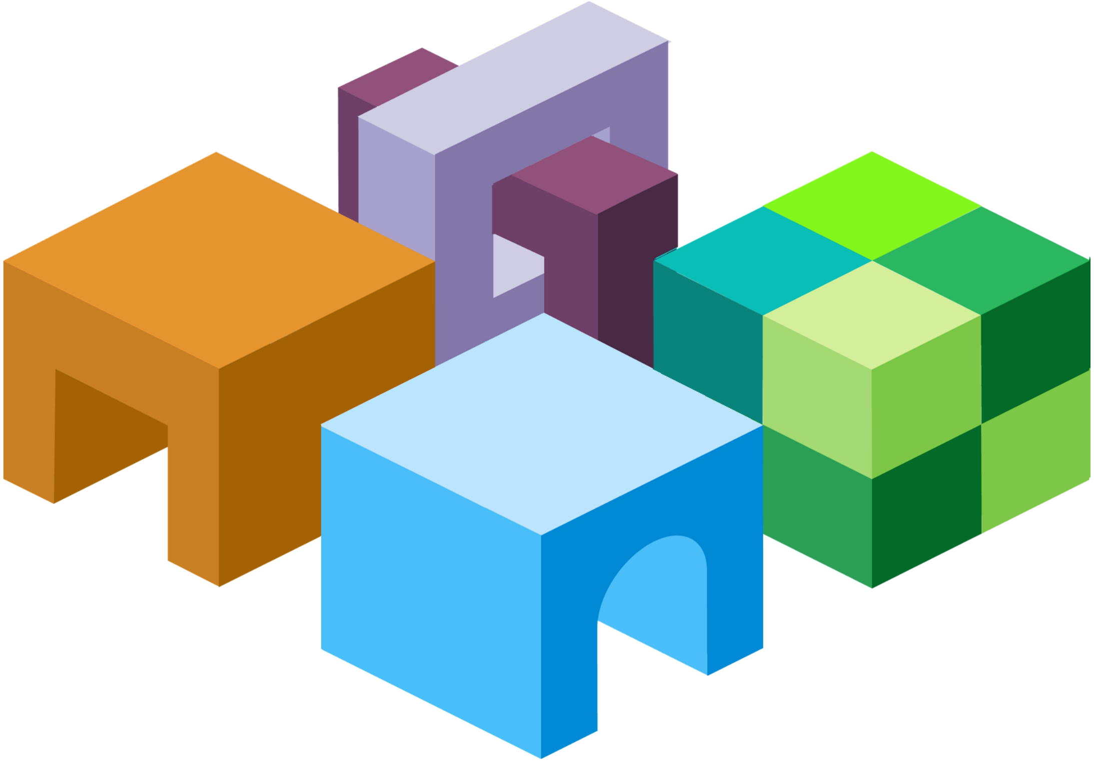


ORACLE® HYPERION ENTERPRISE PERFORMANCE MANAGEMENT SYSTEM

RELEASE 11.1.1.2

SECURITY ADMINISTRATION GUIDE

ORACLE®
ENTERPRISE PERFORMANCE
MANAGEMENT SYSTEM

EPM System Security Administration Guide, 11.1.1.2

Authors: EPM Information Development Team

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

This software and documentation may provide access to or information on content, products and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third party content, products and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third party content, products or services.

Contents

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at http://www.oracle.com/accessibility/.

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, seven days a week. For TTY support, call 800.446.2398.

1 About EPM System Security

In This Chapter

Security Components

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

- "User Authentication" on page 15
- "Provisioning (Role-based Authorization)" on page 19

User Authentication

User authentication enables single sign-on (SSO) functionality across EPM System products by validating the login information of each user to determine authenticated users. User authentication, along with product-specific authorization, grants the user access to EPM System products. Authorization is granted through provisioning.

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

Authentication Components

The following sections describe the components that support SSO:

- "Security API" on page 16
- "Native Directory" on page 16
- "User Directories" on page 16

Security API

The Security Application Programming Interface (Security API) is the main interface to validate users and interpret user access to EPM System products. It is a Java API that enables EPM System products to authenticate users against user directories configured in Oracle's Hyperion® Shared Services. It also allows integration with a security agents such as Oracle Access Manager and CA SiteMinder, and retrieval of users and groups based on names and identities. Each EPM System application uses the Security API to support user authentication.

