Oracle® Enterprise Performance Management System

User Security Administration Guide

Release 11.2
F12917-06
November 2023

ORACLE

Oracle Enterprise Performance Management System User Security Administration Guide, Release 11.2

F12917-06

Primary Author: EPM Information Development Team

Contents

6 Managing Native Directory

7 Managing Provisioning

8 Managing Taskflows

9 Provisioning Essbase

10 Provisioning Planning

11 Provisioning Financial Management

A EPM System Roles

B EPM System Component Codes

C Accessing EPM System Products

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 that have purchased support 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.

Documentation Feedback

To provide feedback on this documentation, click the feedback button at the bottom of the page in any Oracle Help Center topic. You can also send email to epmdoc_ww@oracle.com.

1

About Shared Services

Related Topics

- What Is Shared Services?
- Launching Shared Services Console
- Overview of Shared Services Console
- Searching for Users, Groups, Roles, and Delegated Lists

What Is Shared Services?

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

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

Launching Shared Services Console

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

To launch the Shared Services Console:

1. Go to:

   `http://`*`web_server_name`*`:`*`port_number`*`/workspace`

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

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

2. Click **Launch Application**.

> **Note:**
>
> Pop-up blockers may prevent EPM Workspace from opening.

3. In **Logon**, enter your user name and password.

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

4. Click **Log On**.

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

Overview of Shared Services Console

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

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

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

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

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

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

The following features are available through Shared Services Console:

- User directory configurations
- Single sign-on configuration
- Native Directory management
- Role-based access control management of users

- Audit configuration and report management
- Access to Oracle Hyperion Enterprise Performance Management System Lifecycle Management and product artifact exploration

Searching for Users, Groups, Roles, and Delegated Lists

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

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

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

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

1. In the View pane, expand **User Directories**.
2. From the user directory that you want to search, select one of the following:
   - **Users**
   - **Groups**
   - **Roles**
   - **Delegated List**

   > **Note:**
   >
   > Roles and Delegated List are available only in Native Directory searches.
   >
   > Delegated List is available only if Shared Services is in Delegated Administration mode. See Delegated User Management for detailed information.

   Available search fields are displayed on the Browse tab.
3. To search for users:
   a. In **User Property**, select a user property to search.

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

      Searchable user properties:

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

b. **Optional**: In **User Filter**, specify a filter for identifying specific users. Use an asterisk (*) as the wildcard in pattern searches.

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

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

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

f. Click **Search**.

4. To search for groups:

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

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

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

c. Click **Search.**

5. To search for roles:

Role search is supported only for Native Directory.

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

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

c. Click **Search.**

6. To search for delegated lists:

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

b. Click **Search**.

2

EPM System Security Concepts

Related Topics

- Security Components
- User Authentication Components
- Provisioning (Role-based Authorization)

Security Components

Oracle Enterprise Performance Management System security comprises two complementary layers that control user access and permissions:

- User Authentication Components
- Provisioning (Role-based Authorization)

User Authentication Components

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

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

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

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

The following sections describe the components that support SSO:

- Native Directory
- User Directories

Native Directory

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

Native Directory functions:

- Maintains and manages the native user accounts
- Maintains and manages the native group accounts
- Central storage for all Oracle Enterprise Performance Management System provisioning information; it stores the relationships among groups, roles, and applications

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

Directory Managers access and manage Native Directory using the Oracle Hyperion Shared Services Console. See Managing Native Directory.

User Directories

User directories refer to any corporate user and identity management system that is compatible with Oracle Enterprise Performance Management System components.

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

Provisioning (Role-based Authorization)

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

Each EPM System component provides several default roles tailored to various business needs. Applications belonging to an EPM System component inherits these roles. Predefined roles from the applications registered with Oracle Hyperion Shared Services are displayed in the Oracle Hyperion Shared Services Console.

To facilitate provisioning, you may create custom Native Directory roles that aggregate the default roles to suit specific requirements. The process of granting roles and object ACLs belonging to EPM System applications to users and groups is called *provisioning*.

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

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

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

Roles

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

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

Access restrictions based on roles enable functional administrators to control and manage application access. See EPM System Roles.

Global Roles

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

Predefined Roles

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

Aggregated Roles

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

Users

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

You can create and manage Native Directory users only from Oracle Hyperion 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 Oracle Hyperion Shared Services, Oracle does not recommend provisioning individual users.

Default EPM System Administrator

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

System Administrator

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

Functional Administrators

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

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

Groups

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

3
Configuring User Directories

Related Topics

- User Directories and EPM System Security
- Operations Related to User Directory Configuration
- Oracle Identity Manager and EPM System
- Active Directory Information
- Configuring OID, Active Directory, and Other LDAP-based User Directories
- Configuring Relational Databases as User Directories
- Testing User Directory Connections
- Editing User Directory Settings
- Deleting User Directory Configurations
- Managing the User Directory Search Order
- Setting Security Options
- Regenerating Encryption Keys
- Using Special Characters

User Directories and EPM System Security

Oracle Enterprise Performance Management 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 relational databases as external user directories.

Generally, EPM System products use Native Directory and external user directories in provisioning. See Oracle Enterprise Performance Management System Certification Matrix 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 Oracle Hyperion Shared Services Console.

By default, EPM System Configurator configures the Shared Services repository as the Native Directory to support EPM System products. Directory Managers access and manage Native Directory using the Shared Services Console.

Operations Related to User Directory Configuration

To support SSO and authorization, System Administrators must configure external user directories. From Oracle Hyperion Shared Services Console, System Administrators 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
  - Configuring Relational Databases as User Directories
- Testing User Directory Connections
- Editing User Directory Settings
- Deleting User Directory Configurations
- Managing the User Directory Search Order
- Setting Security Options

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.

Oracle Enterprise Performance Management 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 Oracle Hyperion 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 Provisioning Managers 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, Administrators must perform these steps:

- Ensure that members (users and groups) of Oracle Identity Manager enterprise roles that are to be used 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.

Active Directory Information

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

DNS Lookup and Host Name Lookup

System Administrators can configure Active Directory so Oracle Hyperion 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 your organization is using a global catalog, use one of these methods to configure Active Directory:

- 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 Oracle Enterprise Performance Management System products to access local and universal groups within the forest.

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

System Administrators 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. Access Oracle Hyperion Shared Services Console as System Administrator. See Launching Shared Services Console.

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

   The Provider Configuration tab opens. This screen lists all configured user directories, including Native Directory.

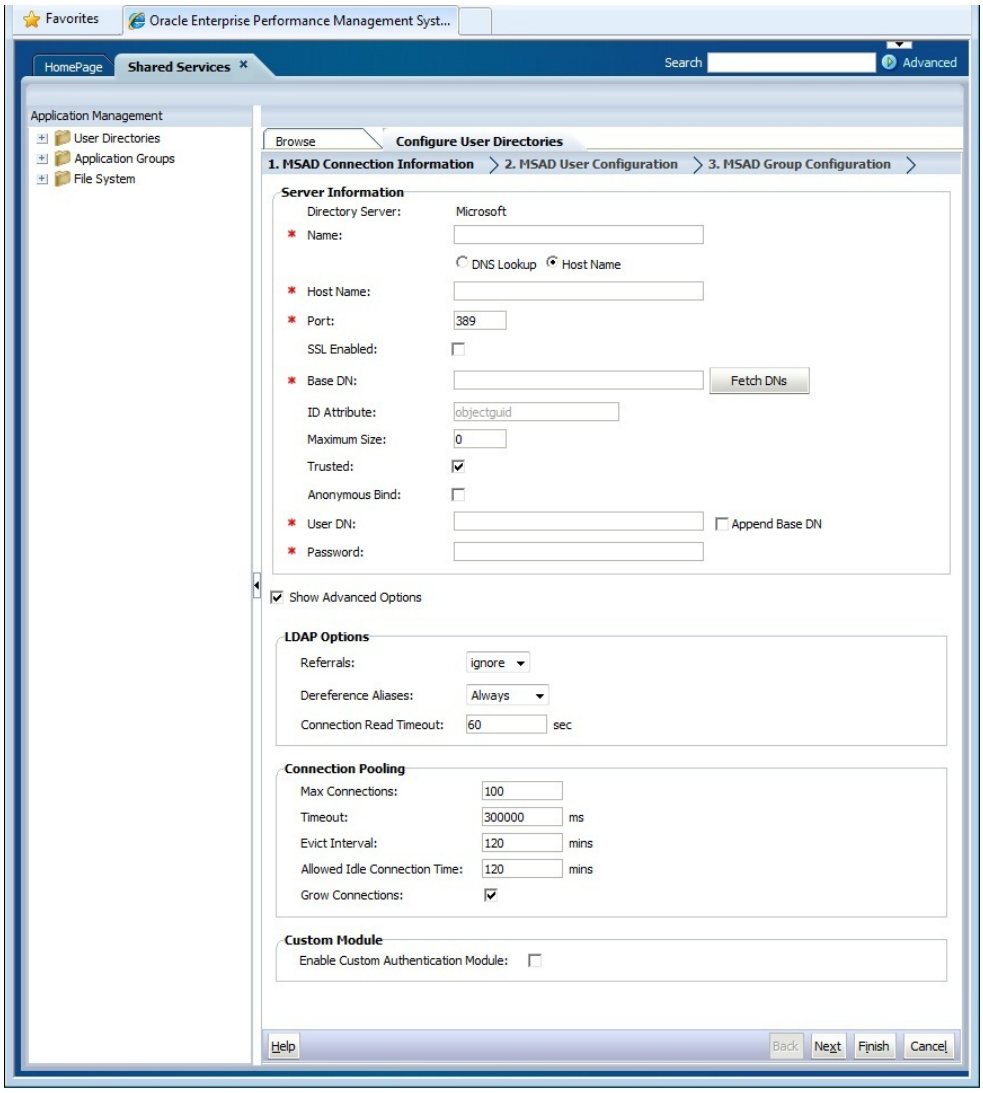
3. Click **New**.

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.

     Active Directory and Active Directory Application Mode (ADAM) only: If you want to use a custom ID attribute (an attribute other than `ObjectGUID`; for example `sAMAccountName` with Active Directory or ADAM, select **Lightweight Directory Access Protocol (LDAP)**, and configure it as Directory Type `Other`.

5. Click **Next**.



6. Enter the required parameters.

Table 3-1 Connection Information Screen

Label	Description
Directory Server	Select a user directory. The **ID Attribute** value changes to the recommended constant unique identity attribute for the selected product. This property is automatically selected if you chose Active Directory in step 4. Select `Other` in the following scenarios: • You are configuring an unlisted user directory type; for example, Oracle Virtual Directory • You are configuring a listed LDAP-enabled user directory (for example, OID), but want to use a custom ID Attribute. • You are configuring Active Directory or ADAM to use a custom ID Attribute. **Note:** Because Oracle Virtual Directory provides a virtualized abstraction of LDAP directories and RDMBS data repositories in one directory view, Oracle Enterprise Performance Management 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`
Name	A descriptive name for the user directory. Used to identify a specific user directory if multiple user directories are configured. Name should not contain special characters other than space and underscore. **Example:** `Corporate_OID`

Table 3-1 (Cont.) Connection Information Screen

Label	Description
DNS Lookup	**Active Directory only:** Select this option to enable DNS lookup. See DNS Lookup and Host Name Lookup. 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. **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. **Example:** `MyServer`

Table 3-1 (Cont.) Connection Information Screen

Label	Description
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. **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 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`
ID Attribute	This attribute value can be modified only if `Other` is selected in **Directory Type**. This attribute must be a common attribute that exists in user and group objects on the directory server. 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` The 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 attribute • Not be location specific • Not change over time

Table 3-1 (Cont.) Connection Information Screen

Label	Description
Maximum Size	The 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 Oracle Hyperion 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 not use anonymous bind. **Note:** Anonymous bind is not supported for OID.
User DN	This option 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 user must have search privileges on the RDN attribute within the DN. For example, in the dn: `cn=John Doe, ou=people, dc=myCompany, dc=com`, the bind user should have search access to the `cn` attribute. Special characters in User DN must be specified using escape characters. See Using Special Characters for restrictions. **Example:** `cn=admin,dc=myCompany,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:** If Active Directory is configured to follow referrals, select `follow` to automatically follow LDAP referrals. Select `ignore` to not use referrals.

Table 3-1 (Cont.) Connection Information Screen

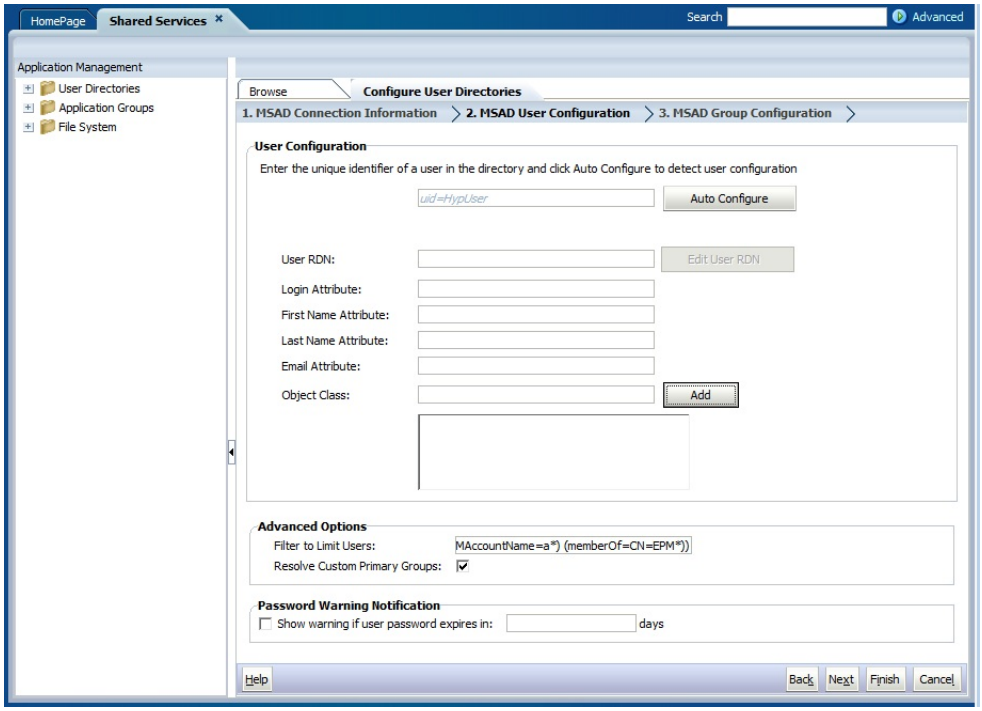
Label	Description
Dereference Aliases	Select the method that Shared Services searches should use to dereference aliases in the user directory so searches retrieve the object to which the DN of the alias points. Select: • **Always**: Always dereference aliases. • **Never**: Never dereference aliases. • **Finding**: Dereference aliases only during name resolution. • **Searching**: Dereference aliases only after name resolution.
Connection Read Timeout	Interval (seconds) after which the LDAP provider aborts the LDAP read attempt if it does not get a response. **Default:** 60 seconds
Max Connections	Maximum connections in the connection pool. Default is 100 for LDAP-based directories, including Active Directory. **Default:** 100
Timeout	Timeout to get a connection from the pool. An exception is thrown after this period. **Default:** 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:** 120 minutes
Allowed Idle Connection Time	**Optional:** The time after which the eviction process removes the idle connections in the pool. **Default:** 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 returns an error if a connection is not available within the time set for `Time Out`.
Enable Custom 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. 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 Enterprise Performance Management System Security Configuration 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 point 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 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 Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

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

Table 3-2 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 for restrictions. **Example:** `ou=People`
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 email address **Default:** `mail`

Table 3-2 (Cont.) User Configuration Screen

Label	Description[1]
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. **Note:** If you are configuring Active Directory or ADAM as user directory type `Other` to use a custom ID attribute, you must set this value to `user`. You can manually add object classes if needed. To add an object class, enter the object class name into the **Object Class** box, and then 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`
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.
User Search Attribute for Multi-Attribute RDN	**LDAP-enabled user directories other than Active Directory only:** Set this value only if your directory server is configured to use a multi-attribute RDN. The value you set must be one of the RDN attributes. The value of the attribute you specify should be unique and the attribute should be searchable. For example, assume that a SunONE directory server is configured to combine the cn (`cn=John Doe`) and uid (`uid=jDoe12345`) attributes to create a multi-attribute RDN similar to the following: `cn=John Doe+uid=jDoe12345, ou=people, dc=myCompany, dc=com` In this case, you can use either `cn` or `uid` if these attributes meet the following conditions: • The attribute is searchable by the user identified in User DN filed on Connection Information tab • The attribute requires you to set a unique value across the user directory

Table 3-2 (Cont.) User Configuration Screen

Label	Description[1]
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.
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.

