taskflows</td>
<td>Required to create and edit taskflows.</td>
</tr>
<tr>
<td>Run Taskflows</td>
<td>Required to enable users to only run and view taskflows. Users with this role cannot create or edit taskflows.</td>
</tr>
</tbody>
</table>

h. Click **Save**.

i. Click **OK**.

3. Repeat step 2 for each Profitability and Cost Management application that you want to provision.
In This Appendix

Foundation Services Roles ................................................................. 137
Essbase Roles .................................................................................. 140
Essbase Studio Roles ...................................................................... 141
Reporting and Analysis Roles .......................................................... 142
Financial Management Roles .......................................................... 144
Disclosure Management Roles ....................................................... 146
Financial Close Management Roles ................................................. 146
Account Reconciliation Management Roles .................................... 147
Planning Roles ................................................................................ 148
Profitability and Cost Management Roles ....................................... 150
Performance Scorecard Roles ......................................................... 154
Strategic Finance Roles .................................................................. 155
Provider Services Roles ................................................................. 155
Data Integration Management Roles ................................................. 155
FDM Roles ..................................................................................... 156
FDMEE Roles ................................................................................. 156
Integrated Operational Planning Roles .............................................. 157

Foundation Services Roles

Foundation Services roles comprise power roles belonging to these components:

- Shared Services
- Performance Management Architect
- Calculation Manager
- “Financial Management Manager Roles” on page 140

Shared Services Roles

All Shared Services roles are power roles. Typically, these roles are granted to power users who are involved in administering Shared Services and other EPM System products.
<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>Provides control over all products that integrate with Shared Services. This is the most powerful EPM System role and should, therefore, be assigned sparingly. Administrators can perform all administrative tasks in Shared Services Console and can provision themselves.</td>
</tr>
<tr>
<td></td>
<td>This role grants broad access to all applications registered with Shared Services. The Administrator role is, by default, assigned to the admin Native Directory user, who is the only user available after you deploy Shared Services.</td>
</tr>
<tr>
<td>Create Integrations</td>
<td>Creates Shared Services data integrations (the process of moving data between applications) using a wizard</td>
</tr>
<tr>
<td>Directory Manager</td>
<td>Creates and manages users and groups within Native Directory</td>
</tr>
<tr>
<td></td>
<td>Granting Directory Manager and Provisioning Manager roles to one user allows the user to gain superior roles. Oracle recommends that you do not assign the Directory Manager role to users who have been assigned the Provisioning Manager role.</td>
</tr>
<tr>
<td>LCM Administrator</td>
<td>Runs Oracle Hyperion Enterprise Performance Management System Lifecycle Management to promote artifacts or data across product environments and operating systems</td>
</tr>
<tr>
<td></td>
<td>This role comprises these roles:</td>
</tr>
<tr>
<td></td>
<td>● Directory Manager</td>
</tr>
<tr>
<td></td>
<td>● LCM Designer</td>
</tr>
<tr>
<td></td>
<td>● Manage Taskflows</td>
</tr>
<tr>
<td></td>
<td>● Run Taskflows</td>
</tr>
<tr>
<td></td>
<td>● Project Manager</td>
</tr>
<tr>
<td></td>
<td>● Run Integrations</td>
</tr>
<tr>
<td>LCM Designer</td>
<td>Designs migration of artifacts and applications by creating a Migration Definition File using the Lifecycle Management Functionality. Users with this role only can design, but not execute a migration.</td>
</tr>
<tr>
<td>Manage Taskflows</td>
<td>Creates, edits, views, schedules, and runs taskflows for any EPM System product. Has full control over all taskflows.</td>
</tr>
<tr>
<td>Run Taskflows</td>
<td>Views, schedules, and runs the taskflows that users with the Manage Taskflows role created. Cannot create or edit taskflows for any EPM System product.</td>
</tr>
<tr>
<td>Project Manager</td>
<td>Creates and views Shared Services application groups.</td>
</tr>
<tr>
<td>Run Integrations</td>
<td>Views and runs Shared Services data integrations</td>
</tr>
<tr>
<td></td>
<td>For Performance Management Architect, executes data synchronizations</td>
</tr>
</tbody>
</table>
Performance Management Architect Roles

All Performance Management Architect roles are power roles. Typically, they are granted to power users who must create applications and administer application dimensions.

Table 14  Performance Management Architect Roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance Management Architect Administrator</td>
<td>Creates and deploys Performance Management Architect applications. Application Creators own all dimensions in undeployed applications. They can create dimensions but can change only the dimensions to which they have access permissions. Required, in addition to the Dimension Editor role, for Financial Management and Planning users to be able to navigate to their product's Classic Application Administration options. When a user with Application Creator role deploys an application from Performance Management Architect, that user automatically becomes the application administrator and provisioning manager for that application. Performance Management Architect Administrators can also perform these Transaction History Purge Utility operations:</td>
</tr>
<tr>
<td>The Performance Management Architect Administrator role comprises these roles:</td>
<td></td>
</tr>
<tr>
<td>• Application Creator</td>
<td></td>
</tr>
<tr>
<td>• Essbase Application Creator</td>
<td></td>
</tr>
<tr>
<td>• Financial Management Application Creator</td>
<td></td>
</tr>
<tr>
<td>• Planning Application Creator</td>
<td></td>
</tr>
<tr>
<td>• Profitability Application Creator</td>
<td></td>
</tr>
<tr>
<td>Essbase Application Creator</td>
<td>Creates Essbase applications and generic applications using Performance Management Architect.</td>
</tr>
<tr>
<td>Financial Management Application Creator</td>
<td>Creates Consolidation applications and generic applications using Performance Management Architect. To create applications, the user must also be a member of the Application Creators group specified in Financial Management Configuration Utility.</td>
</tr>
<tr>
<td>Planning Application Creator</td>
<td>Creates Planning applications and generic applications using Performance Management Architect.</td>
</tr>
<tr>
<td>Profitability Application Creator</td>
<td>Creates Profitability and Cost Management applications generic applications using Performance Management Architect.</td>
</tr>
<tr>
<td>Dimension Editor¹</td>
<td>Only Dimension Editors can create dimensions in the Shared Library.</td>
</tr>
</tbody>
</table>

Calculation Manager Roles

All Calculation Manager roles are power roles. Typically, they are granted to create Calculation Manager Administrators.
Table 15  Calculation Manager Roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calculation Manager Administrator</td>
<td>Administers and manages Calculation Manager functions</td>
</tr>
<tr>
<td>Financial Management Calculation Manager Administrator</td>
<td>Financial Management Calculation Manager Administrator administers Calculation Manager functions in Financial Management</td>
</tr>
<tr>
<td>Planning Calculation Manager Administrator</td>
<td>Planning Calculation Manager Administrator administers Calculation Manager functions in Planning</td>
</tr>
<tr>
<td>Financial Management Calculation Manager Administrator</td>
<td>Administers Calculation Manager functions in Financial Management</td>
</tr>
<tr>
<td>Planning Calculation Manager Administrator</td>
<td>Administers Calculation Manager functions in Planning</td>
</tr>
</tbody>
</table>

Financial Management Manager Roles

These roles allow Shared Services administrators to administer Financial Management applications.