Native Directory

Native Directory refers to the Lightweight Directory Access Protocol (LDAP)-enabled user directory that Shared Services uses to support provisioning. EPM System products can use Oracle Internet Directory (OID) or OpenLDAP as Native Directory. OpenLDAP is an open-source LDAP-based user directory that is bundled and configured with Shared Services. OID is an LDAP version 3 compatible user directory that leverages the scalability, high availability, and security features of the Oracle Database. OID can serve as the central user repository for Oracle identity management, simplifying user administration in the Oracle environment. OID is not bundled with Shared Services; it must be installed separately.

Native Directory functions:

- Used to maintain and manage the default Shared Services user accounts required by EPM System products
- Central storage for all EPM System provisioning information because it stores the relationships among users, groups, and roles

Native Directory is accessed and managed using Oracle's Hyperion® Shared Services Console. See Chapter 8, "Managing Native Directory" for more information on provisioning users.

User Directories

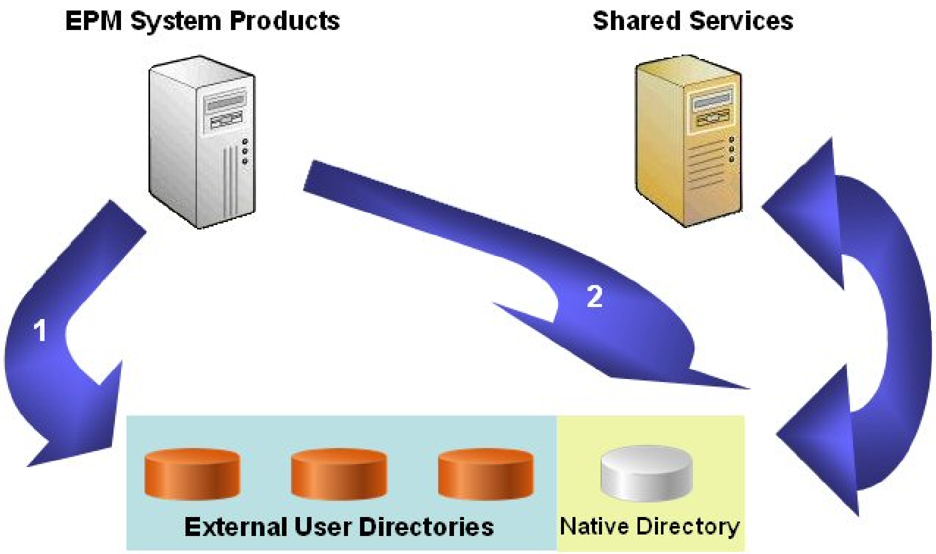
User directories refer to any corporate user and identity management system compatible with Shared Services. EPM System products are supported on several user directories, including LDAP-based user directories, such as OID, Sun Java System Directory Server (formerly SunONE Directory Server), Microsoft Active Directory, and custom-built user directories that implement LDAP version 3. Relational databases, Windows NT LAN Manager (NTLM), and SAP native repository also are supported as user directories.

In addition to Native Directory, one or more user directories can be configured as the user information provider for EPM System products.

User directories used with EPM System products must contain an account for each user who accesses EPM System products. Users may be assigned to groups to facilitate provisioning.

Single Sign-on Directly to EPM System Products

Direct authentication connects EPM System products to available user directories to verify the user name and password (credentials) entered on the Login screen.



1. Through a browser, users access the EPM System product login screen and enter user names and passwords.

   The Security API implemented on the EPM System product queries the configured user directories (including Native Directory) to verify user credentials. A search order establishes the search sequence. Upon finding a matching user account in a user directory, the search is terminated, and the user's information is returned to the EPM System product.

   Access is denied if a user account is not found in any user directory.

