Oracle® Hyperion Enterprise Performance Management System

User and Role Security Guide

RELEASE 11.1.2.1

Updated: July 2011

ORACLE

ENTERPRISE PERFORMANCE MANAGEMENT SYSTEM

EPM System User and Role Security Guide, 11.1.2.1

Authors: EPM Information Development Team

Contents

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.

1 About Shared Services

In This Chapter

What Is Shared Services?

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

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

Launching Shared Services Console

You can access Shared Services Console through the Shared Services URL or through a menu option in an EPM System product; for example, Oracle Enterprise Performance Management Workspace, Fusion Edition.

➤ To launch the Shared Services Console from a URL:

1 **Go to:**

`http://Web_server_name:port_number/interop`

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/interop`.

Note: If you are accessing Shared Services Console 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/interop`.

2 Click **Launch Application**.

Note: Pop-up blockers may prevent Shared Services Console from opening.

3 **On the Logon screen, enter your user name and password.**

Initially, the only user who can access Shared Services Console is `admin` (the password for `admin` is specified in Oracle's Hyperion Enterprise Performance Management System Configurator while deploying Foundation Services).

4 Click **Log On**.

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 log in, the Shared Services Console displays the View pane and a Browse tab.

The View pane is a navigation frame where you can choose objects (such as user directories, users, groups, roles, application groups, and applications). Typically, details of your 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 a report, and a Configure tab opens when you configure a user directory.

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 expand the User Directories node to view a list of configured user directories. You may also search configured user directories for users and groups.

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. The commands displayed in the shortcut menu also are available 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 the Shared Services Console:

- User directory configurations
- Single sign-on configuration
- Native Directory management
- Role-based access control management
- 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 depends on the type of user directory you select. For example, in Native Directory, you can search for all users, active users, or 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 5, "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 e-mail 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 e-mail address

- **SAP and 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 **In Group**, specify one or more 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. Click **Search**.

4 To search for groups:

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

Note: Shared Services considers Oracle, SQL Server, and SAP roles 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 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**.

2 EPM System Security Concepts

In This Chapter

Security Components

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

- "User Authentication Components" on page 17
- "Provisioning (Role-based Authorization)" on page 18

User Authentication Components

EPM System users must be authenticated before their provisioning data is checked to determine the EPM System applications that they can access. By default, users enter a user name and password into a product login screen to gain Single Sign-On (SSO) access to all EPM System products.

You can also configure EPM System products to work with a security agent, which can pass pre-authenticated users to EPM System products. Use of other authentication mechanisms; for example, client certificate authentication, custom Java authentication, and Kerberos are also possible. For detailed information on configuring security agents for EPM System, see the *Oracle Hyperion Enterprise Performance Management System Security Administration Guide*.

User authentication mechanisms, shared across EPM System products, are used to validate the user credentials against configured user directories. User authentication, along with product-specific authorization, grants the user access to EPM System products. Authorization is granted through provisioning.

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.

The following sections describe the components that support SSO:

- "Native Directory" on page 18

- "User Directories" on page 18

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 accounts, and additional users and groups that you create.

Native Directory functions:

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

Native Directory is accessed and managed using Shared Services Console. See Chapter 6, "Managing Native Directory".

User Directories

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

EPM System products are supported on several user directories, including LDAP-based user directories, such as OID, Sun Java System Directory Server (formerly SunONE Directory Server), and Microsoft Active Directory. Relational databases and SAP native repository also are supported as user directories. User directories other than Native Directory are referred to as external user directories throughout this document. See Oracle Enterprise Performance Management Products - Supported Platforms Matrices for supported platform information.

You can configure many external user directories as the user and group information provider for EPM System products. User directories used with EPM System products must contain an account for each user who accesses EPM System products. Users may be assigned to groups in external user directories or to groups in the Native Directory to facilitate provisioning.

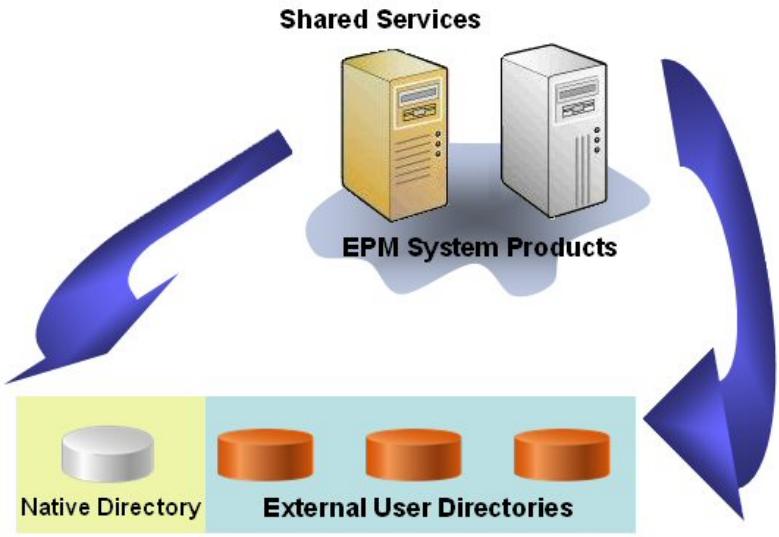
Provisioning (Role-based Authorization)

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

Each EPM System product provides several default roles tailored to various business needs. Each application belonging to an EPM System product inherits these roles. Predefined roles from the applications registered with Shared Services are displayed in the Shared Services Console. You may also create custom roles that aggregate the default roles to suit specific requirements. These roles are used for provisioning. 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. Using Shared Services Console, you can browse and provision users and groups from all configured user directories.

This illustration is an overview of the authorization process:



1. After a user is authenticated, the EPM System product queries user directories to determine the user's groups.
2. EPM System product uses group and user information to retrieve the user's provisioning data from Shared Services. The product uses this data to determine which resources a user can access.

   EPM System application roles determine the features that users can access. Data or object access security is handled through finer permissions defined within each application.

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

Roles

A role is a construct that defines the authorizations granted to users and groups to use a feature of an EPM System application. 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 administrators to control and manage application access. See Appendix A, "EPM System Roles."

Global Roles

Global roles, Shared Services roles that span multiple products, enable users to perform certain tasks across products. These roles, managed by Shared Services, cannot be deleted. See "Foundation Services Roles" on page 149 for a list of global roles.

Predefined Roles

Predefined roles are built-in roles in EPM System products; you cannot delete them. Each application instance of an EPM System product inherits all the predefined product roles. These roles, for each application, are registered with Shared Services when you create 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 Shared Services Administrator or Provisioning Manager can create an aggregated role that combines the Planner and View User roles of a Oracle Hyperion Planning, Fusion Edition, 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 products.

Users

User directories store information about the users who can access EPM System products. 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.

Groups

Groups are containers for users or other groups. Groups from all configured user directories are displayed in Shared Services Console. Oracle recommends that you provision groups to simplify the EPM System provisioning process.

3 Configuring User Directories

In This Chapter

User Directories in EPM System Security

EPM System products are supported on a number of user and identity management systems, which are collectively referred to as user directories. These include Lightweight Directory Access Protocol (LDAP) enabled user directories such as Sun Java System Directory Server (formerly SunONE Directory Server) and Active Directory. EPM System also supports SAP Provider and relational databases as external user directories.

Generally, EPM System products use Native Directory and external user directories in provisioning. See Oracle Enterprise Performance Management Products—Supported Platforms Matrices for a list of supported user directories.

EPM System products require a user directory account for each user who accesses the products. These users may be assigned to groups to facilitate provisioning. Users and groups can be provisioned with EPM System roles and object ACLs. Because of the administrative overhead, Oracle does not recommend the provisioning of individual users. Users and groups from all configured user directories are visible from Shared Services Console.

By default, EPM System Configurator configures the Shared Services repository as the Native Directory to support EPM System products. Native Directory is accessed and managed using the Shared Services Console.

Operations Related to User Directory Configuration

To support SSO and authorization, you must configure external user directories. From Shared Services Console, you can perform several tasks related to configuring and managing user directories. These topics provide instructions:

- Configuring user directories:
  - "Configuring OID, Active Directory, and Other LDAP-based User Directories" on page 24
  - "Configuring the SAP R3 Native Repository" on page 33
  - "Configuring Relational Databases as User Directories" on page 36
- "Testing User Directory Connections" on page 38
- "Editing User Directory Settings" on page 39
- "Deleting User Directory Configurations" on page 39
- "Managing the User Directory Search Order" on page 40
- "Setting Security Options" on page 42

Oracle Identity Manager and EPM System

Oracle Identity Manager is a role and user administration solution that automates the process of adding, updating, and deleting both user accounts and attribute-level entitlements across enterprise resources. Oracle Identity Manager is available as a stand-alone product or as part of Oracle Identity and Access Management Suite Plus.

EPM System integrates with Oracle Identity Manager by using enterprise roles which are LDAP groups. Roles of EPM System components can be assigned to enterprise roles. Users or groups added to Oracle Identity Manager enterprise roles automatically inherit assigned EPM System roles.

For example assume that you have a Planning application named *Budget Planning*. To support this application, you can create three enterprise roles—Budget Planning Interactive User, Budget Planning End User, and Budget Planning Admin—in Oracle Identity Manager. While provisioning EPM System roles, ensure that you provision the enterprise roles from Oracle Identity Manager with the required roles from *Budget Planning* and other EPM System components including Shared Services. All users and groups assigned to the enterprise roles in Oracle Identity Manager inherits the EPM System roles. See Oracle Identity Manager documentation for information on deploying and managing Oracle Identity Manager.

To integrate Oracle Identity Manager with EPM System, you must perform these steps:

- Ensure that members (users and groups) of Oracle Identity Manager enterprise roles that you plan to use for EPM System provisioning are defined in an LDAP-enabled user directory; for example OID or Active Directory.
- Configure the LDAP-enabled user directory where members of the enterprise roles are defined as an external user directory in EPM System. See "Configuring OID, Active Directory, and Other LDAP-based User Directories" on page 24.

Active Directory Information

This section explains Microsoft Active Directory concepts used in this document.

DNS Lookup and Host Name Lookup

You can configure Active Directory so Shared Services can perform a static host name lookup or a DNS lookup to identify Active Directory. Static host name lookup does not support Active Directory failover.

Using the DNS lookup ensures high availability of Active Directory in scenarios in which Active Directory is configured on multiple domain controllers to ensure high availability. When configured to perform a DNS lookup, Shared Services queries the DNS server to identify registered domain controllers and connects to the domain controller with the greatest weight. If the domain controller to which Shared Services is connected fails, Shared Services dynamically switches to the next available domain controller with the greatest weight.

Note: DNS lookup can be configured only if a redundant Active Directory setup that supports failover is available. See Microsoft documentation for information.

Global Catalog

A global catalog is a domain controller that stores a copy of all Active Directory objects in a forest. It stores a complete copy of all objects in the directory for its host domain and a partial copy of all objects for all other domains in the forest, which are used in typical user search operations. See Microsoft documentation for information on setting up a global catalog.

If you are using a global catalog, use one of these methods to configure your Active Directory user directories:

- Configure the global catalog server as the external user directory (recommended).
- Configure each Active Directory domain as a separate external user directory.

Configuring the global catalog instead of individual Active Directory domains allows EPM System products to access local and universal groups within the forest.

Configuring OID, Active Directory, and Other LDAP-based User Directories

Use the procedures in this section to configure LDAP-based corporate user directories, such as OID, Sun Java System Directory Server, Oracle Virtual Directory, Active Directory, IBM Tivoli Directory Server, or an LDAP-based user directory that is not listed on the configuration screen.

➤ To configure OID, Active Directory, and other LDAP-based user directories:

1 Launch Shared Services Console. See "Launching Shared Services Console" on page 13.

2 Select **Administration**, and then **Configure User Directories**.

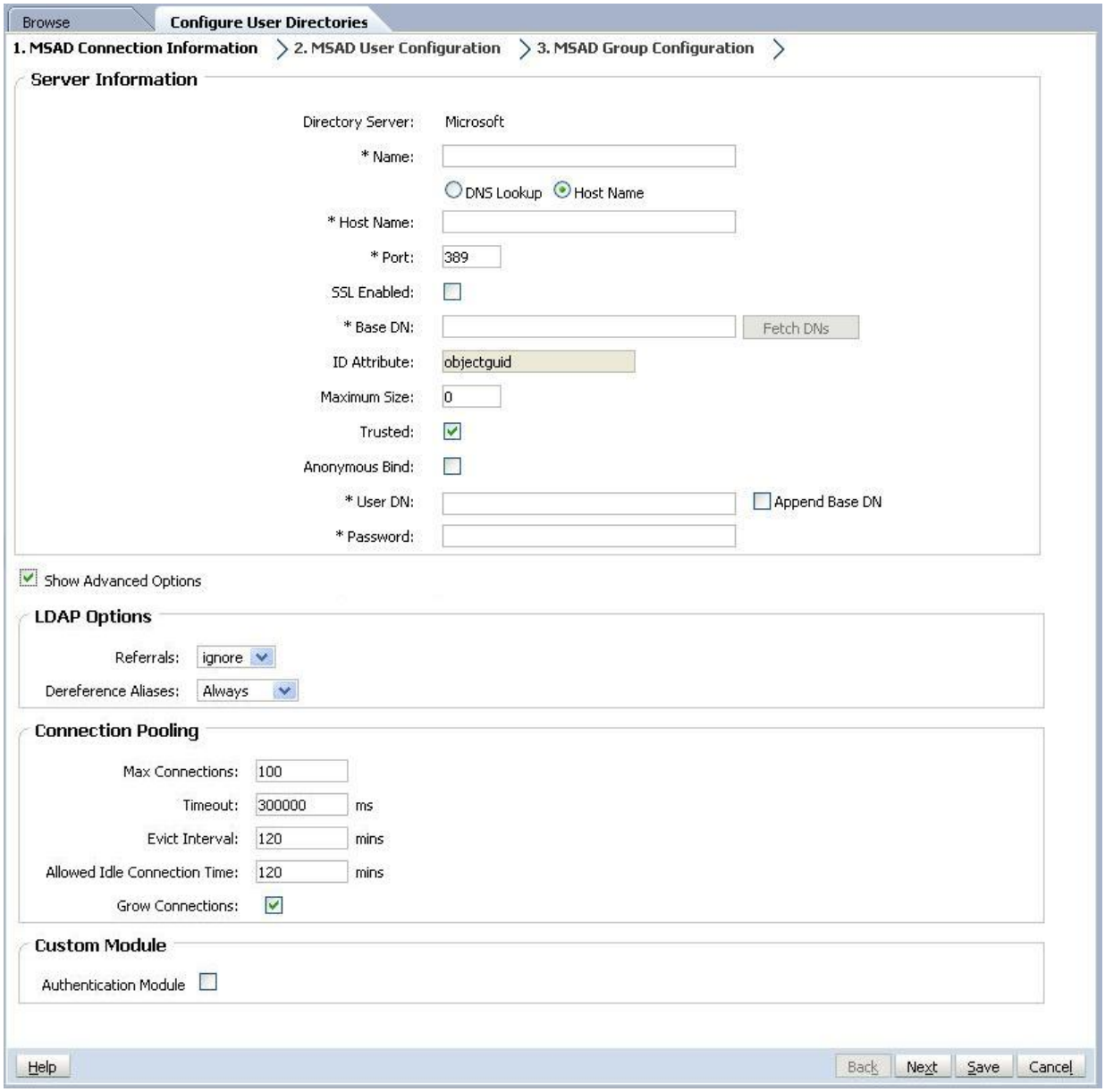
The Defined User Directories screen opens. This screen lists all configured user directories, including Native Directory.

3 Click **New**.

4 Under **Directory Type**, select an option:

- **Lightweight Directory Access Protocol** (**LDAP**) to configure an LDAP-based user directory other than Active Directory. Select this option to configure Oracle Virtual Directory.
- **Microsoft Active Directory** (**MSAD**) to configure Active Directory.

5 Click **Next**.



6 Enter the required parameters.

Table 1 Connection Information Screen

Label	Description
Directory Server	Select a user directory. Select `Other` if you are using an unlisted user directory; for example, Oracle Virtual Directory. This property is automatically selected if you chose Active Directory in step 4. The **ID Attribute** value changes to the recommended constant unique identity attribute for the selected product. **Note:** Because Oracle Virtual Directory provides a virtualized abstraction of LDAP directories and RDMBS data repositories in one directory view, EPM System considers it a single external user directory regardless of the number and type of user directories Oracle Virtual Directory supports. **Example:** `Oracle Internet Directory`

Label	Description
Name	A descriptive name for the user directory. Used to identify a specific user directory if multiple user directories are configured. **Example:** `Corporate_OID`
DNS Lookup	**Active Directory only:** Select this option to enable DNS lookup. See "DNS Lookup and Host Name Lookup" on page 23. Oracle recommends that you configure DNS lookup as the method to connect to Active Directory in production environments to avoid connection failures. **Note:** Do not select this option if you are configuring a global catalog. When you select this option, the following fields are displayed: ● **Domain**: The domain name of an Active Directory forest. **Examples:** `example.com` or `us.example.com` ● **AD Site**: Active Directory site name, generally the relative distinguished name of the site object that is stored in Active Directory configuration container. Typically, AD Site identifies a geographic location such as a city, state, region, or country. **Examples:** `Santa Clara` or `US_West_region` ● **DNS Server**: DNS name of the server that supports DNS server lookup for domain controllers.
Host Name	**Active Directory only:** Select this option to enable static host name lookup. See "DNS Lookup and Host Name Lookup" on page 23. **Note:** Select this option if you are configuring an Active Directory global catalog.
Host Name	DNS name of the user directory server. Use the fully qualified domain name if the user directory is to be used to support SSO from SiteMinder. Oracle recommends using the host name to establish an Active Directory connection for testing purposes only. **Note:** If you are configuring an Active Directory global catalog, specify the global catalog server host name. See "Global Catalog" on page 23. **Example:** `MyServer`
Port	The port number where the user directory is running. **Note:** If you are configuring an Active Directory global catalog, specify the port used by the global catalog server (default is 3268). See "Global Catalog" on page 23. **Example:** `389`
SSL Enabled	The check box that enables secure communication with this user directory. The user directory must be configured for secure communication.
Base DN	The distinguished name (DN) of the node where the search for users and groups should begin. You can also use the **Fetch DNs** button to list available base DNs and then select the appropriate base DN from the list. **Note:** If you are configuring a global catalog, specify the base DN of the forest. See "Using Special Characters" on page 47 for restrictions on the use of special characters. Oracle recommends that you select the lowest DN that contains all EPM System product users and groups. **Example:** `dc=example,dc=com`

Label	Description
ID Attribute	This attribute value can be modified only if `Other` is selected in **Directory Type**. The recommended value of this attribute is automatically set for OID `orclguid`, SunONE (`nsuniqueid`), IBM Directory Server (`Ibm-entryUuid`), Novell eDirectory (`GUID`), and Active Directory (`ObjectGUID`). **Example:** `orclguid` ID attribute value, if you set it manually after choosing `Other` in **Directory Server**; for example to configure an Oracle Virtual Directory, should: ● point to a unique user attribute ● not be location specific ● not change over time
Maximum Size	Maximum number of results that a search can return. If this value is greater than that supported by the user directory settings, the user directory value overrides this value. For user directories other than Active Directory, leave this field blank to retrieve all users and groups that meet the search criteria. For Active Directory, set this value to `0` to retrieve all users and groups that meet the search criteria. If you are configuring Shared Services in Delegated Administration mode, set this value to 0.
Trusted	The check box to indicate that this provider is a trusted SSO source. SSO tokens from trusted sources do not contain the user's password.
Anonymous Bind	The check box to indicate that Shared Services can bind anonymously to the user directory to search for users and groups. Can be used only if the user directory allows anonymous binds. If this option is not selected, you must specify in the User DN an account with sufficient access permissions to search the directory where user information is stored. Oracle recommends that you do not use anonymous bind. **Note:** Anonymous bind is not supported for OID.
User DN	This box is disabled if **Anonymous Bind** is selected. The distinguished name of the user that Shared Services should use to bind with the user directory. This distinguished name must have read privileges within the Base DN. Special characters in User DN must be specified using escape characters. See "Using Special Characters" on page 47 for restrictions. **Example:** `cn=admin,dc=example,dc=com`
Append Base DN	The check box for appending the base DN to the User DN. If you are using Directory Manager account as the User DN, do not append Base DN. This check box is disabled if the Anonymous Bind option is selected.
Password	User DN password This box is disabled if the Anonymous Bind option is selected. **Example:** `UserDNpassword`
Show Advanced Options	The check box to display advanced options.
Referrals	**Active Directory only:** Select `follow` to automatically follow LDAP referrals. Select `ignore` to not use referrals.