Table 16  Financial Management Manager Roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Management Manager Administrator role comprises these roles:</td>
<td>Creates and administers Financial Management applications, and administers Calculation Manager functions in Financial Management</td>
</tr>
<tr>
<td>Financial Management Administrator</td>
<td>Administers Financial Management applications.</td>
</tr>
<tr>
<td>Financial Management Application Creator</td>
<td>Creates Financial Management applications</td>
</tr>
<tr>
<td>Financial Management Calculation Manager Administrator</td>
<td>Administers Calculation Manager functions in Financial Management</td>
</tr>
</tbody>
</table>

Essbase Roles

The following tables describe the roles specific to Essbase. For information on assigning granular access permissions to users and groups for a specific Essbase application or database, see the Oracle Essbase Database Administrator’s Guide.

**Note:** To create Essbase applications, in addition to the Essbase Administrator role, users must be provisioned with the Shared Services Project Manager role.
### Table 17  Essbase Server Roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>Full access to administer Essbase Server, applications, and databases</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The Provisioning Manager role is automatically assigned when you migrate Essbase Administrators; however, when you create an Essbase Administrator in Shared Services Console, you must manually assign the Provisioning Manager role.</td>
</tr>
<tr>
<td>Create/Delete</td>
<td>Creates and deletes applications and databases. Includes Application Manager and Database Manager permissions for the applications and databases created by this user.</td>
</tr>
<tr>
<td>Application</td>
<td>Accesses any application or database belonging to this Essbase Server. This level is the minimum access permission a user must have to access applications and databases.</td>
</tr>
<tr>
<td>Provisioning Manager</td>
<td>Provisions users with roles of this Essbase server</td>
</tr>
</tbody>
</table>

### Table 18  Essbase Application Roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Manager</td>
<td>Creates, deletes, and modifies databases and application settings within the assigned application. Includes Database Manager permissions for databases within the application. An Application Managers can delete only those applications and databases that he created.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The Provisioning Manager role is automatically assigned to you when you migrate Essbase Application Managers; however, when you create an Essbase Application Manager in Shared Services Console, you must manually assign to yourself the Provisioning Manager role.</td>
</tr>
<tr>
<td>Database Manager</td>
<td>Manages the databases, database artifacts, and locks within the assigned application</td>
</tr>
<tr>
<td>Calc</td>
<td>Calculates, updates, and reads data values based on assigned scope, using any assigned calculations and filter</td>
</tr>
<tr>
<td>Write</td>
<td>Updates and reads data values based on assigned scope, using any assigned filter</td>
</tr>
<tr>
<td>Read</td>
<td>Reads data values</td>
</tr>
<tr>
<td>Filter</td>
<td>Accesses specific data and metadata according to filter restrictions</td>
</tr>
<tr>
<td>Start/Stop Application</td>
<td>Starts and stops applications or databases</td>
</tr>
<tr>
<td>Provisioning Manager</td>
<td>Provisions Essbase users with roles from this application</td>
</tr>
</tbody>
</table>

## Essbase Studio Roles

### Table 19  Essbase Studio Roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Essbase Studio Administrator</td>
<td>Performs all Essbase Studio tasks, including deploying cubes and executing drill-through reports</td>
</tr>
<tr>
<td>Essbase Studio Data Source</td>
<td>Performs all tasks related to metadata element creation and maintenance; deploys cubes; executes drill-through reports</td>
</tr>
<tr>
<td>Administrator</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Essbase Studio Metadata Administrator</td>
<td>Performs all tasks related to data source connection creation and maintenance; executes drill-through reports</td>
</tr>
<tr>
<td>Essbase Studio Viewer</td>
<td>Views all Essbase Studio data sources and metadata elements; executes drill-through reports</td>
</tr>
<tr>
<td>Provisioning Manager</td>
<td>Provisions Essbase Studio users</td>
</tr>
</tbody>
</table>