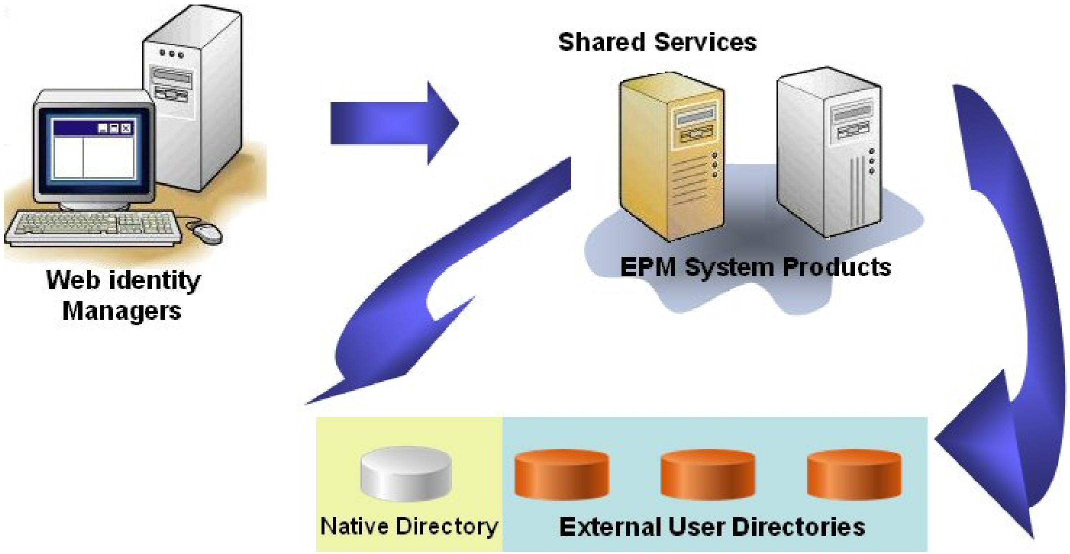
2. Using the retrieved user information, the EPM System product queries Native Directory to obtain provisioning details for the user.
3. EPM System product checks the Access Control List (ACL) in the product to determine the objects that the user can access within the product.

Upon receiving provisioning information from Native Directory, the EPM System product is made available to the user. At this point, SSO is enabled for all EPM System products for which the user is provisioned.

Single Sign-on from External Systems

EPM System products can be configured to accept users who are already authenticated by external sources, such as Oracle Access Manager, Oracle Application Server Single Sign-on (OSSO), CA SiteMinder, and SAP Enterprise Portal to enable SSO. SSO from external systems is available for EPM System Web applications only. In this scenario, EPM System products use the user information provided by a trusted external source to determine access permissions of users. To enhance security, Oracle recommends that direct access to the servers be blocked by firewalls; all requests should be routed through an SSO portal.

SSO with external sources is supported by accepting authenticated user credentials through an acceptable SSO mechanism. See “Supported SSO Methods” on page 26. The external system authenticates the user and passes the user's login name to EPM System, which checks the login name against configured user directories. The illustrated concept:



1. Using a browser, users access the login screen of a Web identity management solution (for example, Oracle Access Manager) or SAP Enterprise Portal. They enter user names and passwords, which are validated against configured user directories in the Web identity management solution to verify user authenticity. EPM System products are also configured to work with these user directories.

   Information about the authenticated user is passed to EPM System product, which accepts the information as valid.

   If the user logged on to SAP Portal, an SAP logon ticket is passed to EPM System product, which decrypts the SAP logon ticket using an SAP certificate.

   The Web identity management solution passes the login name (see the discussion of `Login Attribute` in Table 8 on page 70) of the user to EPM System product using an acceptable SSO mechanism. See "Supported SSO Methods" on page 26.

2. To verify user credentials, EPM System product tries to locate the user in a user directory. If a matching user account is found, user information is returned to EPM System product. Shared Services security sets the SSO token that enables SSO across EPM System products.

3. Using the retrieved user information, EPM System product queries the Native Directory to obtain provisioning details for the user.

   Upon receiving user provisioning information, the EPM System product is made available to the user. SSO is enabled for all EPM System products for which the user is provisioned.

Note:

SSO with SAP is supported by accepting an SAP logon ticket. Users defined in an SAP native repository can navigate between the SAP Portal and EPM System products. If SAP BW or R/3 native repository is configured as an external directory in Shared Services, users can log in to EPM System products using the user ID and password stored in the SAP system.