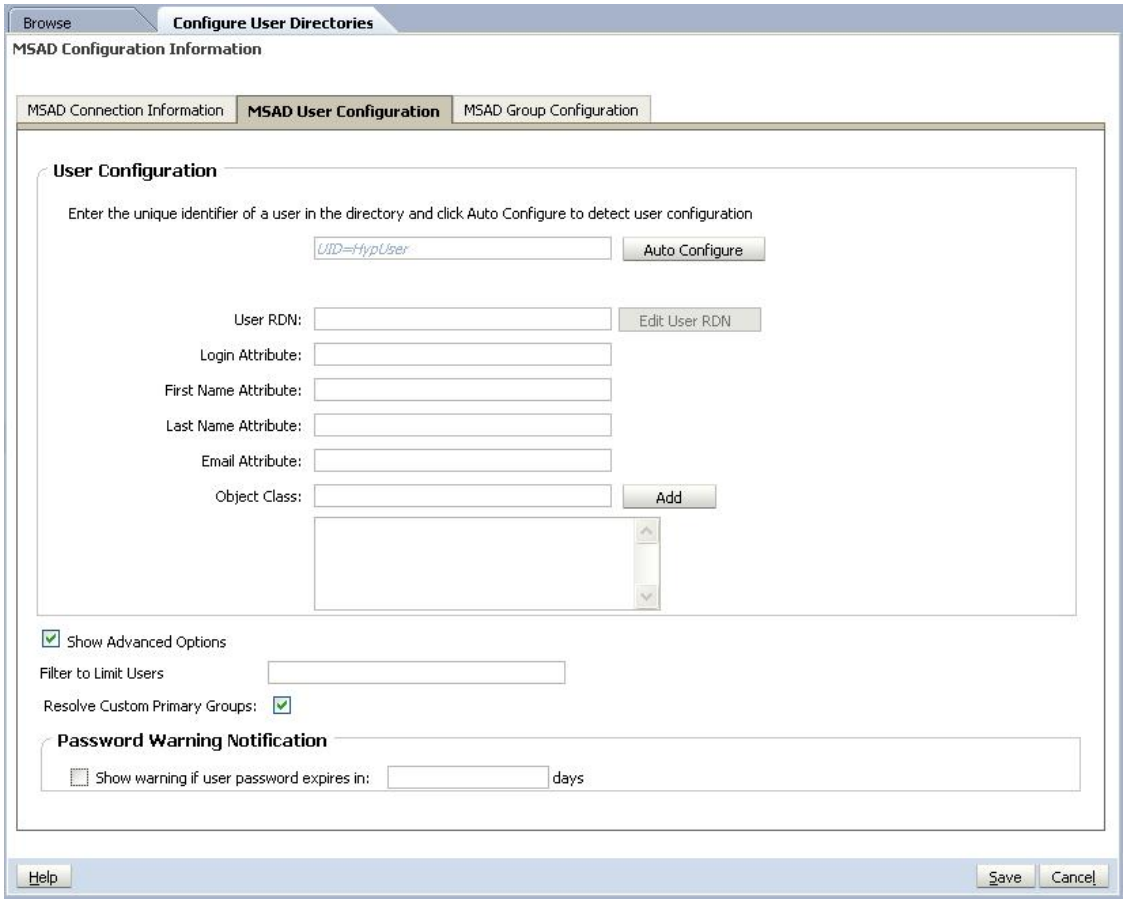
Label	Description
Dereference Aliases	Select the method that Shared Services searches should use to dereference aliases in the user directory so that searches retrieve the object to which the DN of the alias points. Select: ● **Always**: Always dereference aliases. ● **Never**: Never dereference aliases. ● **Finding**: Dereference aliases only during name resolution. ● **Searching**: Dereference aliases only after name resolution.
Max Connections	Maximum connections in the connection pool. Default is 100 for LDAP-based directories, including Active Directory.
Timeout	Timeout to get a connection from the pool. An exception is thrown after this period. Default is 300000 milliseconds (5 minutes).
Evict Interval	**Optional:** The interval for running the eviction process to clean the pool. The eviction process removes idle connections that have exceeded the `Allowed Idle Connection Time`. Default is 120 minutes.
Allowed Idle Connection Time	**Optional:** The time after which the eviction process removes the idle connections in the pool. Default is 120 minutes.
Grow Connections	This option indicates whether the connection pool can grow beyond `Max Connections`. Selected by default. If you do not allow the connection pool to grow, the system throws an error if a connection is not available within the time set for `Time Out`.
Authentication Module	The check box to enable the use of a custom authentication module to authenticate users defined in this user directory. You must also enter the fully qualified Java class name of the authentication module in the Security Options screen. See "Setting Security Options" on page 42. The custom authentication module authentication is transparent to thin and thick clients and does not require client deployment changes. See "Using a Custom Authentication Module" in the *Oracle Hyperion Enterprise Performance Management System Security Administration Guide*.

7 Click **Next**.

Shared Services uses the properties set on the User Configuration screen to create a user URL that is used to determine the node where search for users begins. Using this URL speeds the search.

Caution! The user URL should not point to an alias. EPM System security requires that the user URL points to an actual user.

Oracle recommends that you use the Auto Configure area of the screen to retrieve the required information.



Note: See "Using Special Characters" on page 47 for a list of special characters that can be used in the user configuration.

8 **In Auto Configure, enter a unique user identifier using the format *attribute=identifier*; for example, `uid=jdoe`.**

Attributes of the user are displayed in the User Configuration area.

If you are configuring OID, you cannot automatically configure the user filter, because the root DSE of OID does not contain entries in the Naming Contexts attribute. See Managing Naming Contexts in the *Oracle Internet Directory Administrator's Guide*.

Note: You can manually enter required user attributes into text boxes in the User Configuration area.

Table 2 User Configuration Screen

Label	Description[1]
User RDN	The Relative DN of the user. Each component of a DN is called an RDN and represents a branch in the directory tree. The RDN of a user is generally the equivalent of the `uid` or `cn`. See "Using Special Characters" on page 47 for restrictions. **Example:** `ou=People`

Label	Description[1]
Login Attribute	A unique attribute (can be a custom attribute) that stores the login name of the user. Users use the value of this attribute as the user name while logging into EPM System products. User IDs (value of Login Attribute) must be unique across all user directories. For example, you may use `uid` and `sAMAccountName` respectively as the Login Attribute for your SunONE and Active Directory configurations. The values of these attributes must be unique across all user directories, including Native Directory. **Note:** User IDs are not case sensitive. **Note:** If you are configuring OID as an external user directory for EPM System products deployed on Oracle Application Server in a Kerberos environment, you must set this property to `userPrincipalName`. **Default** ● **Active Directory:** `cn` ● **LDAP directories other than Active Directory:** `uid`
First Name Attribute	The attribute that stores the user's first name **Default:** `givenName`
Last Name Attribute	The attribute that stores the user's last name **Default:** `sn`
Email Attribute	**Optional**: The attribute that stores the user's e-mail address **Default:** `mail`
Object Class	Object classes of the user (the mandatory and optional attributes that can be associated with the user). Shared Services uses the object classes listed in this screen in the search filter. Using these object classes, Shared Services should find all users who should be provisioned. You can manually add object classes if needed. To add an object class, enter the object class name into the **Object Class** box and click **Add**. To delete object classes, select the object class and click **Remove**. **Default** ● **Active Directory:** `user` ● **LDAP directories other than Active Directory:** `person, organizationalPerson, inetorgperson`
Show Advanced Options	The check box that enables the use of a filter to retrieve users during searches.
Filter to Limit Users	An LDAP query that retrieves only the users that are to be provisioned with EPM System product roles. For example, the LDAP query `(uid=Hyp*)` retrieves only users whose names start with `Hyp`. The User Configuration screen validates the User RDN and recommends the use of a user filter, if required. The user filter limits the number of users returned during a query. It is especially important if the node identified by the user RDN contains many users that need not be provisioned. User filters can be designed to exclude the users that are not to be provisioned, thereby improving performance.
Resolve Custom Primary Groups	**Active Directory only:** The check box that indicates whether to identify primary groups of users to determine effective roles. This check box is selected by default. Oracle recommends that you not change this setting.

Label	Description[1]
Show warning if user password expires in:	**Active Directory only:** The check box that indicates whether to display a warning message if the Active Directory user password expires within the specified number of days.

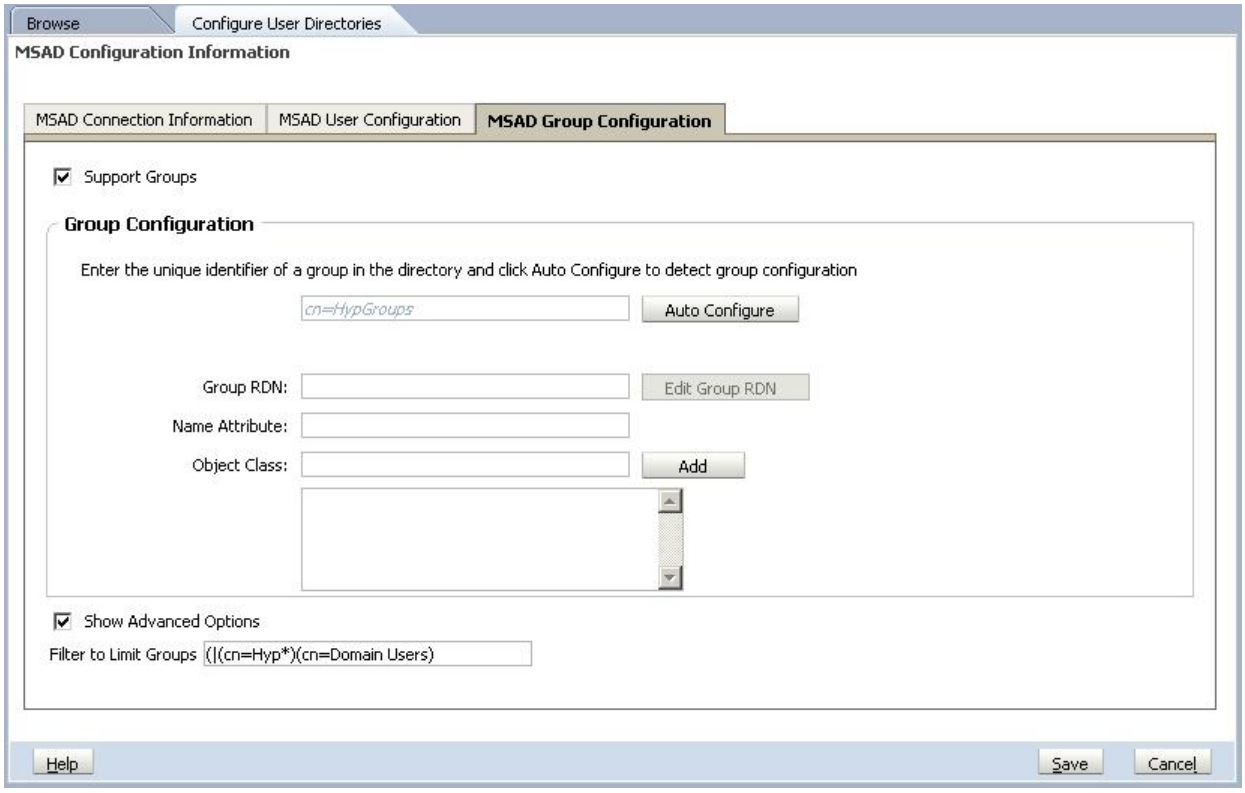
[1]EPM System security may use default values for some fields for which configuration value is optional. If you do not enter values in such fields, default values are used during runtime.

9 **Click Next.**

The Group Configuration screen opens. Shared Services uses the properties set in this screen to create the group URL that determines the node where the search for groups starts. Using this URL speeds the search.

Caution! The Group URL should not point to an alias. EPM System security requires that the group URL point to an actual group. If you are configuring a Novell eDirectory that uses group aliases, the group aliases and group accounts must be available within the group URL.

Note: Data entry in the Group Configuration screen is optional. If you do not enter the group URL settings, Shared Services searches within the Base DN to locate groups, which can negatively affect performance, especially if the user directory contains many groups.



10 Clear **Support Groups** if you do not plan to provision groups, or if users are not categorized into groups on the user directory. Clearing this option disables the fields on this screen.

If you are supporting groups, Oracle recommends that you use the autoconfigure feature to retrieve the required information.

If you are configuring OID as a user directory, you cannot use the autoconfigure feature, because the root DSE of OID does not contain entries in the Naming Contexts attribute. See Managing Naming Contexts in the *Oracle Internet Directory Administrator's Guide*.

11 In the **Auto Configure** text box, enter a unique group identifier, and then click **Go**.

The group identifier must be expressed in *attribute=identifier* format; for example, `cn=western_region`.

Attributes of the group are displayed in the Group Configuration area.

Note: You can enter required group attributes in the Group Configuration text boxes.

Caution! If the group URL is not set for user directories that contain / (slash) or \ (backslash) in its node names, the search for users and groups fails. For example, any operation to list the user or group fails if the group URL is not specified for a user directory in which users and groups exist in a node, such as `OU=child \ou,OU=parent/ou` or `OU=child/ou,OU=parent \ ou`.

Table 3 Group Configuration Screen

Label	Description[1]
Group RDN	The Relative DN of the group. This value, which is path relative to the Base DN, is used as the group URL. Specify a Group RDN that identifies the lowest user directory node in which all the groups that you plan to provision are available. If you use an Active Directory primary group for provisioning, ensure that the primary group falls under the Group RDN. Shared Services does not retrieve the primary group if it is outside the scope of the group URL. The Group RDN has a significant impact on login and search performance. Because it is the starting point for all group searches, you must identify the lowest possible node in which all groups for EPM System products are available. To ensure optimum performance, the number of groups present within the Group RDN should not exceed 10,000. If more groups are present, use a group filter to retrieve only the groups you want to provision. **Note:** Shared Services displays a warning if the number of available groups within the Group URL exceeds 10,000. See "Using Special Characters" on page 47 for restrictions. **Example:** `ou=Groups`
Name Attribute	The attribute that stores the name of the group **Default** • **LDAP directories including Active Directory:** `cn` • **Native Directory:** `cssDisplayNameDefault`

Label	Description[1]
Object class	Object classes of the group. Shared Services uses the object classes listed in this screen in the search filter. Using these object classes, Shared Services should find all groups associated with the user. You can manually add object classes if needed. To add an object class, enter the object class name into the Object class text box and click **Add**. To delete object classes, select the object class and click **Remove**. **Default** ● **Active Directory:** `group?member` ● **LDAP directories other than Active Directory:** `groupofuniquenames?uniquemember, groupOfNames?member` ● **Native Directory:** `groupofuniquenames?uniquemember, cssGroupExtend?cssIsActive`
Show Advanced Options	The check box that enables the use of a filter to retrieve groups during search operations.
Filter to Limit Groups	An LDAP query that retrieves the groups that are to be provisioned with EPM System product roles only. For example, the LDAP query `(|(cn=Hyp*)(cn=Admin*))` retrieves only groups whose names start with `Hyp` or `Admin`. The group filter, used to limit the number of groups returned during a query, is especially important if the node identified by the Group RDN contains a large number of groups that need not be provisioned. Filters can be designed to exclude the groups that are not to be provisioned, improving performance. If you use Active Directory primary group for provisioning, ensure that any group filter that you set can retrieve the primary group contained within the scope of the group URL. For example, the filter `(|(cn=Hyp*)(cn=Domain Users))` retrieves groups that have names that start with `Hyp` and the primary group named `Domain Users`.

[1]EPM System security may use default values for some fields for which configuration value is optional. If you do not enter values in such fields, default values are used during runtime.

12 **Click Save.**

Shared Services saves the configuration and returns to the Defined User Directories screen, which now lists the user directory that you configured.

13 **Test the configuration. See "Testing User Directory Connections" on page 38.**

14 **If needed, change the search order assignment. See "Managing the User Directory Search Order" on page 40 for details.**

15 **If needed, specify security options. See "Setting Security Options" on page 42 for details.**

16 **Restart Shared Services and all EPM System products.**

Configuring the SAP R3 Native Repository

Before configuring an SAP native repository, ensure that you have met the prerequisites described in "Single Sign-on with SAP Enterprise Portal" in the *Oracle Hyperion Enterprise Performance Management System Security Administration Guide*.

By default, EPM System sets a SAP keystore timeout of 10 seconds. After configuring an SAP provider, you can change the timeout by editing the security options. See "Setting Security Options" on page 42.

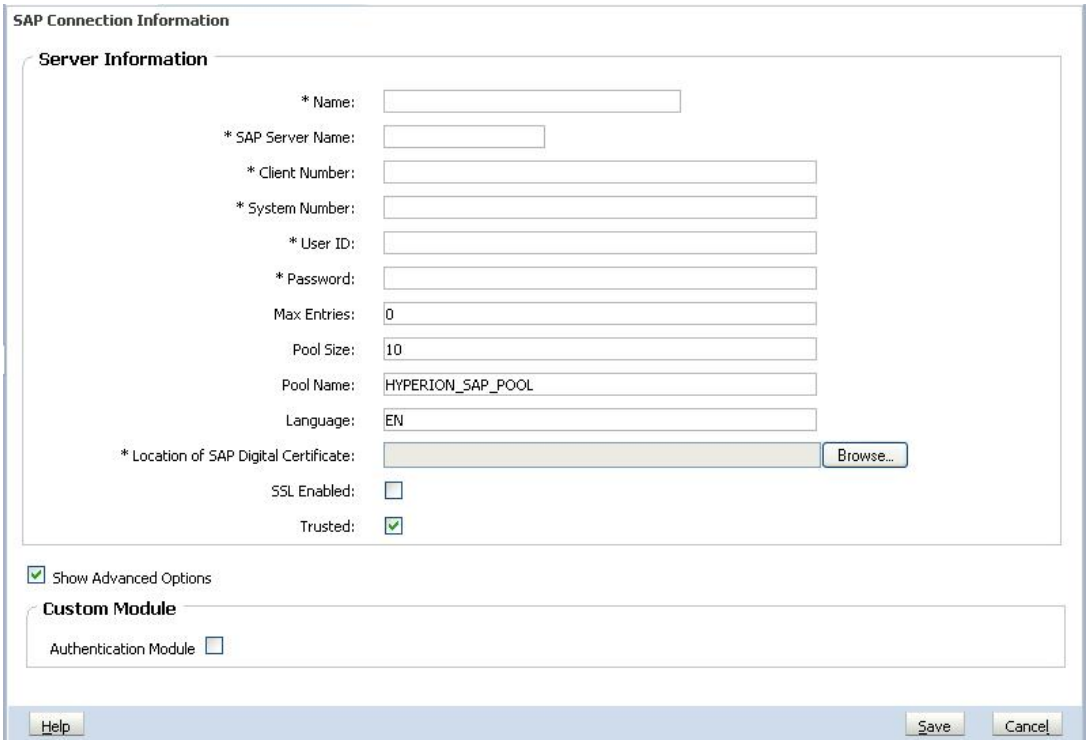
➤ To configure an SAP native repository:

1 Launch Shared Services Console. See "Launching Shared Services Console" on page 13.

2 Select **Administration**, and then **Configure User Directories**.

3 Click **New**.

4 On the **Directory Type** screen, select **SAP**, and then select **Next**.



5 On the SAP Connection Information screen, enter configuration parameters.

Table 4 SAP Connection Information Screen

Label	Description[1]
Name	A unique configuration name for the SAP provider. You use this name to identify the SAP provider in situations in which multiple SAP providers are defined in Shared Services. **Example:** `MY_SAP_DIRECTORY`
SAP Server Name	The DNS name of the computer where the SAP Server is running, or the SAP router address. **Example:** `myserver`
Client Number	The client number of the SAP system to which you want to connect. **Example:** `001`
System Number	The system number of the SAP System to which you want to connect. **Example:** `00`
User ID	The user name that Shared Services should use to access SAP. This user must have access permissions to use Remote Function Calls (RFC) to connect to SAP and to access user, activity groups, and their relationship data. **Example:** `my_sap_user`

Label	Description[1]
Password	The password of the user identified in the User ID box. **Example:** `my_sap_password`
Max Entries	The maximum entries that a query to the SAP provider can return. If you are configuring Shared Services in Delegated Administration mode, set this value to 0. **Example:** `100`
Pool Size	The JCo connection pool size. **Default:** `20`
Pool Name	A unique name for the connection pool that should be used to establish a link between Shared Services and SAP. **Default:** `HYPERION_SAP_POOL`
Language	Language for messages, for example error messages, from SAP. By default, this value is read from the system locale of the server hosting Shared Services. **Example:** `EN`
Location of SAP Digital Certificate	The SAP X.509 certificate to use. EPM System products use this certificate to parse the SAP login ticket and to extract the user ID needed to support SSO. Required only if EPM System products are plugged into SAP Enterprise Portal. **Example:** `C:/Oracle/Middleware/EPMSystem11R1/common/SAP/bin/`*`SAP_cert_name`*.
SSL Enabled	Check box that enables you to use Secure Socket Layer (SSL) to communicate between Shared Services and the SAP provider.
Trusted	Check box that enables you to specify that this provider is a trusted SSO source. SSO tokens from trusted sources do not contain the user's password.
Show Advanced Options	The check box to display custom authentication setting.
Authentication Module	Select this check box to enable the use of a custom authentication module to authenticate users defined in this user directory. You must also enter the fully qualified Java class name of the authentication module in the Security Options screen. See "Setting Security Options" on page 42. See "Using a Custom Authentication Module" in the *Oracle Hyperion Enterprise Performance Management System Security Administration Guide*.