### Reporting and Analysis Roles

**Table 20  Reporting and Analysis Roles**

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power Roles</strong></td>
<td></td>
</tr>
<tr>
<td>Reporting and Analysis Administrator</td>
<td>Conditionally accesses all resources (unless the file is locked by “no access”), but not all functionality; accesses the Administer and Impact Manager modules</td>
</tr>
<tr>
<td></td>
<td>Applies to Financial Reporting, Interactive Reporting, Production Reporting, and Web Analysis</td>
</tr>
<tr>
<td>Reporting and Analysis Global Administrator</td>
<td>Universally and implicitly accesses all resources and functionality; accesses the Administer and Impact Manager modules</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Reporting and Analysis Global Administrators can never be denied access.</td>
</tr>
<tr>
<td></td>
<td>Applies to Financial Reporting, Interactive Reporting, Production Reporting, and Web Analysis</td>
</tr>
<tr>
<td>Content Manager</td>
<td>Manages imported repository content and execute tasks, with implicit access to all resources (unless the file is locked by “no access”); contains the Data Source Publisher role</td>
</tr>
<tr>
<td></td>
<td>Applies to Financial Reporting, Interactive Reporting, Production Reporting, and Web Analysis</td>
</tr>
<tr>
<td>Data Source Publisher</td>
<td>Imports data source connectivity files</td>
</tr>
<tr>
<td></td>
<td>Applies to Interactive Reporting and Web Analysis</td>
</tr>
<tr>
<td>Favorites Distributor</td>
<td>Pushes content to users’ Favorites folders using the Favorites Manager</td>
</tr>
<tr>
<td></td>
<td>Applies to Financial Reporting, Interactive Reporting, Production Reporting, and Web Analysis</td>
</tr>
<tr>
<td>Job Manager</td>
<td>Creates and manages public job parameters, output directories, and output printer locations</td>
</tr>
<tr>
<td></td>
<td>Applies to Interactive Reporting and Production Reporting</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This role does not apply to, and should not be assigned to Financial Management and Planning users who access Financial Reporting or Web Analysis through EPM Workspace.</td>
</tr>
<tr>
<td>Schedule Manager</td>
<td>Creates and manages events, calendars, time events, public parameters, and physical resources; creates batches; contains the Scheduler and Job Manager roles</td>
</tr>
<tr>
<td></td>
<td>Applies to Financial Reporting, Interactive Reporting, and Production Reporting</td>
</tr>
<tr>
<td>Provisioning Manager</td>
<td>Provisions Reporting and Analysis users</td>
</tr>
<tr>
<td>Role</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Interactive Roles</strong></td>
<td></td>
</tr>
<tr>
<td>Analyst</td>
<td>Accesses interactive content using full analytic and reporting functionality&lt;br&gt;Applies to Interactive Reporting and Web Analysis</td>
</tr>
<tr>
<td>Content Publisher</td>
<td>Imports, saves, and modifies batches, books, reports, and documents; creates and modifies shortcuts and folders. Deletes data sources and database connections in Financial Reporting through EPM Workspace.&lt;br&gt;Applies to Financial Reporting, Interactive Reporting, Production Reporting, and Web Analysis.</td>
</tr>
<tr>
<td>Data Editor</td>
<td>Pushes Web Analysis data to Essbase</td>
</tr>
<tr>
<td>Job Publisher*</td>
<td>Imports and modifies documents, jobs, and job output; runs jobs; contains the Smart Form Publisher role&lt;br&gt;Applies to Interactive Reporting and Production Reporting</td>
</tr>
<tr>
<td>Personal Page Publisher*</td>
<td>Publishes Personal Pages to the repository, where they can be viewed by other repository users; contains the Personal Page Editor role.&lt;br&gt;Applies to Interactive Reporting and Production Reporting</td>
</tr>
<tr>
<td>Report Designer</td>
<td>Accesses authoring studios to create and distribute documents&lt;br&gt;Applies to Financial Reporting and Web Analysis</td>
</tr>
<tr>
<td>Scheduler</td>
<td>Schedules jobs and batches using the Schedule module; navigates the repository and assigns access control; contains the Explorer and Job Runner roles&lt;br&gt;Applies to Financial Reporting, Interactive Reporting, and Production Reporting</td>
</tr>
<tr>
<td>Smart Form Publisher*</td>
<td>Loads custom forms for programs (forms prompt job runners to enter information used to define jobs)&lt;br&gt;Applies to Production Reporting&lt;br&gt;<strong>Note:</strong> You must have the Job Publisher role to leverage Smart Form Publisher functionality.</td>
</tr>
<tr>
<td>Personal Page Editor*</td>
<td>Creates, modifies, and customizes Personal Pages; copies content from other users' published Personal Pages&lt;br&gt;Applies to Interactive Reporting and Production Reporting</td>
</tr>
<tr>
<td><strong>View Roles</strong></td>
<td></td>
</tr>
<tr>
<td>Dynamic Viewer*</td>
<td>Views, reprocesses, and prints Interactive Reporting documents</td>
</tr>
<tr>
<td>Explorer</td>
<td>Lists repository content in the Explore module and in context using the Open dialog box; searches, views, and subscribes to content.&lt;br&gt;<strong>Note:</strong> Access to the repository does not grant access to individual files and folders, which are secured by file properties and permissions.&lt;br&gt;Applies to Financial Reporting, Interactive Reporting, Production Reporting, and Web Analysis</td>
</tr>
<tr>
<td>Interactive Reporting Viewer*</td>
<td>Reviews and prints static Interactive Reporting documents</td>
</tr>
<tr>
<td>IR HTML Viewer</td>
<td>Uses the HTML Viewer to browse BQY documents. This role is not automatically assigned to users who were migrated from a previous version.</td>
</tr>
<tr>
<td>IR WebClient Viewer</td>
<td>Uses Interactive Reporting plug-in to browse BQY documents. This role is not automatically assigned to users that were migrated from a previous version.</td>
</tr>
<tr>
<td>Role</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Job Runner*</td>
<td>Runs jobs and views public job parameters and physical resources</td>
</tr>
<tr>
<td></td>
<td>Applies to Interactive Reporting and Production Reporting</td>
</tr>
<tr>
<td>Personal Page Editor*</td>
<td>Creates, modifies, and customizes Personal Pages; copies content from other users' published Personal Pages</td>
</tr>
<tr>
<td></td>
<td>Applies to Interactive Reporting and Production Reporting</td>
</tr>
<tr>
<td>Personal Parameter Editor</td>
<td>Defines points of view and personal parameters on database connections to customize query result sets</td>
</tr>
<tr>
<td></td>
<td>Applies to Interactive Reporting, Production Reporting, and Web Analysis</td>
</tr>
<tr>
<td>Viewer</td>
<td>Reviews EPM Workspace content. The content is static and accessible only from the Favorites folder.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This role provides minimal user functionality; use it only when no other role assignments are possible.</td>
</tr>
<tr>
<td></td>
<td>Applies to Financial Reporting, Interactive Reporting, Production Reporting, and Web Analysis</td>
</tr>
</tbody>
</table>

**System Roles**

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusted Application</td>
<td>Enables credentialed client-server communication of Interactive Reporting database connection files (.oce extension) that encapsulate connectivity, database type, network address, and database user name information</td>
</tr>
</tbody>
</table>

**Financial Management Roles**

Additional Shared Services roles are required for Performance Management Architect and Calculation Manager. See “Foundation Services Roles” on page 137.