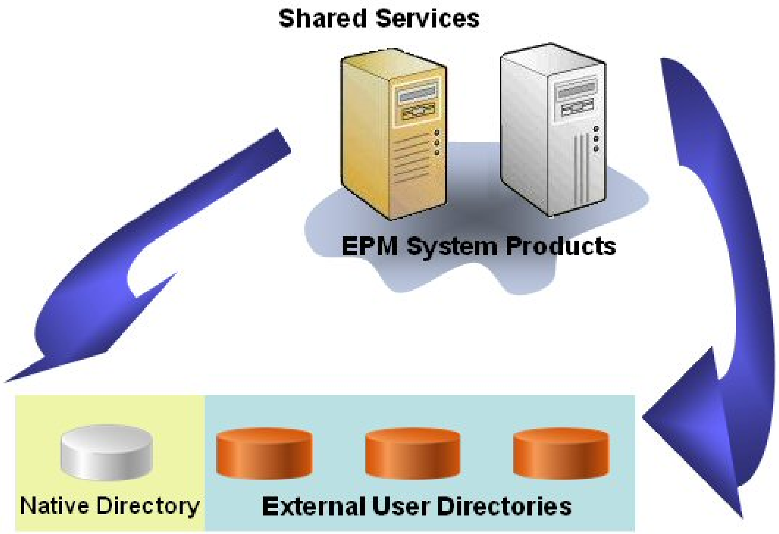
Provisioning (Role-based Authorization)

EPM System application security determines user access to products using the concept of roles, permissions that determine user access to product functions. Some EPM System products enforce object-level ACLs to further refine user access to their objects.

Each EPM System product provides several default roles tailored to various business needs. Predefined roles from each EPM System application registered with Shared Services are available from Shared Services Console. These roles are used for provisioning. You may also create additional roles that aggregate the default roles to suit specific requirements. The process of granting users and groups specific access permissions to EPM System resources is called *provisioning*.

Native Directory and configured user directories are sources for user and group information for the provisioning (authorization) process. You can browse and provision users and groups from all configured user directories from Shared Services Console. You can also use application-specific aggregated roles created in Native Directory in the provisioning process.

This illustration depicts an overview of the authorization process:



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

   Product-specific provisioning tasks, such as setting product-specific access control, are completed from each product. This data is combined with provisioning data to determine the product access for users.

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

Roles

A role is a construct (similar to access control list) that defines the access permissions granted to users and groups to perform functions on EPM System resources. It is a combination of resource or resource types (what users can access; for example, a report) and actions that users can perform on the resource (for example, view and edit).

Access to EPM System application resources is restricted; users can access them only after a role that provides access is assigned to the user or to the group to which the user belongs. Access restrictions based on roles enable administrators to control and manage application access. See Appendix A, "Product Roles."

Global Roles

Global roles, Shared Services roles that span multiple products, enable users to perform certain tasks within the Shared Services Console. See Appendix B, "Shared Services Roles and Permitted Tasks" for a complete list of Shared Services global roles.

Predefined Roles

Predefined roles are built-in roles in EPM System products. You cannot delete these roles from the product. Predefined roles are registered with Shared Services during the application registration process.

Aggregated Roles

Aggregated roles, also known as custom roles, aggregate multiple product roles within an EPM System product. An aggregated role comprises multiple roles, including other aggregated roles. For example, a Shared Services Administrator or Provisioning Manager can create a role for Planning that combines the Planner and View User roles into an aggregated role. Aggregating roles can simplify the administration of products that include several granular roles. Global Shared Services roles can be included in aggregated roles. You cannot create an aggregated role that spans products.

Users

User directories store information about the users who can access EPM System products. Both the authentication and the authorization processes use user information. You can create and manage Native Directory users only from Shared Services Console.

Users from all configured user directories are visible from Shared Services Console. These users can be individually provisioned to grant access rights on the EPM System products registered with Shared Services. Oracle does not recommend provisioning individual users.

Groups

Groups are containers for users or other groups. You can create and manage Native Directory groups from Shared Services Console. Groups from all configured user directories are displayed in Shared Services Console. You can provision these groups to grant permissions for EPM System products registered with Shared Services.

2 Setting Up EPM System Security

In This Chapter

The security environment of EPM System products comprises two complementary layers: authentication and authorization.

Setting up EPM System security to authenticate users directly involves several broad procedures described in the following sections.

"Creating Users" on page 23

"Creating Groups" on page 23

"Identifying User Directories to Shared Services" on page 24

Creating Users

The security environment of EPM System products requires that user credentials be checked against a user directory as a part of the authentication process. This requirement mandates that each EPM System application user have an account in the user directory. A user identifier (typically the user name) defined on the user directory is the foundation on which EPM System application security is built.

In most deployment scenarios, existing user directories (with user accounts) are used to support user authentication. For information on creating user accounts, see vendor documentation. See "Creating Users" on page 110 for information on creating Native Directory users.

Creating Groups

User accounts on user directories can be granted membership to groups based on common characteristics such as the user function and geographical location. For example, users can be categorized into groups such as Staff, Managers, Sales, and Western_Sales based on their function within the organization. A user can belong to one or more groups on the user directory, an important consideration in facilitating the provisioning process.