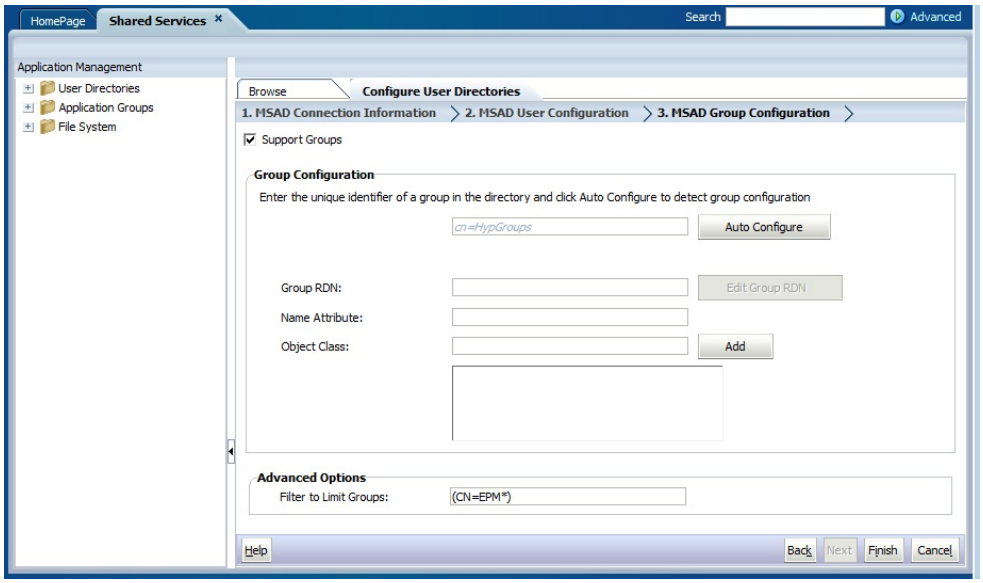
[1] EPM System security may use default values for some fields for which configuration value is optional. If you do not enter values in such fields, default values are used during runtime.

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 your organization does 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 Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

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 3-3 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 that 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 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`

Table 3-3 (Cont.) Group Configuration Screen

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. **Note:** If you are configuring Active Directory or ADAM as user directory type `Other` to use a custom ID attribute, you must set this value to `group?member`. 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 then click **Add**. To delete object classes, select the object class, and then click **Remove**. **Default** • **Active Directory:** `group?member` • **LDAP directories other than Active Directory:** `groupofuniquenames?uniquemember, groupOfNames?member` • **Native Directory:** `groupofuniquenames?uniquemember, cssGroupExtend?cssIsActive`
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 **Finish**.

    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.

14. If needed, change the search order assignment. See Managing the User Directory Search Order for details.

15. If needed, specify security options. See Setting Security Options for details.
16. Restart Oracle Hyperion Foundation Services and other EPM System components.

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, Oracle Hyperion 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. Provisioning Managers can, however, add these users to groups in Native Directory and provision those groups. For supported platform information, see the *Oracle Enterprise Performance Management System Certification Matrix* posted on the Oracle Fusion Middleware Supported System Configurations page on Oracle Technology Network (OTN).

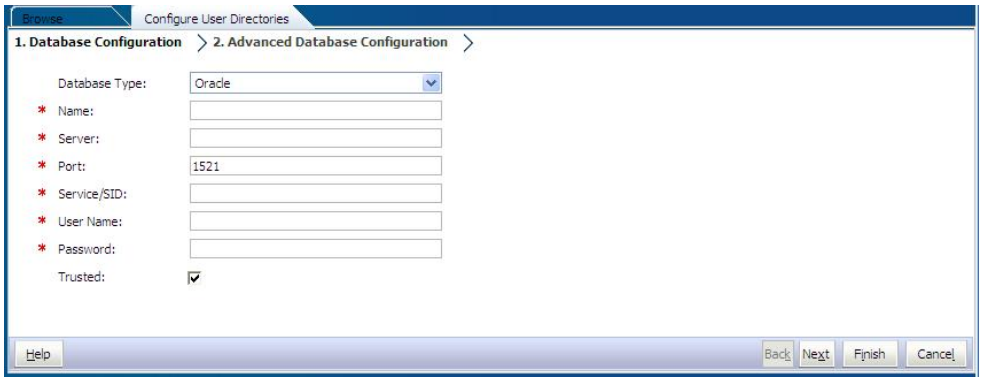
> **Note:**
>
> If you are using a DB2 database, the user name must contain at least eight characters. User names should not exceed 256 characters (Oracle and SQL Server databases), and 1000 characters (DB2).

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 retrieves only active database users for provisioning. Inactive and locked database user accounts are ignored.

To configure database providers:

1. Access Oracle Hyperion Shared Services Console as System Administrator. See Launching Shared Services Console.
2. Select **Administration**, and then **Configure User Directories**.
3. Click **New**.
4. In the **Directory Type** screen, select **Relational Database (Oracle, DB2, SQL Server)**.
5. Click **Next**.



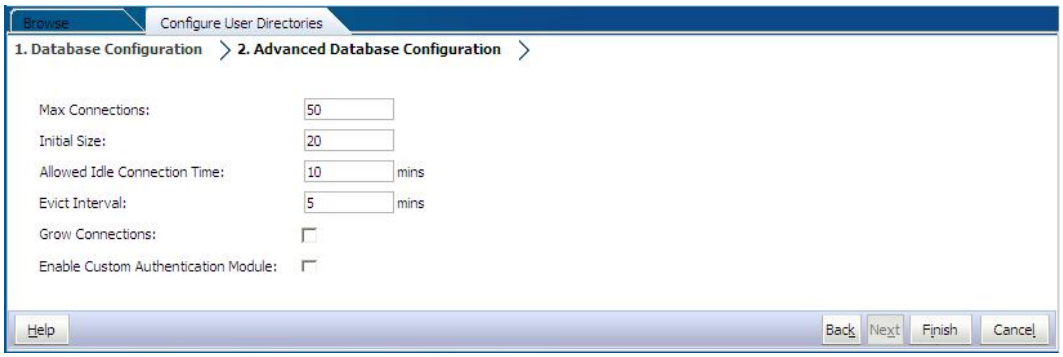
6. On the Database Configuration tab, enter configuration parameters.

Table 3-4 Database Configuration Tab

Label	Description
Database Type	The relational database provider. Shared Services supports only Oracle 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 databases. **Example:** `SYSTEM`
Password	The password of the user identified in the **User Name**. **Example:** `system_password`
Trusted	The 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 3-5 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`.
Enable Custom 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. The custom authentication module authentication is transparent to thin and thick clients. See "Using a Custom Authentication Module" in the *Oracle Enterprise Performance Management System Security Configuration Guide*.

9. Click **Finish**.
10. Click **OK** to return to the Defined User Directories screen.
11. Test the database provider configuration. See Testing User Directory Connections.
12. Change the search order assignment, if needed. See Managing the User Directory Search Order for details.
13. Specify security settings, if needed. See Setting Security Options.
14. Restart Oracle Hyperion Foundation Services and other Oracle Enterprise Performance Management System components.

Testing User Directory Connections

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

To test a user directory connection:

1. Access Oracle Hyperion Shared Services Console as System Administrator. See Launching Shared Services Console.
2. Select **Administration**, and 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

Administrators can modify any parameter, other than the 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. Access Oracle Hyperion Shared Services Console as System Administrator. See Launching Shared Services Console.
2. Select **Administration**, and then **Configure User Directories**.
3. 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 that you can edit, see the following tables:

- Active Directory and other LDAP-based user directories, see the tables in Configuring OID, Active Directory, and Other LDAP-based User Directories.
- Databases: See the table in Configuring Relational Databases as User Directories

6. Click **OK** to save the changes.

Deleting User Directory Configurations

System Administrators 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. Access Oracle Hyperion Shared Services Console as System Administrator. See Launching Shared Services Console.
2. Select **Administration**, and then **Configure User Directories**.
3. Select a directory.
4. Click **Delete**.
5. Click **OK**.
6. Click **OK** again.
7. Restart Oracle Hyperion Foundation Services and other Oracle Enterprise Performance Management System components.

Managing the User Directory Search Order

When a System Administrator configures an external user directory, Oracle Hyperion 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 Oracle Enterprise Performance Management System searches for users and groups.

System Administrators 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. Administrators can perform these tasks to manage the search order:

- Adding a User Directory to the Search Order
- Changing the Search Order
- Removing a Search Order Assignment

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. Access Oracle Hyperion Shared Services Console as System Administrator. See Launching Shared Services Console.
2. Select **Administration**, and then **Configure User Directories**.
3. Select a deactivated 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 Oracle Hyperion Foundation Services and other EPM System components.

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 `Deactivated` status. When an Administrator removes a user directory from the search order, the search sequence assigned to the other user directories is automatically updated.

> **Note:**
>
> Native Directory cannot be removed from the search order.

To remove a user directory from the search order:

1. Access Shared Services Console as System Administrator. See Launching Shared Services Console.
2. Select **Administration**, and then **Configure User Directories**.
3. 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 Foundation Services and other EPM System components.

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. Access Shared Services Console as System Administrator. See Launching Shared Services Console.
2. Select **Administration**, and then **Configure User Directories**.
3. Select a directory whose search order you want to change.
4. Click **Move Up** or **Move Down**.
5. Click **OK**.
6. Restart Foundation Services, other EPM System components, 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. Access Oracle Hyperion Shared Services Console as System Administrator. See Launching Shared Services Console.
2. Select **Administration**, and then **Configure User Directories**.
3. Select **Security Options**.
4. In **Security Options**, set global parameters.

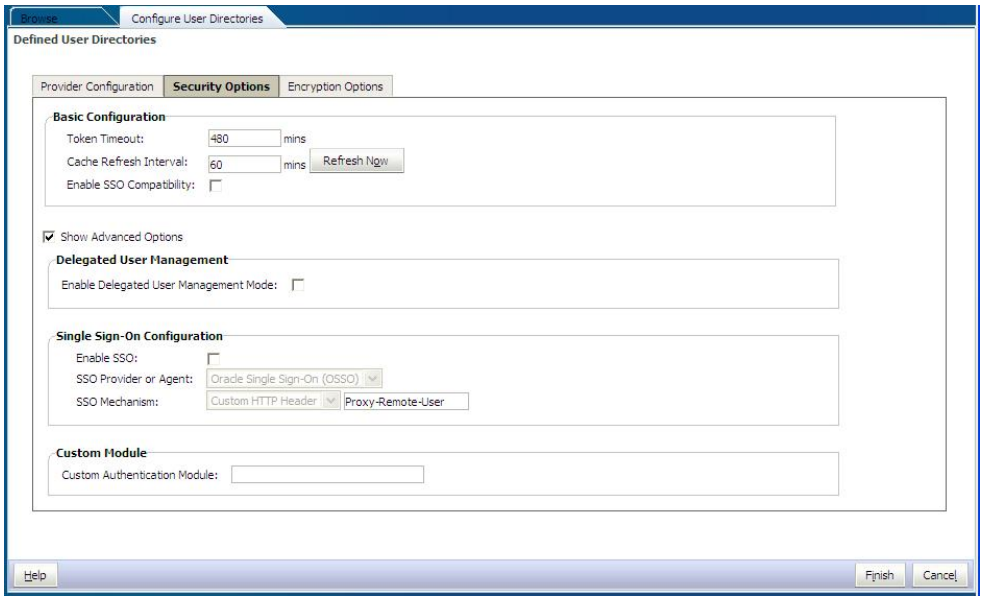


Table 3-6 Security Options for User Directories

Parameter	Description
Token Timeout	Time (in minutes) after which the SSO token issued by Oracle Enterprise Performance Management 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. Default is 480 minutes. **Note:** Token timeout is not the same as session timeout.
Cache Refresh Interval	Interval (in minutes) for refreshing the Oracle Hyperion 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.
Refresh Now	Click this button to manually initiate the refreshing of Shared Services cache that contains groups to users relationship data. You may want to initiate a cache refresh after creating new groups in external user directories and provisioning them or after adding new users to existing groups. The cache is refreshed only after Shared Services makes a call that uses the data in the cache.
Enable SSO Compatibility	Select this option if your deployment is integrated with Oracle Business Intelligence Enterprise Edition Release 11.1.1.5 or earlier.

Table 3-6 (Cont.) Security Options for User Directories

Parameter	Description
Enable Delegated User Management Mode	Option enabling delegated user management of EPM System products to support the distributed management of provisioning activities. See "Delegated User Management" in the *Oracle Enterprise Performance Management System User Security Administration Guide*.
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 mechanism and name are automatically selected when you select the SSO provider. You can change the name of the SSO mechanism (HTTP header or custom login class), if required. If you select `Other` as the SSO provider or agent, you must censure that it supports an EPM System supported SSO mechanism. See "Supported SSO Methods" in the *Oracle Enterprise Performance Management System Security Configuration Guide*.
SSO Mechanism	The method that the selected 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 Enterprise Performance Management System Security Configuration Guide*. • `Custom HTTP Header`: Set the name of the header that the security 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 Enterprise Performance Management System Security Configuration Guide*. **Note:** Custom Login Class 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.

Table 3-6 (Cont.) Security Options for User Directories

Parameter	Description
Custom 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. Oracle Hyperion Foundation Services requires that the custom authentication JAR file be named `CustomAuth.jar`. `CustomAuth.jar` must be available in *`MIDDLEWARE_HOME`*`\user_projects\domains\`*`WEBLOGIC_DOMAIN`*`\lib`, typically, `C:\Oracle/Middleware/user_projects/domains/EPMSystem/lib`. On all client installations, `CustomAuth.jar` must be present in *`EPM_ORACLE_HOME`*`/common/jlib/11.1.2.0`, typically, `C:\Oracle\Middleware\EPMSystem11R1\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 Enterprise Performance Management System Security Configuration Guide*.

5. Click **OK**.
6. Restart Foundation Services and other EPM System components.

Regenerating Encryption Keys

Oracle Enterprise Performance Management 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 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.

Change these keys periodically to strengthen EPM System security. Oracle Hyperion Shared Services and the security subsystem of EPM System use AES encryption with 128-bit key strength.

> **Caution:**
>
> Taskflows used by Oracle Hyperion Financial Management and Oracle Hyperion Profitability and Cost Management are invalidated when you regenerate the Single Sign On Encryption key. After regenerating the key, open and save the taskflows to revalidate them.

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

1. Access Oracle Hyperion Shared Services Console as System Administrator. See Launching Shared Services Console.
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 3-7 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 **Enable SSO Compatibility** is selected on **Security Options**: • **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 (*EPM_ORACLE_HOME*`/common/CSS/ssHandlerTK`) from all EPM System host machines.
Trusted Services Key	Select this option 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 option 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 **OK**.
6. If you chose to generate a new SSO encryption key, complete this step.
   a. Click **Download**.
   b. Click **OK** to save `ssHandlerTK`, the keystore file that supports the new SSO encryption key, into a folder on the server that hosts Oracle Hyperion Foundation Services.

c. Copy `ssHandlerTK` into *EPM_ORACLE_HOME*`/common/CSS` on all EPM System host machines.

7. Restart Foundation Services and other EPM System components.

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 Oracle Hyperion 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. The following table 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 3-8 Supported Special Characters

Character	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

> **Note:**
>
> 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, and 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 3-9 Characters that Need Not be Escaped

Character	Name or Meaning	Character	Name or Meaning
(	open parenthesis	'	single quote
)	close parenthesis	^	caret

Table 3-9 (Cont.) Characters that Need Not be Escaped

Character	Name or Meaning	Character	Name or Meaning
$	dollar	@	at
&	Ampersand		

Note:

& 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 3-10 Escape for Special Characters in User Directory Configuration Settings

Special Character	Escape	Example 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 (<)	backslash (\)	ou=test<ou	ou=test\<ou
greater than (>)	backslash (\)	ou=test>ou	ou=test\>ou
quotation mark (")	two backslashes (\\)	ou=test"ou	ou=test\\"ou
backslash (\)	three backslashes (\\\)	ou=test\ou	ou=test\\\\ou

Note:

- 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 DNs, a backslash (\) must be escaped with one backslash. For example, ou=test\ou must be specified as ou=test\\ou.