[1]EPM System security may use default values for fields for which configuration values are optional. If you do not enter values in such fields, default values are used during runtime.

6 **Click Save.**

Shared Services saves the configuration and returns to the Defined User Directories screen, which now lists the SAP provider that you configured.

7 **Test the SAP native repository configuration. See "Testing User Directory Connections" on page 38.**

8 **If needed, change the search order assignment. See "Managing the User Directory Search Order" on page 40 for details.**

9 **If needed, specify security options. See "Setting Security Options" on page 42 for details.**

10 **Restart Shared Services and all EPM System products.**

Configuring Relational Databases as User Directories

User and group information from the system tables of Oracle, SQL Server, and IBM DB2 relational databases can be used to support provisioning. If group information cannot be derived from the database's system schema, Shared Services does not support the provisioning of groups from that database provider. For example, Shared Services cannot extract group information from older versions of IBM DB2, because the database uses groups defined on the operating system. You can, however, add these users to groups in Native Directory and provision those groups. See Oracle Enterprise Performance Management Products—Supported Platforms Matrices for supported platform information.

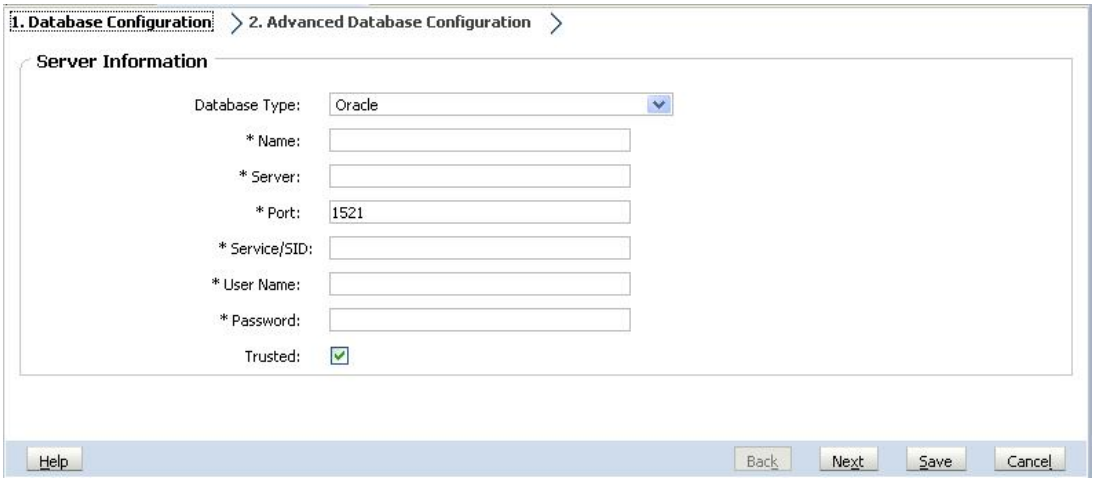
Note: If you are using a DB2 database, the user name must contain at least eight characters. User names should not exceed 256 characters (Oracle and SQL Server databases), and 1000 characters (DB2).

You must configure Shared Services to connect to the database as the database administrator; for example, Oracle `SYSTEM` user, to retrieve the list of users and groups.

Note: Shared Services can retrieve only active database users for provisioning. Inactive and locked database user accounts are ignored.

➤ To configure database providers:

1. Launch Shared Services Console. See "Launching Shared Services Console" on page 13.
2. Select **Administration**, and then **Configure User Directories**.
3. Click **Add**.
4. In the **Directory Type** screen, select **Relational Database (Oracle, DB2, SQL Server)**.
5. Click **Next**.



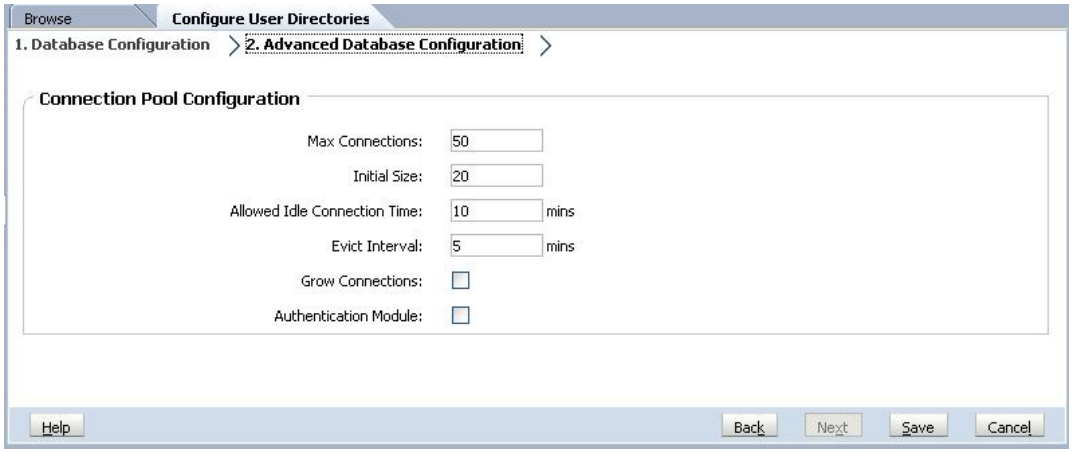
6. On the Database Configuration tab, enter configuration parameters.

Table 5 Database Configuration Tab

Label	Description
Database Type	The relational database provider. Shared Services supports only Oracle, IBM DB2, and SQL Server databases as database providers. **Example:** `Oracle`
Name	A unique configuration name for the database provider. **Example:** `Oracle_DB_FINANCE`
Server	The DNS name of the computer on which the database server is running. **Example:** `myserver`
Port	The database server port number **Example:** `1521`
Service/SID (Oracle only)	The system identifier (default is `orcl`) **Example:** `orcl`
Database (SQL Server and DB2 only)	The database to which Shared Services should connect **Example:** `master`
User Name	The user name that Shared Services should use to access the database. This database user must have access privileges to database system tables. Oracle recommends that you use the `system` account for Oracle databases and the database administrator's user name for SQL Server and IBM DB2 databases. **Example:** `SYSTEM`
Password	The password of the user identified in the **User Name**. **Example:** `system_password`
Trusted	Check box that specifies that this provider is a trusted SSO source. SSO tokens from trusted sources do not contain the user's password.

7 **Optional:** Click **Next** to configure the connection pool.

The Advanced Database Configuration tab opens.



8 On Advanced Database Configuration, enter connection pool parameters.

Table 6 Advanced Database Configuration Tab

Label	Description
Max Connections	Maximum connections in the pool. Default is 50.
Initial Size	Available connections when the pool is initialized. Default is 20.
Allowed Idle Connection Time	**Optional:** The time after which the eviction process removes the idle connections in the pool. Default is 10 minutes.
Evict Interval	**Optional:** The interval for running the eviction process to clean up the pool. Eviction removes idle connections that have exceeded the `Allowed Idle Connection Time`. Default is five minutes.
Grow Connections	Indicates whether the connection pool can grow beyond `Max Connections`. By default, this option is cleared, indicating that the pool cannot grow. If you do not allow the connection pool to grow, the system returns an error if a connection is not available within the time set for `Time Out`.
Authentication Module	Enable a custom authentication module to authenticate users defined in this relational database. You must also enter the fully qualified Java class name of the authentication module in the Security Options screen. See "Setting Security Options" on page 42. See "Using a Custom Authentication Module" in the *Oracle Hyperion Enterprise Performance Management System Security Administration Guide*.

9 Click **Save**.

10 Click **OK** to return to the Defined User Directories screen.

11 Test the database provider configuration. See "Testing User Directory Connections" on page 38.

12 Change the search order assignment, if needed. See "Managing the User Directory Search Order" on page 40 for details.

13 Specify security settings, if needed. See "Setting Security Options" on page 42.

14 Restart Shared Services and all EPM System products.

Testing User Directory Connections

After configuring a user directory, test the connection to ensure that Shared Services can connect to the user directory using the current settings.

➤ To test a user directory connection:

1 Launch Shared Services Console. See "Launching Shared Services Console" on page 13.

2 Select **Administration**, then **Configure User Directories**.

3 From the list of user directories, select an external user directory configuration to test.

4 Click **Test**, and then **OK**.

Editing User Directory Settings

You can modify any parameter, other than name, of a user directory configuration. Oracle recommends that you not edit the configuration data of user directories that were used for provisioning.

Caution! Editing some settings, for example, the `ID Attribute`, in the user directory configuration invalidates provisioning data. Exercise extreme care when modifying the settings of a user directory that has been provisioned.

➤ To edit a user directory configuration:

1. **Launch the Shared Services Console. See "Launching Shared Services Console" on page 13.**
2. **Select Administration, and then Configure User Directories.**
3. **From Defined User Directories screen, select a user directory to edit.**
4. **Click Edit.**
5. **Modify the configuration settings.**

   Note: You cannot modify the configuration name. If you are modifying an LDAP user directory configuration, you can choose a different directory server or `Other` (for custom LDAP directories) from the Directory Server list. You cannot edit Native Directory parameters.

   For an explanation of the parameters you can edit, see the following tables:

   - Active Directory and other LDAP-based user directories:
     - Table 1, "Connection Information Screen," on page 25
     - Table 2, "User Configuration Screen," on page 29
     - Table 3, "Group Configuration Screen," on page 32
   - SAP Native Repository: See Table 4, " SAP Connection Information Screen," on page 34
   - Databases: See Table 5, "Database Configuration Tab," on page 37
6. **Click Finish to save the changes.**

Deleting User Directory Configurations

You can delete an external user directory configuration anytime. Deleting a configuration invalidates all the provisioning information for the users and groups derived from the user directory and removes the directory from the search order.

Tip: If you do not want to use a configured user directory that was used for provisioning, remove it from the search order so that it is not searched for users and groups. This action maintains the integrity of provisioning information and enables you to use the user directory later.

➤ To delete a user directory configuration:

1. Launch the Shared Services Console. See "Launching Shared Services Console" on page 13.
2. Select **Administration**, and then **Configure User Directories**.
3. From **Defined User Directories**, select a directory.
4. Click **Delete**.
5. Click **OK**.
6. Click **OK** again.
7. Restart Shared Services and other EPM System products.

Managing the User Directory Search Order

When you configure an external user directory, Shared Services automatically adds the user directory to the search order and assigns it the next available search sequence preceding that of Native Directory. The search order is used to cycle through configured user directories when EPM System searches for users and groups.

You can remove a user directory from the search order, in which case Shared Services automatically reassigns the search order of the remaining directories. User directories not included in the search order are not used to support authentication and provisioning.

Note: Shared Services terminates the search for the user or group when it encounters the specified account. Oracle recommends that the corporate directory that contains most of the EPM System users be placed at the top of the search order.

By default, Native Directory is set as the last directory in the search order. You can perform these tasks to manage the search order:

- "Adding a User Directory to the Search Order" on page 40
- "Changing the Search Order" on page 41
- "Removing a Search Order Assignment" on page 41

Adding a User Directory to the Search Order

A newly configured user directory is automatically added to the search order. If you removed a directory from the search order, you can add it to the end of the search order.

➤ To add a user directory to the search order:

1 Launch Shared Services Console. See "Launching Shared Services Console" on page 13.

2 Select **Administration**, and then **Configure User Directories**.

3 From **Defined User Directories** screen, select a user directory to add to the search order.

4 Click **Include**.

This button is available only if you have selected a user directory that is not in the search order.

5 Click **OK** to return to the Defined User Directories screen.

6 Restart Shared Services for the new search order to take effect.

7 Restart other EPM System products and custom applications that use the Shared Services security APIs.

Changing the Search Order

The default search order assigned to each user directory is based on the sequence in which the directory was configured. By default, Native Directory is set as the last directory in the search order.

➤ To change the search order:

1 Launch Shared Services Console. See "Launching Shared Services Console" on page 13.

2 Select **Administration**, and then **Configure User Directories**.

3 From **Defined User Directories**, select a directory whose search order you want to change.

4 Click **Move Up** or **Move Down**.

5 Click **Save**.

6 Restart Shared Services for the new search order to take effect.

7 Restart other EPM System products and custom applications that use the Shared Services security APIs.

Removing a Search Order Assignment

Removing a user directory from the search order does not invalidate the directory configuration; it removes the user directory from the list of directories that are searched for authenticating users. A directory that is not included in the search order is set to `Not Used` status. When you remove a user directory from the search order, the search sequence assigned to the other user directories is automatically updated.

Note: You cannot remove Native Directory from the search order.

➤ To remove a user directory from the search order:

1 Launch Shared Services Console. See "Launching Shared Services Console" on page 13.

2 Select **Administration**, and then **Configure User Directories**.

3 From **Defined User Directories**, select a directory to remove from the search order.

4 Click **Exclude**.

5 Click **OK**.

6 Click **OK** on the Directory Configuration result screen.

7 Restart Shared Services for the new search order to take effect.

8 Restart other EPM System products and custom applications that use the Shared Services security APIs.

Setting Security Options

Security options comprise the global parameters applicable to all user directories included in the search order.

➤ To set security options:

1 Launch Shared Services Console. See "Launching Shared Services Console" on page 13.

2 Select **Administration**, and then **Configure User Directories**.

3 Select **Security Options**.

4 In **Security Options**, set global parameters.

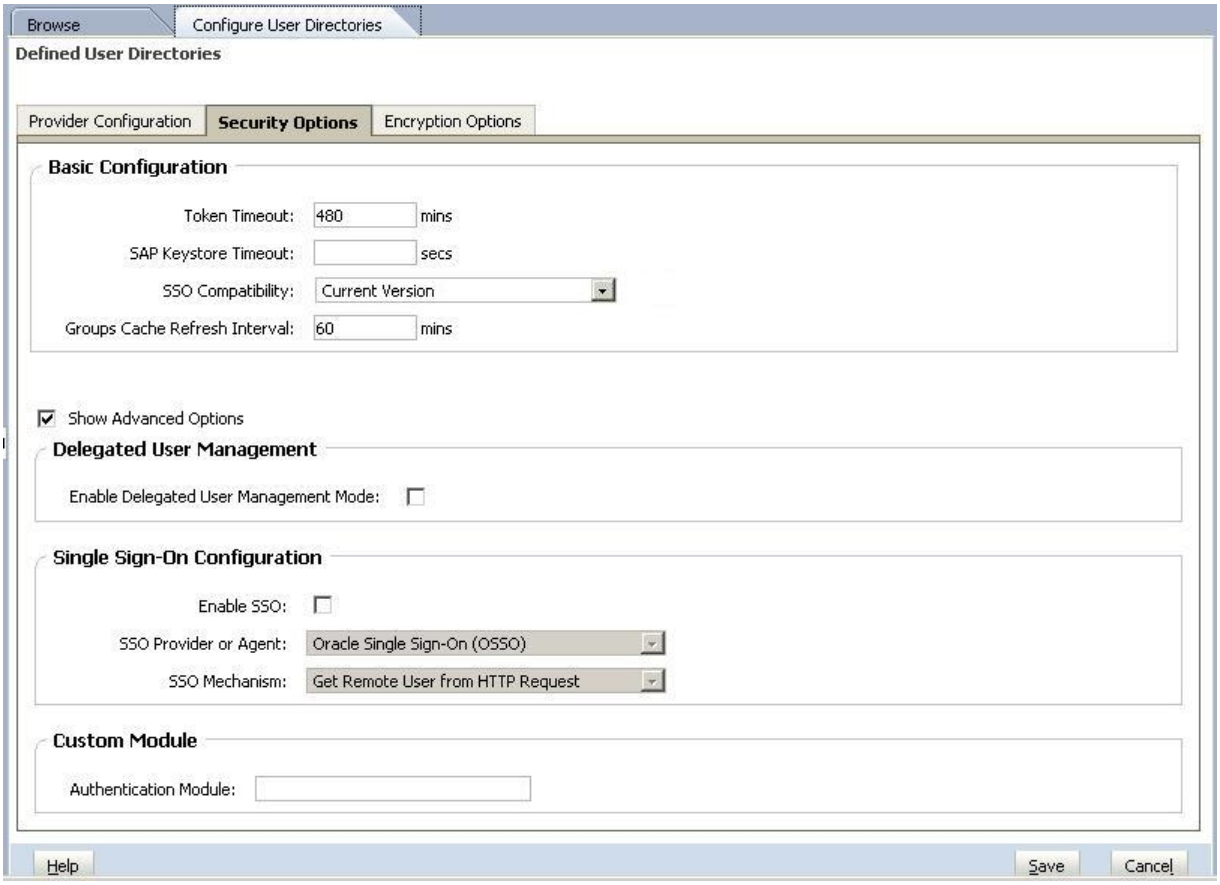


Table 7 Security Options for User Directories

Parameter	Description
Token Timeout	Time (in minutes) after which the SSO token issued by EPM System products or the Web identity management solution expires. Users must log in again after this period. Token timeout is set based on the server's system clock. **Note:** Token timeout is not the same as session timeout. **Example:** `480`
SAP Keystore Timeout	The time limit (in seconds) for resolving the SAP keystore file. Default is `10`. **Example:** `20`
SSO Compatibility	By default set to `Current Version`, which works for EPM System Release 11.1.2.1 components only. Select `11.1.2.0 and below` if your deployment environment comprises components from previous EPM System releases. This setting supports backward compatibility of EPM System components.
Groups Cache Refresh Interval	Interval (in minutes) for refreshing the Shared Services cache of groups to users relationship data. Default is 60 minutes. Shared Services caches information about new external user directory groups and new users added to existing groups only after the next cache refresh. Users provisioned through a newly created external user directory group do not get their provisioned roles until the cache is refreshed. **Example:** `120`
Show Advanced Options	Option that allows you to display settings related to Delegated Administration and SSO configuration and custom authentication module class
Enable Delegated User Management Mode	Option enabling delegated user management of EPM System products to support the distributed management of provisioning activities. See Chapter 5, "Delegated User Management."
Enable SSO	Option enabling support for SSO from security agents such as Oracle Access Manager
SSO Provider or Agent	Select the Web identity management solution from which EPM System products should accept SSO. Select **Other** if your Web identity management solution; for example, Kerberos, is not listed. The preferred SSO method is automatically selected when you select the SSO provider. You can change the name of the HTTP header or custom login class, if required. **Note:** If you are using OSSO as the identity management solution, choose `Other` in **SSO Provider or Agent**, `Custom HTTP Header` in **SSO Mechanism**, and enter `Proxy-Remote-User` as the name of the custom HTTP header. If you select `Other` as the SSO provider or agent, you must choose the SSO mechanism used by the agent. See "Supported SSO Methods" in the *Oracle Hyperion Enterprise Performance Management System Security Administration Guide*. ● `Custom HTTP Header`: Set the name of the header that the agent passes to EPM System. ● `Custom Login Class`: Specify the custom Java class that handles HTTP requests for authentication. See "Custom Login Class" in the *Oracle Hyperion Enterprise Performance Management System Security Administration Guide*. **Note:** This is not the same as custom authentication. ● `HTTP Authorization Header`: The standard HTTP mechanism. ● `Get Remote User from HTTP Request`: Select this option if the security agent populates the remote user in the HTTP request.

Parameter	Description
SSO Mechanism	The method that the Web identity management solution uses to provide user's login name to EPM System products. For a description of acceptable SSO methods, see "Supported SSO Methods" in the *Oracle Hyperion Enterprise Performance Management System Security Administration Guide*.
Authentication Module	The fully qualified Java class name of the custom authentication module (for example, `com.mycompany.epm.CustomAuthenticationImpl`) that should be used to authenticate users on all user directories for which the custom authentication module is selected. The authentication module is used for a user directory only if the directory configuration has enabled (default) its use. Foundation Services requires that the custom authentication JAR file be named `CustomAuth.jar`. `CustomAuth.jar` must be available in *EPM_ORACLE_HOME*`/common/jlib/11.1.2.0`. You can use any package structure and class name within the JAR file. For more information, see "Using a Custom Authentication Module" in the *Oracle Hyperion Enterprise Performance Management System Security Administration Guide*.

5 **Click Save.**

6 **Restart Shared Services and other EPM System products.**

Regenerating Encryption Keys

EPM System uses the following keys to ensure security:

- Single Sign On Token encryption key, used to encrypt and decrypt EPM System SSO tokens. This key is stored in Oracle's Hyperion Shared Services Registry.
- Trusted Services key, used by EPM System components to verify the authenticity of the service that is requesting an SSO token.
- Provider Configuration encryption key, used to encrypt the password (user DN password for LDAP-enabled user directories) that EPM System security uses to bind with a configured external user directory. This password is set while configuring an external user directory.

Caution! If your deployment comprises System 9 release 9.2.x components, regenerating the encryption key causes SSO failure because System 9 release 9.2.x components work with its default encryption key only.