The procedures to create groups and assign group membership vary depending on the user directory. For information on creating groups and assigning group membership, see vendor documentation. See “Managing Native Directory Groups” on page 113 for information on creating Native Directory groups.

Identifying User Directories to Shared Services

The Shared Services installation and deployment process sets up and configures Native Directory as the default user directory for EPM System products. Each additional user directory that you use to support user authentication and SSO must be configured separately using Shared Services Console.

During user directory configuration, you assign the search order for each user directory. This order determines the sequence in which the authentication process searches within configured user directories to locate the user account that matches the user login credentials. By default, EPM System application security is configured to terminate the search process when a matching user account is found. If you are using multiple user directories, Oracle recommends that user accounts be normalized across user directories.

Information on configuring user directories:

- “Configuring OID, MSAD, and Other LDAP-Based User Directories” on page 65
- “Configuring an SAP R3 Native Repository” on page 74
- “Modifying NTLM External User Directory Configurations” on page 82

3 Enabling SSO with Security Agents

In This Chapter

Overview

EPM System products can be configured to accept authenticated user credentials for SSO from Web identity management solutions such as Oracle Access Manager, OSSO, CA SiteMinder, and Kerberos. The Web identity management solution sends credentials of authenticated users to EPM System products, which verifies the credentials against the user directories configured in Shared Services. If the user is available in a configured user directory, EPM System security issues an SSO token that grants the user access to all products for which the user is provisioned.

Where SSO from Web identity management solutions is implemented, the users are challenged by the Web identity management solutions either while logging into the client systems or while accessing protected resources such as EPM System products. EPM System products support SSO by trusting the identity passed to them by Web identity management solution.

To enable SSO, the Web identity management solution and EPM System products must be configured to use the same set of user directories. Also, the user directories configured in Shared Services must be set up to support Web identity management solution for single sign on. See "Setting Security Options" on page 86.

Note:

The corporate user directories configured with Shared Services must be trusted when SSO from a Web identity management solution is enabled.

Supported SSO Methods

SSO requires that the Web identity management solution pass the login name of the authenticated user to EPM System products. The following methods can be used:

HTTP Header

If you are using Oracle Access Manager or SiteMinder (or a custom SSO provider) as the Web identity management solution, use an HTTP header to pass the login name of the authenticated user to EPM System products.

The login name of an EPM System product user is determined by the `Login Attribute` that is specified while configuring user directories in Shared Services. See Table 8 on page 70.

The HTTP header must contain the value of the attribute that is set as the `Login Attribute`. For example, if `uid` is the `Login Attribute` value, the HTTP header must carry the value of the `uid` attribute.

See your Web identity management solution documentation for detailed information on defining and issuing custom HTTP headers.

The security API implemented on the EPM System product parses the HTTP header and validates the login name it carries against the user directories configured on Shared Services.

Custom Login Class

When a user logs in, the Web identity management solution authenticates the user against a directory server and encapsulates the credentials of the authenticated user in an SSO mechanism to enable SSO with other systems. If the Web identity management solution uses a mechanism unsupported by EPM System products or if the value of the `Login Attribute` is not available in the SSO mechanism, use a custom login class to derive and pass the value of the `Login Attribute` to EPM System products.

Using a custom login class as the authentication mechanism requires using standard Shared Services APIs to define the SSO interface between EPM System products and the Web identity management solution. The custom login class must pass the value of the `Login Attribute` to EPM System products. See Table 8 on page 70.

To use a custom login class, an implementation of `com.hyperion.css.CSSSecurityAgentIF` interface must be available in the classpath. `CSSSecurityAgentIF` defines the getter method for retrieving user name and password (optional). If the interface returns a null password, security authentication treats the provider as trusted and verifies the existence of the user in configured providers. If the interface returns a non-null value for password, EPM System attempts to authenticate the request using the user name and password returned by this implementation.