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.

Special Characters in Native Directory

special characters are supported in user and group names in Native Directory.

Table 3-11 Supported Special Characters: Native Directory

Character	Name or Meaning	Character	Name or Meaning
@	at	,	comma
#	pound	=	equal to
$	dollar	+	plus
^	caret	;	semicolon
(	open parenthesis	!	exclamation
)	close parenthesis	%	percent
'	single quotation mark		

4

Working with Application Groups and Applications

Related Topics

- Overview
- Working with Application Groups
- Managing Applications
- Exploring Applications

Overview

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

Working with Application Groups

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

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

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

Topics detailing application group management tasks:

- Creating Application Groups
- Modifying Application Group Properties
- Deleting Application Groups

> **Note:**
>
> You must be a Functional Administrator or LCM Administrator to create and manage application groups. While a Functional Administrator can work with all registered applications. A Project Manager can view 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. Access Oracle Hyperion Shared Services Console as a Functional Administrator. See Launching Shared Services Console.
2. In the View pane, right-click **Application Groups**, and then select **New Application Group**.
3. In **Name**, enter a unique application group name, and then, in **Description**, enter an optional description.

   Application group names are case-sensitive. For example, `Test_1`, `TEst_1`, and `test_1` are unique group names.
4. To assign applications to this application group:
   a. From **List Applications in Application Group**, select an application group that contains the application that you want to assign.
   b. Click **Update List**. The Available Applications list displays the applications that you can assign to the application group.
   c. From **Available Applications**, select the applications to assign to the application group, and then click  .
   d. To remove an assigned application, from **Assigned Applications**, select the application to remove, and then click  .
5. Click **Finish**.
6. Click **Create Another** to create another application group, or click **OK** to close the status screen.

Modifying Application Group Properties

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

> **Note:**
>
> Functional Administrators can also add applications to application groups by moving them from another application group. See Moving Applications.

To modify an application group:

1. Access Oracle Hyperion Shared Services Console as a Functional Administrator. See Launching Shared Services Console.
2. In the View pane, right-click an application group, and then select **Open**.
3. Modify the application group properties as needed. See step 4 of "Creating Application Groups" for information on assigning or removing applications.

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

4. Click **Save**.

Deleting Application Groups

Deleting an application group removes the association of applications with the application group and deletes the application group but does not remove provisioning assignments from applications. You cannot delete the following application groups:

- Default Application Group
- Foundation
- File System

To delete an application group:

1. Access Oracle Hyperion Shared Services Console as Functional Administrator. See Launching Shared Services Console.
2. In the View pane, right-click the application group, and then select **Delete**.

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

3. Click **Yes**.
4. Click **OK**.

Managing Applications

Oracle Hyperion Shared Services tracks registered Oracle Enterprise Performance Management System applications.

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

Registration of some applications creates application groups and assigns applications to them. If registration does not create an application group, then the application is listed under

Default Application Group. Provisioning Managers can provision these applications. When a Functional Administrator moves applications from Default Application Group to another application group, Shared Services retains the provisioning information.

Topics addressing application management tasks:

- Moving Applications
- Copying Provisioning Information Across Applications
- Deleting an Application
- Provisioning Essbase Application Artifacts

Moving Applications

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

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

To move an application:

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

Copying Provisioning Information Across Applications

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

To copy provisioning information across applications:

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

Copy Provisioning opens. This tab lists the target application to which you can copy provisioning information.

4. Select the destination application.
5. Click **Save**.

Deleting Multiple Applications

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

To delete applications:

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

> **Note:**
>
> You cannot delete application groups from this screen. See Deleting Application Groups.

4. Click **Delete**.
5. Click **OK**.

Deleting an Application

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

To delete an application:

1. Access Oracle Hyperion Shared Services Console as Functional Administrator. See Launching Shared Services Console.
2. In then View pane, expand the node of the application group that contains the application that you want to delete.
3. Right-click the application, and then select **Delete**.
4. Click **OK**.

Provisioning Essbase Application Artifacts

Oracle Enterprise Performance Management System enforces application- and artifact-level provisioning to ensure application and data security. Access to each EPM System application is restricted by provisioning users and groups with application roles. Typically, a Provisioning Manager uses the Oracle Hyperion Shared Services Console to provision users and groups to EPM System applications.

Some EPM System applications create their own artifacts; for example, reports and calculation scripts that belong only to the application. In most cases, access to application artifacts can be controlled by provisioning application users and groups. For example, a user creates filters and calculation scripts for an Oracle Essbase application using the Oracle Essbase Administration Services Console or MaxL. A Provisioning Manager for the Essbase application can use the Shared Services Console to provision these filters and calculation scripts.

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

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

To assign application-specific access permissions:

1. Access Shared Services Console as Provisioning Manager. See Launching Shared Services Console.
2. In the View pane, expand the application group that contains the application for which you want to assign access permissions.
3. Right-click the application and select **Assign Access Control**. This option is available only for applications for which access permissions can be set.

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

4. Assign access permissions. See EPM System Roles for a list of product roles.

Exploring Applications

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

5

Delegated User Management

Related Topics

- About Delegated User Management
- Hierarchy of Administrators
- Enabling Delegated User Management Mode
- Creating Delegated Administrators

About Delegated User Management

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

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

Hierarchy of Administrators

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

System Administrator

System Administrators are Information technology experts who are tasked with managing Oracle Enterprise Performance Management System security and system environment.

Functional Administrators

The System Administrator creates Functional Administrators by provisioning a corporate user with the LCM Administrator role of Oracle Hyperion Foundation Services and the Administrator role of each deployed Oracle Enterprise Performance Management System component. This Functional Administrator can perform all provisioning activities across applications.

The Functional Administrator can create other Functional Administrators with more limited access within EPM System. For example, to administer Oracle Hyperion Planning application `PlanApp1`, the Functional Administrator may provision a user with the LCM Administrator role of Foundation Services and the Administrator role of the Planning application `PlanApp1`.

Delegated Administrators

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

The scope of actions that Delegated Administrators can perform on EPM System components is controlled by the access rights that the Functional Administrator granted them through provisioning. For example, assume that a Delegated Administrator is granted the Directory Manager global role in Oracle Hyperion 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 Oracle Hyperion Shared Services deployment does not support delegated administration. You must enable Delegated User Management mode for Shared Services before you can create Delegated Administrators. Additional screens and menu options become available after you switch to Delegated User Management mode.

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

To enable Delegated User Management mode:

1. Access Oracle Hyperion Shared Services Console as the Functional Administrator. See Launching Shared Services Console.
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 **OK**.
6. Click **OK**.
7. Restart Oracle Hyperion Foundation Services and other Oracle Enterprise Performance Management System components.

Creating Delegated Administrators

- Planning Steps
- Provisioning Delegated Administrators
- Creating Delegated Lists

- Viewing Delegated Reports

Planning Steps

- User Accounts for Delegated Administrators
- Create a Delegation Plan

User Accounts for Delegated Administrators

The Functional Administrator creates Delegated Administrators from user accounts in the user directories configured in Oracle Hyperion 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 Oracle Enterprise Performance Management System components and the tasks that they should be allowed to perform. The plan should identify these users, groups, and roles:

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

Provisioning Delegated Administrators

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

Delegated Administrators can be granted roles from Oracle Enterprise Performance Management System products; for example, Provisioning Manager from Oracle Hyperion 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:**
>
> Oracle Hyperion Shared Services displays the Delegated List node only if the current user is assigned to manage delegated lists.

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

To create delegated lists:

1. Access Oracle Hyperion Shared Services Console. See Launching Shared Services Console.
2. Under in View pane, right-click **Delegated List**, and then select **New Delegated**.
3. On **General**, enter a unique delegated list name and an optional description.
4. **Optional**: To add groups that the Delegated Administrator assigned to this list can administer, click **Next**.

   Group Members is displayed.

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

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

   c. Click **Search**.

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

   e. Click  .

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

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

5. **Optional**: Click **Next** to add users that the Delegated Administrator of this list can administer.

   User Members is displayed.

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

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

c. Click **Search**.

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

e. Click  .

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

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

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

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

Managed By is displayed.

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

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

c. Click **Search**.

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

e. Click  .

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

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

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

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

Modifying Delegated Lists

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

To modify delegated lists:

1. Access Oracle Hyperion Shared Services Console. See Launching Shared Services Console.
2. Select **Delegated Lists** from the node in the View pane.

3. Search for the delegated list to modify. See Searching for Users, Groups, Roles, and Delegated Lists.

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

4. Right-click the delegated list, and then select **Properties**.
5. **Optional:** On **General**, modify the list name and description.
6. **Optional**: Click **Group Members** to modify group assignments.
   a. In **Directory**, select the user directory from which groups are to be displayed. If you are a Delegated Administrator, only groups assigned to you can be searched.
   b. Select a group attribute (group name or description) that you want to search in the drop-down list, and enter a search filter.
   c. Click **Search**.
   d. From **Available Groups**, select groups.
   e. Click  .

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

   f. **Optional:** From **Assigned Groups**, select a group, and then click  to unassign a group.
7. **Optional**: Click **User Members** to modify user assignments.
   a. In **Directory**, select the user directory from which users are to be displayed. If you are a Delegated Administrator, the search lists only the users assigned to you.
   b. Select a user attribute that you want to search in the drop-down list, and enter a search filter.
   c. Click **Search**.
   d. From **Available Users**, select users.
   e. Click  .

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

   f. **Optional:** From **Assigned Users**, select a user, and then click  to unassign a user.
8. **Optional**: Click **Managed By** to modify Delegated Administrator assignment.
   a. In **Directory**, select the user directory from which users are to be displayed.
   b. Select a user attribute that you want to search in the drop-down list, and enter a search filter.

c. Click **Search**.

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

e. Click  .

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

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

9. Click **OK**.
10. Click **OK**.

Deleting Delegated Lists

To delete delegated lists:

1. Access Oracle Hyperion Shared Services Console. See Launching Shared Services Console.
2. Select **Delegated Lists** from the node in the View pane.
3. Search for the delegated list to modify. See Searching for Users, Groups, Roles, and Delegated Lists.

   Delegated lists that meet the search criterion are listed on the Browse tab.
4. Right-click the delegated list, and then select **Delete**.
5. Click **Yes**.
6. Click **OK**.

Viewing Delegated Reports

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

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

To view delegated reports:

1. Access Oracle Hyperion Shared Services Console. See Launching Shared Services Console.
2. In node in the View pane, right-click **Delegated List**, and then select **View Delegated Report**.
3. In **Delegated List Name**, enter the name of the list for which the report is to be generated. Use * as wildcard for pattern searches.
4. In **Managed By**, enter the user ID of the Delegated Administrator whose assignments in the specified list are to be reported. Use * as the wildcard for pattern searches.
5. Click **Create**.
6. Click **OK** to close the report or **Print Preview** to preview the report.

   If you preview the report:

   a. Click **Print** to print the report.

b. Click **Close** to close the View Report window.

6

Managing Native Directory

Related Topics

- About Native Directory
- Default Native Directory Users and Groups
- Managing Native Directory Users
- Managing Native Directory Groups
- Managing Roles
- Backing Up Native Directory

About Native Directory

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

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

Default Native Directory Users and Groups

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

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

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

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

Managing Native Directory Users

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

- Creating Users

- Viewing and Modifying User Accounts
- Deactivating User Accounts
- Deleting User Accounts
- Provisioning Users and Groups
- Deprovisioning Groups
- Generating Provisioning Reports

> **Note:**
>
> Users in external user directories cannot be managed from Oracle Hyperion Shared Services Console.

Creating Users

To create users:

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

Table 6-1 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`).
Password	Passwords are case-sensitive and can contain any combination of characters.
Confirm Password	Re-enter password.
First Name	User's first name (optional)
Last Name	User's last name (optional)
Description	User's description (optional)
Email Address	User's email address (optional). The email server domain extension; for example, .com, .org, and .gov, cannot contain more than four characters.

4. **Optional:** To assign the user to Native Directory groups, click **Next**.
   a. Using the fields above the **Available Groups** list, search for groups.
      i. From the drop-down list, select **Group Name** to search based on group names. Select **Description** to search based on group descriptions.
      ii. Enter the criterion for retrieving groups. Use * (asterisk) as the wildcard to retrieve all available groups.
      iii. Click **Search**.

      Groups that match the search criterion are listed under **Available Groups**.
   b. From **Available Groups**, select groups.
   c. Click  .

      The selected groups are listed under **Assigned Groups** list.
   d. **Optional:** To retrieve and assign additional groups, repeat step 4.a.

      Using the fields above the **Assigned Groups** list, you can search assigned groups to identify the groups that you want to remove.

      To remove assigned groups, from **Assigned Groups**, select the groups to remove, and then click  .
5. Click **Finish**.
6. Click **Create Another** to create another user or **Finish** to close **Create User**.

Viewing and Modifying User Accounts

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

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

To view and modify user information:

1. Access Oracle Hyperion Shared Services Console as a Functional Administrator or Directory Manager. See Launching Shared Services Console.
2. From the node in the View pane, select **Users**.
3. Search for the user account. See Searching for Users, Groups, Roles, and Delegated Lists.
4. Right-click the user account to modify and select **Properties**.

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

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

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

6. **Optional:** Modify the user's associations with Native Directory groups.
   a. Click **Member Of**.
   b. Using the fields above **Available Groups**, search for groups.
      i. From the drop-down list, select **Group Name** to search based on group names. Select **Description** to search based on group descriptions.
      ii. Enter the criterion for retrieving groups. Use * (asterisk) as the wildcard to retrieve all available groups.
      iii. Click **Search**.

      Groups that match the search criterion are listed under **Available Groups**.
   c. From **Available Groups**, select groups.
   d. Click  .

      The selected groups are listed under **Assigned Groups**.
   e. **Optional:** To retrieve and assign additional groups, repeat step 6.b.

      Using the fields above the **Assigned Groups** list, you can search assigned groups to identify the groups that you want to remove.

      To remove assigned groups, from **Assigned Groups**, select the groups to remove, and then click  .
7. **Optional:** Click **Delegated List** to view the user's delegated list assignment.
8. Click **Finish**.

Deactivating User Accounts

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

- Inactive user accounts cannot be used to log on to EPM System applications, including Oracle Hyperion Shared Services Console.
- Group associations of inactive accounts are maintained and remain visible to Functional Administrators.
- Role associations of inactive accounts are maintained.
- Inactive user accounts are not displayed on the product-specific access-control screens.
- Inactive user accounts are not deleted from Native Directory.

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

To deactivate user accounts:

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

Activating Inactive User Accounts

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

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

To activate deactivated user accounts:

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

Deleting User Accounts

Deleting a user account removes the user's associations with Native Directory groups, the role assignments of the user, and the user account from Native Directory.

> **Note:**
>
> The System Administrator account (by default, `admin`) cannot be deleted.

To delete user accounts:

1. Access Oracle Hyperion Shared Services Console as a Functional Administrator or Directory Manager. See Launching Shared Services Console.
2. Search for users to delete. See Searching for Users, Groups, Roles, and Delegated Lists.
3. Right-click the user account, and then select **Delete**.
4. Click **Yes**.
5. Click **OK**.

Changing Native Directory User Password

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

To change Native Directory password of the current user:

1. Launch Oracle Hyperion Enterprise Performance Management Workspace. See Launching Shared Services Console.
2. Select **Tools**, and then **Change Password**.
3. In **Current Password**, enter your password.
4. In **New Password** and **Confirm Password**, enter the new password.
5. Click **Save**.