**Table 21  Financial Management Roles**

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power Roles</strong></td>
<td></td>
</tr>
<tr>
<td>Application Administrator</td>
<td>Performs all Financial Management tasks. Access to this role overrides any other access setting for the user.</td>
</tr>
<tr>
<td>Load System</td>
<td>Loads rules and member lists</td>
</tr>
<tr>
<td>Inter-Company Transaction Admin</td>
<td>Opens and closes periods, locks and unlocks entities, and manages reason codes. Users with the role can also perform all intercompany tasks.</td>
</tr>
<tr>
<td><strong>Interactive Roles</strong></td>
<td></td>
</tr>
<tr>
<td>Rules Administrator</td>
<td>Performs any Calculation Manager tasks for the specific application</td>
</tr>
<tr>
<td>Rules Designer</td>
<td>Creates new rules objects and modifies or deletes rules objects</td>
</tr>
<tr>
<td>Approve Journals</td>
<td>Approves or rejects journals</td>
</tr>
<tr>
<td>Create Journals</td>
<td>Creates, modifies, deletes, submits, and unsubmits journals</td>
</tr>
<tr>
<td>Create Unbalanced Journals</td>
<td>Creates unbalanced journals</td>
</tr>
<tr>
<td>Role</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Default</td>
<td>Opens and closes applications; manages documents and favorites; manages Smart View; and accesses running tasks, data tasks, and load and extract tasks. Cannot extract metadata or rules.</td>
</tr>
<tr>
<td>Journals Administrator</td>
<td>Performs all tasks related to journals</td>
</tr>
<tr>
<td>Post Journals</td>
<td>Posts and unposts journals</td>
</tr>
<tr>
<td>Manage Templates</td>
<td>Grants access to the journals templates for managing journals</td>
</tr>
<tr>
<td>Generate Recurring</td>
<td>Grants access to the generate recurring task for managing journals</td>
</tr>
<tr>
<td>Review Supervisor</td>
<td>Starts process management units and approves and publishes process management data. Can promote or reject process units, depending on process level.</td>
</tr>
<tr>
<td>Reviewer 1 through Reviewer 10</td>
<td>Views and edits a block of data when that data is at the user’s designated process management level</td>
</tr>
<tr>
<td>Submitter</td>
<td>Submits a block of data for final approval</td>
</tr>
<tr>
<td>Lock Data</td>
<td>Locks data in Data Explorer</td>
</tr>
<tr>
<td>Unlock Data</td>
<td>Unlocks data in Data Explorer</td>
</tr>
<tr>
<td>Consolidate All</td>
<td>Runs consolidate all</td>
</tr>
<tr>
<td>Consolidate</td>
<td>Runs consolidate</td>
</tr>
<tr>
<td>Consolidate All with Data</td>
<td>Runs consolidate with all data</td>
</tr>
<tr>
<td>Run Allocation</td>
<td>Runs allocations</td>
</tr>
<tr>
<td>Manage Data Entry Forms</td>
<td>Manages data entry forms on the web</td>
</tr>
<tr>
<td>Save System Report On Server</td>
<td>Saves system reports on server</td>
</tr>
<tr>
<td>Load Excel Data</td>
<td>Loads data from Smart View</td>
</tr>
<tr>
<td>Inter-Company Transaction User</td>
<td>Creates, edits, deletes, loads, and extracts transactions. Runs matching report by account or ID, runs transaction report, and drills through from modules.</td>
</tr>
<tr>
<td>Inter-Company Transaction Match Template</td>
<td>Manages intercompany matching templates</td>
</tr>
<tr>
<td>Inter-Company Transaction Auto Match by Account</td>
<td>Automatically matches intercompany transactions by account</td>
</tr>
<tr>
<td>Inter-Company Transaction Auto Match by ID</td>
<td>Automatically matches intercompany transactions by ID</td>
</tr>
<tr>
<td>Inter-Company Transaction Manual Match with Tolerance</td>
<td>Manually matches intercompany transactions with tolerance check</td>
</tr>
<tr>
<td>Inter-Company Transaction Manual Match</td>
<td>Manually matches intercompany transactions</td>
</tr>
<tr>
<td>Inter-Company Transaction Unmatch</td>
<td>Unmatches intercompany transactions</td>
</tr>
<tr>
<td>Inter-Company Transaction Post/Unpost</td>
<td>Posts and unposts intercompany transactions</td>
</tr>
<tr>
<td>Role</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enable write back in Web Grid</td>
<td>Enters and saves data directly to a Web Grid</td>
</tr>
<tr>
<td>Database Management</td>
<td>Copies and clears data and deletes invalid records</td>
</tr>
<tr>
<td>Manage Ownership</td>
<td>Enters and edits ownership information</td>
</tr>
<tr>
<td>Manage Custom Documents</td>
<td>Loads and extracts custom documents to and from the server</td>
</tr>
<tr>
<td>Extended Analytics</td>
<td>Exports data to a database</td>
</tr>
<tr>
<td>Data Form Write Back from Excel</td>
<td>Submits data from Smart View while using a Web Data Entry Form</td>
</tr>
</tbody>
</table>

**View Roles**

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced User</td>
<td>Uses the Browser View and can access Running Tasks</td>
</tr>
<tr>
<td>Rules Viewer</td>
<td>Views rules objects</td>
</tr>
<tr>
<td>Read Journals</td>
<td>Reads journals</td>
</tr>
<tr>
<td>Receive Email Alerts for Process Control</td>
<td>Receives e-mails</td>
</tr>
<tr>
<td>Receive Email Alerts for Intercompany</td>
<td>Receives e-mails</td>
</tr>
<tr>
<td>Reserved</td>
<td>Not currently used</td>
</tr>
<tr>
<td>View Data Audit</td>
<td>View and export data audit information</td>
</tr>
<tr>
<td>View Task Audit</td>
<td>View and export task audit information</td>
</tr>
</tbody>
</table>

**Disclosure Management Roles**

Table 22  Disclosure Management Roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provisioning Manager</td>
<td>Provisions users and groups with Oracle Hyperion Disclosure Management roles</td>
</tr>
<tr>
<td>Disclosure Management User</td>
<td>Performs Disclosure Management actions</td>
</tr>
</tbody>
</table>

**Financial Close Management Roles**

Native Directory users cannot perform tasks granted by Oracle Hyperion Financial Close Management roles, because they cannot use single sign-on with Fusion Middleware. If Native Directory users must perform Financial Close Management tasks, they must be created as Fusion Middleware users too.
### Table 23  Financial Close Management Roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Close Manager Administrator</td>
<td>Administers Financial Close Management. Performs the tasks that Close Power User and Close User can perform.</td>
</tr>
<tr>
<td>Close Manager Power User</td>
<td>Performs tasks that Close User can perform</td>
</tr>
<tr>
<td></td>
<td>Create and manage alert types</td>
</tr>
<tr>
<td>Close Manager User</td>
<td>Performs these tasks:</td>
</tr>
<tr>
<td></td>
<td>Views templates</td>
</tr>
<tr>
<td></td>
<td>Accesses Reporting and Analysis and transactional dashboards</td>
</tr>
<tr>
<td></td>
<td>Modifies status</td>
</tr>
<tr>
<td></td>
<td>Creates and modifies alerts, comments, and questions</td>
</tr>
<tr>
<td></td>
<td>Creates and manages filters</td>
</tr>
</tbody>
</table>

### Account Reconciliation Management Roles

### Table 24  Account Reconciliation Management Roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reconciliation Administrator</td>
<td>Full access to system setup, filters, attributes, periods, reconciliation instances, rates, and reporting</td>
</tr>
<tr>
<td></td>
<td>Adds and remove own comments</td>
</tr>
<tr>
<td></td>
<td>Removes commentary from reconciliations to accommodate cases where the commentary that was entered by a user who separated from the company must be removed</td>
</tr>
<tr>
<td></td>
<td>Cannot prepare or view account reconciliations</td>
</tr>
<tr>
<td>Reconciliation Power User</td>
<td>Full access to filters, reconciliation profiles, reconciliation instances, and reporting</td>
</tr>
<tr>
<td></td>
<td>Adds and remove own comments</td>
</tr>
<tr>
<td></td>
<td>Removes commentary from reconciliations to accommodate cases where the commentary that was entered by a user who separated from the company must be removed</td>
</tr>
<tr>
<td>Reconciliation Commentator</td>
<td>Adds comments to reconciliations and associated transactions</td>
</tr>
<tr>
<td></td>
<td>Creates reports</td>
</tr>
<tr>
<td></td>
<td>Creates private filters</td>
</tr>
<tr>
<td>Reconciliation Preparer</td>
<td>Performs all functions related to preparation of reconciliations including adding, editing, flagging, and removing transactions; adding and removing comments; adding and removing attachments; answering questions; and submitting reconciliations for review</td>
</tr>
<tr>
<td></td>
<td>Creates reports</td>
</tr>
<tr>
<td></td>
<td>Creates private filters</td>
</tr>
<tr>
<td>Reconciliation Reviewer</td>
<td>Reviews reconciliations including flagging transactions, adding and removing comments, rejecting reconciliations; and approving reconciliations</td>
</tr>
<tr>
<td></td>
<td>Creates reports</td>
</tr>
<tr>
<td></td>
<td>Creates private filters</td>
</tr>
<tr>
<td>Role</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Reconciliation Viewer</td>
<td>- Views reconciliations to which Viewer privileges are granted</td>
</tr>
<tr>
<td></td>
<td>- Creates reports</td>
</tr>
<tr>
<td></td>
<td>- Creates private filters</td>
</tr>
</tbody>
</table>

**Planning Roles**

Additional Foundation Services roles are required for Performance Management Architect and Calculation Manager. See “Foundation Services Roles” on page 137.