`CSSSecurityAgentIF` comprises two methods: `getUserName` and `getPassword`.

getUserName Method

This method returns the user name for authentication.

```
java.lang.String getUserName(
                    javax.servlet.http.HttpServletRequest req,
                    javax.servlet.http.HttpServletResponse res)
                    throws java.lang.Exception
```

The `req` parameter identifies the HTTP request that carries the information that is used to determine the user name. The `res` parameter is not used (preset for backward compatibility).

getPassword Method

This method returns clear-text password for authentication. Password retrieval is optional.

```
java.lang.String getPassword(
                    javax.servlet.http.HttpServletRequest req,
                    javax.servlet.http.HttpServletResponse res)
                    throws java.lang.Exception
```

The `req` parameter identifies the HTTP request that carries the information that is used to determine the password. The `res` parameter is not used (preset for backward compatibility).

HTTP Authorization Header

Select this option if the Web identity management solution uses an HTTP authorization header to pass value the of `Login Attribute` to EPM System products. EPM System products parse the authorization header to retrieve user's login name.

Get Remote User from HTTP Request

Select this option if the Web identity management solution has the ability to `setRemoteUser` value in the HTTP request to pass the value of `Login Attribute` to EPM System products.

This method is used for OSSO and Oracle Application Server integrated with Integrated Windows Authentication.

SSO from Oracle Access Manager

SSO with Oracle Access Manager requires that Oracle Access Manager pass an HTTP header containing the value of the `Login Attribute` (see Table 8 on page 70) to EPM System products.

Integration with Oracle Access Manager requires that you enable Oracle Access Manager authentication for EPM System products. See the following topics:

- "Configuring Shared Services for SSO" on page 40

- “Configuring EPM Workspace for SSO” on page 41

Note:

Be sure to configure the user directories that Oracle Access Manager uses to authenticate users as external user directories in Shared Services. See “Configuring OID, MSAD, and Other LDAP-Based User Directories” on page 65.

Oracle Application Server Single Sign-on

OSSO enables you to use a user name and password defined in an OID to log in to EPM System products.

Assumptions

This discussion assumes the following:

- A fully functional Oracle Identity Management Infrastructure (OID, Oracle Database, and Oracle Application Server). Use Identity Management Suite 10.1.4.0.1, which installs Oracle Application Server 10.1.2.0.2.
- The OID that supports Oracle Identity Management Infrastructure contains all users who must access EPM System products.
- Fully functional Oracle Application Server instance to host EPM System products. This instance is different from the Oracle Application Server installed with Oracle Identity Management Infrastructure. See *Oracle Hyperion Enterprise Performance Management System Installation Start Here* for the supported Oracle Application Server version.

Configuring OSSO

Integration with OSSO requires that you enable OSSO authentication in Shared Services.

➤ To configure OSSO:

1. **Configure EPM System products for SSO. See the following topics:**
   - “Configuring Shared Services for SSO” on page 40
   - “Configuring EPM Workspace for SSO” on page 41

   Note:

   You must configure the OID of Oracle Identity Management Infrastructure as an external user directory in Shared Services. See “Configuring OID, MSAD, and Other LDAP-Based User Directories” on page 65.
2. **Provision at least one OID user as Shared Services administrator.**
3. **Restart Shared Services.**

4 **Configure Oracle Application Server instances for SSO.**

See "Configuring Instances to Use 10.1.4 or 10.1.2 Oracle Identity Management" in the *Oracle Application Server Administrator's Guide* for instructions.

5 **Restart Oracle Identity Management Infrastructure, including OID.**

6 **Restart EPM System products and custom applications that use the Shared Services security APIs.**

Note:

Ensure that the external user directories configured with Shared Services are running before starting EPM System products.

Using IIS

- "Assumptions" on page 29
- "Configuring OSSO with IIS" on page 29

Assumptions

This discussion assumes the following:

- A fully functional Oracle Identity Management Infrastructure (OID, Oracle Database, and Oracle Application Server). Use Identity Management Suite 10.1.4.0.1, which installs Oracle Application Server 10.1.2.0.2.
- An Oracle Identity Management Infrastructure installation is available on the server that hosts IIS. OSSO requires some binaries installed with Identity Management Infrastructure. You may disable Oracle Identity Management Infrastructure services.
- The OID that supports Oracle Identity Management Infrastructure contains all users who must access EPM System products.
- EPM System products that do not use IIS as the application server are hosted on Oracle Application Server. See *Oracle Hyperion Enterprise Performance Management System Installation Start Here* for supported Oracle Application Server version.

Configuring OSSO with IIS

Begin by installing and deploying Shared Services to Oracle Application Server. See *Oracle Hyperion Enterprise Performance Management System Installation and Configuration Guide* for instructions.

Note:

To secure the authentication system, you must use two-way SSL for communication between the Web server running the OSSO plug-in and OC4J.