Managing Native Directory Groups

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

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

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

Tasks performed by Functional Administrators and Directory Managers:

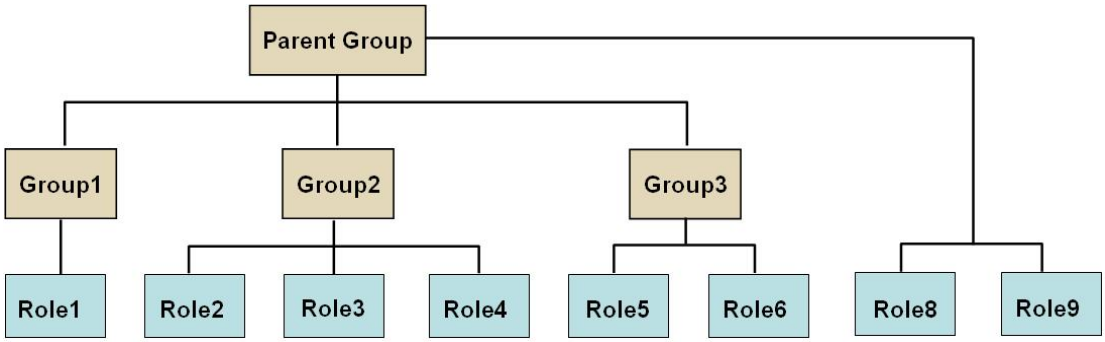
- Creating Groups
- Modifying Groups
- Deleting Groups
- Provisioning Users and Groups
- Deprovisioning Groups
- Generating Provisioning Reports

> **Note:**
>
> Groups on external user directories cannot be managed from Oracle Hyperion Shared Services Console.

Nested Groups

Nested groups are groups that are members of other groups (parent groups). You use nested groups to facilitate provisioning. Group members inherit the roles assigned to

the parent group. You can create nested groups in Native Directory using groups from any configured user directory. Using very complex nested groups is not recommended. The illustrated concept:



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

Creating Groups

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

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

To create Native Directory groups:

1. Access Oracle Hyperion Shared Services Console as a Functional Administrator or Directory Manager. See Launching Shared Services Console.
2. In the View pane, expand **Native Directory**.
3. Right-click **Groups**, and then select **New Group**.
4. In **Name**, enter a unique group name (maximum 256 characters).

   Group names are not case-sensitive.
5. **Optional:** Enter a group description.
6. Perform an action:
   - Click **Finish** to create the group without adding groups or users, and go to step 11.
   - Click **Next** to create a nested group or assign users to the group.
7. Create a nested group. To skip this step, click **Next**.
   a. Using the fields above **Available Groups**, search for the groups that you want to add as group members.
      i. In **Directory**, select the user directory from which you want to add the child group. Select **All** to search for groups in all configured user directories.
      ii. From the drop-down list, select **Group Name** to search based on group names. Select **Description** to search based on group descriptions.

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

iv. Click **Search**.

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

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

c. Click  .

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

d. **Optional:** To retrieve and assign additional groups, repeat step 7.a through 7.c.

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

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

8. Perform an action:

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

9. To assign users to the group:

a. Using the fields above the **Available Users** list, search for the users that you want to add as group members.

i. In **Directory**, select the user directory from which you want to add user members. Select **All** to search for users in all configured user directories.

ii. From the drop-down list, select **User Name** to search based on user names. Select **Description** to search based on user descriptions.

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

iv. Click **Search**.

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

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

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

d. **Optional:** To retrieve and assign additional users, repeat step 9.a through 9.c.

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

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

10. Click **Finish**.

11. Select **Create Another** to create another group or **Finish**.

Modifying Groups

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

To modify groups:

1. Access Oracle Hyperion Shared Services Console as a Functional Administrator or Directory Manager. See Launching Shared Services Console.
2. Search for a group. See Searching for Users, Groups, Roles, and Delegated Lists.
3. Right-click a group, and then select **Properties**.

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

4. On the **General** tab, edit the name and description to modify the general properties of the group.
5. Open the **Group Members** tab and perform the actions from either step 5.a, step 5.b, or from both, to modify group assignments:
   a. To add groups to the group:
      - In **Directory**, select the user directory from which you want to add the nested group. Select **All** to search for groups in all configured directories.
      - Select **Group Name** to search based on group names. Select **Description** to search based on group descriptions.
      - Enter the criterion for retrieving groups. Use * (asterisk) as the wildcard to retrieve all available groups.
      - Click **Search**.
      - From **Available Groups**, select groups and click  .

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

        Shared Services enables you to search the assigned groups to identify the groups to remove. Use the fields above the **Assigned Groups** list to define the search criteria for searching within the assigned groups list.
      - Click  .
6. Select the **User Members** tab, and then perform actions from either step 6.a, step 6.b, or from both, to modify user assignments:

a. To add users to group:
   - In **Directory**, select the user directory from which you want to add users. Select **All** to search for users in all configured directories.
   - Select the user property (**User Name**, **First Name**, **Last Name**, **Email Address**, or **Description**) to search.
   - Enter the criterion for retrieving users. Use * (asterisk) as the wildcard to retrieve all available users.
   - Click **Search**.
   - From **Available Users**, select users to assign to the group.
   - Click  .

     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  .

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

Deleting Groups

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

To delete groups:

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

Managing Roles

Roles define the tasks that users can perform in Oracle Enterprise Performance Management System applications. Roles from all registered EPM System applications

can be viewed but cannot be updated or deleted from Oracle Hyperion Shared Services Console. Functional Administrators and Provisioning Managers can perform these tasks:

- Creating Aggregated Roles
- Modifying Aggregated Roles
- Deleting Aggregated Roles
- Generating Provisioning Reports

> **Note:**
>
> You can provision newly created users and groups. However, the roles provisioned to the new users and groups become effective only after Oracle Hyperion Shared Services refreshes its cache. By default, the cache refresh interval is 60 minutes, which you can modify by updating the value of `Shared Services Security Cache Refresh Interval`. Setting this value to a shorter interval, for example, 30 minutes, may cause performance degradation.
>
> See Setting Security Options in the *Oracle Enterprise Performance Management System User Security Administration Guide*.

Creating Aggregated Roles

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

For information on aggregated roles, see Aggregated Roles.

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

To create aggregated roles:

1. Access Oracle Hyperion Shared Services Console as a Functional Administrator or Provisioning Manager. See Launching Shared Services Console.
2. In the **View pane**, expand **Native Directory**.
3. Right-click **Roles**, and then select **New Role**.
4. For **Name**, enter a role name (maximum 256 characters).

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

   See Using Special Characters 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 **Search** to retrieve all roles from the selected application.
   - Enter the role name in **Role Name**, and then click **Search** to search for a specific role. Use * (asterisk) as the wildcard in pattern searches.
9. From **Available Roles**, select the application roles to assign.
10. Click  .

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

    From **Assigned Roles**, select the role, and then click  to remove a selected role.
11. Click **Finish**.
12. Click **OK** to return the **Browse** tab or **Create Another** to create another custom role.

Modifying Aggregated Roles

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

To modify aggregated roles:

1. Access Oracle Hyperion Shared Services Console as a Functional Administrator or Provisioning Manager. See Launching Shared Services Console.
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.
5. Right-click the role, and then select **Properties**.
6. On the **General** tab, edit the name and description to modify general properties of the role.
7. To modify role member assignments, on **Role Members**, perform actions from step 7.a, step 7.b, or both:
   a. To add role members:
      - Retrieve the roles to add.
        - Click **Search** to retrieve all roles.
        - Enter the role name in **Role Name** and click **Search** to retrieve a specific role. Use * (asterisk) as the wildcard in pattern searches.
      - From **Available Roles**, select one or more.
      - Click  . The selected roles are listed under **Assigned Roles**.

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

b. To remove role assignments:

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

8. Click **OK**.

Deleting Aggregated Roles

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

To delete aggregated roles:

1. Access Oracle Hyperion Shared Services Console as a Functional Administrator or Provisioning Manager. See Launching Shared Services Console.
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.
5. Right-click a role, and then select **Delete**.
6. Click **Yes**.
7. Click **OK**.

Backing Up Native Directory

Native Directory is a part of the Oracle Hyperion 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

Related Topics

- About Provisioning
- Provisioning Users and Groups
- Deprovisioning Groups
- Auditing Security Activities and Lifecycle Management Artifacts
- Manually Purging Audit Data
- Selecting Objects for Application and Application Group-Level Audits
- Changing Purge Interval
- Generating Reports
- Importing and Exporting Native Directory Data

About Provisioning

Each organization has unique provisioning requirements. This section presents a typical flow for provisioning users and groups with Oracle Hyperion 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. Oracle Enterprise Performance Management 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 Oracle Enterprise Performance Management System products:
  - Understand the available roles. See Foundation Services Roles 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 Oracle Hyperion Planning artifact for which access rights can be set.
  - Configure the external user directories that contain accounts for EPM System users and groups. See 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 Delegated User Management.

Overview of Provisioning Steps

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

Provisioning users and groups should follow a provisioning plan tailored for your organization. Typically, you should create Functional Administrators and application-specific provisioning managers to provision Oracle Enterprise Performance Management 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 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 Oracle Hyperion 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 Oracle Hyperion Shared Services Console to assign the required Oracle Enterprise Performance Management System product administrator roles. For example, the Oracle Hyperion Planning Provisioning Manager role enables the recipient to provision users and groups with Planning roles. Other EPM System products have similar administrative roles. A Functional Administrator must assign these administrative roles to users and groups using the Shared Services Console.

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

Provisioning EPM System Users

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

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

   EPM System roles are described in EPM System Roles.

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

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

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

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

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

   a. In the View pane of Shared Services Console, expand **Application Groups**.
   b. Expand the application group node that contains the application.
   c. Right-click the application to provision.
   d. Select **Assign Access Control**. A product administration screen, which is not a part of Shared Services Console, opens.
   e. Provision users.

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

Provisioning Users and Groups

Provisioning is the process of granting Oracle Enterprise Performance Management System roles to users and groups. Provisioning is performed by Provisioning Managers or Functional Administrators by assigning EPM System application roles to a group. See Provisioning (Role-based Authorization).

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

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

To provision users or groups:

1. Access Oracle Hyperion Shared Services Console as a Functional Administrator or Provisioning Manager. See Launching Shared Services Console.
2. Find and select groups to provision. See Searching for Users, Groups, Roles, and Delegated Lists.

3. Select **Administration** and then **Provision**.
4. **Optional:** Select a view.

   Roles can be displayed in a hierarchy (tree) or a list. You must drill down the hierarchy to display available roles. The list view lists available roles but does not show their hierarchy.
5. Select roles, and then click  .
6. Click **OK**.

Deprovisioning Groups

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

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

To deprovision groups:

1. Access Oracle Hyperion Shared Services Console as a Functional Administrator or Provisioning Manager. See Launching Shared Services Console.
2. Find the group to deprovision. See Searching for Users, Groups, Roles, and Delegated Lists.
3. Right-click the group, and then select **Deprovision**.
4. Perform an action:
   - To remove role assignments from specific applications, make selections.
   - To remove all provisioned roles, select **Check All**.
5. Click **OK**.
6. In the confirmation dialog box, click **Yes**.
7. In the Deprovision Summary screen, click **OK**.

Auditing Security Activities and Lifecycle Management Artifacts

Oracle Hyperion 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 Oracle Hyperion Enterprise Performance Management System 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 Oracle Essbase, cannot be audited.

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

To change the auditing configuration:

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

Manually Purging Audit Data

Oracle Enterprise Performance Management System automatically removes audit data from the Oracle Hyperion Shared Services database based on the purge settings specified in Oracle Hyperion Shared Services Registry. Use this procedure to manually purge audit data.

> **Caution:**
>
> Functional Administrators must purge the data based on your company's audit data retention policies. Before purging data, back up the Shared Services database.

To purge audit data:

1. Access Oracle Hyperion Shared Services Console as a Functional Administrator. See Launching Shared Services Console.
2. Select **Administration** and then **Configure Auditing**.
3. In **Purge Data Older than**, set the number of days for which audit data is to be retained.
4. Click **OK**.

Selecting Objects for Application and Application Group-Level Audits

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

To select objects for auditing:

1. Access Oracle Hyperion Shared Services Console as a Functional Administrator. See Launching Shared Services Console.
2. In the View pane, right-click one of the following, and then select **Configure Auditing**:
   - An application group to enable auditing for all the applications in the application group
   - An application to enable auditing for the application

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

Changing Purge Interval

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

To modify the purge interval:

1. Start a command prompt on the Oracle Hyperion Foundation Services server host machine, and navigate to *`EPM_ORACLE_HOME`*`bin`; for example, `C:\Oracle\Middleware\user_projects\epmsystem1\bin` on a Windows server.
2. Use the following command to view the current purge interval:

   ```
   epmsys_registry.bat view SHARED_SERVICES_PRODUCT/
   @AUDIT.PURGE.EARLIERTO.DAYS
   ```

3. Use the following command to update the purge interval:

   ```
   epmsys_registry.bat updateproperty SHARED_SERVICES_PRODUCT/
   @AUDIT.PURGE.EARLIERTO.DAYS NEW_PURGE_INTERVAL
   ```

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

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

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

Generating Reports

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

- Generating Provisioning Reports
- Generating Audit Reports
- Generating Migration Status Report

Generating Provisioning Reports

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

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

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

To generate provisioning reports:

1. Access Shared Services Console as a Functional Administrator or Provisioning Manager. See Launching Shared Services Console.
2. Select a role. See Searching for Users, Groups, Roles, and Delegated Lists.
3. Select **Administration** and then **View Report**.
4. Enter report generation parameters.

Table 7-1 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.
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 Oracle Hyperion Enterprise Performance Management System Lifecycle Management.

Functional 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.

To generate audit reports:

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

   > **Note:**
   >
   > These reports are automatically generated to show the data for users for the last 30 days.

4. To regenerate the report, select parameters:
   a. In **Performed By**, select the users for which the report is to be generated.
   b. In **Performed During**, select the period for which the report is to be generated. You can set the period as number of days or as a date range.
   c. **Optional:** Select **Detailed View** to group the report data based on the attribute that was modified and the new attribute value.
   d. **Optional:** In **Per Page**, select the number of rows of data to display in a report page.
   e. Click **View Report**.
5. To create a CSV file containing the report data, click **Export**.

a. Select **Save as CSV**.

b. Click **OK**.

c. Click **Open** to open the file or **Save** to save the file to the file system. By default, the Security Report file is named `auditsecurityreport.csv`, the Artifact Report is named `AuditArtifactReport.csv`, and the Config Report is named `AuditConfigReport.csv`.

6. Click **Close**.

Generating Migration Status Report

The Migration Status Report contains information on the artifact migrations performed using the Oracle Hyperion Enterprise Performance Management System Lifecycle Management functionality. For each migration, this report presents information such as the user who performed the migration, source, destination, start time, completed time, duration, and status.

For failed migrations, you can view the information such as the source and destination applications, artifact path, artifact name, and error that cause the migration to fail.

To generate Migration Status Report:

1. Access Oracle Hyperion Shared Services Console as a Functional Administrator.
2. Select **Administration**, and then **Migration Status Report**.

   This report is automatically generated to show all migrations performed in the last 30 days.
3. To regenerate the report, click **Refresh**.
4. To close the report, click **Cancel**.

Importing and Exporting Native Directory Data

Use Oracle Hyperion Enterprise Performance Management System Lifecycle Management to perform the following tasks:

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

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

8
Managing Taskflows

Related Topics

- About Taskflows
- Taskflow Components
- Prerequisites for Working with Taskflows
- Creating and Managing Taskflows
- Viewing Taskflow Information
- Scheduling Taskflows
- Manually Running Taskflows
- Viewing Taskflow Status and Execution Details
- Taskflow Scripts Location

About Taskflows

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

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

Taskflow Components

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

Stages

A stage describes a step in a taskflow usually performed by one individual. Each stage has one application action or event in the taskflow. Actions can have parameters for which values are supplied at runtime.

Many default actions are available for each Oracle Enterprise Performance Management System component that uses taskflows. These actions are defined and managed by taskflow-enabled EPM System components. Oracle Hyperion Shared Services default actions are described in Table 1. See the *Oracle Hyperion Financial Management User's Guide* for a description of Oracle Hyperion Financial Management actions.

Table 8-1 Default Stage Actions and Parameters: Shared Services

Action	Parameters
Email [1]	This action automatically sends an email message. Complete these parameters for the email action: • To: Enter the recipient's email address • Subject: Enter a subject for the e-mail • Message: Select a variable (by double-clicking a variable from the variables list) to display success or failure • Variables: Lists the available variables for the email action
Execute	This action runs an external program from a command line. Complete these parameters for the execute action: Command: Enter a command to run an external program. The external program can be a valid command line script (such as a `.bat` script on Windows) and any valid program execution command. Ensure that your script file does not resolve the path dynamically; if the file uses any variables to resolve the path, it will not work. For example, to launch Internet Explorer, enter: `IEXPLORE.EXE`. See Taskflow Scripts Location.