Table 25  Planning Application Roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power Roles</strong></td>
<td></td>
</tr>
<tr>
<td>Administrator</td>
<td>Performs all application tasks except those reserved for the Application Owner and Mass Allocate roles. Creates and manages applications, manages access permissions, initiates the budget process, and designates the e-mail server for notifications. Can use the Copy Data function.</td>
</tr>
<tr>
<td>Provisioning Manager</td>
<td>Provisions users to the Planning application</td>
</tr>
<tr>
<td>Mass Allocation</td>
<td>Accesses the Mass Allocate feature to spread data multidimensionally down a hierarchy, even to cells not visible in the data form and to which the user does not have access. Any user type can be assigned this role, but it should be assigned sparingly.</td>
</tr>
</tbody>
</table>
| Essbase Write Access | For planners and interactive users: Grants users access to Planning data in Essbase equivalent to their Planning access permissions.  
                         | If security filters that limit access to year and period dimensions are not created, this role grants write access to all periods and years.  
                         | Enables users having write access to change Planning data directly in Essbase using another product such as Financial Reporting or a third-party tool. |
| Approvals Administrator | Approvals Administrators are typically business users in charge of a region in an organization who need to control the Approvals process for their region but do not need to be granted the Planning Administrator role. Users with Approvals Administrator role can resolve any approval issue by manually taking ownership of the process. They can perform these tasks:  
                         | - Control approvals process  
                         | - Perform actions on Planning units to which they have write access  
                         | - Assign owners and reviewers for the organization under their charge  
                         | - Change the secondary dimension or update validation rules |

**Approvals Administrator role comprises these roles:**
- Approvals Ownership Assigner
- Approvals Process Designer
- Approvals Supervisor
<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approvals Ownership Assigner</td>
<td>Performs tasks assigned to Planner role.</td>
</tr>
<tr>
<td></td>
<td>Approvals Ownership Assigners perform the following tasks for any member of the planning unit hierarchy to which they have write access:</td>
</tr>
<tr>
<td></td>
<td>● Assign owners</td>
</tr>
<tr>
<td></td>
<td>● Assign reviewers</td>
</tr>
<tr>
<td></td>
<td>● Specify users to be notified</td>
</tr>
<tr>
<td>Approvals Process Designer</td>
<td>Performs tasks assigned to Planner and Approvals Ownership Assigner roles.</td>
</tr>
<tr>
<td></td>
<td>Approvals process designers perform the following tasks for any member of the planning unit hierarchy to which they have write access:</td>
</tr>
<tr>
<td></td>
<td>● Change secondary dimensions and members of entities to which they have write access</td>
</tr>
<tr>
<td></td>
<td>● Change the scenario and version assignment for a planning unit hierarchy</td>
</tr>
<tr>
<td></td>
<td>● Edit data validation rules of data forms to which they have access</td>
</tr>
<tr>
<td>Approvals Supervisor</td>
<td>Perform the following tasks for any member of the planning unit hierarchy to which they have write access even if they do not own the planning unit:</td>
</tr>
<tr>
<td></td>
<td>● Stop and start a planning unit</td>
</tr>
<tr>
<td></td>
<td>● Take any action on a planning unit</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Approval Supervisors cannot change data in planning units that they do not own.</td>
</tr>
<tr>
<td>Ad Hoc Grid Creator</td>
<td>Creates and saves Smart Slices in addition to performing the tasks that an Ad Hoc User can perform</td>
</tr>
<tr>
<td>Ad Hoc User</td>
<td>Analyzes data forms using ad hoc features.</td>
</tr>
<tr>
<td>Task List Access Manager</td>
<td>Not applicable to this release; reserved for future use.</td>
</tr>
<tr>
<td>Planner Roles</td>
<td></td>
</tr>
<tr>
<td>Planner</td>
<td>Enters and submits plans for approval and adapter processes. Uses reports that others have created, views and uses task lists, enables e-mail notification for themselves, and creates data using Smart View.</td>
</tr>
<tr>
<td>Interactive Roles</td>
<td></td>
</tr>
<tr>
<td>Interactive User</td>
<td>Creates and maintains data forms, Smart View worksheets, business rules, task lists, Financial Reporting reports, and adapter processes. Manages the budget process. Can create Smart Slices in Smart View, use the Clear Cell Details function, and perform all Planner tasks. Interactive users are typically department heads and business unit managers.</td>
</tr>
<tr>
<td>View Roles</td>
<td></td>
</tr>
<tr>
<td>View User</td>
<td>Views and analyzes data through Planning data forms and any data access tools for which they are licensed (for example, Oracle Hyperion Financial Reporting, Web Analysis, and Smart View). Typical View users are executives who want to see business plans during and at the end of the budget process.</td>
</tr>
</tbody>
</table>
# Profitability and Cost Management Roles

## Standard Profitability and Cost Management Roles

<table>
<thead>
<tr>
<th>Security Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power Roles</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Administrator  | ● Create and maintain user accounts and security roles, and provision users, using Shared Services  
                   ● Generate Essbase databases  
                   ● Set up and maintain application preferences  
                   ● Build the model database using Performance Management Architect to select the common dimensions and members  
                   ● Create and maintain elements within the model, such as stages, drivers, POVs, driver selections, assignments, and application preferences  
                   ● Perform POV Copy, calculation, validation, data entry, and trace allocations  
                   ● Deploy to Essbase and generate calculation scripts  
                   ● Import and export data  
                   ● Use the Lifecycle Management Utility to promote data from one environment, such as development or testing, to another environment, such as production.  
                   ● Back up and restore Profitability and Cost Management model components.  
                   ● Monitor changes made to business objects.  
                   ● Access Profitability Application Home screen to create, maintain, register, duplicate and update Profitability and Cost Management applications using Application Loader for Exalytics.  
                   ● Create, edit, copy, delete, and launch queries from Smart View Connections screen  
                   **Note:** The Power User does not necessarily require specific security roles to perform tasks. For example, if a Power User runs a calculation from the Calculate screen, this action creates and executes a taskflow behind the scenes. The Power User does not require the Manage Taskflow role to perform this task, unless the Power User wants to access this task directly from the Manage Taskflows task. |
| Power User     | ● Create and maintain elements within the model, such as stages, drivers, POVs, driver selections, assignments, and application preferences.  
                   ● Perform POV Copy, calculation, validation, data entry and trace allocations.  
                   ● Deploy to Essbase and generate calculation scripts.  
                   ● Import and export data  
                   ● Access Profitability Application Home screen to create, maintain, register, duplicate and update Profitability and Cost Management applications using Application Loader for Exalytics.  
                   ● Create, edit, copy, delete, and launch queries from Smart View Connections screen |
| **Interactive Roles**|                                                                                                                                                                                                                       |
| Interactive User | ● View all modelling screens  
                     ● View and modify data in the Data Entry screen  
                     ● View Trace Allocations  
                     ● Launch queries from Smart View Connections screen |
<table>
<thead>
<tr>
<th>Security Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View User</td>
<td>View only access for these functions:</td>
</tr>
<tr>
<td></td>
<td>• Trace Allocations</td>
</tr>
<tr>
<td></td>
<td>• Application Preferences</td>
</tr>
<tr>
<td></td>
<td>• Model Stages, Drivers and POVs</td>
</tr>
</tbody>
</table>