Caution! Taskflows used by Oracle Hyperion Financial Management, Fusion Edition; Oracle Hyperion EPM Architect, Fusion Edition; and Oracle Hyperion Profitability and Cost Management, Fusion Edition, are invalidated when you regenerate the Single Sign On Encryption key. After regenerating the key, you must open and save the taskflows to revalidate them.

➤ To regenerate Single Sign On Encryption key, Provider Configuration key, or Trusted Services key:

1 **Launch Shared Services Console. See "Launching Shared Services Console" on page 13.**

2 Select **Administration**, and then **Configure User Directories**.

3 Select **Encryption Options**.

4 In **Encryption Options**, select the key that you want to regenerate.

Table 8 EPM System Encryption Options

Option	Description
Single Sign On Token	Select to regenerate the encryption key that is used to encrypt and decrypt EPM System SSO tokens. Select one of the following buttons if **SSO Compatibility** in Security Options screen is set to `11.1.2.0 and below`: ● **Generate new key** to create a new SSO token encryption key. ● **Reset to default** to restore the default SSO token encryption key. **Note:** If you revert to the default encryption key, you must delete the existing keystore file. See Table 9.
Trusted Services Key	Select this to regenerate the trusted authentication key, used by EPM System components to verify the authenticity of the service that is requesting an SSO token.
Provider Configuration Key	Select this to regenerate the key that is used to encrypt the password (user DN password for LDAP-enabled user directories) that EPM System security uses to bind with a configured external user directory. This password is set while configuring an external user directory.

5 Click **Save**.

6 **Optional:** If you chose to generate a new SSO encryption key, complete this step.

a. Click **Download**.

b. Click **OK** to download `ssHandlerTK`, the keystore file that supports the new SSO encryption key, into a folder on the server that hosts Foundation Services.

c. **Optional:** Copy `ssHandlerTK` into required locations. See following table for details.

Table 9 Encryption key compatibility and location of keystore

EPM System Interoperability Mode[1]	SSO Encryption Key Regeneration Support	Where to Locate `ssHandlerTK`[2]
11.1.2.1 with 9.2.x	No	Not applicable
11.1.2.1 with 9.3.x	Yes	*HYPERION_HOME*`/common/CSS` on all EPM System host machines
11.1.2.1 with 11.1.1.1	Yes	*HYPERION_HOME*`/common/CSS` on all EPM System host machines
11.1.2.1 with 11.1.1.2	Yes	*EPM_ORACLE_HOME*`/common/CSS` on all EPM System host machines
11.1.2.1 with 11.1.1.3	Yes	*EPM_ORACLE_HOME*`/common/CSS` on all EPM System host machines
11.1.2.1	Yes	*EPM_ORACLE_HOME*`/common/CSS` on all EPM System host machines

[1]Some interoperability modes listed in this table may not be supported. See Release 11.1.2.1 Certification Matrix.

[2]If you revert to the default encryption key, you must delete `ssHandlerTK` from these locations

7 Restart Shared Services and other EPM System products.

Changing the Identity Attribute of an Existing User Directory Configuration

When you configure a new user directory, the recommended value of the identity attribute is automatically set if you choose Oracle Internet Directory, SunONE Directory Server, IBM Directory Server, Novell eDirectory, or Active Directory as the user directory. In some cases, users select `Other` as the user directory to configure these LDAP-based user directories so as to use a custom identity attribute; for example, `DN`. If you want to change the identity attribute of a configured LDAP-enabled user directory of type `Other` to the recommended attribute for the user directory, you must complete the following migration procedure:

➤ To migrate from a custom identity attribute to the recommended attribute:

1 Launch the Shared Services Console. See "Launching Shared Services Console" on page 13.

2 Select **Administration**, and then **Configure User Directories**.

3 From **Defined User Directories** screen, select the user directory for which you want to change the identity attribute.

4 Click **Edit**.

5 In **ID Attribute**, change the existing value to the default ID attribute value for the user directory. For example, if this is an Oracle Internet Directory, enter `orclguid` in place of the existing value. See Table 10.

Table 10 Default ID Attributes for Supported User Directories

Directory Server	Default Attribute
Sun One LDAP	`nsuniqueid`
IBM Directory Server LDAP	`Ibm-entryUuid`
Novel eDirectory LDAP	`GUID`
Oracle Internet Directory	`orclguid`
Active Directory	`ObjectGUID`

6 Click **Finish**.

7 In the View pane of Shared Services Console, expand **Application Groups** and then **Foundation**.

8 Select **Deployment Metadata**.

9 On **Artifact List**, expand **Shared Services Registry**, then **Foundation Services**, and then **Shared Services**.

10 Right-click **Properties** and then select **Export for Edit**.

11 On **File Download**, select **Save**, and then follow on screen prompt to save the file to a directory on your server. Name the file `Component.properties`.

12 **Using a text editor, open** `Component.properties`.

13 **Locate** `CSS.MIGRATION.STATE` **property and change its value to** `FORCE_MIGRATION`.

> **Caution!** If `CSS.MIGRATION.STATE` is set to `FORCE_MIGRATION` and the custom ID Attribute value (for example, `DN`) is not reset to the default value for your LDAP-enabled user directory (for example, `orclguid` for Oracle Internet Directory), you will lose group membership and provisioning information when you restart Shared Services. See step 1 - step 5.

14 **Save and close** `Component.properties`.

15 **On Artifact List, right-click Properties and then select Import after Edit.**

If **Artifact List** is not open, repeat step 7 through step 9.

16 **on Load Artifact, select** `Component.properties` **and then select Finish.**

17 **Restart Shared Services and other EPM System products and processes.**

Handling SSO Compatibility in Interoperability Mode with Earlier Releases

Because default SSO compatibility is set to work with current EPM System release components only, you must modify security settings if you have a deployment environment comprising release 11.1.2.1 and earlier EPM System release components.

➤ To update security settings to support interoperability:

1 **Launch Shared Services Console. See "Launching Shared Services Console" on page 13.**

2 **Select Administration, and then Configure User Directories.**

3 **Select Security Options.**

4 **In SSO Compatibility, select** `11.1.2.0 and below` **as the value.**

See "Setting Security Options" on page 42 for description of other security options. If you set SSO compatibility to `11.1.2.0 and below`, additional buttons are enabled on the Encryption Options screen. See "Regenerating Encryption Keys" on page 44.

5 **Restart Shared Services and other EPM System products.**

Using Special Characters

Active Directory and other LDAP-based user directories allow special characters in entities such as DNs, user names, roles, and group names. Special handling may be required for Shared Services to understand such characters.

Generally, you must use escape characters while specifying special characters in user directory settings; for example, Base DN and user and group URLs. Table 11 lists the special characters

that can be used in user names, group names, user URLs, group URLs, and in the value of OU in user DN.

Table 11 Supported special characters

Character[1]	Name or Meaning	Character	Name or Meaning
(	open parenthesis	$	dollar
)	close parenthesis	+	plus
“	quotation mark	&	ampersand
'	single quotation mark	\	backslash
,	comma	^	caret
=	equal to	;	semicolon
<	less than	#	pound
>	greater than	@	at

[1]Do not use / (slash) in organization unit names that come within the Base DN

- Special characters are not permitted in the value of the Login User attribute.
- The asterisk (*) is not supported in user names, group names, user and group URLs, or in the name of the OU in User DN.
- Attribute values containing a combination of special characters are not supported.
- The ampersand (&) can be used without an escape character. For Active Directory settings, & must be specified as `&`.
- User and group names cannot contain both a backslash (\) and slash (/). For example, names such as `test/\user` and `new\test/user` are not supported.

Table 12 Characters that need not be escaped

Character	Name or Meaning	Character	Name or Meaning
(	open parenthesis	'	single quote
)	close parenthesis	^	caret
$	dollar	@	at
&[1]	Ampersand		

[1]Must be stated as `&`.

These characters must be escaped if you use them in user directory settings (user names, group names, user URLs, group URLs and User DN).

Table 13 Escape for Special Characters in User Directory Configuration Settings

Special Character	Escape	Sample Setting	Escaped Example
comma (,)	backslash (\)	`ou=test,ou`	`ou=test\,ou`
plus sign (+)	backslash (\)	`ou=test+ou`	`ou=test\+ou`
equal to (=)	backslash (\)	`ou=test=ou`	`ou=test\=ou`
pound (#)	backslash (\)	`ou=test#ou`	`ou=test\#ou`
semicolon (;)	backslash (\)	`ou=test;ou`	`ou=test\;ou`
less than (<)	\<	`ou=test<ou`	`ou=test\<ou`
greater than (>)	\>	`ou=test>ou`	`ou=test\>ou`
" (quotation mark)[1]	\\ (two backslashes)	`ou=test"ou`	`ou=test\\"ou`
\ (backslash)[2]	\\\ (three backslashes)	`ou=test\ou`	`ou=test\\\\ou`

[1]In User DNs, quotation mark (") must be escaped with one backslash. For example, `ou=test"ou` must be specified as `ou=test\"ou` in User DN.

[2]In User DNs, back slash (\) must be escaped with one backslash. For example, `ou=test\ou` must be specified as `ou=test\\ou` in User DN.

Caution! If the user URL is unspecified, users created within the RDN root must not contain / (slash) or \ (backslash). Similarly, these characters should not be used in the names of groups created within the RDN root if a group URL is not specified. For example, group names such as `OU=child\ou,OU=parent/ou` or `OU=child/ou,OU=parent\ou` are not supported. This issue does not apply if you are using a unique attribute as the `ID Attribute` in the user directory configuration.

4 Working with Application Groups and Applications

In This Chapter

Overview

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

This chapter contains information on creating and managing application groups and applications.

Working with Application Groups

Generally, when you deploy an application, EPM System places the application 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's Hyperion Reporting and Analysis applications. While an application can belong to only one application group, an application group can contain multiple applications.

EPM System products place their applications into their own application groups. If an EPM System product does not create its own application group, you 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. You can provision users and groups with roles from applications listed in the Default Application Group node and then move the application to an application group without losing provisioning information. You can create custom application groups, if needed.

Topics detailing application group management tasks:

- "Creating Application Groups" on page 52

- "Modifying Application Group Properties" on page 52
- "Deleting Application Groups" on page 53

Note: You must be a Shared Services Administrator or Project Manager to create and manage application groups. Shared Services Administrators can work with all registered applications; a Project Manager can work only with the applications for which that person is the provisioning manager.

Creating Application Groups

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

➤ To create an application group:

1 **Launch the Shared Services Console. See "Launching Shared Services Console" on page 13.**

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

3 **In Name, enter a unique application group name, and, 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 **Add**.

d. To remove an assigned application, from **Assigned Applications**, select the application to remove, and then click **Remove**. To remove all applications that you assigned in the current session, click **Reset**.

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: You can also add applications to application groups by moving them from another application group. See "Moving Applications" on page 54.

➤ To modify an application group:

1 Launch the Shared Services Console. See "Launching Shared Services Console" on page 13.

2 From the View pane, select **Application Groups**.

3 On the **Browse** tab, right-click the application group and select **Open**.

4 Modify the application group properties as needed. See step 4 on page 52 for information on assigning or removing applications.

5 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 Launch Shared Services Console. See "Launching Shared Services Console" on page 13.

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

3 Click **Yes**.

Managing Applications

Shared Services tracks registered EPM System applications. Generally, EPM System products are registered with Shared Services when you deploy them using the EPM System Configurator. EPM System application instances are registered with Shared Services when you deploy them.

Registration of some applications creates application groups and assigns applications to them. If registration does not create an application group, the application is listed under Default Application Group. You can provision these applications. When you move applications from Default Application Group to an application group, Shared Services retains the provisioning information.

Topics addressing application management tasks:

Provisioning 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 Shared Services administrator uses the Shared Services Console to provision users and groups to EPM System applications.

Some EPM System applications can 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, you create Oracle Essbase filters and calculation scripts using Oracle Essbase Administration Services Console or MaxL. Typically, a Shared Services administrator or the EPM System application administrator uses Shared Services Console to initiate the artifact provision process.

Shared Services Administrators can provision groups and users with roles from all applications. Application Administrators can provision groups with roles from the application for which they are administrators.

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

➤ To assign application-specific access permissions:

1 Launch Shared Services Console. See "Launching Shared Services Console" on page 13.

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 Permissions**. This option is available only for applications for which access permissions can be set.

The Assign Preferences tab for the selected application is displayed.

Note: If the application is not running, an error message is displayed when you select the application. Restart the product server 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.

Moving Applications

You 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 applications cannot be moved from the Foundation application group.

➤ To move an application:

1 Launch Shared Services Console. See "Launching Shared Services Console" on page 13.

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

You can copy provisioning information across EPM System application instances; for example, from onePlanning application to another. When you 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 Launch Shared Services Console. See "Launching Shared Services Console" on page 13.

2 In 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 select **Copy Provisioning**.

If another application of the same type is registered with Shared Services, the Copy Provisioning tab opens. This tab lists the target application to which you can copy provisioning information.

4 Select the destination application.

5 Click **Save**.

Deleting Multiple Applications

When Shared Services administrators delete applications, the provisioning information also is deleted.

➤ To delete applications:

1 Launch Shared Services Console. See "Launching Shared Services Console" on page 13.

2 In the View pane, right-click **Application Groups** and select **Delete Applications**.

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 53.

4 Click **Delete**.

5 Click **OK**.

Deleting an Application

Shared Services 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. Launch Shared Services Console. See "Launching Shared Services Console" on page 13.
2. In View pane, expand the node of the application group that contains the application that you want to delete.
3. Right-click the application and select **Delete**.
4. Click **OK**.

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 Hyperion Enterprise Performance Management System Lifecycle Management Guide*.

5 Delegated User Management

In This Chapter

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—EPM System Administrator, Shared Services Administrators, and Delegated Administrators—exist in delegated administration mode.

Default EPM System Administrator

The default *admin* user account is the most powerful EPM System account. The EPM System Configurator automatically provisions this user with the administrator role of each EPM System product.

Shared Services Administrators

Shared Services Administrators are provisioned with the Shared Services Administrator role. Generally, the EPM System Administrator creates Shared Services Administrators. You can pair the Shared Services Administrator role with the Administrator role of an EPM System

application to create administrators who can perform all provisioning activities for an application. For example, to administer Planning application `PlanApp1`, you may provision a user with the Shared Services Administrator role and the Administrator role of the Planning application `PlanApp1`.

Delegated Administrators

Delegated Administrators have limited administrator-level access to Shared Services and EPM System products. 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 products is controlled by the access rights that a Shared Services 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. Launch the Shared Services Console. See "Launching Shared Services Console" on page 13.
2. From **Administration**, select **Configure User Directories**.
3. Select **Security Options**, and then **Show Advanced Options**.
4. Select **Enable Delegated User Management Mode**.
5. Click **Save**.
6. Click **OK**.
7. Restart Shared Services and other EPM System products.

Creating Delegated Administrators

Planning Steps

User Accounts for Delegated Administrators

Shared Services Administrators create 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 products 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 60.
- Shared Services and EPM System product roles that each Delegated Administrator should be granted

Provisioning Delegated Administrators

Shared Services Administrators provision Delegated Administrators by granting them roles based on the delegation plan, which defines the activities they should perform. See "Foundation Services Roles" on page 149.

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. A Shared Services 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. Launch Shared Services Console. See "Launching Shared Services Console" on page 13.
2. Under **Native Directory** in View pane, right-click **Delegated List**, and then select **New**.
3. In **Name**, enter a unique name for the delegated list.
4. **Optional:** In **Description**, enter a list description.
5. **Optional:** To add groups to the list, click **Next**. These are the groups that the Delegated Administrator assigned to this list can administer.
   a. In **Search for Groups**, enter the name of the group to assign to the list. Leave this field empty to retrieve all groups. Use * as the wildcard for pattern searches. If you are a Delegated Administrator, only groups assigned to you are displayed.
   b. In **Directory**, select the user directory from which groups are to be displayed.
   c. Click **Go**.
   d. From **Available Groups**, select groups.
   e. Click **Add**.

      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 click **Remove** to unassign a group. Click **Reset** to unassign all groups that you assigned in the current session.
6. **Optional:** Click **Next** to add users that the Delegated Administrator assigned to this list can administer.

a. In **Search for Users**, enter the name of the user to assign to the list. Leave this field blank to retrieve all users. Use * as the wildcard for pattern searches. If you are a Delegated Administrator, only users assigned to you are displayed.

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

c. Click **Go**.

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

e. Click **Add**.

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

f. **Optional:** From **Assigned Users**, select a user and click **Remove** to unassign a user. Click **Reset** to unassign all users that you assigned in the current session.

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

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

a. In **Search for Users**, enter the user to assign as the Delegated Administrator of the list. Leave this field blank to retrieve all users. Use * as the wildcard for pattern searches. If you are a Delegated Administrator, only users assigned to you are displayed.

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

c. Click **Go**.

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

e. Click **Add**.

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

f. **Optional:** From **Assigned Users** list, select the user and click **Remove** to unassign a user. Click **Reset** to unassign all users that you assigned in the current session.

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

8 Click **Save**.

9 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. Users with the Shared Services Administrator role can modify all delegated lists.

➤ To modify delegated lists:

1 Launch Shared Services Console. See "Launching Shared Services Console" on page 13.

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 15.

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

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

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

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

a. In **Search for Groups**, enter the name of the group to assign to the list. Leave this field empty to retrieve all groups. Use * as the wildcard for pattern searches. If you are a Delegated Administrator, only groups assigned to you are displayed.

b. In **Directory**, select the user directory from which groups are to be displayed.

c. Click **Go**.

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

e. Click **Add**.

f. **Optional:** From **Assigned Groups**, select the group and click **Remove** to unassign a group. Click **Reset** to unassign all groups that you assigned in the current session.

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

a. In **Search for Users**, enter the name of the user to assign to the list. Leave this field blank to retrieve all users. Use * as the wildcard for pattern searches. If you are a Delegated Administrator, only users assigned to you are displayed.

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

c. Click **Go**.

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

e. Click **Add**.

f. **Optional:** From **Assigned Users**, select the user and click **Remove** to unassign a user. Click **Reset** to unassign all users that you assigned in the current session.

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

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

a. In **Search for Users**, enter the name of the user to assign as the Delegated Administrator of the list. Leave this field blank to retrieve all users. Use * as the wildcard for pattern searches. If you are a Delegated Administrator, the users assigned to you are displayed.

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

c. Click **Go**.

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

e. Click **Add**.

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

f. **Optional:** From **Assigned Users**, select the user and click **Remove** to unassign a user. Click **Reset** to unassign all users that you assigned in the current session.

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

9 Click **Save**.

10 Click **OK**.

Deleting Delegated Lists

➤ To delete delegated lists:

1 Launch Shared Services Console. See "Launching Shared Services Console" on page 13.

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 15.

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

4 Right-click the delegated list and 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.

Shared Services 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 Launch Shared Services Console. See "Launching Shared Services Console" on page 13.

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

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.

6 Managing Native Directory

In This Chapter

About Native Directory

Shared Services uses a relational database as the Native Directory to store user provisioning data and product registration data.

After the initial logon to an EPM System product, the product directly queries Native Directory for user provisioning information.

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.

Default Users and Groups in Native Directory

Native Directory, by default, contains the `admin` user account. The password of this account is defined in EPM System Configurator during configuration. Using this account, you can 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 any role 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

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

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

Creating Users

➤ To create users:

1 Launch Shared Services Console. See "Launching Shared Services Console" on page 13.

2 In the **Native Directory** node in the View pane, right-click **Users**, and select **New**.

3 In **Create User**, enter the required information.

Table 14 Create User Screen

Label	Description
User Name	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*) User names can contain any number or combination of characters. 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`).
First Name	User's first name (optional)
Last Name	User's last name (optional)
Description	User's description (optional)
Email Address	User's e-mail address (optional). The e-mail server domain extension; for example, .com, .org, and .gov, cannot contain more than four characters.
Password	Passwords are case-sensitive and can contain any combination of characters.
Confirm Password	Re-enter password.

4 **Optional:** To add the user to one or more groups, click **Next**.

a. On the **Group Membership** page, in **Search for Groups**, enter the name of the group to assign to the user (type * to list all available groups).

b. Click **Go**.

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

d. Click **Add**.

e. **Optional:** From **Assigned Groups**, select the group and click **Remove** to unassign a group. Click **Reset** to undo all changes that you made to **Assigned Groups**.

5 Click **Save**.

6 Click **Create Another** to create another user or **OK** to close the **Create User** screen.

Modifying User Accounts

For the default `admin` account, you can modify only e-mail address, password, and group membership. For all other user accounts, you can modify any property.

➤ To modify user accounts:

1 Launch Shared Services Console. See "Launching Shared Services Console" on page 13.

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 15.

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

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

5 On **General**, modify user properties.

See Table 14 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. Select `Group Name` or `Description`.

c. In the available groups search box, enter the name or description of the group to assign to this user (type * to list all available groups), and click **Go**.

d. From **Available Groups**, select groups to assign to the user, and then click **Add**.

From **Assigned Groups**, select the group to remove, and then click **Remove** to remove an assigned group.