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

Links

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

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

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

Variables

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

Prerequisites for Working with Taskflows

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

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

Creating and Managing Taskflows

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

Accessing the Manage Taskflow Screen

Typically, you use the Manage Task Flow screen to work with taskflows. This screen is accessible from Oracle Hyperion Financial Management and Oracle Hyperion Profitability and Cost Management. Generally, you require the following roles to access this screen:

- Manage Taskflow role of Oracle Hyperion Foundation Services
- Administrator role of the component (Financial Management or Profitability and Cost Management) from which you access this screen

To access Manage Task Flows screen:

1. Log into Oracle Hyperion Enterprise Performance Management Workspace.
2. To access Manage Task Flow screen from Financial Management:
   a. Select **Navigate**, and then **Administer**, and then **Consolidation Administration**.
   b. Select **Administration**, then **Taskflows**, and then **Manage Taskflows**.
3. To access Manage Task Flow screen from Profitability and Cost Management:
   a. Select **Navigate**, then **Applications**, then **Profitability**, and then a Profitability and Cost Management application.
   b. In **Task Areas**, expand **Job Status**, and then select **Manage Taskflows**.

Creating Taskflows

To create taskflows:

1. Open the Manage Task Flows screen. See Accessing the Manage Taskflow Screen.
2. In Manage Task Flows, click **New**.
3. In **Name**, enter a unique taskflow name.
4. In **Application**, enter the name of the application to which this taskflow belongs.

The application name is used to categorize applications in the Manage Taskflows screen.

5. For **Description**, enter a taskflow description.
6. Click **Submit**.

   The taskflow editor, which allows you to add stages and links, is displayed.
7. Add stages to the taskflow:
   a. On General, enter the following information:
      - **Name**: Enter a stage name.
      - **UserName**: Enter the Oracle Enterprise Performance Management System user whose account will be used to initiate the taskflow stage.
      - **Password**: Enter the password of the user identified in the UserName field.
   b. On Processing, enter the following information:
      i. In **Application**, select an application from which to run the task.
      ii. In **Action**, select an action to perform and then enter the required information.

      Actions available in **Actions** list reflect the selected application. For a list of actions for each EPM System component, see the following topics:
      - See Table 1 for a list of available Oracle Hyperion Shared Services actions.
      - See the *Oracle Hyperion Financial Management User's Guide* for a list of Oracle Hyperion Financial Management actions.
   c. On Starting Event, enter the following information to schedule an event:
      i. In **Starting Event**, select **Scheduled Event**.
      ii. In **Start Date**, enter the date on which the task is to be run.
      iii. In **Start Time**, select a time at which the task should start.
      iv. If this task is to be repeated, select the **Recurrence**, and in **Recurrence Pattern**, select the task frequency.
      v. Select an option for the task end date and time:
         - **No End Date**
         - **End After occurrences**, and enter the number of occurrences.
         - **End Date**, enter an end date, and then select an **End Time**.
   d. **Optional:** add more stages to the taskflow.
8. Add links to taskflow stages:
   a. Select the stage for which link is to be added, and then click **Add Link**.
   b. In General, enter a unique link name and an optional description.
   c. In **Receiving Stage** select the next stage in the taskflow.
   d. **Optional**: Set link conditions if needed.
9. Click **Save**.

Editing Taskflows

To edit taskflows:

1. Open the Manage Task Flows screen. See Accessing the Manage Taskflow Screen.
2. From Taskflow Listing Summary, select a taskflow, and then click **Edit**.

   The first stage of the task flow is selected by default.
3. In **Password**, enter the password of the Oracle Enterprise Performance Management System user whose account is used to initiate the taskflow stage.
4. Edit the current stage, if required, or select another stage by clicking the stage name.
   a. In General, complete these steps.
      i. **Optional**: Change the stage name and the EPM System user whose account is used to initiate the taskflow.
      ii. In **Password**, enter the password of the EPM System user whose account is used to initiate the current taskflow stage.
   b. In Processing, modify the following stage processing information. You can change the values in any field on this tab.
      - See Table 1 for a list of available Oracle Hyperion Shared Services actions.
      - See the *Oracle Hyperion Financial Management User's Guide* for a list of Oracle Hyperion Financial Management actions.
   c. In Starting Event, modify schedule for starting the stage.
   d. **Optional**: Modify links, if needed.

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

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

Viewing Taskflow Information

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

To view taskflow information:

1. Open the Manage Task Flows screen. See Accessing the Manage Taskflow Screen.
2. Select the taskflow that you want to view.

3. Click **Edit**.

Scheduling Taskflows

You can schedule taskflow execution from the Manage Taskflows screen.

To schedule an existing taskflow:

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

Manually Running Taskflows

To run a taskflow:

1. Open the Manage Taskflows screen. See Accessing the Manage Taskflow Screen.
2. Select the taskflow that you want to run.
3. Click **Run Now**.

Viewing Taskflow Status and Execution Details

Use the Taskflow Status Summary screen to monitor taskflow status.

To view taskflow status:

1. Log into Oracle Hyperion Enterprise Performance Management Workspace.
2. Select **Navigate**, and then **Application Library**.
3. Select **Administration**, and then **View Taskflow Status**.

4. In Manage Taskflows, select the search criteria to locate the taskflow that you want to monitor.
   - To search for taskflows in a specific execution status, in **Status**, select a taskflow status. Select **All** to search for taskflows in any status.
   - To search for taskflows belonging to a specific application, in **Application**, select the application to which the taskflow belongs.
   - To search for a specific taskflow, in **Taskflow**, select taskflow name.
5. To limit the search to a specific time period, set start and end values in values **Initiated Between**.
6. Click **Search**.
7. **Optional:** Click **Refresh** to update status information.
8. **Optional:** To end a running taskflow, select the taskflow, and then click **Stop**.

   The taskflow stops when the application returns the results of the selected step. The results for previous steps are not discarded; however, if the taskflow is rerun, it begins at the first step.
9. To view detailed taskflow execution details, click the taskflow ID.

   The Taskflow Participant Summary is displayed, showing details of the task and its status.
10. Click **Cancel** to return to Taskflow Status Summary.

Taskflow Scripts Location

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

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

```
epmsys_registry.bat updateproperty SHARED_SERVICES_PRODUCT/
@workflowEngine.ces.location SCRIPT_LOCATION
```

For example, you may run the following command:

```
epmsys_registry.bat updateproperty
 SHARED_SERVICES_PRODUCT/@workflowEngine.ces.location C:\taskflowscripts
```

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

Restart Oracle Enterprise Performance Management System after updating Shared Services Registry.

9
Provisioning Essbase

Related Topics

- Essbase Security Model
- Prerequisites
- Accessing EPM System Products
- Provisioning Process

Essbase Security Model

Oracle Essbase enforces two levels of roles: Essbase Server roles and Essbase application roles. These roles are granted and maintained through Oracle Hyperion 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 Oracle Hyperion 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

Foundation Services

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

  See Configuring User Directories.

Web Server

The Oracle Enterprise Performance Management System web server must be running.

Essbase Server

Oracle Essbase Server must be running. See the *Oracle Enterprise Performance Management System Installation and Configuration Guide*.

Administration Services

Oracle Essbase 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 Oracle Hyperion Shared Services if Oracle 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 added to the server, if they have been installed. You can use these applications to become familiar with the provisioning process if you do not want to create an application.

Accessing EPM System Products

You must access Oracle Enterprise Performance Management System components such as Oracle Hyperion Shared Services and Oracle Hyperion Enterprise Performance Management Workspace during provisioning. See the following topics:

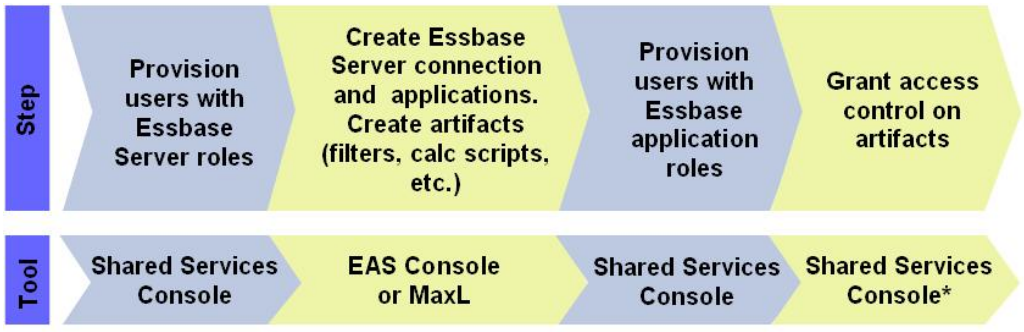
- Launching Shared Services Console
- Accessing EPM Workspace
- Accessing Administration Services Console

Provisioning Process

You can use Oracle Essbase Administration Services Console to create Oracle Essbase applications.

Essbase applications created through Administration Services Console are stand-alone applications that do not share dimensions and members with other applications.

The following illustration shows the steps involved in provisioning anEssbase application.



* Accesses Essbase Application

Provisioning Users and Groups with Essbase Server Roles

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

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

To provision users with Essbase server roles:

1. Log in to Oracle Hyperion Shared Services Console as a Functional Administrator. See Launching Shared Services Console.
2. From a configured user directory, find the user or group to provision. See Searching for Users, Groups, Roles, and Delegated Lists.
3. Provision the user or group with an Essbase Server role.
   a. Right-click the user or group, and then select **Provision**.
   b. **Optional:** Select a view.

      Roles can be displayed in a hierarchy (tree) or a list. You must drill down the hierarchy to display available roles. The list view lists available roles but does not show their hierarchy.
   c. In Available Roles, expand the Essbase node; for example, `EssbaseCluster-1`.
   d. In the Essbase node, expand the node that represents the Essbase Server; for example, `EssbaseCluster-1`.
   e. Select Essbase Server roles and click  .

      See Essbase Roles for description of Essbase Server roles.
   f. Click **OK**.
   g. Click **OK** to close the confirmation screen.

Creating Essbase Server Connection

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

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

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

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

To create an Essbase Server connection:

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

Creating Classic Essbase Applications

Each Oracle Essbase server can support multiple applications, each with its own database. The Essbase application that you create is automatically registered with Oracle Hyperion 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 Oracle Essbase Administration Services Console as a Functional Administrator.

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

2. Create an Essbase application.

> **Note:**
>
> Oracle Enterprise Performance Management System automatically assigns Provisioning Manager and Application Manager roles to the user who creates the Essbase application.

   a. Under **Essbase Servers**, right-click **Applications**.
   b. Select **Create application**, and then either **Using aggregate storage** or **Using block storage**.
   c. Enter required information. Consult online help for assistance.
3. Add a database for the application.
   a. Right-click the application that you created, and then select **Create database**.
   b. Enter the required information. Consult online help for assistance.
4. Add dimensions and members to the outline.
   a. Expand the node representing the application database you created.
   b. Right-click **Outline**, and then select **Edit**.
   c. On the Outline tab, right-click **Outline**, and then select **Add child**.

d. Enter member name. Click **Help** for assistance.

e. Click **Verify** to validate the outline.

f. Add additional members by repeating step 4.c–step 4.e.

g. Click **Save**.

h. Click **Close**.

Creating Essbase Artifacts

You must create filters and calculation scripts in the Oracle 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 Oracle Essbase 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 Oracle 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 Oracle Essbase Administration Services Console as a Functional Administrator or as a user provisioned with the Essbase Administrator role. See Accessing Administration Services Console.
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 Oracle Essbase users and groups.

To create a calculation script:

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

Provisioning Users with Essbase Application Roles

Each Oracle 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 Oracle Hyperion Shared Services Console as a Functional Administrator. See Launching Shared Services Console.

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

2. Find a user or group to provision.

   See Searching for Users, Groups, Roles, and Delegated Lists.

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  .

   See Essbase Roles for a list of Essbase application roles and their embedded permissions.

8. Click **OK**.
9. Click **OK**.
10. **Optional:** Repeat step 2—step 8 to provision other users with roles from this Essbase application.
11. **Optional:** Repeat step 6—step 9 to provision the selected user with roles from other Essbase applications belonging to this Essbase Server.

Defining Access Controls

Oracle 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 Oracle Hyperion Shared Services Console as a Functional Administrator. See Launching Shared Services Console.
2. In the View Pane, expand **Application Groups**, and then expand the Essbase server node; for example, `EssbaseCluster-1`.
3. Right-click the Essbase application for which artifact access permissions are to be set, and then select **Assign Access Control**.

   The Application tab opens. By default, this tab lists the users who are provisioned with roles belonging to this Essbase application. You can list all users and groups or only available groups.
4. Select the users and groups for which artifact access controls are to be set and move them to the selected list.
5. Click **Next**.
6. Select the users who should receive access to artifacts.
7. From **Filter**, select the database security filter to which the users should be granted access.
8. From **Calc**, select the calculation script that the selected users can access.
9. Select the check mark next to **Calc**.
10. Repeat step 7–step 9 to assign access to more filters and calculation scripts.
11. Click **OK**.

10

Provisioning Planning

Related Topics

- Planning Security Model
- Prerequisites
- Accessing EPM System Products
- Planning Provisioning Process

Planning Security Model

Oracle Hyperion Planning enforces two types of roles: Planning global roles and Planning application roles. All Planning roles are granted using Oracle Hyperion 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

Foundation Services

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

  See Configuring User Directories.

Web Server

The Oracle Enterprise Performance Management System web server must be running.

Essbase Server

Oracle Essbase Server is running.

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

Administration Services (Optional)

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

Administration Services is running.

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

Relational Database

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

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

Accessing EPM System Products

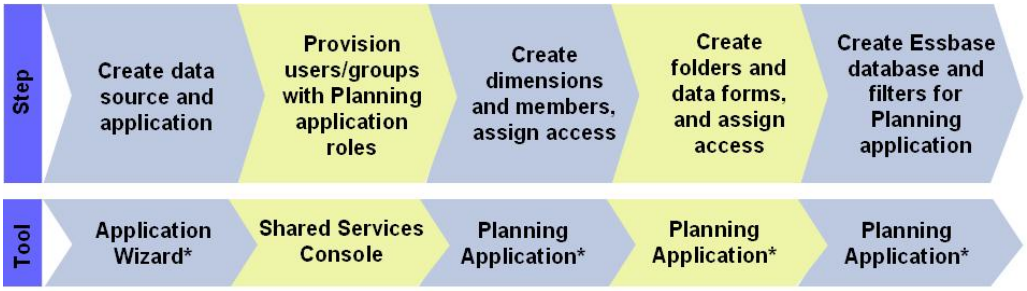
You must access Oracle Enterprise Performance Management System components such as Oracle Hyperion Shared Services and Oracle Hyperion Enterprise Performance Management Workspace during provisioning. See the following topics:

- Launching Shared Services Console
- Accessing EPM Workspace
- Accessing Administration Services Console

Planning Provisioning Process

Oracle Hyperion Planning applications are stand-alone applications that do not share dimensions and members with other Planning applications. These applications are created using the Application Wizard.

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



* Accessed through EPM Workspace

Creating Planning Data Source

Each Oracle Hyperion Planning application requires a unique data source, which comprises connection information for a Planning application database and an Oracle 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.

To create a data source:

1. Access Oracle Hyperion Enterprise Performance Management Workspace as a Functional Administrator. See Accessing EPM Workspace.
2. Select **Navigate**, then **Administer**, and then **Planning & Budgeting Service**.
3. In Planning Administration, click **Manage Data Source**.
4. From **Actions** in **Manage Data Source**, select **Create**.
5. In **Data Source Name**, enter a name.
6. From **Database**, select the database type for the Planning application database.
7. Enter connection information for application database and Essbase server. Ensure that you enter information for an Essbase Server administrator (or Functional Administrator) in Essbase Server settings. Consult online help for assistance.
8. Click **Validate** to validate the Application Database Connection and the Essbase Server Connection.
9. Click **Save** to create the data source.

Creating Planning Applications with Dimensions and Members

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

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

- Creating Planning Applications
- Accessing Planning Applications
- Creating Dimensions and Members

Creating Planning Applications

To create an application:

1. Access Oracle Hyperion Enterprise Performance Management Workspace as a Functional Administrator. See Accessing EPM Workspace.
2. Select **Navigate**, then **Administer**, and then **Planning and Budgeting Service**.
3. In Planning Administration, click **Manage Applications**.
4. From **Actions** in **Manage Applications**, select **Create**.
5. In **Data Source**, select a data source.
6. In **Application**, enter an application name (maximum eight characters). Application names should not contain special characters (for example, a space or an asterisk).