➤ To configure OSSO with IIS:

1. **Configure OSSO for products that use Oracle Application Server. See "Configuring OSSO" on page 28.**
2. **On the IIS host machine, configure the IIS plug-in. For instructions, see "Using Oracle Application Server SSO Plug-in" in the *Oracle HTTP Server Administrator's Guide*.**
3. **Ensure that `IIS_WPG`, `NETWORK`, and `NETWORK_SECURITY` have the read and execute permissions on the following directories. See "Oracle SSO Plug-In for Microsoft IIS Listener Fails with dependency libraries Error" in Oracle Fusion Middleware Administrator's Guide for Oracle Single Sign-on.**
   - Directory where `oracle_osso.dll` is stored
   - *`ORACLE_HOME`*`/bin`
   - Directory where log files and configuration file are stored
4. **Ensure that the path for `ORACLE_HOME/bin` is the first entry in the PATH environment variable.**

Note:

You can use IIS plug-in to protect applications that work with IIS. To learn how to use Oracle Application Server SSO Plug-in, see "Resource Protection" in *Oracle HTTP Server Administrator's Guide*.

Protecting EPM System Products for SSO

You must protect EPM System resources so that SSO requests from users are redirected to the security agent (OAS, OSSO, or SiteMinder).

Oracle HTTP Server uses `mod_osso` to redirect users to the OSSO server. Users are redirected only if the URLs that they request are configured in `mod_osso` to be protected. See Managing Security in *Oracle HTTP Server Administrator's Guide*.

For information on protecting resources for SiteMinder SSO, see SiteMinder documentation.

Resources to Protect

Table 1 lists the contexts that must be protected. The syntax for protecting a resource (using `interop` as an example) for OSSO is as follows:

```
<Location /interop>
Require valid-user
AuthType Basic
order deny,allow
deny from all
allow from myServer.example.com
satisfy any
</Location>
```

The `allow from` parameter specifies servers from which the protection of the context can be bypassed.

For Oracle Enterprise Performance Management Workspace, Fusion Edition, Oracle Hyperion Financial Reporting, Fusion Edition, and Oracle's Hyperion® Web Analysis, you need to set only the parameters indicated in the following example:

```
<Location /workspace>
Require valid-user
AuthType Basic
</Location>
```

Table 1 EPM System Resources to Protect

EPM System Product	Context to Protect
Shared Services	/interop
EPM Workspace	/workspace
Financial Reporting	/hr
Web Analysis	/WebAnalysis
Oracle Hyperion EPM Architect, Fusion Edition	/awb
Oracle Hyperion Planning, Fusion Edition	/HyperionPlanning
Oracle Smart Space, Fusion Edition	/SmartSpace
Oracle Hyperion Performance Scorecard, Fusion Edition	● /HPSWebReports ● /HPSAlerter
Oracle's Hyperion Reporting and Analysis	/biplus_webservices*
Oracle Hyperion Strategic Finance, Fusion Edition	/HSFWebServices

*Needed only if Smart Space is deployed and configured.

Resources to Unprotect

Table 2 lists the contexts that must be unprotected. The syntax for unprotecting a resource (using `/interop/framework(.*)` as an example) for OSSO:

```
<LocationMatch /interop/framework(.*)>
Require valid-user
AuthType Basic
allow from all
satisfy any
</LocationMatch>
```

Table 2 EPM System Resources to Unprotect

EPM System Product	Contexts to Unprotect
Shared Services	● /interop/framework(.*) ● /interop/Audit(.*) ● /interop/content(.*)

EPM System Product	Contexts to Unprotect
	● /interop/taskflow* ● /interop/WorkflowEngine/* ● /interop/TaskReceiver ● /framework/lcm/HSSMigration
Performance Management Architect	● /awb/ces.executeAction.do ● /awb/lcm.executeAction.do ● /awb/appmanager.deployStatusUpdate.do ● /awb/jobstask.updateJobStatus.do
EPM Workspace[*][†]	● /workspace/browse/listXML ● /workspace/wsrp4j(.*) ● /workspace/ResourceProxy(.*)
Web Analysis[*]	● /WebAnalysis/wsrp4j(.*) ● /WebAnalysis/ResourceProxy(.*)
Financial Reporting[*]	● /hr/common/HRLogon.jsp ● /hr/wsrp4j(.*) ● /hr/ResourceProxy(.*)
Smart Space	/SmartSpace/ClickOnce(.*)
Hyperion Calculation Manager	/common.performAction.do (for Performance Management Architect)
Oracle Essbase Administration Services	● /eas ● /easconsole ● /hbrlauncher ● /easdocs ● /eas?op=com.essbase.eas.essbase.defs.awb.AWBCommands* (for Performance Management Architect)
Performance Management Architect	/awb/lcm.executeAction.do
Oracle Hyperion Financial Management, Fusion Edition	/EIE/EIEListener.asp (for Performance Management Architect)
Planning	● /HyperionPlanning/servlet/HspLCMServlet ● /HyperionPlanning/servlet/HspAppManagerServlet (for Performance Management Architect)
Performance Scorecard	● /HPSWebReports/wsrp4j(.*) ● /HPSWebReports/ResourceProxy(.*)