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

8 Click **Save**.

9 Click **OK**.

Deactivating User Accounts

You can deactivate user accounts that should not have access to EPM System applications. Account deactivations are, typically, temporary suspensions that the Native Directory 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 Native Directory administrators.
- Role associations of inactive accounts are maintained.
- Inactive user accounts are not displayed on the product-specific access-control screens of items for which access is disabled.
- Inactive user accounts are not deleted from Native Directory.

Note: The admin account cannot be deactivated.

➤ To deactivate user accounts:

1. Launch Shared Services Console. See "Launching Shared Services Console" on page 13.
2. Search for **Native Directory** users to deactivate. See "Searching for Users, Groups, Roles, and Delegated Lists" on page 15.
3. Right-click the user account and select **Deactivate**.
4. Click **OK**.

Activating Inactive User Accounts

Activating inactive 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.

➤ To activate deactivated user accounts:

1. Launch Shared Services Console. See "Launching Shared Services Console" on page 13.
2. Search for **Native Directory** users to reactivate. See "Searching for Users, Groups, Roles, and Delegated Lists" on page 15.
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 `admin` account cannot be deleted.

➤ To delete user accounts:

1. Launch Shared Services Console. See "Launching Shared Services Console" on page 13.
2. Search for **Native Directory** users to delete. See "Searching for Users, Groups, Roles, and Delegated Lists" on page 15.
3. Right-click the user account and select **Delete**.
4. Click **Yes**.
5. Click **OK**.

Changing Native Directory User Password

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

You change your password by modifying your Native Directory user account.

➤ To change a Native Directory password:

1. Launch Shared Services Console. See "Launching Shared Services Console" on page 13.
2. In the **Native Directory** node in the View pane, select **Users**.
3. Search for your user account. See "Searching for Users, Groups, Roles, and Delegated Lists" on page 15.
4. Right-click your user account, and select **Properties**.

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

5. Perform a step:
   - If you are changing the password of `admin`:
     a. In **Current Password**, enter your password.
     b. In **New Password** and **Confirm Password**, enter the new password.
   - If you are changing the password of a user other than `admin`, in **Password** and **Confirm Password**, enter the new password.
6. Click **Save**.
7. Click **OK**.

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 one or more 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.

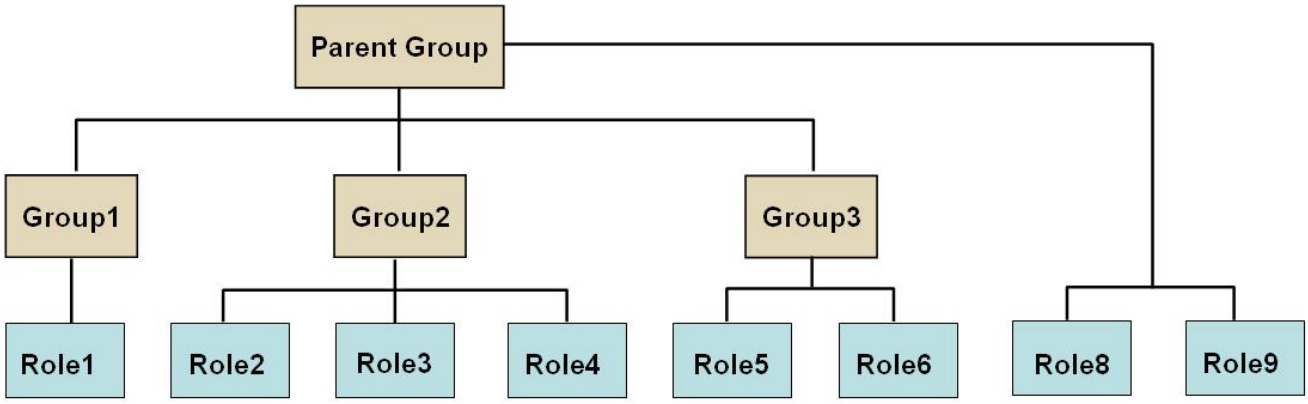
Tasks performed by Shared Services administrators or directory managers:

- "Creating Groups" on page 71
- "Modifying Groups" on page 72
- "Deleting Groups" on page 74
- "Provisioning Users and Groups" on page 81
- "Deprovisioning Users and Groups" on page 82
- "Generating Provisioning Reports" on page 85

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 on 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 Launch Shared Services Console. See "Launching Shared Services Console" on page 13.

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

3 Right-click **Groups** and select **New**.

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

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

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

d. Click **Go**.

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

e. From **Available Groups**, select the member groups for the new group.

f. Click **Add**.

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

g. **Optional:** To retrieve and assign groups from other user directories, repeat step 7.a-step 7.f.

Shared Services enables you to search the assigned groups to identify the groups that you want to remove. Use the fields above the **Assigned Groups** list to define the search criteria for searching within assigned groups list. For instructions on searching within assigned groups, see step 7.a-step 7.d.

From **Assigned Groups**, select the group to remove and click **Remove** to remove an assigned group. Click **Reset** to remove all the groups that you assigned in the current session.

8 Perform an action:

- Click **Save** to create the group without adding users, and go to step 11.
- Click **Next** to assign users to the group.

9 To assign users to the group:

a. In **Directory**, select the user directory from which to retrieve users. To search for users in all configured user directories, select **All**.

b. Select the user property (**User Name**, **First Name**, **Last Name**, **Email Address** or **Description**) to search.

c. Enter the search criterion. Use * (asterisk) as the wildcard to retrieve all users.

d. Click **Go**.

User accounts matching the search criteria are listed under Available Users.

e. From **Available Users**, select the users to add to the group.

f. Click **Add**.

The selected user accounts are listed under Assigned Users.

g. **Optional:** To retrieve and assign users from other user directories, repeat step 9.a-step 9.f.

Shared Services enables you to search the assigned users to identify the users that you want to remove. Use the fields above the **Assigned Users** list to define the search criteria for searching within assigned users list. For instructions on searching within the assigned users list, see step 9.a-step 9.d.

From **Assigned Users**, select the user to remove and click **Remove** to remove an assigned user. Click **Reset** to remove all users that you assigned in the current session.

10 Click **Save**.

11 In the confirmation screen, select **Create Another** (to create another group) or **OK** (to return to the Browse tab).

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 Launch Shared Services Console. See "Launching Shared Services Console" on page 13.

2 Search for a group. See "Searching for Users, Groups, Roles, and Delegated Lists" on page 15.

3 Right-click a group, and 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 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 **Go**.
- From **Available Groups**, select groups and click **Add**.

  Selected groups are listed in the **Assigned Groups** list. From **Assigned Groups**, choose the group and click **Remove** 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 **Remove**.
- **Optional:** Click **Reset** to undo the changes you made to **Assigned Groups**.

6 Select the **User Members** tab and 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 **Go**.
- From **Available Users**, select users to assign to the group.
- Click **Add**.

  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 **Remove**.
- **Optional:** Click **Reset** to undo the changes you made to **Assigned Users**.

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

8 Click **Save**.

9 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 Launch Shared Services Console. See "Launching Shared Services Console" on page 13.

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 15.

4 Right-click the group, and 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. Shared Services Administrators can perform these tasks:

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 lower interval; for example, 30 minutes, may cause performance degradation. See "Configuring OID, Active Directory, and Other LDAP-based User Directories" on page 24.

Creating Aggregated Roles

To facilitate administration and provisioning, Shared Services Administrators 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. Shared Services Administrators can create aggregated roles for all EPM System applications.

For information on aggregated roles, see "Aggregated Roles" on page 20.

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

➤ To create aggregated roles:

1. Launch Shared Services Console. See "Launching Shared Services Console" on page 13.
2. In the **View pane**, expand **Native Directory**.
3. Right-click **Roles**, and then select **New**.
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). See "Using Special Characters" on page 47 for more information.
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 **Go** to retrieve all roles from the selected application.
   - Enter the role name in **Search for Roles**, and then click **Go** 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 **Add**.

    The selected roles are listed in **Assigned Roles**.

    From **Assigned Roles**, select the role and click **Remove** to remove a selected role. Click **Reset** to undo all of your actions on this tab.

11 Click **Save**.

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 Launch Shared Services Console. See "Launching Shared Services Console" on page 13.

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 15.

5 Right-click the role and select **Properties**.

6 On the **General** tab, edit the name and description to modify general properties of the role.

7 To modify role member assignments, open the **Role Members** tab and perform actions from step 7.a, step 7.b, or both:

a. To add role members:

- Retrieve the roles to add.
  - Click **Go** to retrieve all roles.
  - Enter the role name in **Search for Roles** and click **Go** 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 one or more, and then click **Remove** to remove the selected role. Click **Reset** to undo your actions on this tab.

b. To remove role assignments:

- From **Assigned Roles**, select roles to remove.
- Click **Remove**.

8 Click **Save**.

9 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 Launch Shared Services Console. See "Launching Shared Services Console" on page 13.

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 15.

5 Right-click a role and 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.

7 Managing Provisioning

In This Chapter

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 149 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.
  - Configure the external user directories that contain accounts for EPM System users and groups. See Chapter 3, "Configuring User Directories."

- 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 5, "Delegated User Management."

Overview of Provisioning Steps

All Shared Services provisioning activities must be performed by a Shared Services Administrator or Provisioning Manager. A built-in `admin` account is available to initiate provisioning.

Provisioning users and groups should follow a provisioning plan tailored for your organization. Typically, you should create Shared Services 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 149 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 administrative 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 Shared Services Administrator must assign administrative roles from Shared Services.

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

Provisioning EPM System Users

The Shared Services Console is the administrative interface for Shared Services. All users defined in the user directories configured in Shared Services can log in to Shared Services Console. End users need not be provisioned with Shared Services roles.

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

1. From Shared Services Console, identify and select the users (or the groups to which they belong) who need access to the EPM System product. See "Searching for Users, Groups, Roles, and Delegated Lists" on page 15.
2. Assign product roles that allow users to access EPM System product. For example, all Essbase users should have the Server Access role. See "Provisioning Users and Groups" on page 81. Not all EPM System products enforce product-level roles.

   EPM System product 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 product administration screen 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 Users and Groups

Provisioning is the process of granting EPM System roles to users and groups. Provisioning is performed by a Provisioning Managers or Shared Services Administrators by assigning EPM System application roles to a user or group. See "Provisioning (Role-based Authorization)" on page 18.

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. Launch Shared Services Console. See "Launching Shared Services Console" on page 13.
2. Find and select users or groups to provision.

   See "Searching for Users, Groups, Roles, and Delegated Lists" on page 15.
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 click **Add**.
6. Click **Save**.
7. Click **OK**.

Deprovisioning Users and Groups

Deprovisioning removes all the roles the user or group is assigned from an application. Shared Services 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 Financial Management. If this group is deprovisioned by a Planning Provisioning Manager, only the roles from Planning are removed.

➤ To deprovision users or groups:

1. Launch Shared Services Console. See "Launching Shared Services Console" on page 13.
2. Find and select users or groups to deprovision.

   See "Searching for Users, Groups, Roles, and Delegated Lists" on page 15.
3. Select **Administration** and then **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. You must enable auditing to allow Shared Services Administrators to view audit reports to track the changes that have occurred. See "Generating Audit Reports" on page 86.

Only Shared Services 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.

- "Purging Audit Data" on page 84
- "Selecting Objects for Application and Application Group-Level Audits" on page 84

➤ To change the auditing configuration:

1. Using Shared Services Administrator credentials, log in to the Shared Services Console. See "Launching Shared Services Console" on page 13.
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 to retain the audit data and click **Purge**.
   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.

Purging Audit Data

Shared Services does not automatically remove audit data from the Shared Services database. Retaining large amounts of data can degrade performance while generating an audit report.

Caution! Shared Services 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:

1. Using Shared Services Administrator credentials, log in to Shared Services Console. See "Launching Shared Services Console" on page 13.
2. Select **Administration** and then **Configure Auditing**.
3. In **Purge Data Older than**, set the number of days for retaining the audit data.
4. Click **Purge**.
5. Click **OK**.

Selecting Objects for Application and Application Group-Level Audits

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

➤ To select objects for auditing:

1. Using Shared Services Administrator credentials, log in to Shared Services Console. See "Launching Shared Services Console" on page 13.
2. In the View pane, right-click one of the following and 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 83.
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**.

Generating Reports

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

- "Generating Provisioning Reports" on page 85
- "Generating Audit Reports" on page 86
- "Generating Migration Status Report" on page 87

Generating Provisioning Reports

Shared Services 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 administrators 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. Log in to the Shared Services Console. See "Launching Shared Services Console" on page 13.
2. Select a user or role. See "Searching for Users, Groups, Roles, and Delegated Lists" on page 15.
3. Select **Administration** and then **View Report**.
4. Enter report generation parameters.

Table 15 View Report Screen

Label	Description
Find All	Select the object type (user, group, or role) for which the report is to be generated.
For Users or **For Roles**	The label of this changes depending on what is selected in **Find All**.
Filter By	The criterion to use to filter the report data.
Show Effective Roles	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.
Group By	Select how to group the data in the report. Available grouping criteria depend on the selection in **Find All**.
Results Per Page	Number of report results to display in a page. Default is 500.

Label	Description
In Application	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.

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.

Shared Services Administrators can generate and view audit reports to track historical changes to the security data.

Note: Auditing must be configured before you can generate audit reports. See "Auditing Security Activities and Lifecycle Management Artifacts" on page 83.

➤ To generate audit reports:

1 Select **Administration**, and then **Audit Reports**.

2 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.

3 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**.

4 **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`.

5 **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 **Select Administration, and then Migration Status Report.**

This report is automatically generated to show all migrations performed in the last 30 days.

2 **To regenerate the report, click Refresh.**

3 **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 Hyperion Enterprise Performance Management System Lifecycle Management Guide*.

8 Provisioning Essbase

In This Chapter

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
- 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

Foundation Services Web Server

Foundation Services 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 Hyperion 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 EPM 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 automatically added to the server. 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 Web application is running.

  See the *Oracle Hyperion 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 products such as Shared Services, EPM Workspace, and Administration Services during provisioning. See the following topics:

- "Launching Shared Services Console" on page 13
- "Accessing EPM Workspace" on page 169
- "Accessing Administration Services Console" on page 170

Provisioning Process

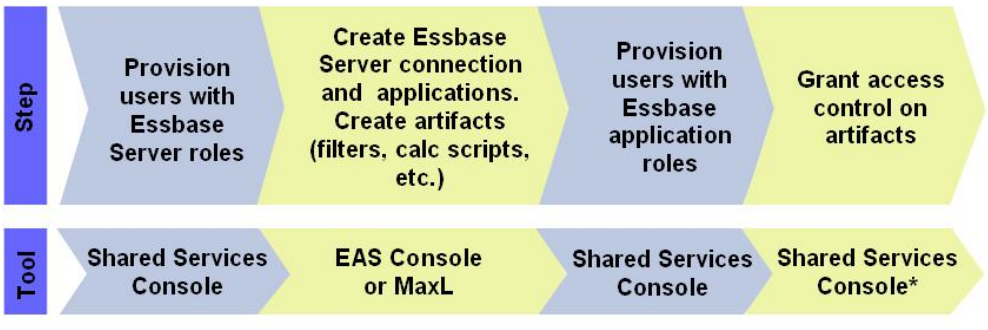
You can use three interfaces to create Essbase applications: Administration Services Console, Essbase Studio, and the Application Library. Access Application Library through EPM Workspace.

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

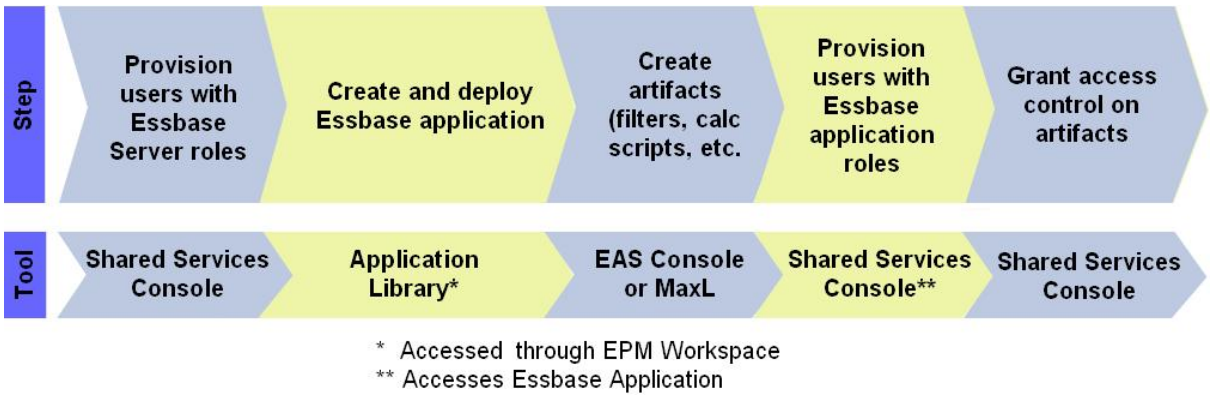
The following illustration shows the steps involved in provisioning a classic Essbase application.



* 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 Shared Services 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, the Shared Services *admin* user 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 *admin*.** See **"Launching Shared Services Console" on page 13**.

2 **From a configured user directory, find the user or group to provision.** See **"Searching for Users, Groups, Roles, and Delegated Lists" on page 15**.

3 **Provision the user or group with an Essbase Server role.**

   a. Right-click the user or group and 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 Add (right arrow). Table 16 describes Essbase Server roles.

Table 16 Essbase Server Roles

Role	Description
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 **Save**.

g. Click **OK**.

Creating Essbase Server Connection

Before you can perform tasks from Administration Services Console, you must connect to an Essbase Server installation. Initially, `admin` 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.

By default, seven Essbase sample applications—`ASOsamp`, `Demo`, `DMDemo`, `Sampeast`, `Sample`, `Sample_U`, and `Samppart`—are registered with Shared Services. These applications are listed under the **Application** node.

Sample Essbase applications are owned by `admin`. They can be used to practice Essbase application provisioning. Essbase Server Administrators can manage sample applications from the Administration Services Console.

➤ To create an Essbase Server connection:

1 **Log in to Administration Services Console as `admin`. See "Accessing Administration Services Console" on page 170.**

2 **Right-click Essbase Servers and 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 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. See the *Oracle Essbase*

Administration Services Online Help or *Oracle Essbase Technical Reference* for detailed information.

➤ To create Essbase applications and artifacts:

1 **Log in to Administration Services Console as** `admin`.

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 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:

1 Access EPM Workspace. See "Accessing EPM Workspace" on page 169.

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 `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

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 `admin` or as a user provisioned with the Essbase Administrator role. See "Accessing Administration Services Console" on page 170.
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 *admin* 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 Shared Services Administrator.

See "Accessing EPM System Products" on page 91.

Note: Users provisioned with Provisioning Manager role from 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 15.

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 Add (right arrow). Table 17 describes Essbase application roles and their embedded permissions.

Table 17 Essbase Application Roles

Role	Description
Application Manager	Creates, deletes, and modifies databases and application settings within the assigned application. Includes Database Manager permissions for databases within the application. **Note:** 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.
Database Manager	Manages the databases, database artifacts, and locks within the assigned application
Calc	Calculates, updates, and reads data values based on assigned scope, using any assigned calculations and filter

Role	Description
Write	Updates and reads data values based on assigned scope, using any assigned filter
Read	Reads data values
Filter	Accesses specific data and metadata according to filter restrictions
Start/Stop Application	Starts and stops applications or databases
Provisioning Manager	Provisions Essbase users with roles from this application

8 Click **Save**.

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 Shared Services Administrator. See "Accessing EPM System Products" on page 91.

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 **Save**.

9 Provisioning Planning

In This Chapter

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
- 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. See Chapter 3, "Configuring User Directories."

Foundation Services Web Server

Foundation Services Web server must be running.

Essbase Server

- Essbase is deployed in Shared Services mode by default. See the *Oracle Hyperion 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 Hyperion 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 Hyperion 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 Web application is running.

  See *Oracle Hyperion 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 Hyperion 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 13
- "Accessing EPM Workspace" on page 169
- "Accessing Administration Services Console" on page 170

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.