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

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

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

   Oracle Enterprise Performance Management System does not create a default Planning application group. You can create it as a custom group inOracle Hyperion Shared Services Console if needed. See Creating Application Groups.

9. Click **Next**.

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

11. Click **Create** to create the Planning application.

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

Accessing Planning Applications

To open your Oracle Hyperion Planning application:

1. Access Oracle Hyperion Enterprise Performance Management Workspace. See Accessing EPM Workspace.
2. Select **File**, then **Open**, then **Applications**, and then **Planning**.
3. Select the Planning application that you created.

Creating Dimensions and Members

When you create a Oracle Hyperion 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.
2. Select **Administration**, then **Manage**, and then **Dimensions**.
3. **Optional**: Add a custom dimension.

   a. On **Dimensions**, click  .

   b. Enter a dimension name and other required values. Consult online help for assistance.

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

c. Click **Save**.

   Custom dimensions that you create in Planning are not automatically written to the Oracle Essbase database. See Working with Essbase Database.

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 for instructions.

Provisioning Users and Groups with Planning Application Roles

Each Oracle Hyperion Planning deployment can support multiple Planning applications. You must provision Planning users separately to each application.

Functional Administrator and Planning Provisioning Managers can provision Planning application users using the Oracle Hyperion Shared Services Console.

To provision users or groups with Planning application roles:

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

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.

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

   c. **Optional:** Select a view.

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

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

   e. Expand the node that represents your application.

   f. Select roles and click **Add**.

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

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

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

To populate users and groups in the Planning database:

1. Access Oracle Hyperion Enterprise Performance Management Workspace. See Accessing EPM Workspace.
2. Open the Planning application. See Accessing Planning Applications.
3. Select **Administration**, then **Application**, and then **Refresh Database**.
4. Select **Security Filters**.
5. Optionally select other database refresh options. See the *Oracle Hyperion Planning Administrator's Guide*.
6. Click **Refresh**.
7. Click **Finish**.

Assigning Access for Dimension Members

Application dimensions can be protected by defining the users and groups that can access them. Access control can be defined for members of secure dimensions (default dimensions other than Currency, Period, and Year).

Only the custom dimensions that were created with the **Apply Security** option support the assigning of access control to members.

To define access control:

1. Access Oracle Hyperion Enterprise Performance Management Workspace. See Accessing EPM Workspace.
2. Open the Oracle Hyperion Planning application. See Accessing Planning Applications.

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

   You can add members from this screen.

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

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

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

Working with Data Forms

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

Creating Data Form Folders

To create data form folders:

1. Access Oracle Hyperion Enterprise Performance Management Workspace. See Accessing EPM Workspace.
2. Open a Oracle Hyperion Planning application. See Accessing Planning Applications.
3. Select **Administration**, then **Manage**, and then **Forms and Ad Hoc Grids**.
4. Expand a folder in **Form Folders**, and then click  .
5. Enter a folder name.
6. Click **OK**.

Creating Data Forms

Because composite data forms are comprised on simple data forms, you must create simple data forms before creating composite data forms. Composite data forms display many data forms simultaneously, including those associated with different plan types. Users can enter

data and see results aggregated to an upper-level intersection, such as Total Revenue. Some tasks for creating composite data forms are the same as for regular data forms.

To create data forms:

1. Access Oracle Hyperion Enterprise Performance Management Workspace. See Accessing EPM Workspace.
2. Open a Oracle Hyperion Planning application. See Accessing Planning Applications.
3. Select **Administration**, then **Manage**, and then **Forms and Ad Hoc Grids**.
4. To create a data form, select an option from **Actions**:
   - Select **Create simple form** to create a simple data form.
   - Select **Create composite form** to create a composite data form.
5. Define form properties, layout and business rules. Consult online help for assistance.

Granting Access to Data Form Folders

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

To grant access to data form folders:

1. Access Oracle Hyperion Enterprise Performance Management Workspace. See Accessing EPM Workspace.
2. Open a Oracle Hyperion Planning application. See Accessing Planning Applications.
3. Select **Administration**, then **Manage**, and then **Forms and Ad Hoc Grids**.
4. Select a folder.
5. Click  .
6. Click  .
7. Select the users and groups that are to be granted access to the folder.

> **Note:**
>
> Only the users and groups provisioned to the current application, but have not been granted access to folder, are listed on the Add Access screen.

8. Select the type of access (**Read**, **Write**, or **None**) to grant.
9. Click **Add**.
10. Click **OK**.
11. In the Add Access window, click **Close**.
12. In the Assign Access window, click**Close**.

Granting Access to Data Forms

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

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

To grant access to data forms:

1. Open a Oracle Hyperion Planning application. See Accessing Planning Applications.
2. Select **Administration**, then **Manage**, and then **Forms and Ad Hoc Grids**.
3. Select the folder that contains the form to which access is to be granted.
4. In **Forms and Ad Hoc Grid Management**, select a form.
5. Click 
6. In Assign Access window, click  .
7. Select the users or groups that are to be granted access to the form.

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

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

Working with Task Lists

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

Creating Task List Folders

To create task list folders:

1. Open a Oracle Hyperion Planning application. See Accessing Planning Applications.
2. Select **Administration**, then **Manage**, and then **Task Lists**.
3. In **Manage Task Lists**, select a task list folder, and then click  .
4. Enter a folder name.
5. Click **OK**.

Creating Task Lists

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

To create task lists:

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

Creating Tasks

To create a task:

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

Granting Access to Task Lists

To grant access to task lists:

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

> **Note:**
>
> Only the users and groups provisioned to the current application, but do not have access to the task list, are listed on the Add Access window.

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

Working with Essbase Database

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

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

To work with the Essbase database:

1. Open the Planning application. See Accessing Planning Applications.
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 Oracle Essbase 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 Oracle Hyperion Planning applications are placed in maintenance mode, which permits only Planning administrators to access them.

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

To put Planning applications in production mode:

1. Open the Planning application. See Accessing Planning Applications.
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 Oracle Hyperion Shared Services Console, you can view current access permissions and print reports.

To generate access control report:

1. Open the Planning application.
2. Navigate: Tools.
3. Select **Reports**, and then click the **Access Control** tab.
4. Select the following for which the report is to be generated:
   - Users or groups
   - Application objects
5. Set report settings. Consult online help for assistance.
6. Click **Finish**.

11

Provisioning Financial Management

Related Topics

- Financial Management Security Model
- Prerequisites
- Accessing EPM System Products
- Financial Management Provisioning Process

Financial Management Security Model

Oracle Hyperion Financial Management roles are assigned to users from the Oracle Hyperion 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

Foundation Services

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

  See Configuring User Directories.

Web Server

The web server that front-ends Oracle Enterprise Performance Management System components must be running.

Relational Database

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

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

Accessing EPM System Products

You must access Oracle Enterprise Performance Management System components such as Oracle Hyperion Shared Services and Oracle Hyperion Enterprise Performance Management Workspace during provisioning. See the following topics:

- Launching Shared Services Console
- Accessing EPM Workspace
- Accessing Administration Services Console

Financial Management Provisioning Process

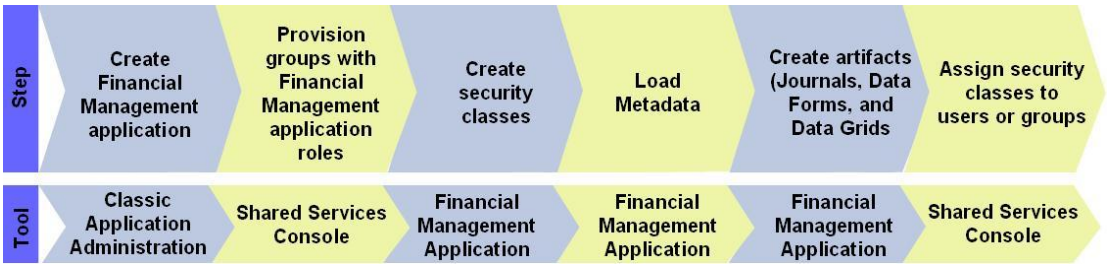
You can use the Application Administration Console and the Oracle Hyperion Financial Management Desktop to create Financial Management applications. Application Administration Console is accessed through Oracle Hyperion Enterprise Performance Management Workspace.

Financial Management applications created through the Application Administration Console and Financial Management Desktop are stand-alone applications with their own profiles that define their calendar and the languages. Each application has its own metadata file that defines its dimensions. These applications do not share dimensions and members with other Financial Management applications.

Financial Management applications require that you create a security class before you can load or deploy metadata using that security class. You can create or load security classes after you create the application.

Process Overview

The steps involved in creating and provisioning Oracle Hyperion Financial Management applications using the Consolidation Administration menu option in Oracle Hyperion Enterprise Performance Management Workspace are depicted in the following illustration:



Creating Applications

Creating Oracle Hyperion Financial Management applications involves these steps:

- Creating Application Profiles
- Creating Financial Management Applications

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. See "Creating Application Profiles" in the *Oracle Hyperion Financial Management Administrator's Guide* for detailed information.

To create application profiles:

1. Access Oracle Hyperion Enterprise Performance Management Workspace. See Accessing EPM Workspace.
2. Select **Navigate**, then **Administer**, and then **Consolidation Administration**.
3. In Consolidation Administration, select **Profile Editor**.
4. In Select Profile, select **Create a New Application Profile**, and then click **OK**.
5. 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.
6. Click **Save**.
7. Select a file format, and then click **OK**.
8. Click **Save File** to download application profile into the default download directory specified in your browser.

Creating a Data Source

You must set up a data source name (DSN) to store star schemas. See "Configuring a Data Source Name (DSN)" in the *Oracle Hyperion Financial Management Administrator's Guide* for details.

To create a data source:

1. Access Oracle Hyperion Enterprise Performance Management Workspace. See Accessing EPM Workspace.
2. Select **Navigate**, then **Administer**, and then **Consolidation Administration**.
3. In Consolidation Administration, select **Configure DSN**.
4. In Configure DSN, click **Actions**, and then select **Create Data Source**.
5. Enter settings to create a data source. See "Configuring a Data Source Name (DSN)" in *Oracle Hyperion Financial Management Administrator's Guide* for details.
6. Click **Test Connection** to ensure that the data source properties that you set are valid.
7. Click **Save**.

Creating Financial Management Applications

Oracle Hyperion Financial Management applications are created using the Consolidation Administration menu option in Oracle Hyperion Enterprise Performance Management Workspace.

To create Financial Management applications:

1. Access EPM Workspace. See Accessing EPM Workspace.
2. Select **Navigate**, then **Administer**, and then **Consolidation Administration**.
3. In Consolidation Administration, select **Application**.
4. From Applications, select **Actions**, and then **New**.
5. Enter information.
    a. In **Cluster**, select the serverFinancial Management cluster on which to run the application.
    b. In **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 (*).
    c. In **Description** enter an application description.
    d. In **Profile**, select the profile that you want to use for this application. See Creating Application Profiles.
    e. In **User Management Project**, select an existing Oracle Hyperion Shared Services application group to which the application should be added.

       You can create a custom application group in Shared Services if needed.
    f. In **Application Type**, select **Consolidation** or **Tax Provisioning** as the application type.
6. Click **Create**.

> **Note:**
>
> The Financial Management application that you create is listed in Oracle Hyperion Shared Services Console under the node representing the application group that you selected in step 5.e.

Provisioning Groups with Financial Management Application Roles

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

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

To provision users or groups with Financial Management application roles:

1. Access Shared Services Console as a Functional Administrator or as a user provisioned with the Provisioning Manager role for the Financial Management application that you want to provision. See Launching Shared Services Console.
2. Provision users or groups to the Financial Management application.
   a. Find a user or group to provision.
   b. Right-click the user or group, and then select **Provision**.
   c. **Optional:** Select a view.

      Roles can be displayed in a hierarchy (tree) or a list. You must drill down the hierarchy to display available roles. The list view lists available roles but does not show their hierarchy.
   d. In **Available Roles**, expand the application group (for example, Financial Management) that contains your Financial Management application.
   e. Expand the node that represents your application.
   f. Select the roles that you want to assign to the users or groups, and click  .

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

Provisioning Managers and Oracle Hyperion Shared Services Administrators can define security classes for applications at any time. They can also load security classes from a

security (`.sec`) file. See "Loading Application Security" in the *Oracle Hyperion Financial Management Administrator's Guide*.

Provisioning Managers and Shared Services Administrators can define security classes for applications at any time. They can also load security classes for Oracle Hyperion Financial Management application from a security (`.sec`) file. See "Loading Application Security" in the *Oracle Hyperion Financial Management Administrator's Guide*.

Creating Financial Management Artifacts

Oracle Hyperion 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 Oracle Hyperion Financial Management application. If necessary, you can edit the file before loading it into your Financial Management application.

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

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

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

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

To load journals:

1. Open a Financial Management application.
2. Expand **Application Tasks**, and then select **Load**, and then **Journals**.

3. In **Journal File**, enter the file name to load, or click **Browse** and find the file to load.
4. In **Delimiter Character**, specify the character that is used to separate information in the file.
5. Specify other settings as needed. Consult online help for assistance.
6. Click **Load**.

Creating Data Forms

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

- Using a script
- Using the Form Builder

See the *Oracle Hyperion Financial Management Administrator's Guide* for the data form script syntax.

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

To create data forms using the Form Builder:

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

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

Creating Data Grids

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

To create data grids:

1. Open a Financial Management application.
2. In Document Manager, select **New**, and then **Data Grids**.
3. Click **New Data Grid**.

4. Enter POV information, Row and Column information, and grid display options. Consult Online Help for assistance.
5. Select **Actions**, and then **Save**.
6. Specify the data grid name, description, security class and location, and the directory in which to store it.

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

Provisioning Security Classes

Security classes determine the access that users have to Oracle Hyperion 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 Oracle Hyperion Shared Services Console as Oracle Hyperion 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.
2. In the View Pane, perform these steps:
   a. Expand **Application Groups**.
   b. Expand the application group that contains your Financial Management application.
   c. Right-click the Financial Management application for which security roles access is to be set, and then select **Assign Access Control**.

      Users and groups that are provisioned with roles from the selected application, along with their current security class assignments, are listed on **Applications**. Security classes can be assigned to these users and groups only.
3. **Optional:** Add security classes for classic applications.
   a. From **Actions**, select **Add Security Classes**.
   b. In **Class Name**, enter a name for the new security class.
   c. Click **OK**.
4. On **Application**, set the access right each user or group has to each security class. By default, no access right is granted to nely provisioned application users and groups. Consult online help for assistance.

- To change all the security class access assignment of one user or group, right-click the user or group name and then select an access level.
- To set the same all the security class access assignment levels for many users and group, while holding down the control key, right-click the user or group names and then select an access level.
- To change the access level for one security class, right-click the cell that lists the access level and then select a level.

Available access levels are explained in Table 1.

Table 11-1 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.
All	User can modify data for elements assigned to the security class and promote and reject.

5. From **Actions**, select **Save**.
6. **Optional:** Select **Actions** and then Security Reports to generate a Security Report to verify that the security classes are properly assigned to provisioned users and groups.

12

Provisioning Financial Reporting (Document Repository)

Related Topics

- Financial Reporting Security Model
- Prerequisites
- Accessing EPM System Products
- Provisioning Process

Financial Reporting Security Model

Oracle Hyperion Financial Reporting roles are assigned to users from the Oracle Hyperion Shared Services Console.Usually, access privileges on artifacts are assigned to groups of users.

Financial Reporting require you to access data from a data source (for example, Planning and Oracle Hyperion Financial Management) to create meaningful reports. Because the data that Financial Reporting access is owned by the data source, a provisioning interdependency exists between the data source and Financial Reporting. For example, assume that user *JDoe* is provisioned with Financial Reporting roles but is not provisioned for Planning application *Vision*. In this scenario, *JDoe* cannot view Financial Reporting reports that contain data from *Vision*.

Prerequisites

Financial ReportingComponents

The Oracle Financial Reporting Java Web Application must be running.

Access to Data Source

Oracle Hyperion Financial Reporting users and groups must be provisioned with data source roles that allow them to access data. Data sources include Oracle Hyperion Planning and Oracle Hyperion Financial Management applications.