**Shared Services Roles**

<table>
<thead>
<tr>
<th>Security Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage Taskflows</td>
<td>Required to create and edit taskflows.</td>
</tr>
<tr>
<td>Run Taskflows</td>
<td>Required to enable users to only run and view taskflows. Users with this role cannot create or edit taskflows.</td>
</tr>
</tbody>
</table>
### Detailed Profitability and Cost Management Roles

#### Table 27 Detailed Profitability and Cost Management Roles

<table>
<thead>
<tr>
<th>Security Role</th>
<th>Description</th>
</tr>
</thead>
</table>
| Administrator | - Set up and maintain application preferences  
- Build the model database using Performance Management Architect to select the common dimensions and members  
- Create and deploy reporting views to the relational database  
- Create, Read (View), Update and Delete the following functions:  
  - Stages  
  - Drivers  
  - POVs  
  - Driver Associations  
  - Assignments  
  - Application Preferences  
  - Calculation Rules  
  - Calculation Process Administration  
  - Jobs Library and Status  
  - Table Registration  
- Perform the following tasks:  
  - POV Copy  
  - Validate  
  - Deploy  
  - Calculate  
  - Stop Jobs  
- Use the Lifecycle Management Utility to promote data from one environment, such as development or testing, to another environment, such as production.  
- Import and export data  
- Back up and restore Profitability and Cost Management model components.  
- Monitor changes made to business objects.  
- Create, edit, copy, delete, and launch queries from Smart View Connections screen  
- Access Profitability Application Home screen to create, maintain, register, duplicate and update Profitability and Cost Management applications using Application Loader for Exalytics. |
<table>
<thead>
<tr>
<th>Security Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power Roles</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Power User | - Create and maintain user accounts and security roles, and provision users, using Shared Services  
- Create and deploy reporting views to the relational database  
- Access Profitability Application Home screen to create, maintain, register, duplicate and update Profitability and Cost Management applications using Application Loader for Exalytics.  
- Create, edit, copy, delete, and launch queries from Smart View Connections screen  
- Create, Read (View), Update and Delete the following functions:  
  - Stages  
  - Drivers  
  - POVs  
  - Driver Associations  
  - Assignments  
  - Application Preferences  
  - Calculation Rules  
  - Calculation Process Administration  
  - Jobs Library and Status  
  - Table Registration  
- Perform the following tasks:  
  - POV Copy  
  - Validate  
  - Deploy  
  - Calculate  
  - Stop Jobs |
| **Interactive Roles** | |
| Interactive User | - View (Read) the following functions:  
  - Stages  
  - Drivers  
  - POVs  
  - Driver Association  
  - Assignments  
  - Application Preferences  
  - Calculation Rules  
  - Calculation Process Administration  
  - Jobs Library and Status  
  - Table Registration  
- Launch queries from Oracle Smart View for Office Connections screen |

**Note:** The Power User does not necessarily require specific security roles to perform tasks. For example, if a Power User runs a calculation from the Calculate screen, this action creates and executes a taskflow behind the scenes. The Power User does not require the manage Taskflow role to perform this task, unless the Power User wants to access this task directly from Manage Taskflows task.
### Security Role

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View User</td>
</tr>
<tr>
<td>• View (Read) the following functions:</td>
</tr>
<tr>
<td>- Stages</td>
</tr>
<tr>
<td>- Drivers</td>
</tr>
<tr>
<td>- POVs</td>
</tr>
<tr>
<td>- Driver Association</td>
</tr>
<tr>
<td>- Assignments</td>
</tr>
<tr>
<td>- Application Preferences</td>
</tr>
<tr>
<td>- Calculation Rules</td>
</tr>
<tr>
<td>- Calculation Process Administration</td>
</tr>
<tr>
<td>- Jobs Library and Status</td>
</tr>
<tr>
<td>- Table Registration</td>
</tr>
</tbody>
</table>

### Shared Services Role

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage Taskflows</td>
<td>Required to create and edit taskflows.</td>
</tr>
<tr>
<td>Run Taskflows</td>
<td>Required to enable users to only run and view taskflows. Users with this role cannot create or edit taskflows.</td>
</tr>
</tbody>
</table>

### Performance Scorecard Roles

#### Table 28  Performance Scorecard Roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power Roles</strong></td>
<td></td>
</tr>
<tr>
<td>Power Manager</td>
<td>Provides the administrative capability within an Oracle Hyperion Performance Scorecard, environment</td>
</tr>
<tr>
<td>Provisioning Manager</td>
<td>Provisions users and groups with Performance Scorecard, roles.</td>
</tr>
<tr>
<td><strong>Interactive Roles</strong></td>
<td></td>
</tr>
<tr>
<td>Basic</td>
<td>Grants access to reports, scorecards, measures, and initiatives with the additional role of result collection administration</td>
</tr>
<tr>
<td>Interactive</td>
<td>Primarily a designer role, the Interactive User has access to all business objects for creation and modification. These include maps (accountability, strategy, cause and effect) as well as scorecards, initiatives, and measures.</td>
</tr>
</tbody>
</table>
### Strategic Finance Roles

#### Table 29  Strategic Finance Roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power Roles</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Administrator         | Administers Oracle Hyperion Strategic Finance, and assigns access to entities. Includes Interactive User capabilities. Administrators perform these tasks:  
  - Adds and maintain servers  
  - Adds and maintain databases  
  - Adds and maintain users  
  - Adds and maintain user groups  
  - Creates and maintain entities  
  - Designs and view reports |
| Provisioning Manager  | Provisions users and groups with Strategic Finance, roles.                                             |
| **Interactive Roles** |                                                                                                       |
| Basic User            | Enters data into entities, adds scenarios and subaccounts, and views reports                          |
| Interactive User      | Interactive users perform these tasks:  
  - Create and maintain entities  
  - Enter data into entities  
  - Add scenarios  
  - Add subaccounts  
  - Add dimensions  
  - Design and view reports |
| **View Roles**        |                                                                                                       |
| View User             | Views entities and reports                                                                           |

#### Provider Services Roles

Oracle Hyperion Provider Services provides the Administrator power role, which allows users to create, modify, and delete Essbase Server clusters.