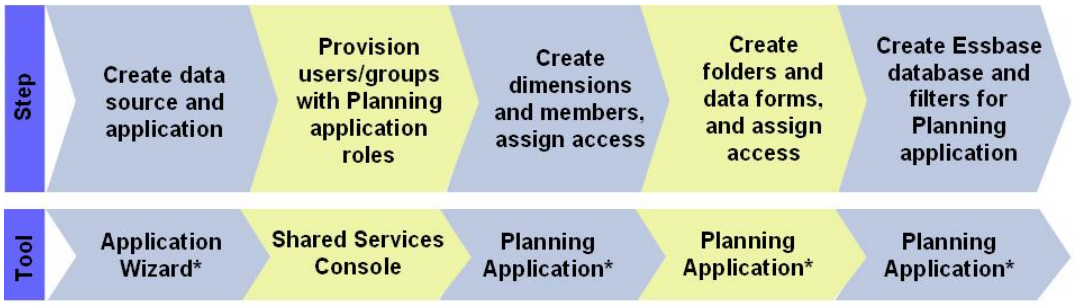
Process Overview

Subtopics

- Classic Planning
- Performance Management Architect Planning

Classic Planning

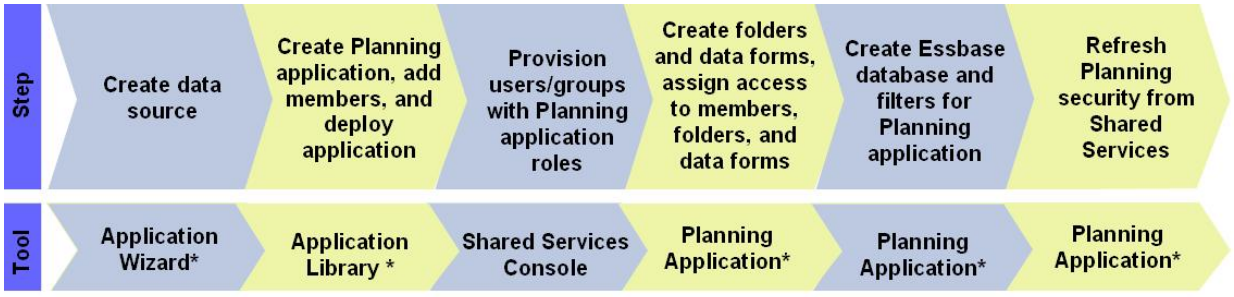
The steps involved in provisioning Classic Planning applications are depicted in the following illustration.



* Accessed through EPM Workspace

Performance Management Architect Planning

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



* Accessed through EPM Workspace

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:

1. From EPM Workspace, select **Navigate**, then **Administer**, then **Classic Application Administration**, and then **Planning Administration**.
2. Select **Manage Data Source**.
3. Select **Create Data Source**.
4. In **Data Source Name**, enter a name.
5. From **Select Database Platform**, select the database type for the Planning application database.

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

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

8 Select **Finish** 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 103
- "Accessing Planning Applications" on page 104
- "Creating Dimensions and Members in Classic Planning Applications" on page 104

Creating Classic Planning Application

➤ To create an application:

1 From EPM Workspace, select **Navigate**, then **Administer**, then **Classic Application Administration**, and then **Planning Administration**.

2 Select **Create Application**.

3 In **Data Source**, select a data source.

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

5 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 if needed. See "Creating Application Groups" on page 52.

6 In **Instance**, select a Planning instance to support this application. The default instance is created when you deploy Planning using the EPM System Configurator.

To add a Planning instance to create a Planning cluster, use the Oracle's Hyperion Enterprise Performance Management System Configurator. See the *Oracle Hyperion Enterprise Performance Management System Installation and Configuration Guide*.

7 **Optional:** Select **Sample Application** to use sample Planning application settings.

If you choose this option, you cannot select information on **Calendar**, **Currencies**, and **Plan Types** tabs.

8 **Optional:** Enter or select information on the **Calendar**, **Currencies**, or on **Plan Types** tabs. Click **Next** after entering information on a tab. Consult online help for assistance.

9 On the **Finish** tab, review the information that you selected. Click **Finish** 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 5.

Accessing Planning Applications

➤ To open your Planning application:

1 From EPM Workspace, select **File**, then **Open**, then **Applications**, and then **Planning**.

2 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 104.

2 Select **Administration**, then **Manage**, and then **Dimensions**.

3 **Optional:** Add a custom dimension.

a. From **Dimensions**, select **Add Dimension**.

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 115.

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 115 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 102.

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:

1 **Access EPM Workspace. See "Accessing EPM Workspace" on page 169.**

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, Fusion Edition, data cube in Essbase, select **Workforce** and enter a name.

c. To create an Oracle Hyperion Capital Asset Planning, Fusion Edition, 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 From the Dimension Selection window, choose the dimensions for the application. You must create the required default dimensions—Entity, Version, Scenario, Account, Year, Period, and Alias—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 the Application Settings tab, expand the node representing your application.

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

c. 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 102 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 instance (deployment) can support multiple Planning applications. You must provision Planning users separately to each application.

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

➤ To provision users or groups with Planning application roles:

1 **Access Shared Services Console as `admin` or as a user provisioned with the Provisioning Manager role of the Planning application that you want to provision. See:**

- "Launching Shared Services Console" on page 13
- "Launching Shared Services Console from EPM Workspace" on page 170

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 15.

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 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 18 for a list of Planning application roles and the tasks to which they provide access.

Table 18 Planning Application Roles

Role	Description
Power Roles	
Administrator	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.
Provisioning Manager	Provisions users to the Planning application
Mass Allocation	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.
Analytic Services Write Access	For planners and interactive users: Grants users access to Planning data in Essbase equivalent to their Planning access permissions. Enables users having write access to change Planning data directly in Essbase using another product such as Oracle Hyperion Financial Reporting, Fusion Edition or a third-party tool.

Role	Description
Approvals Administrator Approvals Administrator role comprises these roles: ● Approvals Ownership Assigner ● Approvals Process Designer ● Approvals Supervisor	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 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.
Planner Roles	
Planner	Enters and submits plans for approval and runs business rules 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 Hyperion Smart View for Office, Fusion Edition.
Interactive Roles	
Interactive User	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.

Role	Description
View Roles	
View User	Views and analyzes data through Planning data forms and any data access tools for which they are licensed (for example, Financial Reporting, Oracle's 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.

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.

To populate users and groups in the Planning database, administrators can perform a procedure:

- Refresh security filters. To refresh security filters, in Planning, select **Administration**, then **Application**, then **Create Database** or **Refresh Database**, and then select **Security Filters**.

  See the *Oracle Hyperion Planning, Fusion Edition Administrator's Guide*.

- Run the ProvisionUsers utility. See the *Oracle Hyperion Planning, Fusion Edition Administrator's Guide*.

Additionally, users and groups are added to the database when Planning administrators select **Add Access** in Planning.

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:

1 **Access EPM Workspace. See "Accessing EPM Workspace" on page 169.**

2 **Open the Planning application. See "Accessing Planning Applications" on page 104.**

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 Select **Expand** to display dimension members and their children.

6 Select a dimension member.

7 Select **Assign Access**.

8 In Assign Access window, select **Add Access**.

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

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:

1 Access EPM Workspace. See "Accessing EPM Workspace" on page 169.

2 Open a Planning application. See "Accessing Planning Applications" on page 104.

3 Select **Administration**, then **Manage**, and then **Data Forms and Ad Hoc Grids**.

4 Click **Create** above the Data Form Folders List.

5 Enter a folder name.

Creating Data Forms

You can create simple or composite data forms. Composite data forms display several 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 169.

2 Open a Planning application. See "Accessing Planning Applications" on page 104.

3 Select **Administration**, then **Manage**, and then **Data Forms and Ad Hoc Grids**.

4 To create a data form, click a button above the Data Form List:

- Click **Create** to create a simple data form.
- Click **Create Composite** to create a composite data form.

5 Define options. Consult online help for assistance.

- Data form properties
- Row and column layout
- Page and Point of View layout
- Precision, display, printing, and Smart View
- Display options
- Business rules

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 169.

2 Open a Planning application. See "Accessing Planning Applications" on page 104.

3 Select **Administration**, then **Manage**, and then **Data Forms and Ad Hoc Grids**.

4 Select a folder.

5 Above the Data Forms Folders list, click **Assign Access**.

6 Select **Add Access**.

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 are listed on the Add Access screen.

8 Select the type of access (**Read** or **Write**) to grant.

9 Select **Add**.

10 In the Add Access window, select **Close**.

11 In the Assign Access window, select **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 104.

2 Select **Administration**, then **Manage**, and then **Data Forms and Ad Hoc Grids**.

3 Select data forms.

4 Above the Data Forms list, click **Assign Access**.

5 Select **Add Access**.

6 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 are listed on the Add Access screen.

7 Select the type of access (**Read** or **Write**) to grant.

8 Select **Add**. Consult online help for assistance.

9 In the Add Access window, select **Close**.

10 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

➤ To create task list folders:

1 Open a Planning application. See "Accessing Planning Applications" on page 104.

2 Select **Administration**, then **Manage**, and then **Task Lists**.

3 Above the Task List Folders list, click **Create**.

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.

➤ To create task lists:

1. Open a Planning application. See "Accessing Planning Applications" on page 104.
2. Select **Administration**, then **Manage**, and then **Task Lists**.
3. From **Task List Folders**, select a folder in which to store the task list.
4. Above **Task List**, click **Create**.
5. Enter a task list name, and click **OK**.

Creating Tasks

➤ To create a task:

1. Open a Planning application. See "Accessing Planning Applications" on page 104.
2. Select **Administration**, then **Manage**, and then **Task Lists**.
3. From **Task List Folders**, select the folder containing the task list to which you want to add the task.
4. Select a task list.
5. Click **Edit**.
6. In the Edit Task List window, click **Add Child**.
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 104.
2. Select **Administration**, then **Manage**, and then **Task Lists**.
3. Select a task list folder.
4. Select a task list.
5. Click **Assign Access**.
6. In the Assign Access window, select **Add Access**.
7. Select the users and groups that are to be granted access to the task list.

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

8 Select the type of access (**Assign**, **Manage**, **Manage and Assign**, or **None**) to grant. Consult online help for assistance.

9 Select **Add**.

10 In Add Access window, select **Close**.

11 In Assign Access window, select **Close**.

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, if needed. See "Accessing Planning Applications" on page 104.

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.

3 Select database options. Consult online help for assistance.

4 Click **Create**.

Setting Applications in Production Mode

By default, newly created Planning applications are put in maintenance mode, which allows 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, if needed. See "Accessing Planning Applications" on page 104.

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 169.
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 select **Access Control Report**.
5. Select the following for which the report is to be generated:
   - Users or groups
   - Application objects
6. Set report settings. Consult online help for assistance.
7. Click **Finish**.

10 Provisioning Financial Management

In This Chapter

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 an 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:

- Shared Services
- EPM Workspace

- **Optional:** The external user directories that are the sources for user and group information for Financial Management are configured in Shared Services. See Chapter 3, "Configuring User Directories."

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 Web application is running.

  See *Oracle Hyperion 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 Hyperion 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 13
- "Accessing EPM Workspace" on page 169
- "Accessing Administration Services Console" on page 170

Financial Management Provisioning Process

Subtopics

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.

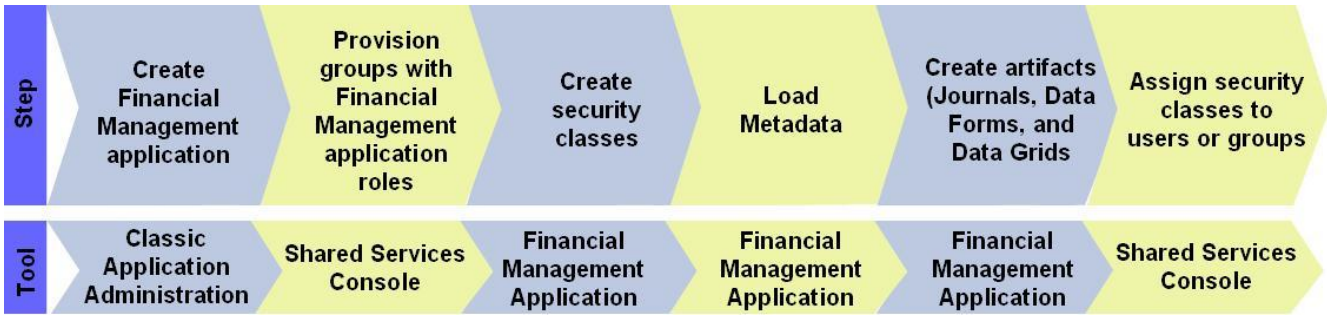
The behavior of Financial Management applications is identical regardless of how you created them.

Process Overview

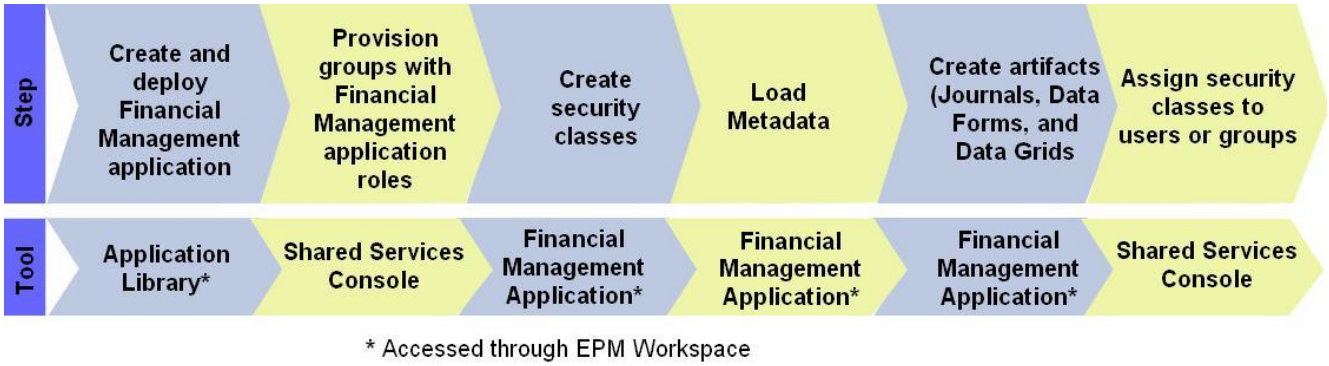
The steps involved in creating and provisioning Financial Management applications using the Classic Application Administration menu option in EPM Workspace are depicted in the following illustration.

Note: This document does not contain a procedure to create applications using Financial Management Desktop. See *Oracle Hyperion Financial Management Administrator's Guide* for a procedure.

The provisioning process is identical regardless of how you created the Financial Management application.



The steps involved in creating Financial Management applications using Performance Management Architect Application Library and provisioning them are depicted in the following illustration.



Creating Classic Applications

Creating classic Financial Management applications involves these steps:

- "Creating Application Profiles" on page 120
- "Creating Classic Financial Management Applications" on page 121

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 must create application profiles using the Financial Management Desktop.

➤ To create application profiles:

1 From the Financial Management Windows desktop, 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:

1 Access EPM Workspace. See "Accessing EPM Workspace" on page 169.

2 From EPM Workspace, select **Navigate**, then **Administer**, then **Classic Application Administration**, then **Consolidation Administration**, and then **Create Application**.

3 From the **Server** list, select the application server cluster on which to run the application.

4 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 (*).

5 In **Application Profile**, select the profile that you want to use for this application. See "Creating Application Profiles" on page 120.

6 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.

7 In **Financial Management Web Server URL for Security Administration**, enter the Financial Management Web server URL.

8 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 6.

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

1 Access EPM Workspace. See "Accessing EPM Workspace" on page 169.

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**.

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 Click **Next**.

8 In the Dimension Selection window, choose the dimensions for the application. You must create the required default dimensions—Entity, Account, Scenario, Year, Period, ICP, View, Value, Custom1, Custom2, Custom3, Custom4, Alias, Currency, Consolidation Method, and Security Class—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**.

b. In the Add New Dimension window, enter a dimension name and an optional description.

c. Click **OK**.

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

10 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**.

11 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.

12 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 *admin* 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 169.

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 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 **Add**.

See Table 19 for a list of Financial Management roles and the tasks to which they provide access.

Table 19 Financial Management Roles

Role	Description
Power Roles	
Application Administrator	Performs all Financial Management tasks. Access to this role overrides any other access setting for the user.
Load System	Loads rules and member lists
Inter-Company Transaction Admin	Opens and closes periods, locks and unlocks entities, and manages reason codes. Users with the role can also perform all intercompany tasks.
Interactive Roles	
Rules Administrator	Performs any Hyperion Calculation Manager tasks for the specific application
Rules Designer	Creates new rules objects and modifies or deletes rules objects
Approve Journals	Approves or rejects journals
Create Journals	Creates, modifies, deletes, submits, and unsubmits journals
Create Unbalanced Journals	Creates unbalanced journals
Default	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.
Journals Administrator	Performs all tasks related to journals
Post Journals	Posts and unposts journals
Manage Templates	Grants access to the journals template task in the Setup Journals module
Generate Recurring	Grants access to the generate recurring task in the Setup Journals module
Review Supervisor	Starts process management units and approves and publishes process management data. Can promote or reject process units, depending on process level.
Reviewer 1 through Reviewer 10	Views and edits a block of data when that data is at the user's designated process management level

Role	Description
Submitter	Submits a block of data for final approval
Lock Data	Locks data in Data Explorer
Unlock Data	Unlocks data in Data Explorer
Consolidate All	Runs consolidate all
Consolidate	Runs consolidate
Consolidate All with Data	Runs consolidate with all data
Run Allocation	Runs allocations
Manage Data Entry Forms	Manages data entry forms on the Web
Save System Report On Server	Saves system reports on server
Load Excel Data	Loads data from Smart View
Inter-Company Transaction User	Creates, edits, deletes, loads, and extracts transactions. Runs matching report by account or ID, runs transaction report, and drills through from modules.
Inter-Company Transaction Match Template	Manages intercompany matching templates
Inter-Company Transaction Auto Match by Account	Automatically matches intercompany transactions by account
Inter-Company Transaction Auto Match by ID	Automatically matches intercompany transactions by ID
Inter-Company Transaction Manual Match with Tolerance	Manually matches intercompany transactions with tolerance check
Inter-Company Transaction Manual Match	Manually matches intercompany transactions
Inter-Company Transaction Unmatch	Unmatches intercompany transactions
Inter-Company Transaction Post/Unpost	Posts and unposts intercompany transactions
Enable write back in Web Grid	Enters and saves data directly to a Web grid
Database Management	Copies and clears data and deletes invalid records
Manage Ownership	Enters and edits ownership information
Task Automation	Sets up automated tasks
Manage Custom Documents	Loads and extracts custom documents to and from the server
Extended Analytics	Creates and executes extended anlaytics queries
Data Form Write Back from Excel	Submits data from Smart View while using a Web Data Entry Form
View Roles	
Advanced User	Uses the Browser View and can access Running Tasks

Role	Description
Rules Viewer	Views rules objects
Read Journals	Reads journals
Receive Email Alerts for Process Control	Receives e-mails
Receive Email Alerts for Intercompany	Receives e-mails
Reserved	Not currently used

g. Click **Save**.

A dialog box indicates successful provisioning.

h. Click **OK**.

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.

You can load security classes for classic Financial Management application from a security (`.sec`) file. See "Loading Application Security" in the *Oracle Hyperion Financial Management Administrator's Guide*.

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. **In Browser View, expand Tasks, and then select Load Tasks.**
3. **Select Load Journals.**
4. **In Journal File, enter the file name to load, or click Browse and find the file to load.**
5. **In Delimiter Character, specify the character that is used to separate information in the file.**
6. **Specify other settings as needed. Consult online help for assistance.**
7. **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 Select **Administration**, then **Manage Documents**, and then **Data Forms**.

3 Click **New**.

4 Enter information on each tab. Consult Online Help for assistance.

- To scan the form for proper syntax, select **Scan**.
- To post changes to the server, select **Update**.
- To reset the form values, select **Reset**.

5 Select **Save**.

6 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 Select **Administration**, then **Manage Documents**, and then **Data Grids**.

3 Click **New Data Grid**.

4 Enter information. Consult online help for assistance.

5 Select **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 169.

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**.

      Use the Select Users and Groups tab to find the application users or groups that are provisioned with roles belonging to this Financial Management application. You can list all users and groups, or only those that match your search criteria.

3 Select users or groups.

   a. Search for the users or groups to which you want to grant access to security classes.

   b. Select users or groups, and move them to **Selected Users and Groups**.

4 Click **Next**.

5 **Optional:** Add security classes for classic applications.

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

   b. Click **Add**. The new security class is listed in **Available Classes**.

6 From **Available Classes**, select and move security classes to **Selected Classes**.

7 Click **Next**.

8 On **Assign Access** tab, set the access right each user or group has to each security class. By default, no access right is granted to the selected users and groups. Consult online help for assistance.

   a. Select security classes for which access rights are to be defined.

   b. From **Access Rights**, select the level of security class access that you want to assign to the user or group. Available access are explained in Table 20.

Table 20 User Access Levels on Artifacts

Access Level	Permitted Tasks
None	No access to elements assigned to the security class.
Metadata	User can view a specified member in a list but cannot view or modify data for the member.
Read	User can view data for elements assigned to the security class but cannot promote or reject.
Promote	User can view data for elements assigned to the security class and promote or reject.

Access Level	Permitted Tasks
All	User can modify data for elements assigned to the security class and promote and reject.

c. Click **Set**.

d. **Optional:** Click **Add Alert** to add an e-mail alert.

e. Click **Save**.

9 **Click Next.**

Use the Security Reports tab to create security report that details the information that you selected while setting up application security. Consult online help for assistance.