Planning (Optional)

If you are using a Oracle Hyperion Planning application as the data source for Oracle Hyperion Financial Reporting, ensure that the following are running:

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

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

Financial Management (Optional)

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

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

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

Accessing EPM System Products

You must access Oracle Enterprise Performance Management System components such as Oracle Hyperion Shared Services and Oracle Hyperion Enterprise Performance Management Workspace during provisioning. See the following topics:

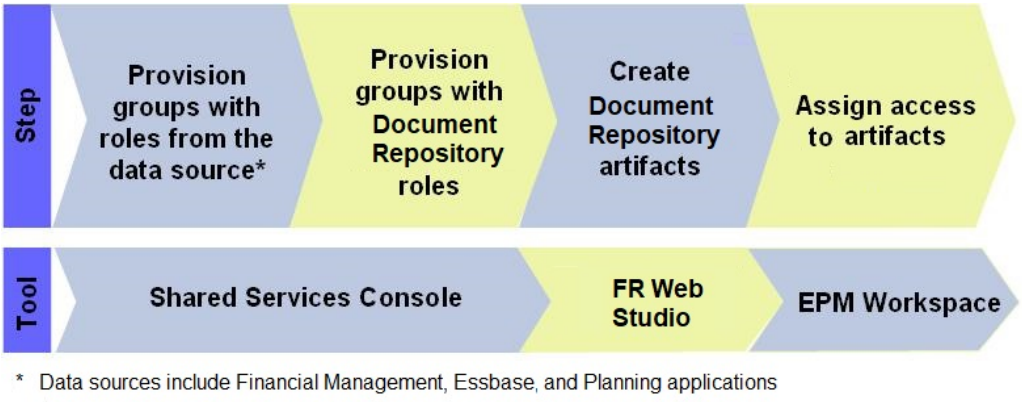
- Launching Shared Services Console
- Accessing EPM Workspace
- Accessing Administration Services Console

Provisioning Process

The Security Administrator Document Repository roles must be granted to the Functional Administrator to facilitate provisioning:

Process Overview

The steps involved in provisioning Document Repository users and groups are depicted in the following illustration.



Provisioning Steps

Provisioning the Data Source

Data sources for the Oracle Hyperion Financial Reporting includes Oracle Hyperion Planning and Oracle Hyperion Financial Management applications. Financial Reporting 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 Planning or Financial Management applications. For detailed provisioning steps, see:

- Provisioning Planning
- Provisioning Financial Management

Provisioning Users and Groups withDocument Repository Roles

Document Repository roles allow users to access the Oracle Hyperion Financial Reporting Web Studio and Oracle Hyperion Financial Reporting. The data that users can view and analyze using Financial Reporting Web Studio and reports is controlled by the roles that they have in the data source. Users can view Oracle Hyperion 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 Document Repository roles:

1. Access Oracle Hyperion Shared Services Console as Security Administrator. See Accessing Shared Services.
2. Provision users or groups.
   a. Find users or groups to provision.

      See Searching for Users, Groups, Roles, and Delegated Lists.
   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 theDocument Repository application group.
   e. Select the roles that you want to assign to the users or groups, and click **Add**.

      See Financial Reporting (Document Repository) Roles for information on the roles that you can assign to users and groups.
   f. Click **Save**.
   g. Click **OK**.

Creating Financial Reporting Artifacts in Document Repository

Document Repository artifacts include reports, books and batches, and the directories that store them. Each artifact can be separately provisioned. You use Oracle Hyperion Financial Reporting Web Studio to create reports and the Oracle Hyperion Enterprise Performance Management Workspace to create books and batches.

See the *Oracle Hyperion Financial Reporting Studio User's Guide* for instructions on creating artifacts.

Controlling Access to Artifacts

Oracle Hyperion Financial Reporting artifacts in the Document Repository are available to users after they are granted access to the artifacts by a Security Administrator.

To set access control:

1. Access Oracle Hyperion Enterprise Performance Management Workspace as a Document Repository Security Administrator. See Accessing EPM Workspace.
2. Select **Navigate**, and then **Explore**.
3. From **Folders**, select the folder where Financial Reporting 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**, find the user, group, or role for which you want to specify access to the artifact and then click  (**Add**).
7. In **Selected Users, Groups and Roles** pane:
   a. Click in the **Access to File** column and select an access privilege.

      The level and type of access that you can set changes depending on the selected artifact. For example, for artifacts of type Plain Text, access levels include Inherit, Full Control, Modify, View, and No Access. Consult online help for assistance.

   b. Click in the **Favorite** column and select whether the artifact is to be pushed as a favorite for the current user, group or role.
8. Click **OK**.

13

Provisioning Profitability and Cost Management

Related Topics

- Standard Profitability and Cost Management Security Model
- Prerequisites
- Accessing EPM System Products
- Profitability and Cost Management Provisioning Process

Standard Profitability and Cost Management Security Model

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

Prerequisites

Foundation Services

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

  See Configuring User Directories.

Foundation Services Web Server

Oracle Hyperion Foundation Services web server must be running.

Essbase Server (for Standard Profitability Only)

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

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

Administration Services

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

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

Relational Databases (for Detailed Profitability)

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

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

Accessing EPM System Products

You must access Oracle Enterprise Performance Management System components such as Oracle Hyperion Shared Services and Oracle Hyperion Enterprise Performance Management Workspace during provisioning. See the following topics:

- Launching Shared Services Console
- Accessing EPM Workspace
- Accessing Administration Services Console

Profitability and Cost Management Provisioning Process

You create Oracle Hyperion Profitability and Cost Management applications using a Wizard

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

Creating and Deploying Profitability and Cost Management Applications

You can create two types of Oracle Hyperion Profitability and Cost Management applications—Standard and Detailed. For information on these application types, see the *Oracle Hyperion Profitability and Cost Management User's Guide*.

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

Creating and Deploying Standard Profitability Applications

Standard Oracle Hyperion Profitability and Cost Management must abide by these conditions:

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

To create Standard Profitability and Cost Management applications:

1. Access Oracle Hyperion Enterprise Performance Management Workspace. See Accessing EPM Workspace.
2. Select **Navigate**, then **Administer**, and then **New Application**.
3. In **Name**, enter an application name (maximum seven characters). Application names should not contain special characters (for example, a space or an asterisk).
4. In **Type**, select **Profitability**.

> **Note:**
>
> You can create an empty application, into which you can import metadata. To create an application outline, select **Create Blank Application**, and then click **Finish**.

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

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

6. Click **Next**.

7. In the Dimension Selection window, choose the dimensions for the application. You must select the required default dimensions as local dimensions:

   - Measures
   - AllocationType
   - POV (At least one and up to four POV dimensions may be included)
   - At least one Business dimension
   - Alias (optional)
   - Attribute (optional)

   To create the dimensions for the application:

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

   b. Enter a dimension name and an optional description.

   c. Click **OK**.

8. Click **Next** to create the application.

9. 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**.

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

11. Click **Finish**.

12. Deploy the application. The deployment process registers the application with Oracle Hyperion 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**.

Creating and Deploying Detailed Profitability Applications

Detailed Oracle Hyperion Profitability and Cost Management must abide by these conditions:

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

To create Detailed Profitability and Cost Management applications:

1. Create dimensions by performing a flat file import.

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

2. Access Oracle Hyperion Enterprise Performance Management Workspace. See Accessing EPM Workspace.
3. Select **Navigate**, then **Administer**, and then **Create New 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 import metadata. To create an empty application, select **Create Blank Application**, and then click **Finish**.

6. **Optional:** Under **Description**, enter a description.
7. **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.
8. Under **Profitability**, click **Create as Detailed Application**.
9. Click **Next**.
10. In the **Dimension Selection** window, choose the dimensions for the application. You must select the required default dimensions as local dimensions:

- MeasuresDetailed (Required)
- At least one Business Dimension (Required)
- Alias Dimension (Optional)
- Attribute Dimensions (Optional)

To create the dimensions for the application:

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

b. Enter a dimension name and an optional description.

c. Click **OK**.

11. Click **Next** to create the application.
12. In Application Settings window, do the following tasks as outlined in the *Oracle Hyperion Profitability and Cost Management Administrator's Guide*.
    a. Set the Dimension Sort Order for all model dimensions.
    b. Reorder the `NoMember` to display this member as the last generation 2 member on the list.
    c. Set the Properties for POV Dimensions, and the POV Display Order for multiple POV dimensions, if required.
    d. Select `Deploy when finished`. This selection launches the Deploy window when you click **Finish**.
13. Click **Validate** and correct reported errors. You can find detailed validation information in the Library Job Console. To open the Library Job Console, select **Navigate**, then **Administer**, and then **Library Job Console**. See the *Oracle Hyperion Profitability and Cost Management Administrator's Guide* for a list of validations.
14. Click **Finish**.
15. Deploy the application. The deployment process registers the application with Oracle Hyperion 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**.

Deploying Standard Profitability and Cost Management Applications to Essbase

You must do the following tasks before you can deploy Standard Oracle Hyperion Profitability and Cost Management application to Oracle Essbase. When you deploy Standard Profitability to Essbase, you use the model information from the application to create an Essbase database that can be fine-tuned for profitability and cost analysis without needing to understand a scripting language.

Standard Profitability and Cost Management model design contains the information needed to generate Essbase outline and the calculation script required by the Essbase component of the model. Each model requires access to the following databases:

- A relational database to store the model design

- An Essbase database that includes a Calculation database (BSO) and a Reporting database (ASO).

> **Note:**
>
> Multiple models can be stored in a database.

Deploying Standard Profitability and Cost Management applications to Essbase involves these tasks:

- Adding Stages to the Application
- Adding POV to the Application

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

Adding Stages to the Application

Standard Oracle Hyperion 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 Oracle Essbase.

> **Note:**
>
> You can import model stage data into Standard Profitability and Cost Management. See the *Oracle Hyperion Profitability and Cost Management Administrator's Guide*.

To add stages:

1. Open a Standard Profitability and Cost Management application.
   a. Access Oracle Hyperion Enterprise Performance Management Workspace. See Accessing EPM Workspace.
   b. From EPM Workspace, select **File**, then **Open**, then **Applications**, and then **Profitability**.
   c. Select the Standard Profitability and Cost Management application that you created.
2. From **Manage Model** in the View pane, select **Stages**.
3. Click the Add icon above the Stage list.
4. Enter required stage information. Consult online help for assistance.
5. Click **OK**.

Adding POV to the Application

POVs are used to create various versions of a model; for example, to hold budget versus actual figures, or to play scenarios to measure the impact of various changes on the bottom line. You add a POV to view information and calculation for a model for the select year,

period, scenario, or status. Newly deployed applications do not contain POV manager definitions.

> **Note:**
>
> You can import model stage data into Standard Oracle Hyperion Profitability and Cost Management. See the *Oracle Hyperion Profitability and Cost Management Administrator's Guide*.

To add POV managers:

1. Open the Standard Profitability and Cost Management application.
   a. Access Oracle Hyperion Enterprise Performance Management Workspace. See Accessing EPM Workspace.
   b. From EPM Workspace, select **File**, then **Open**, then **Applications**, and then **Profitability**.
   c. Select the Standard Profitability and Cost Management application that you created.
2. From **Manage Model** in the View pane, select **POV Manager**.
3. Click **Add**.
4. Enter required POV information. Consult online help for assistance.
5. Click **OK**.

Provisioning Users and Groups with Profitability and Cost Management Roles

Each Standard Oracle Hyperion Profitability and Cost Management instance (deployment) can support multiple applications. You must provision Standard Profitability and Cost Management users separately to each application.

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

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

1. Access Shared Services Console as a Functional Administrator or as a user provisioned with the Provisioning Manager role of the Profitability and Cost Management application that you want to provision. See Accessing Shared Services.
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.
   b. Right-click the user or group, and select **Provision**.
   c. **Optional:** Select a view.

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

e. Expand the node that represents your application.

f. **Optional:** For Standard Profitability applications, select roles that you want to assign to the users or groups, and click **Add**.

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

g. **Optional:** For Detailed Profitability applications, select roles that you want to assign to the users or groups, and then click **Add**. See Profitability and Cost Management Roles for a list of Detailed Profitability roles and the tasks to which they provide access.

h. Click **Save**.

i. Click **OK**.

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

A

EPM System Roles

Foundation Services Roles

Oracle Hyperion Foundation Services roles comprise power roles belonging to these components:

- Oracle Hyperion Shared Services. See Shared Services Roles.
- Oracle Hyperion EPM Architect. See EPMA Roles.
- Oracle Hyperion Calculation Manager. See Calculation Manager Roles.
- Financial Management Manager. See Financial Management Manager Roles.

Shared Services Roles

All Oracle Hyperion Shared Services roles are power roles. Typically, these roles are granted to power users who are involved in administering Shared Services and other Oracle Enterprise Performance Management System products.

Table A-1 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 Oracle Hyperion 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.

Table A-1 (Cont.) Shared Services Roles (Global Roles)

Role	Description
LCM Administrator This role comprises these roles: • Directory Manager • LCM Designer • Manage Taskflows • Run Taskflows • Project Manager • Provisioning Manager	Runs Oracle Hyperion Enterprise Performance Management System Lifecycle Management to promote artifacts or data across product environments and operating systems
LCM Designer	Designs migration of artifacts and applications by creating a by creating a Migration Definition File using the Lifecycle Management Functionality. Users with this role only can design, but not execute a migration.
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 views Shared Services application groups.
Run Integrations	Views and runs Shared Services data integrations

EPMA Roles

All Oracle Hyperion EPM Architect roles are power roles. Typically, they are granted to power users who must create applications and administer application dimensions.

Table A-2 EPMA 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 various 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 Oracle Hyperion Financial Management and Oracle Hyperion Planning users to be able to navigate to their product's Classic Application Administration options. The user who creates the application automatically becomes the application administrator and provisioning manager for the application.
Essbase Application Creator	Creates Oracle Essbase applications.

Table A-2 (Cont.) EPMA Roles

Role	Description
Financial Management Application Creator	Creates Consolidation applications. 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
Profitability Application Creator	Creates Oracle Hyperion Profitability and Cost Management applications.
Dimension Editor	Creates, manages, and imports profiles to create dimensions. Creates and manages dimensions manually. Required to access Classic Application Administration options for Financial Management and Planning using web navigation.

Calculation Manager Roles

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

Table A-3 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 Oracle Hyperion Financial Management Planning Calculation Manager Administrator administers Calculation Manager functions in Oracle Hyperion Planning
Financial Management Calculation Manager Administrator	Administers Calculation Manager functions in Financial Management
Planning Calculation Manager Administrator	Administers Calculation Manager functions in Planning

Financial Management Manager Roles

These roles allow Oracle Hyperion Shared Services administrators to administer Oracle Hyperion Financial Management applications.

Table A-4 Financial Management Manager Roles

Role	Description
Financial Management Manager Administrator role comprises these roles: • Financial Management Administrator • Financial Management Application Creator • Financial Management Calculation Manager Administrator	Creates and administers Financial Management applications, and administers Oracle Hyperion Calculation Manager functions in Financial Management
Financial Management Administrator	Administers Financial Management applications.
Financial Management Application Creator	Creates Financial Management applications
Financial Management Calculation Manager Administrator	Administers Calculation Manager functions in Financial Management

Planning Roles

Additional Oracle Hyperion Foundation Services roles are required for Oracle Hyperion Calculation Manager. See Foundation Services Roles.

Table A-5 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 Oracle Hyperion 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.
Essbase Write Access	For planners and interactive users: Grants users access to Planning data in Oracle Essbase equivalent to their Planning access permissions. If security filters that limit access to year and period dimensions are not created, this role grants write access to all periods and years. Enables users having write access to change Planning data directly in Essbase using another product such as Oracle Hyperion Financial Reporting or a third-party tool.

Table A-5 (Cont.) Planning Application Roles

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 Approval Supervisors cannot change data in planning units that they do not own.
Ad Hoc Grid Creator	Creates and saves Smart Slices in addition to performing the tasks that an Ad Hoc User can perform
Ad Hoc User	Analyzes data forms using ad hoc features.
Task List Access Manager	Not applicable to this release; reserved for future use.
Planner Roles	
Planner	Enters and submits plans for approval and adapter processes. Uses reports that others have created, views and uses task lists, enables e-mail notification for themselves, and creates data using Oracle Smart View for Office.
Interactive Roles	

Table A-5 (Cont.) Planning Application Roles

Role	Description
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, Financial Reporting and Smart View). Typical View users are executives who want to see business plans during and at the end of the budget process.
Ad Hoc Read Only User	Views data in smart slices.