#### Data Integration Management Roles

Oracle Hyperion Data Integration Management does not use the security environment established by Shared Services.

If you are upgrading to the current version of Data Integration Management, and you used the Shared Services authentication plug-in, you must deregister the Shared Services authentication.
plug-in and then use Informatica PowerCenter Repository Manager to recreate users. This version of Data Integration Management supports only native Informatica authentication. See Oracle Hyperion Data Integration Management documentation for detailed information.

## FDM Roles

### Table 30  FDM Roles

<table>
<thead>
<tr>
<th>Roles</th>
<th>Tasks per Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>Manages applications and performs any action. Has access to every location and rights to every form and control.</td>
</tr>
<tr>
<td>Basic Reviewer</td>
<td>Reviews financial controls questions</td>
</tr>
<tr>
<td>Basic Reviewer and Submitter</td>
<td>Submits certification or assessment after it has been reviewed</td>
</tr>
<tr>
<td>Intermediate 2–9</td>
<td>Loads data to the target system. Roles for intermediate levels are defined by the Oracle Hyperion Financial Data Quality Management administrator. When a user is assigned a user level, that user has access to every object that has been assigned that level and higher. For example, a user who is assigned Intermediate-7 role has access to each object that can be accessed using Intermediate-7 through Intermediate-9, and All roles. Objects accessible to Power level and Intermediate 2 through 6 are unavailable to Intermediate-7 user.</td>
</tr>
</tbody>
</table>

## FDMEE Roles

### Table 31  FDMEE Roles

<table>
<thead>
<tr>
<th>Roles</th>
<th>Tasks per Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>Manages applications and performs any action</td>
</tr>
<tr>
<td>Provisioning Manager</td>
<td>Provisions users and groups with Oracle Hyperion Financial Data Quality Management, Enterprise Edition roles</td>
</tr>
<tr>
<td>Drill Through</td>
<td>Applies to FDMEE and FDM. Controls the ability to drill through to the source system.</td>
</tr>
<tr>
<td></td>
<td>In FDM, this role is applied as a permissible task to an Intermediate role to control drilling back to the source system.</td>
</tr>
<tr>
<td></td>
<td>In FDMEE, this role controls whether the user can drill to the FDMEE landing page, which controls drilling to the source system.</td>
</tr>
<tr>
<td>Create Integration</td>
<td>Creates FDMEE metadata and data rules.</td>
</tr>
<tr>
<td>Run Integration</td>
<td>Runs FDMEE metadata and data rules and fills out runtime parameters. Can view transaction logs. FDM users who need to extract data from Oracle General Ledger must be granted this role to run data rules.</td>
</tr>
<tr>
<td>GL Write Back</td>
<td>Enables data write-back to the ERP source system.</td>
</tr>
</tbody>
</table>
## Integrated Operational Planning Roles

<table>
<thead>
<tr>
<th>Roles</th>
<th>Tasks per Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provisioning Manager</td>
<td>Provisions users and groups with Disclosure Management roles</td>
</tr>
<tr>
<td>IOP Administrator</td>
<td>Administers Oracle Integrated Operational Planning. IOP Administrators can modify models, access ACL pages, and perform all Integrated Operational Planning tasks.</td>
</tr>
<tr>
<td>IOP User</td>
<td>Performs Integrated Operational Planning actions as a normal user</td>
</tr>
</tbody>
</table>
Roles define the tasks that users can perform in EPM System applications. Roles from all registered EPM System applications can be viewed from the Roles View in Oracle Hyperion Shared Services Console.

The Roles View lists the roles name and the product code, which is the internal product name, along with a brief role description. The product codes used by EPM System products are indicated in Table 33.

<table>
<thead>
<tr>
<th>Product Code</th>
<th>Product Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>HUB</td>
<td>Shared Services</td>
</tr>
<tr>
<td>CES</td>
<td>Oracle Hyperion Shared Services (Workflow)</td>
</tr>
<tr>
<td>HP</td>
<td>Planning</td>
</tr>
<tr>
<td>ESB</td>
<td>Essbase</td>
</tr>
<tr>
<td>BPM</td>
<td>Oracle Essbase Studio</td>
</tr>
<tr>
<td>ESBAPP</td>
<td>Essbase Application</td>
</tr>
<tr>
<td>BPMA</td>
<td>Performance Management Architect</td>
</tr>
<tr>
<td>HAVA</td>
<td>Reporting and Analysis products such as the following:</td>
</tr>
<tr>
<td></td>
<td>● EPM Workspace</td>
</tr>
<tr>
<td></td>
<td>● Web Analysis</td>
</tr>
<tr>
<td></td>
<td>● Interactive Reporting</td>
</tr>
<tr>
<td></td>
<td>● Oracle Hyperion SQR Production Reporting</td>
</tr>
<tr>
<td>FDM</td>
<td>Oracle Hyperion Financial Data Quality Management</td>
</tr>
<tr>
<td>EAL</td>
<td>Oracle Essbase Analytics Link for Hyperion Financial Management</td>
</tr>
<tr>
<td>EALBRIDGE</td>
<td>Oracle Essbase Analytics Link for Hyperion Financial Management Bridge</td>
</tr>
<tr>
<td>HFM</td>
<td>Oracle Hyperion Financial Management</td>
</tr>
<tr>
<td>HPS</td>
<td>Oracle Hyperion Performance Scorecard</td>
</tr>
<tr>
<td>HPM</td>
<td>Oracle Hyperion Profitability and Cost Management</td>
</tr>
<tr>
<td>Product Code</td>
<td>Product Name</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------------------------------------------</td>
</tr>
<tr>
<td>CALC</td>
<td>Oracle Hyperion Calculation Manager</td>
</tr>
<tr>
<td>HSF</td>
<td>Oracle Hyperion Strategic Finance</td>
</tr>
<tr>
<td>AIF</td>
<td>Oracle Hyperion Financial Data Quality Management, Enterprise Edition</td>
</tr>
<tr>
<td>IOP</td>
<td>Oracle Integrated Operational Planning</td>
</tr>
<tr>
<td>BIEE</td>
<td>Oracle Business Intelligence Enterprise Edition</td>
</tr>
<tr>
<td>DISCMAN</td>
<td>Oracle Hyperion Disclosure Management</td>
</tr>
<tr>
<td>FCC</td>
<td>Oracle Hyperion Financial Close Management</td>
</tr>
<tr>
<td>BIP</td>
<td>Oracle Business Intelligence Publisher</td>
</tr>
</tbody>
</table>
Accessing EPM System Products

In This Appendix

Accessing Shared Services .............................................................. 161
Accessing EPM Workspace .............................................................. 161
Accessing Administration Services Console .................................. 162

Accessing Shared Services

See “Launching Shared Services Console” on page 15.