11 Provisioning Reporting and Analysis

In This Chapter

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's 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 *JDoe* is provisioned with Reporting and Analysis roles but is not provisioned for Essbase application *Esb_Demo1*. In this scenario, *JDoe* cannot use Web Analysis to analyze data from *Esb_Demo1* if the user logs into Essbase as *jDoe*. This user may, however, log into Essbase as a different user who is provisioned for Essbase application.

Prerequisites

Subtopics

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. See Chapter 3, "Configuring User Directories."

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 Products

The Reporting and Analysis product for which you want to provision users and groups, and their tools, should be running. Reporting and Analysis products and tools:

- Financial Reporting
- Interactive Reporting
- Oracle's Hyperion® SQR® Production Reporting
- Web Analysis
- Financial Reporting Studio
- Interactive Reporting Studio
- Production Reporting Studio
- Oracle's 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 Hyperion 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 Hyperion 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 Hyperion 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 13

- "Accessing EPM Workspace" on page 169
- "Accessing Administration Services Console" on page 170

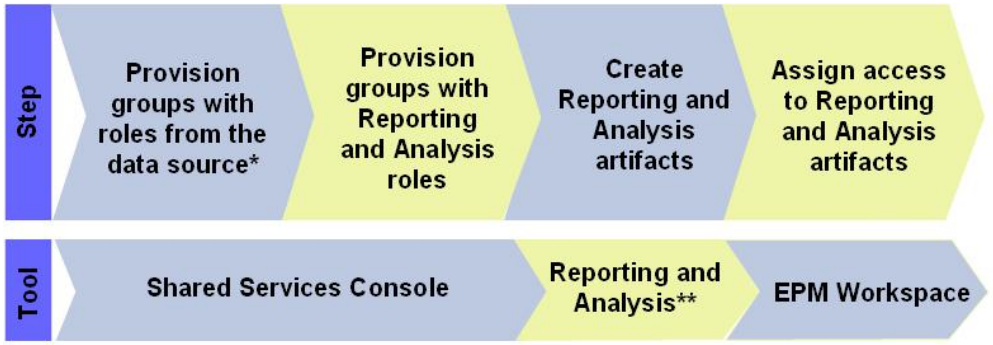
Reporting and Analysis Provisioning Process

The following Reporting and Analysis roles are automatically granted to the Shared Services administrator (*admin*) to facilitate provisioning:

- Provisioning Manager
- Reporting and Analysis 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 `admin` or as a user provisioned with Reporting and Analysis Provisioning Manager role. See:**

- "Launching Shared Services Console" on page 13
- "Accessing Administration Services Console" on page 170

2 **Provision users or groups.**

a. Find users or groups to provision.

See "Searching for Users, Groups, Roles, and Delegated Lists" on page 15.

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 21 for a list of Reporting and Analysis roles and Table 22 for useful role combinations.

Table 21 Reporting and Analysis Roles

Role	Description
Power Roles	
Reporting and Analysis Administrator	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

Role	Description
Reporting and Analysis Global Administrator	Universally and implicitly accesses all resources and functionality; accesses the Administer and Impact Manager modules **Note:** Reporting and Analysis Global Administrators can never be denied access. Applies to Financial Reporting, Interactive Reporting, Production Reporting, and Web Analysis
Content Manager	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
Data Source Publisher	Imports data source connectivity files Applies to Interactive Reporting and Web Analysis
Favorites Distributor	Pushes content to users' Favorites folders using the Favorites Manager Applies to Financial Reporting, Interactive Reporting, Production Reporting, and Web Analysis
Job Manager	Creates and manages public job parameters, output directories, and output printer locations Applies to Interactive Reporting and Production Reporting **Note:** 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.
Schedule Manager	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
Provisioning Manager	Provisions Reporting and Analysis users
Interactive Roles	
Analyst	Accesses interactive content using full analytic and reporting functionality Applies to Interactive Reporting and Web Analysis
Content Publisher	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.
Data Editor	Pushes Web Analysis data to Essbase
Job Publisher*	Imports and modifies documents, jobs, and job output; runs jobs; contains the Smart Form Publisher role Applies to Interactive Reporting and Production Reporting
Personal Page Publisher*	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
Report Designer	Accesses authoring studios to create and distribute documents Applies to Financial Reporting and Web Analysis

Role	Description
Scheduler	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
Smart Form Publisher*	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.
Personal Page Editor*	Creates, modifies, and customizes Personal Pages; copies content from other users' published Personal Pages Applies to Interactive Reporting and Production Reporting
View Roles	
Dynamic Viewer*	Views, reprocesses, and prints Interactive Reporting documents
Explorer	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
Interactive Reporting Viewer*	Reviews and prints static Interactive Reporting documents
IR HTML Viewer	Uses the HTML Viewer to browse BQY documents. This role is not automatically assigned to users who were migrated from a previous version.
IR Webclient Viewer	Uses Interactive Reporting plug-in to browse BQY documents. This role is not automatically assigned to users that were migrated from a previous version.
Job Runner*	Runs jobs and views public job parameters and physical resources Applies to Interactive Reporting and Production Reporting
Personal Page Editor*	Creates, modifies, and customizes Personal Pages; copies content from other users' published Personal Pages Applies to Interactive Reporting and Production Reporting
Personal Parameter Editor	Defines points of view and personal parameters on database connections to customize query result sets Applies to Interactive Reporting, Production Reporting, and Web Analysis
Viewer	Reviews EPM Workspace content. The content is static and accessible only from the Favorites folder. **Note:** 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

Role	Description
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 22 Reporting and Analysis Role Combinations

Combined Role	Tasks	Access Permissions
Explorer + Favorites Distributor + Personal Page Editor + Personal Parameter Editor	• Review interactive Web Analysis and Financial Reporting content in EPM Workspace • List and subscribe to repository content • Review accessible interactive content in Web Analysis Studio • Access Personal Page • Access Favorites Manager • Define Web Analysis points of view, personal variables, and personal parameters, to customize the query result set	Share interactive content without modifying content or saving changes to the repository
Explorer + Analyst + Content Publisher	• Review interactive Web Analysis, Financial Reporting, and Interactive Reporting content in the EPM Workspace • List and subscribe to repository content • Review accessible interactive content in Web Analysis Studio • Edit queries, rerun queries, and arrange data • Create Financial Reporting batches and books • Import and modify content	Interactively use document types to edit queries, rerun queries, and save changes back to the repository
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, Fusion Edition • 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

Combined Role	Tasks	Access Permissions
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
- Dashboard Studio
- Oracle's 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 Studio User's Guide*
- *Oracle Hyperion Web Analysis Studio User's Guide*

Controlling Access to Reporting and Analysis Artifacts

Reporting and Analysis artifacts are available to users after they are given 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 169**.

2 **Select Navigate, and then Explore.**

3 In the Explore tab, 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 screen or in Apply Permissions to Selected Items screen, 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**.

12 Provisioning Profitability and Cost Management

In This Chapter

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
- Administration Services

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 Web application is running.

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

Essbase Server

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

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

Administration Services

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

Ensure that Administration Services is running. See the *Oracle Hyperion 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:

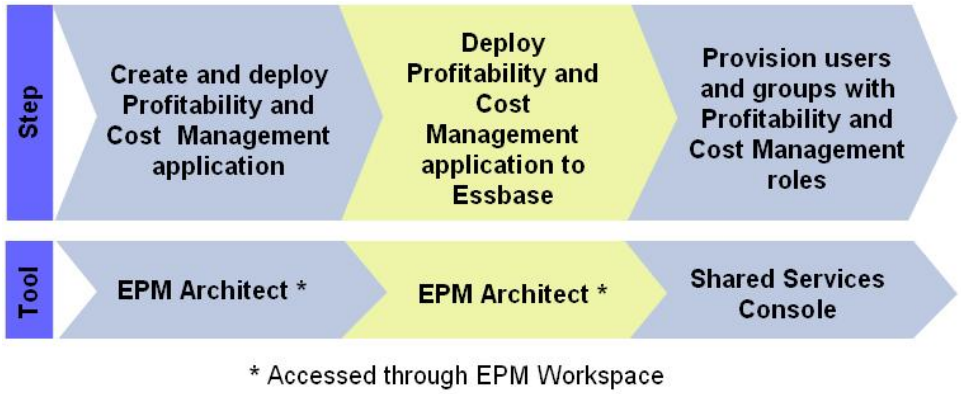
- "Launching Shared Services Console" on page 13
- "Accessing EPM Workspace" on page 169
- "Accessing Administration Services Console" on page 170

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.



Creating and Deploying Profitability and Cost Management Applications

Profitability and Cost Management applications are created using the Application Library, accessed from EPM Workspace.

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

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 Profitability and Cost Management applications:

1 Access EPM Workspace. See "Accessing EPM Workspace" on page 169.

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**.

6 **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.

7 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—Measure, Allocation Type, POV (up to four POVs can be included), Alias (optional), and Business Dimension—as local dimensions.

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**.

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.

Deploying Profitability and Cost Management Applications to Essbase

You must do the following tasks before you can deploy Profitability and Cost Management application to Essbase. When you deploy Profitability and Cost Management 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.

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 Profitability and Cost Management applications to Essbase involves these tasks:

- "Adding Stages to the Application" on page 145
- "Adding POV to the Application" on page 146

After completing these tasks, you must deploy the applications to Essbase.

Adding Stages to the Application

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 Profitability and Cost Management. See the *Oracle Hyperion Profitability and Cost Management Administrator's GuideOracle Hyperion Profitability and Cost Management Administrator's Guide*.

➤ To add stages:

1 **Open a Profitability and Cost Management application.**

   a. Access EPM Workspace. See "Accessing EPM Workspace" on page 169.

   b. From EPM Workspace, select **File**, then **Open**, then **Applications**, and then **Profitability**.

   c. Select the 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 Profitability and Cost Management. See the *Oracle Hyperion Profitability and Cost Management Administrator's Guide*.

➤ To add POV managers:

1 **Open the Profitability and Cost Management application.**

   a. Access EPM Workspace. See "Accessing EPM Workspace" on page 169.

   b. From EPM Workspace, select **File**, then **Open**, then **Applications**, and then **Profitability**.

   c. Select the 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 Profitability and Cost Management instance (deployment) can support multiple applications. You must provision Profitability and Cost Management users separately to each application.

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

➤ To provision users or groups with Profitability and Cost Management application roles:

1 Access Shared Services Console as *admin* 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 169.

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 15.

   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 Profitability and Cost Management application.

   e. Expand the node that represents your application.

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

      See Table 23 for a list of Profitability and Cost Management roles and the tasks to which they provide access.

Table 23 Profitability and Cost Management Roles

Role	Description
Power Roles	
Administrator (*admin*)	The Administrator role provides the administrative capability within Profitability and Cost Management to perform these tasks: ● 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 associations, assignments, and application preferences ● Create staging tables in the source database to import model data and metadata from relational databases into Profitability and Cost Management ● Perform POV copy, calculation, validation, data entry, and trace allocations ● Deploy to Essbase and generate calculation scripts ● Import and export data ● Use Lifecycle Management 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
Power User	The Power User role manages the majority of model functions and can perform these tasks: ● Create and maintain elements within the model, such as stages, drivers, POVs, driver associations, 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
Interactive Roles	
Interactive User	Can perform these tasks: ● View all modeling screens ● View and modify data on the Data Entry screen
View User	View-only access for these functions: ● Data entry ● Trace allocations ● Application preferences ● Model stages, drivers, and POVs

g. Click **Save**.

h. Click **OK**.

3 **Repeat step 2 for each Profitability and Cost Management application that you want to provision.**

A EPM System Roles

In This Appendix

Foundation Services Roles

Foundation Services roles comprise power roles belonging to these EPM System products:

- Shared Services
- Performance Management Architect
- Calculation Manager
- Oracle Hyperion Financial Close Management
- Oracle Hyperion Disclosure Management

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 24 Shared Services Roles (Global Roles)

Role	Description
Administrator Shared Services Administrator role comprises these roles: ● Create Integrations ● Directory Manager ● LCM Administrator ● Manage Taskflows ● Run Taskflows ● Project Manager ● Run Integrations	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. 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.
Create Integrations	Creates Shared Services data integrations (the process of moving data between applications) using a wizard
Directory Manager	Creates and manages users and groups within Native Directory 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 Manger role to users who have been assigned the Provisioning Manager role.
LCM Administrator This role comprises these roles: ● Directory Manager ● Manage Taskflows ● Run Taskflows ● Project Manager ● Provisioning Manager	Runs Lifecycle Management to promote artifacts or data across product environments and operating systems In addition to the Provisioning Manager role, the LCM Administrator role comprises Directory Manager and Project Manager roles of Shared Services.
Manage Taskflows	Creates, edits, views, schedules, and runs taskflows for any EPM System product. Has full control over all taskflows.
Run Taskflows	Views, schedules, and runs the taskflows that users with the Manage Taskflows role created. Cannot create or edit taskflows for any EPM System product.
Project Manager	Creates and manages Shared Services application groups.
Run Integrations	Views and runs Shared Services data integrations For Performance Management Architect, executes data synchronizations

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 25 Performance Management Architect Roles

Role	Description
EPMA Administrator The EPMA Administrator role comprises these roles: ● Application Creator ❍ Essbase Application Creator ❍ Financial Management Application Creator ❍ Planning Application Creator ❍ Profitability Application Creator ● Dimension Editor	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. EPMA Administrators can also perform these Transaction History Purge Utility operations: ● Access all applications, even if the user did not deploy the application ● Manually mark a stalled job as timed out ● View hidden jobs ● Open the application diagnostics screen to run tests and solutions on all applications
Essbase Application Creator	Creates Essbase applications and generic applications using Performance Management Architect
Financial Management Application Creator	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.
Planning Application Creator	Creates Planning applications and generic applications using Performance Management Architect
Profitability Application Creator	Creates Profitability and Cost Management applications generic applications using Performance Management Architect
Dimension Editor[1]	Creates, manages, and imports profiles to create dimensions in Performance Management Architect. Creates and manages dimensions manually within Performance Management Architect. Required to access Classic Application Administration options for Financial Management and Planning using Web navigation.

[1]Only Dimension Editors can create dimensions in the Shared Library.

Calculation Manager Roles

All Calculation Manager roles are power roles. Typically, they are granted to create Calculation Manager Administrators.

Table 26 Calculation Manager Roles

Role	Description
Calculation Manager Administrator Calculation Manager Administrator role comprises these roles: ● Financial Management Calculation Manager Administrator ● Planning Calculation Manager Administrator	Administers and manages Calculation Manager functions Financial Management Calculation Manager Administrator administers Calculation Manager functions in Financial Management Planning Calculation Manager Administrator administers Calculation Manager functions in Planning

Role	Description
Financial Management Calculation Manager Administrator	Administers Calculation Manager functions in Financial Management
Planning Calculation Manager Administrator	Administers Calculation Manager functions in Planning

Financial Close Management Roles

Native Directory users cannot perform tasks granted by 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 27 Financial Close Management Roles

Role	Description
Close Administrator	Administers Financial Close Management. Performs the tasks that Close Power User and Close User can perform.
Close Power User	• Performs tasks that Close User can perform • Create and manage alert types
Close User	Performs these tasks: • Views templates • Accesses Reporting and Analysis and transactional dashboards • Modifies status • Creates and modifies alerts, comments, and questions • Creates and manages filters

Disclosure Management Roles

Table 28 Disclosure Management Roles

Role	Description
Provisioning Manager	Provisions users and groups with Disclosure Management roles
Disclosure Management User	Performs Disclosure Management actions

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 29 Essbase Server Roles

Role	Description
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

Table 30 Essbase Application Roles

Role	Description
Application Manager	Creates, deletes, and modifies databases and application settings within the assigned application. Includes Database Manager permissions for databases within the application. **Note:** 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.
Database Manager	Manages the databases, database artifacts, and locks within the assigned application
Calc	Calculates, updates, and reads data values based on assigned scope, using any assigned calculations and filter
Write	Updates and reads data values based on assigned scope, using any assigned filter
Read	Reads data values
Filter	Accesses specific data and metadata according to filter restrictions
Start/Stop Application	Starts and stops applications or databases
Provisioning Manager	Provisions Essbase users with roles from this application

Essbase Studio Roles

Table 31 Essbase Studio Roles

Role	Description
cpViewer	Viewer ● Views and previews all Essbase Studio artifacts, including metadata elements (dimension elements, hierarchies, data sets, alias sets, drill-through reports) and data source connections ● Executes drill-through reports
cpDSAdmin	Data Source Administrator ● Has all privileges of cpViewer ● Creates, updates, and destroys data source connections
cpDM	Data Modeler (administrator of metadata elements)* ● Has all privileges of cpViewer ● Creates, updates, and destroys metadata elements (dimension elements, hierarchies, cube schemas, Essbase models, alias sets, drill-through reports) ● Deploys Essbase cubes and updates cube linkage in Essbase cubes
cpDMDSAdmin	Administrator* Has all privileges of cpDSAdmin and cpDM **Note:** This role is obtained by selecting both the cpDM and cpDSAdmin roles when provisioning.
cpAdmin	System Administrator* ● Has all privileges of cpDMDSAdmin ● Export/imports Essbase Studio catalog and selected Essbase Studio catalog artifacts ● Upgrades Essbase Studio catalog

* To deploy cubes in Essbase Studio, cpDM, cpDMDSAdmin, and cpAdmin users must be provisioned for, at the minimum, the Shared Services Project Manager role. Users also require an Essbase Server role such as Create/Delete Application or Administrator.

Reporting and Analysis Roles

Table 32 Reporting and Analysis Roles

Role	Description
Power Roles	
Reporting and Analysis Administrator	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

Role	Description
Reporting and Analysis Global Administrator	Universally and implicitly accesses all resources and functionality; accesses the Administer and Impact Manager modules **Note:** Reporting and Analysis Global Administrators can never be denied access. Applies to Financial Reporting, Interactive Reporting, Production Reporting, and Web Analysis
Content Manager	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
Data Source Publisher	Imports data source connectivity files Applies to Interactive Reporting and Web Analysis
Favorites Distributor	Pushes content to users' Favorites folders using the Favorites Manager Applies to Financial Reporting, Interactive Reporting, Production Reporting, and Web Analysis
Job Manager	Creates and manages public job parameters, output directories, and output printer locations Applies to Interactive Reporting and Production Reporting **Note:** 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.
Schedule Manager	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
Provisioning Manager	Provisions Reporting and Analysis users
Interactive Roles	
Analyst	Accesses interactive content using full analytic and reporting functionality Applies to Interactive Reporting and Web Analysis
Content Publisher	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.
Data Editor	Pushes Web Analysis data to Essbase
Job Publisher*	Imports and modifies documents, jobs, and job output; runs jobs; contains the Smart Form Publisher role Applies to Interactive Reporting and Production Reporting
Personal Page Publisher*	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
Report Designer	Accesses authoring studios to create and distribute documents Applies to Financial Reporting and Web Analysis

Role	Description
Scheduler	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
Smart Form Publisher*	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.
Personal Page Editor*	Creates, modifies, and customizes Personal Pages; copies content from other users' published Personal Pages Applies to Interactive Reporting and Production Reporting
View Roles	
Dynamic Viewer*	Views, reprocesses, and prints Interactive Reporting documents
Explorer	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
Interactive Reporting Viewer*	Reviews and prints static Interactive Reporting documents
IR HTML Viewer	Uses the HTML Viewer to browse BQY documents. This role is not automatically assigned to users who were migrated from a previous version.
IR Webclient Viewer	Uses Interactive Reporting plug-in to browse BQY documents. This role is not automatically assigned to users that were migrated from a previous version.
Job Runner*	Runs jobs and views public job parameters and physical resources Applies to Interactive Reporting and Production Reporting
Personal Page Editor*	Creates, modifies, and customizes Personal Pages; copies content from other users' published Personal Pages Applies to Interactive Reporting and Production Reporting
Personal Parameter Editor	Defines points of view and personal parameters on database connections to customize query result sets Applies to Interactive Reporting, Production Reporting, and Web Analysis
Viewer	Reviews EPM Workspace content. The content is static and accessible only from the Favorites folder. **Note:** 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
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

Financial Management Roles

Additional Shared Services roles are required for Performance Management Architect and Calculation Manager. See "Foundation Services Roles" on page 149.