Essbase Roles

The following tables describe the roles specific to Oracle 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 Oracle Hyperion Shared Services Project Manager role.

Table A-6 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 Oracle Hyperion 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.

Table A-6 (Cont.) Essbase Server Roles

Role	Description
Provisioning Manager	Provisions users with roles of this Essbase server

Table A-7 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. An Application Managers can delete only those applications and databases that he created. **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

Financial Management Roles

Additional Oracle Hyperion Shared Services roles are required for Oracle Hyperion Calculation Manager. See Foundation Services Roles.

Table A-8 Financial Management Roles

Role	Description
Power Roles	
Application Administrator	Performs all Oracle Hyperion Financial Management tasks. Access to this role overrides any other access setting for the user.
Load System	Loads rules and member lists, and extracts application elements.

Table A-8 (Cont.) Financial Management Roles

Role	Description
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. Cannot create folders.
Journals Administrator	Performs all tasks related to journals
Post Journals	Posts and unposts journals
Manage Templates	Grants access to the journals templates for managing journals
Generate Recurring	Grants access to the generate recurring task for managing journals
Review Supervisor	Starts process management units and approves and publishes process management data. Can promote or reject process units, depending on process level. Assigns process management groups to phases.
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
Consolidate	Runs consolidate
Consolidate All with Data	Runs consolidate with all data
Run Allocation	Runs allocations
Run EquityPickUp	Performs equity pickup tasks and calculates equity pickup adjustments
Manage Data Entry Forms	Manages data entry forms on the web
Manage Models	Not used in this release
Save System Report On Server	Saves system reports on server
Load Excel Data	Loads data from Oracle Smart View for Office
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.

Table A-8 (Cont.) Financial Management Roles

Role	Description
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
Manage Custom Documents	Loads and extracts custom documents to and from the server
Extended Analytics	Exports data to a database
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. Creates folders.
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
View Data Audit	Views and exports data audit information
View Task Audit	Views and exports task audit information
Dashboard Viewer	Accesses dashboards

Financial Reporting (Document Repository) Roles

Table A-9 Financial Reporting Roles

Role	Description
Administrator	Accesses all Document Repository resources.
Security Administrator	Provisions Document Repository users; 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 Oracle Hyperion Enterprise Performance Management Workspace.
Designer	Imports, saves, and modifies batches, books, reports, and documents; creates and modifies shortcuts and folders. Creates, modifies, and deletes data sources and database connections in Oracle Hyperion Financial Reportingthrough EPM Workspace.

Table A-9 (Cont.) Financial Reporting Roles

Role	Description
Report Designer Scheduler	Manages repository content and execute tasks, with implicit access to all resources, unless resource permissions are set to "no access".
Scheduler	Creates and schedules jobs and batches using the Batch Scheduler module; navigates the repository and assigns access control.
Viewer	Lists repository content in the Explore module and in context using the Open dialog box; searches, views, and subscribes to content. Access to the repository does not grant access to individual files and folders, which are secured by file properties and permissions.

Financial Close Management Roles

Native Directory users cannot perform tasks granted by Oracle Hyperion Financial Close Management roles, because they cannot use single sign-on with Fusion Middleware. If Native Directory users must perform Financial Close Management tasks, they must be created as Fusion Middleware users too.

Close Manager Roles

Table A-10 Close Manager Roles

Role	Description
Close Administrator	Administers Oracle Hyperion 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 transactional dashboards • Modifies status • Creates and modifies alerts, comments, and questions • Creates and manages filters
Close Report Designer	Designs Financial Close Management reports

Account Reconciliation Manager Roles

These roles are displayed under Oracle Hyperion Financial Close Management.

Table A-11 Account Reconciliation Management Roles

Role	Description
Reconciliation Administrator	• Full access to system setup, filters, attributes, periods, reconciliation instances, rates, and reporting • Adds and remove own comments • Removes commentary from reconciliations to accommodate cases where the commentary that was entered by a user who separated from the company must be removed • Cannot prepare or view account reconciliations
Reconciliation Power User	• Full access to filters, reconciliation profiles, reconciliation instances, and reporting • Adds and remove own comments • Removes commentary from reconciliations to accommodate cases where the commentary that was entered by a user who separated from the company must be removed
Reconciliation Commentator	• Adds comments to reconciliations and associated transactions • Creates reports • Creates private filters
Reconciliation Preparer	• Performs all functions related to preparation of reconciliations including adding, editing, flagging, and removing transactions; adding and removing comments; adding and removing attachments; answering questions; and submitting reconciliations for review • Creates reports • Creates private filters
Reconciliation Reviewer	• Reviews reconciliations including flagging transactions, adding and removing comments; rejecting reconciliations; and approving reconciliations • Creates reports • Creates private filters
Reconciliation Viewer	• Views reconciliations to which Viewer privileges are granted • Creates reports • Creates private filters

Supplemental Data Manager Roles

Table A-12 Supplemental Data Manager Roles

Role	Description
Supplemental Data Administrator	• Provisions users and groups with Supplemental Data Manager roles • Performs all Supplemental Data Manager tasks including one-time system set up (define system currency, specify available currencies, periods, and frequency), dimension tables set up, and import of dimension table definition and members from Oracle Hyperion Financial Management
Supplemental Data Power User	• Performs tasks that SDM Dimension Editor can perform • Creates data sets, forms and summary views from data sets • Attaches reference material; for example, Excel spreadsheet, to data forms • Manages data set columns • Deletes data set, form or view • Assigns access control for forms • Opens, closes and locks periods
Supplemental Data Dimension Editor	• Performs all tasks that SDM User can perform • Adds or deletes dimension members
Supplemental Data User	• Enters, approves or views data based on the access control granted on forms • Runs validations and fixes data errors • Submits data for review • Posts data to Financial Management if access is granted through a workflow
Supplemental Data Drill Through User	Drills through to the detailed data that was posted to Financial Management

Tax Management Roles

Tax Governance Roles

In addition to the Provisioning Manager role Oracle Hyperion Tax Governance roles include the roles belonging to Tax Operations and Tax Supplemental Schedules. See:

- Tax Operations Roles
- Tax Supplemental Schedules Roles

Tax Operations Roles

Table A-13 Tax Operations Roles

Role	Description
Tax Operations Administrator	Administers Tax Operations. Performs the tasks that Close Power User and Close User can perform.
Tax Operations Power User	• Create and manage alert types • Performs tasks that Tax Operations User can perform
Tax Operations User	Performs these tasks: • Views templates • Accesses transactional dashboards • Modifies status • Creates and modifies alerts, comments, and questions • Creates and manages filters
Tax Operations Report Designer	Designs reports that display Tax Operations data.

Tax Supplemental Schedules Roles

Table A-14 Tax Supplemental Schedules Roles

Role	Description
Tax Supplemental Schedules Administrator	• Provisions users and groups with Tax Supplemental Schedules roles • Administers Tax Supplemental Schedules • Performs the tasks that Tax Supplemental Schedules Power User and Tax Supplemental Schedules User can perform
Tax Supplemental Schedules Power User	• Performs tasks that Tax Supplemental Schedules User can perform • Views the data set and form templates for data collection • Deploys data set and form templates to a new data collection period and sets the status to Open to activate included data entry forms
Tax Supplemental Schedules User	Enters data into assigned forms and submits them
Drill Through	Drills through to the detailed data that was posted to Oracle Hyperion Financial Management

Profitability and Cost Management Roles

Standard Profitability and Cost Management Roles

Table A-15 Standard Profitability and Cost Management Roles

Security Role	Description
Power Roles	
Administrator	• Create and maintain user accounts and security roles, and provision users, using Oracle Hyperion Shared Services • Generate Oracle Essbase databases • Set up and maintain application preferences • Build the model database by selecting the common dimensions and members • Create and maintain elements within the model, such as stages, drivers, POVs, driver selections, assignments, and application preferences • Perform POV Copy, calculation, validation, data entry, and trace allocations • Deploy to Essbase and generate calculation scripts • Import and export data • Use the Lifecycle Management Utility to promote data from one environment, such as development or testing, to another environment, such as production. • Back up and restore Oracle Hyperion Profitability and Cost Management model components. • Monitor changes made to business objects. • Access Profitability Application Home screen to create, maintain, register, duplicate and update Profitability and Cost Management applications using Application Loader for Exalytics. • Create, edit, copy, delete, and launch queries from Oracle Smart View for Office Connections screen **Note:** The Power User does not necessarily require specific security roles to perform tasks. For example, if a Power User runs a calculation from the Calculate screen, this action creates and executes a taskflow behind the scenes. The Power User does not require the Manage Taskflow role to perform this task, unless the Power User wants to access this task directly from the Manage Taskflows task.

Table A-15 (Cont.) Standard Profitability and Cost Management Roles

Security Role	Description
Power User	• Create and maintain elements within the model, such as stages, drivers, POVs, driver selections, assignments, and application preferences. • Perform POV Copy, calculation, validation, data entry and trace allocations. • Deploy to Essbase and generate calculation scripts. • Import and export data • Access Profitability Application Home screen to create, maintain, register, duplicate and update Profitability and Cost Management applications using Application Loader for Exalytics. • Create, edit, copy, delete, and launch queries from Smart View Connections screen
Interactive Roles	
Interactive User	• View all modelling screens • View and modify data in the Data Entry screen • View Trace Allocations • Launch queries from Smart View Connections screen
View User	View only access for these functions: • Trace Allocations • Application Preferences • Model Stages, Drivers and POVs
Shared Services Roles	
Manage Taskflows	Required to create and edit taskflows.
Run Taskflows	Required to enable users to only run and view taskflows. Users with this role cannot create or edit taskflows.

Detailed Profitability and Cost Management Roles

Table A-16 Detailed Profitability and Cost Management Roles

Security Role	Description
Administrator	• Set up and maintain application preferences • Build the model database by selecting the common dimensions and members • Create and deploy reporting views to the relational database • Create, Read (View), Update and Delete the following functions: – Stages – Drivers – POVs – Driver Associations – Assignments – Application Preferences – Calculation Rules – Calculation Process Administration – Jobs Library and Status – Table Registration • Perform the following tasks: – POV Copy – Validate – Deploy – Calculate – Stop Jobs • Use the Lifecycle Management Utility to promote data from one environment, such as development or testing, to another environment, such as production. • Import and export data • Back up and restore Oracle Hyperion Profitability and Cost Management model components. • Monitor changes made to business objects. • Create, edit, copy, delete, and launch queries from Oracle Smart View for Office Connections screen • Access Profitability Application Home screen to create, maintain, register, duplicate and update Profitability and Cost Management applications using Application Loader for Exalytics.
Power Roles	

Table A-16 (Cont.) Detailed Profitability and Cost Management Roles

Security Role	Description
Power User	• Create and maintain user accounts and security roles, and provision users, using Oracle Hyperion Shared Services • Create and deploy reporting views to the relational database • Access Profitability Application Home screen to create, maintain, register, duplicate and update Profitability and Cost Management applications using Application Loader for Exalytics. • Create, edit, copy, delete, and launch queries from Smart View Connections screen • Create, Read (View), Update and Delete the following functions: – Stages – Drivers – POVs – Driver Associations – Assignments – Application Preferences – Calculation Rules – Calculation Process Administration – Jobs Library and Status – Table Registration • Perform the following tasks: – POV Copy – Validate – Deploy – Calculate – Stop Jobs **Note:** The Power User does not necessarily require specific security roles to perform tasks. For example, is a Power User runs a calculation from the Calculate screen, this action creates and executes a taskflow behind the scenes. The Power User does not require the manage Taskflow role to perform this task, unless the Power User wants to access this task directly from Mange Taskflows task.
Interactive Roles	

Table A-16 (Cont.) Detailed Profitability and Cost Management Roles

Security Role	Description
Interactive User	• View (Read) the following functions: – Stages – Drivers – POVs – Driver Association – Assignments – Application Preferences – Calculation Rules – Calculation Process Administration – Jobs Library and Status – Table Registration • Launch queries from Smart View Connections screen
View User	View (Read) the following functions: • Stages • Drivers • POVs • Driver Association • Assignments • Application Preferences • Calculation Rules • Calculation Process Administration • Jobs Library and Status • Table Registration
Shared Services Role	
Manage Taskflows	Required to create and edit taskflows.
Run Taskflows	Required to enable users to only run and view taskflows. Users with this role cannot create or edit taskflows.

Provider Services Roles

Oracle Hyperion Provider Services provides the Administrator power role, which allows users to create, modify, and delete Essbase Server clusters.

Data Integration Management Roles

Oracle Hyperion Data Integration Management does not use the security environment established by Oracle Hyperion 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 Data Integration Management documentation for detailed information.

FDMEE Roles

Table A-17 FDMEE 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, Enterprise Edition roles
Drill Through	Applies to FDMEE and Oracle Hyperion Financial Data Quality Management. 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 FDMEE, this role controls whether the user can drill to the FDMEE landing page, which controls drilling to the source system.
Create Integration	Creates FDMEE metadata and data rules.
Run Integration	Runs FDMEE metadata and data rules and fills out runtime parameters. Can view transaction logs. FDM users who need to extract data from Oracle General Ledger must be granted this role to run data rules.
GL Write Back	Enables data write-back to the ERP source system.
Intermediate 2–9	Loads data to the target system. Roles for intermediate levels are defined by the FDM 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.

B

EPM System Component Codes

Roles define the tasks that users can perform in Oracle Enterprise Performance Management System applications. Roles from all registered EPM System applications can be viewed from the Roles View in Oracle Hyperion Shared Services Console.

The Roles View lists the roles name and the product code, which is the internal product name, along with a brief role description. The product codes used by EPM System products are indicated in Table 1.

Table B-1 Product Codes Used by EPM System Products

Product Code	Product Name
HUB	Oracle Hyperion Shared Services
CES	Shared Services (Workflow)
HP	Oracle Hyperion Planning
ESB	Oracle Essbase
ESBAPP	Essbase Application
FDM	Oracle Hyperion Financial Data Quality Management
EAL	Oracle Essbase Analytics Link for Hyperion Financial Management
EALBRIDGE	Analytics Link Bridge
HFM	Oracle Hyperion Financial Management
HPM	Oracle Hyperion Profitability and Cost Management
CALC	Oracle Hyperion Calculation Manager
AIF	Oracle Hyperion Financial Data Quality Management, Enterprise Edition
IOP	Oracle Integrated Operational Planning
BIEE	Oracle Business Intelligence Enterprise Edition
FCC	Oracle Hyperion Financial Close Management
BIP	Oracle Business Intelligence Publisher

C

Accessing EPM System Products

Accessing Shared Services

See Launching Shared Services Console.

Accessing EPM Workspace

Oracle Hyperion Enterprise Performance Management Workspace is a Oracle Hyperion Foundation Services component from which you can access Oracle Enterprise Performance Management System products, for example, Oracle Hyperion Planning and Oracle Hyperion Shared Services. 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, `http://myWebserver:19000/workspace`.

   > **Note:**
   >
   > If you are accessing EPM Workspace in secure environments, use `https` (not `http`) as the protocol and the secure web Server port number. For example, use a URL such as: `https://myWebserver:19443/workspace`.

   Pop-up blockers may prevent EPM Workspace from opening.
2. Click **Launch Application**.
3. In the Logon window, enter a user name and password.
4. Click **Log On**.

Accessing Administration Services Console

Before starting these procedures, ensure that Oracle Hyperion Foundation Services, web server, Oracle Essbase, and Oracle Essbase Administration Services are running.

To access Administration Services Console from a URL:

1. Go to:

   `http://Web_server_name:port_number/easconsole/console.html`

In the URL, *Web_server_name* indicates the name of the computer where the web server used by Foundation Services is running, and *port_number* indicates the web server port; for example, `https://myWebserver:19000/easconsole`.

> **Note:**
>
> If you are accessing Oracle Hyperion Enterprise Performance Management Workspace, in secure environments, use `https` (not `http`) as the protocol and the secure web server port number. For example, use a URL such as: `https://myWebserver:19443/easconsole`.

2. Click **Launch**.
3. Download and install Administration Services Console.
4. In the Administration Services Login screen, enter your user name and password.
5. Click **OK**.