Accessing EPM Workspace

EPM Workspace is a Foundation Services component from which you can access Oracle Enterprise Performance Management System products such as Oracle Hyperion Planning; Oracle Hyperion EPM Architect; and Oracle Hyperion Reporting and Analysis components such as Oracle Hyperion Interactive Reporting and Oracle Hyperion Web Analysis. A logon window is displayed when you access EPM Workspace using a URL.

1. Go to:

   http://Web_server_name:port_number/workspace/index.jsp

   In the URL, Web_server_name indicates the name of the computer where the web server used by Foundation Services is running, and port_number indicates the web server port; for example, http://myWebserver:19000/workspace.

   Note: If you are accessing EPM Workspace in secure environments, use https (not http) as the protocol and the secure web server port number. For example, use a URL such as: https://myWebserver:19443/workspace.

   Pop-up blockers may prevent EPM Workspace from opening.

2. Click Launch Application.

3. In the Logon window, enter a user name and password.
4  Click Log On.
5  In EPM Workspace, select Navigate.
6  Select Administer, and then Shared Services Console.

**Accessing Administration Services Console**

Before starting these procedures, ensure that Foundation Services, web server, Oracle Essbase, and Administration Services are running.

► To access Administration Services Console from a URL:

1  Go to:

   http://Web_server_name:port_number/easconsole/console.html

   In the URL, Web_server_name indicates the name of the computer where the web server used by Oracle Hyperion Foundation Services is running, and port_number indicates the web server port; for example, https://myWebserver:19000/easconsole.

   **Note:** If you are accessing Oracle Hyperion Enterprise Performance Management Workspace, in secure environments, use https (not http) as the protocol and the secure web server port number. For example, use a URL such as: https://myWebserver:19443/easconsole.

2  Click Launch.

3  Download and install Administration Services Console.

4  In the Oracle Essbase Administration Services Login screen, enter your user name and password.

5  Click OK.
**access permissions**  A set of operations that a user can perform on a resource.

**aggregated role**  A custom role that aggregates multiple predefined roles within a Hyperion product.

**application**  1) A software program designed to run a specific task or group of tasks such as a spreadsheet program or database management system; 2) A related set of dimensions and dimension members that are used to meet a specific set of analytical requirements, reporting requirements, or both.

**Application Migration Utility**  A command-line utility for migrating applications and artifacts.

**artifact**  An individual application or repository item; for example, scripts, forms, rules files, Interactive Reporting documents, and financial reports. Also known as an object.

**authentication**  Verification of identity as a security measure. Authentication is typically based on a user name and password. Passwords and digital signatures are forms of authentication.

**automated stage**  A stage that does not require human intervention; for example, a data load.

**backup**  A duplicate copy of an application instance.

**business process**  A set of activities that collectively accomplish a business objective.

**context variable**  A variable that is defined for a particular task flow to identify the context of the taskflow instance.

**external authentication**  Logging on to Oracle EPM System products with user information stored outside the application. The user account is maintained by the EPM System, but password administration and user authentication are performed by an external service, using a corporate directory such as Oracle Internet Directory (OID) or Microsoft Active Directory (MSAD).

**filter**  A constraint on data sets that restricts values to specific criteria; for example, to exclude certain tables, metadata, or values, or to control access.

**group**  A container for assigning similar access permissions to multiple users.

**identity**  A unique identification for a user or group in external authentication.

**integration**  A process that is run to move data between Oracle’s Hyperion applications using Shared Services. Data integration definitions specify the data moving between a source application and a destination application, and they enable the data movements to be grouped, ordered, and scheduled.

**lifecycle management**  The process of migrating an application, a repository, or individual artifacts across product environments.

**link**  1) A reference to a repository object. Links can reference folders, files, shortcuts, and other links; 2) In a taskflow, the point where the activity in one stage ends and another begins.

**link condition**  A logical expression evaluated by the taskflow engine to determine the sequence of launching taskflow stages.

**load balancing**  Distribution of requests across a group of servers, which helps to ensure optimal end user performance.

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

**manual stage**  A stage that requires human intervention.

**migration**  The process of copying applications, artifacts, or users from one environment or computer to another; for example, from a testing environment to a production environment.
migration audit report  A report generated from the migration log that provides tracking information for an application migration.

migration definition file (.mdf)  A file that contains migration parameters for an application migration, enabling batch script processing.

migration log  A log file that captures all application migration actions and messages.

migration snapshot  A snapshot of an application migration that is captured in the migration log.

model  1) A file or content string containing an application-specific representation of data. Models are the basic data managed by Shared Services, of two major types: dimensional and nondimensional application objects; 2) In Business Modeling, a network of boxes connected to represent and calculate the operational and financial flow through the area being examined.

product  In Shared Services, an application type, such as Planning or Performance Scorecard.

project  An instance of Oracle's Hyperion products grouped together in an implementation. For example, a Planning project may consist of a Planning application, an Essbase cube, and a Financial Reporting Server instance.

provisioning  The process of granting users and groups specific access permissions to resources.

repository  Storage location for metadata, formatting, and annotation information for views and queries.

role  The means by which access permissions are granted to users and groups for resources.

security agent  A web access management provider (for example, Oracle Access Manager, Oracle Single Sign-On, or CA SiteMinder) that protects corporate web resources.

security platform  A framework enabling Oracle EPM System products to use external authentication and single sign-on.

Shared Services Registry  The part of the Shared Services repository that manages EPM System deployment information for most EPM System products, including installation directories, database settings, computer names, ports, servers, URLs, and dependent service data.

single sign-on (SSO)  The ability to log on once and then access multiple applications without being prompted again for authentication.

stage  1) A task description that forms one logical step within a taskflow, usually performed by an individual. A stage can be manual or automated; 2) For Profitability, logical divisions within the model that represent the steps in the allocation process within your organization.

stage action  For automated stages, the invoked action that executes the stage.

sync  Synchronization of Shared Services and application models.

synchronized  The condition that exists when the latest version of a model resides in both the application and in Shared Services. See also model.

task list  A detailed status list of tasks for a particular user.

taskflow  The automation of a business process in which tasks are passed from one taskflow participant to another according to procedural rules.

taskflow definition  Business processes in the taskflow management system that consist of a network of stages and their relationships; criteria indicating the start and end of the taskflow; and information about individual stages, such as participants, associated applications, associated activities, and so on.

taskflow instance  A single instance of a taskflow including its state and associated data.

taskflow management system  A system that defines, creates, and manages the execution of a taskflow, including definitions, user or application interactions, and application executables.

taskflow participant  The resource that performs the task associated with the taskflow stage instance for both manual and automated stages.

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

transformation  A process that transforms artifacts so that they function properly in the destination environment after application migration.
**upgrade**  The process of deploying a new software release and moving applications, data, and provisioning information from an earlier deployment to the new deployment.

**user directory**  A centralized location for user and group information, also known as a repository or provider. Popular user directories include Oracle Internet Directory (OID), Microsoft Active Directory (MSAD), and Sun Java System Directory Server.