Table 33 Financial Management Roles

Role	Description
Power Roles	
Application Administrator	Performs all Financial Management tasks. Access to this role overrides any other access setting for the user.
Load System	Loads rules and member lists
Inter-Company Transaction Admin	Opens and closes periods, locks and unlocks entities, and manages reason codes. Users with the role can also perform all intercompany tasks.
Interactive Roles	
Rules Administrator	Performs any Calculation Manager tasks for the specific application
Rules Designer	Creates new rules objects and modifies or deletes rules objects
Approve Journals	Approves or rejects journals
Create Journals	Creates, modifies, deletes, submits, and unsubmits journals
Create Unbalanced Journals	Creates unbalanced journals
Default	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.
Journals Administrator	Performs all tasks related to journals
Post Journals	Posts and unposts journals
Manage Templates	Grants access to the journals template task in the Setup Journals module
Generate Recurring	Grants access to the generate recurring task in the Setup Journals module
Review Supervisor	Starts process management units and approves and publishes process management data. Can promote or reject process units, depending on process level.
Reviewer 1 through Reviewer 10	Views and edits a block of data when that data is at the user's designated process management level
Submitter	Submits a block of data for final approval
Lock Data	Locks data in Data Explorer
Unlock Data	Unlocks data in Data Explorer
Consolidate All	Runs consolidate all

Role	Description
Consolidate	Runs consolidate
Consolidate All with Data	Runs consolidate with all data
Run Allocation	Runs allocations
Manage Data Entry Forms	Manages data entry forms on the Web
Save System Report On Server	Saves system reports on server
Load Excel Data	Loads data from Smart View
Inter-Company Transaction User	Creates, edits, deletes, loads, and extracts transactions. Runs matching report by account or ID, runs transaction report, and drills through from modules.
Inter-Company Transaction Match Template	Manages intercompany matching templates
Inter-Company Transaction Auto Match by Account	Automatically matches intercompany transactions by account
Inter-Company Transaction Auto Match by ID	Automatically matches intercompany transactions by ID
Inter-Company Transaction Manual Match with Tolerance	Manually matches intercompany transactions with tolerance check
Inter-Company Transaction Manual Match	Manually matches intercompany transactions
Inter-Company Transaction Unmatch	Unmatches intercompany transactions
Inter-Company Transaction Post/Unpost	Posts and unposts intercompany transactions
Enable write back in Web Grid	Enters and saves data directly to a Web grid
Database Management	Copies and clears data and deletes invalid records
Manage Ownership	Enters and edits ownership information
Task Automation	Sets up automated tasks
Manage Custom Documents	Loads and extracts custom documents to and from the server
Extended Analytics	Creates and executes extended anlaytics queries
Data Form Write Back from Excel	Submits data from Smart View while using a Web Data Entry Form
View Roles	
Advanced User	Uses the Browser View and can access Running Tasks
Rules Viewer	Views rules objects
Read Journals	Reads journals
Receive Email Alerts for Process Control	Receives e-mails
Receive Email Alerts for Intercompany	Receives e-mails
Reserved	Not currently used

Planning Roles

Additional Foundation Services roles are required for Performance Management Architect and Calculation Manager. See "Foundation Services Roles" on page 149.

Table 34 Planning Application Roles

Role	Description
Power Roles	
Administrator	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.
Provisioning Manager	Provisions users to the Planning application
Mass Allocation	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.
Analytic Services Write Access	For planners and interactive users: Grants users access to Planning data in Essbase equivalent to their Planning access permissions. 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 Administrator role comprises these roles: ● Approvals Ownership Assigner ● Approvals Process Designer ● Approvals Supervisor	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 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

Role	Description
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.
Planner Roles	
Planner	Enters and submits plans for approval and runs business rules 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.
Interactive Roles	
Interactive User	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.
View Roles	
View User	Views and analyzes data through Planning data forms and any data access tools for which they are licensed (for example, Oracle Hyperion Financial Reporting, Fusion Edition, Web Analysis, and Oracle Hyperion Smart View for Office, Fusion Edition). Typical View users are executives who want to see business plans during and at the end of the budget process.

Business Rules Roles

Table 35 Business Rules Roles

Role	Description
Power Roles	
Administrator	Creates, launches, edits, validates, and manages business rules, sequences, macros, variables, and projects. Assigns access permissions to business rules, sequences, macros, variables, and projects.
Provisioning Manager	Provisions users and groups with Oracle's Hyperion® Business Rules roles.
Interactive Roles	
Interactive User	Creates business rules, sequences, macros, variables, and projects. Assigns access permissions to business rules, sequences, macros, variables, and projects.
Basic User	Launches business rules and sequences to which the user has access. Views variables and macros, business rules, and sequences to which the users has access. Edits business rules, sequences, macros, variables, and projects for which the user has editing permissions.

Business Modeling Roles

Table 36 Business Modeling Roles

Role	Description
Power Roles	
Administrator	Manages the users, security, and databases for the application, on the desktop and the Web. Sets up and maintain databases and containers, installs and configures application (authentication, users and groups, provisioning). Sets up global tools on the Web Home Page.
Interactive Roles	
Builder	Creates the original model or enterprise model by defining all elements of the model, such as boxes, links, variables, and financial values, and by attaching financial data.
View Roles	
End User	Updates model periods. Uses business and operational knowledge to adjust parameters for the original model, experiments with the workings of the scenario on the Web to search for process improvements, time or money savings, or unexpected bottlenecks or benefits.

Profitability and Cost Management Roles

Table 37 Profitability and Cost Management Roles

Role	Description
Power Roles	
Administrator (*admin*)	The Administrator role provides the administrative capability within Profitability and Cost Management to perform these tasks: ● 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 associations, assignments, and application preferences ● Create staging tables in the source database to import model data and metadata from relational databases into Profitability and Cost Management ● Perform POV copy, calculation, validation, data entry, and trace allocations ● Deploy to Essbase and generate calculation scripts ● Import and export data ● Use Oracle Hyperion Enterprise Performance Management System Lifecycle Management 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

Role	Description
Power User	The Power User role manages the majority of model functions and can perform these tasks: ● Create and maintain elements within the model, such as stages, drivers, POVs, driver associations, 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
Interactive Roles	
Interactive User	Can perform these tasks: ● View all modeling screens ● View and modify data on the Data Entry screen
View User	View-only access for these functions: ● Data entry ● Trace allocations ● Application preferences ● Model stages, drivers, and POVs

Performance Scorecard Roles

Table 38 Performance Scorecard Roles

Role	Description
Power Roles	
Power Manager	Provides the administrative capability within an Oracle Hyperion Performance Scorecard, Fusion Edition, environment
Provisioning Manager	Provisions users and groups with Performance Scorecard, roles.
Interactive Roles	
Basic	Grants access to reports, scorecards, measures, and initiatives with the additional role of result collection administration
Interactive	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.

Strategic Finance Roles

Table 39 Strategic Finance Roles

Role	Description
Power Roles	
Administrator	Administers Oracle Hyperion Strategic Finance, Fusion Edition, 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's 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's Hyperion® Data Integration Management documentation for detailed information.

FDM Roles

Table 40 FDM Roles

Roles	Tasks per Role
Administrator	Manages applications and performs any action. Has access to every location and rights to every form and control.
Basic Reviewer	Reviews financial controls questions
Basic Reviewer and Submitter	Submits certification or assessment after it has been reviewed
Intermediate 2–9	Loads data to the target system. Roles for intermediate levels are defined by the Oracle Hyperion Financial Data Quality Management, Fusion Edition 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.

ERP Integrator Roles

Table 41 ERP Integrator Roles

Roles	Tasks per Role
Administrator	Manages applications and performs any action
Provisioning Manager	Provisions users and groups with Oracle Hyperion Financial Data Quality Management ERP Integration Adapter for Oracle Applications roles
Drill Through	Applies to ERP Integrator and FDM. Controls the ability to drill through to the source system. In FDM, this role is applied as a permissible task to an Intermediate role to control drilling back to the source system. In ERP Integrator, this role controls whether the user can drill to the ERP Integrator landing page, which controls drilling to the source system.
Create Integration	Creates ERP Integrator metadata and data rules.
Run Integration	Runs ERP Integrator 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.
GL Write Back	Enables data write-back to the ERP source system.

Integrated Operational Planning Roles

Table 42 Integrated Operational Planning Roles

Roles	Tasks per Role
Provisioning Manager	Provisions users and groups with Disclosure Management roles
IOP Administrator	Administers Oracle Integrated Operational Planning, Fusion Edition. IOP Administrators can modify models, access ACL pages, and perform all Integrated Operational Planning tasks.
IOP User	Performs Integrated Operational Planning actions as a normal user

B EPM System Product Codes

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 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 43.

Table 43 Product Codes Used by EPM System Products

Product Code	Product Name
HUB	Shared Services
CES	Shared Services (Workflow)
HP	Planning
ESB	Essbase
BPM	Oracle Essbase Studio
ESBAPP	Essbase Application
BPMA	Performance Management Architect
HAVA	Reporting and Analysis products such as the following: ● EPM Workspace ● Web Analysis ● Interactive Reporting ● Oracle's Hyperion® SQR® Production Reporting
FDM	Oracle Hyperion Financial Data Quality Management, Fusion Edition
EAL	Oracle Essbase Analytics Link for Hyperion Financial Management
EALBRIDGE	Oracle Essbase Analytics Link for Hyperion Financial Management Bridge
HFM	Oracle Hyperion Financial Management, Fusion Edition
HPS	Oracle Hyperion Performance Scorecard, Fusion Edition
HBR	Oracle's Hyperion® Business Rules

Product Code	Product Name
HPM	Oracle Hyperion Profitability and Cost Management, Fusion Edition
CALC	Hyperion Calculation Manager
HSF	Oracle Hyperion Strategic Finance, Fusion Edition
AIF	Oracle Hyperion Financial Data Quality Management ERP Integration Adapter for Oracle Applications
IOP	Oracle Integrated Operational Planning, Fusion Edition
BIEE	Oracle Business Intelligence Enterprise Edition
DISCMAN	Oracle Hyperion Disclosure Management
FCC	Oracle Hyperion Financial Close Management
BIP	Oracle Business Intelligence Publisher

C Accessing EPM System Products

In This Appendix

Accessing Shared Services

See "Launching Shared Services Console" on page 13.

Accessing EPM Workspace

EPM Workspace is a Foundation Services component from which you can access EPM System products such as Oracle Hyperion Planning, Fusion Edition; Oracle Hyperion EPM Architect, Fusion Edition; and Oracle's Hyperion Reporting and Analysis components such as Oracle's Hyperion® Interactive Reporting and Oracle's Hyperion® Web Analysis. A logon window is displayed when you access EPM Workspace using a URL.

➤ To access EPM Workspace from 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, `https://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**.

Launching Shared Services Console from EPM Workspace

The process of accessing Shared Services Console from EPM Workspace uses the single sign-on capabilities of Oracle Hyperion Enterprise Performance Management System to bypass the Shared Services logon window.

Note: The Shared Services roles assigned to the current EPM Workspace user determines the resources available to the user in Shared Services Console.

➤ To access Shared Services Console from EPM Workspace:

1 From EPM Workspace, select **Navigate**.

2 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 Web application 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's Hyperion® Foundation Services is running, and *`port_number`* indicates the Web server port; for example, `https://myWebserver:19000/easconsole/easconsole.html`.

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/easconsole/easconsole.html`.

2 Select a locale.

3 Click **Launch**.

4 Download and install Administration Services Console.

5 In the Oracle Essbase Administration Services Login screen, enter your user name and password.

6 Click **OK**.

D

Accessibility

In This Appendix

About Accessibility

Subtopics

- Viewing Shared Services Console in an Accessible Mode
- Using JAWS Screen Reading Software
- Known Issues

This appendix describes the accessibility features of Shared Services Console. For information regarding supported assistive technologies, refer to the *Oracle Hyperion Enterprise Performance Management System Installation Start Here*.

Viewing Shared Services Console in an Accessible Mode

To view Shared Services Console in an accessible mode, append `accessibilityMode=true` to the Shared Services URL; for example, `http://Web_server_name:port_number/interop/index.jsp?accessibilityMode=true`.

If launching Shared Services Console from EPM Workspace, enable the accessibility mode in the Oracle Enterprise Performance Management Workspace, Fusion Edition user preferences.

To view Shared Services Console with high contrast, append `themeSelection=BpmTadpoleHc` to Shared Services URL, for example, `http://Web_server_name:port_number/interop/index.jsp?themeSelection=BpmTadpoleHc`.

Using JAWS Screen Reading Software

If you are using JAWS® Screen Reading Software, Oracle recommends using the Internet Explorer browser.

For JAWS to read the content of some editable text fields within Shared Services Console, enable the Virtual PC Cursor mode. The following procedures provide two methods for enabling the JAWS Virtual PC Cursor mode.

Note: These procedures apply if you are viewing Shared Services Console in an accessible mode (by appending `accessibilityMode=true` to the Oracle's Hyperion® Shared Services URL).

➤ To enable the Virtual PC Cursor in JAWS Configuration Manager:

1. From the JAWS **Utilities** menu, select **Configuration Manager**.
2. From the **Set Options** menu, select **Advanced Options**.
3. Select **Use Virtual PC Cursor**.
4. Click **OK**.

➤ To toggle between enabling or disabling the JAWS Virtual PC Cursor using a keyboard shortcut, press the plus (+) key on the numeric key pad.

Caution! The other Shared Services Console components will not work while in Virtual PC Cursor mode (for example, users will not be able to traverse the provisioning tree). To work with other components, you must disable the Virtual PC Cursor mode after reading the text field content. Therefore, Oracle recommends using the keyboard shortcut method to toggle between enabling and disabling the Virtual PC Cursor mode.

Known Issues

- Screens used to create and modify the following artifacts do not support high contrast mode.
  - Users
  - Groups
  - Roles
  - Delegated Lists
- JAWS Screen Reading Software reads only the title and first paragraph of each help topic. All text that comes after the first paragraph is skipped.
- The following issues were observed in the View Report screen in high contrast mode:
  - Drop-down lists associated with combo boxes failed to display.
  - When users expand the nodes in **In Application**, lower level nodes are highlighted while header level nodes are not.
  - JAWS reads value only from the 1st cell of the 1st row of the View Report table.

Using Keyboard Shortcuts

Subtopics

Use shortcut keys as an alternative to the mouse when working in Shared Services Console. You can activate interface components, menu items, or tasks using keyboard shortcuts.

This section lists the keyboard shortcuts for interface components, menu items, and tasks completed in Shared Services Console.

- The underlined letter that typically appears in a menu title, menu item, or the text of a button or other component is called a mnemonic. Because Oracle considers mnemonics to be "self-documenting," no additional documentation of these keys is provided. However, it is important to note that some mnemonics are repeated. For example, on the File menu, the underlined mnemonic D is used for both the Delete menu item and the Deactivate menu item. When this occurs, the first time you press D, highlights the item to be deleted. Press Enter to Delete or press D again to highlight the Deactivate button, and then press Enter to Deactivate.
- If you are using a version of the Firefox browser later than release 1.5, substitute Alt+Shift for Alt as the modifier.

Global Keyboard Shortcuts

Use these global shortcuts to navigate Shared Services Console.

Table 44 Global Keyboard Shortcuts

Task	Keyboard Shortcut
Focus and activate the first menu on the menu bar.	F10
Focus on the first object listed in the View pane.	Ctrl+0
Focus on the task tabs. Focus shifts to the current task tab.	Ctrl+G
Focus on the toolbar. Focus shifts to the toolbar itself, and then you can use Tab to select individual buttons.	Ctrl+T
Focus on the current task tab in the content area.	Ctrl+Y
Close the current tab (except the Browse tab).	Ctrl+F4
Activate the selected object in the View pane.	Space bar
Display the shortcut menu for the selected object in the View pane.	F9

Task	Keyboard Shortcut
Focus away from a task tab to the page frame.	Ctrl+F6

For an overview of Shared Services Console (View pane, task tabs, and so on), see Chapter 1, "About Shared Services."

Menus

Use these keyboard shortcuts when Oracle's Hyperion® Shared Services Console is displayed.

Note: Keyboard shortcuts for menus are context sensitive. In other words, different menu options are available for each type of task.

Table 45 File Menu

Menu Item	Keyboard Shortcut
New	Ctrl+N
Open	Ctrl+O
Properties	Ctrl+Shift+R
Delete	Ctrl+D or DEL
Activate	Ctrl+E
Deactivate	Ctrl+D

Table 46 View Menu

Menu Item	Keyboard Shortcut
View Masthead	Ctrl+Alt+O
Refresh	Ctrl+F
Explore	Ctrl+X

Table 47 Administration Menu

Menu Item	Keyboard Shortcut
View Provisioning Report	Ctrl+Shift+T
Security Reports/Performed By	Ctrl+Shift+B
Security Reports/Performed On	Ctrl+O
Provision	Ctrl+Shift+P

Menu Item	Keyboard Shortcut
Deprovision	Ctrl+Shift+D
Delete Applications	Ctrl+L
Audit Report	Ctrl+U
Config Report	Ctrl+P
Configure Auditing	Ctrl+R

Note: To access the Security Reports, Artifact Reports, and Config Reports submenu items under Audit Reports, use the down arrow key to highlight Audit Reports, and then press the right arrow key to display the sub-menu items. Press S (for Security Reports), F (for Artifact Reports), or P (for Config Reports) to launch the corresponding reports.

Administration Tasks

Use these keyboard shortcuts when performing administration tasks.

Table 48 Configure User Directories: Provider Configuration Tab

Interface Component	Keyboard Shortcut
New	Alt+N
Edit	Alt+I
Delete	Alt+E
Move Up	Alt+P
Move Down	Alt+W
Include	Alt+U
Exclude	Alt+X
Test	Alt+T

Table 49 Audit Configuration Window

Interface Component	Keyboard Shortcut
Purge	Alt+P

Table 50 Audit Reports

Interface Component	Keyboard Shortcut
View Report	Alt+E

Interface Component	Keyboard Shortcut
Export	Alt+X

Table 51 Select User or Group Screen

Interface Component	Keyboard Shortcut
Select All	Alt+E
Select	Alt+T
Close	Alt+L
Search	Alt+R

Provisioning Tasks

Use these keyboard shortcuts when provisioning users, groups, tasks, or delegated lists.

Table 52 Provisioning Users

Task	Keyboard Shortcut
New	Ctrl+N
Properties	Ctrl+Shift+R
Delete	Delete
Activate	Ctrl+E, Enter
Deactivate	Ctrl+D, Enter
View Provisioning Report	Ctrl+Shift+T
Security Reports/Performed By	Ctrl+Shift+B
Security Reports/Performed On	Ctrl+O
Provision	Ctrl+Shift+P
Deprovision	Ctrl+Shift+D

Table 53 Provisioning Groups

Task	Keyboard Shortcut
New	Ctrl+N
Properties	Ctrl+Shift+R
Delete	DEL
Security Reports/Performed On	Ctrl+O

Task	Keyboard Shortcut
Provision	Ctrl+Shift+P
Deprovision	Ctrl+Shift+D

Table 54 Provisioning Roles

Task	Keyboard Shortcut
New	Ctrl+N
Properties	Ctrl+Shift+R
Delete	DEL
View Provisioning Report	Ctrl+Shift+T

Table 55 Provisioning Delegated Lists

Task	Keyboard Shortcut
New	Ctrl+N
Properties	Ctrl+Shift+R
Delete	DEL
View Delegated Report	Ctrl+Shift+T

Table 56 Users, Groups, Roles, or Delegated Lists Properties: Member Of Tab

Interface Component	Keyboard Shortcut
Reset	Alt+R

Application Management Tasks

You can use these keyboard shortcuts when working with application groups.

Table 57 Application Management Tasks

Interface Component	Keyboard Shortcut
New	Ctrl+N
Delete Applications	Ctrl+D
Open	Ctrl+O
Delete	Ctrl+D
Audit Report	Ctrl+U

Interface Component	Keyboard Shortcut
Config Report	Ctrl+P
Configure Auditing	Ctrl+R
Move To	Ctrl+M
Copy Provisioning	Ctrl+I
Explore	Ctrl+X

Table 58 Artifact List Tab

Interface Component	Keyboard Shortcut
Artifact List button	Alt+T
Selected Artifacts button	Alt+E
Search Artifacts button	Alt+S
Select All/Clear Selections button	Alt+C
Define Migration button	Alt+M
View Audit Report button	Alt+U
Search button	Alt+R

Table 59 New/Modify Application Group Screen

Interface Component	Keyboard Shortcut
Update List	Alt+U
Reset	Alt+R

Table 60 Migration Wizard

Interface Component	Keyboard Shortcut
Source	Alt+E
Source Option	Alt+U
Destination	Alt+T
Destination Option	Alt+I
Summary	Alt+M
Execute Migration button	Alt+G
Save Migration Definition button	Alt+V

Table 61 Move To Tab

Interface Component	Keyboard Shortcut
Search	Alt+R
Display All	Alt+Y

Table 62 Copy Provisioning Tab

Interface Component	Keyboard Shortcut
Search	Alt+R
Display All	Alt+Y

Table 63 Edit/Execute Migration Screen

Interface Component	Keyboard Shortcut
Finish	Alt+I

Table 64 Purge Screen

Interface Component	Keyboard Shortcut
Purge	Alt+E

Table 65 Migration Status Report

Interface Component	Keyboard Shortcut
Refresh	Alt+R

Glossary

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 ofcopying 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) In data mining, a collection of an algorithm's findings about examined data. A model can be applied against a wider data set to generate useful information about that data; 2) 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; 3) 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 1) A process that transforms artifacts so that they function properly in the destination environment after application migration; 2) In data mining, the modification of data (bidirectionally) flowing between the cells in the cube and the algorithm.

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.

Index

B

C

D

E

F

G

H

I

K

L

M

N

O

R

V

W