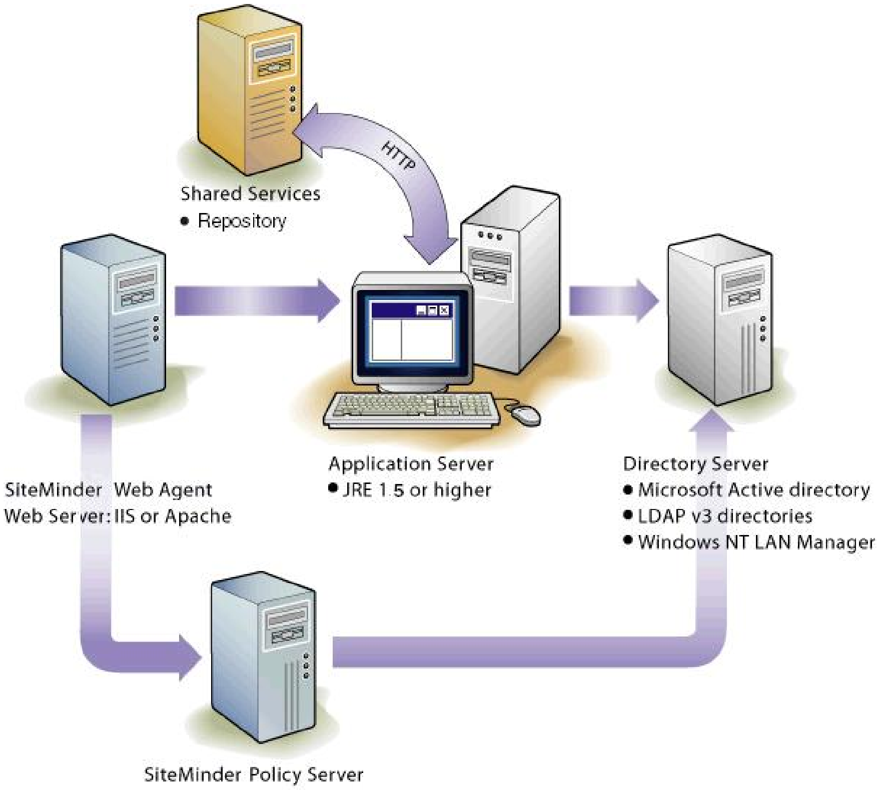
EPM System Product	Contexts to Unprotect
	● /HPSWebReports/action/IcmCallBack
Data Sync	/services*
Strategic Finance	● /HSFWebServices/HSFWebService.asmx ● /HSFWebServices/HSFEntityWebService.asmx
Oracle Hyperion Profitability and Cost Management, Fusion Edition	/HPMApplicationListener

[*] When a security agent is enabled for EPM Workspace, Web Analysis, or Financial Reporting that uses SAP Portal, unprotect only the `wsrp4j` URLs (`/workspace/wsrp4j`, `/WebAnalysis/wsrp4j`, and `/hr/wsrp4j`). Also remove the line `com.hyperion.portlet.sso.filter.SMAuthHandler` from `\WEB-INF\classes\auth-handlers.config` in the web application deployments of EPM Workspace, Web Analysis, and Financial Reporting. In this scenario, portlets authentication is done using the SAP token. For other portals, protect `wsrp4j` URLs in the security agent.

[†] If you are using Oracle Web Center or Oracle Portal for Portlets, Oracle recommends that you use a security agent such as Oracle Access Manager to protect the system. In this scenario, you must also protect `wsrp4j` urls using the security agent.

Single Sign-on from SiteMinder

The SiteMinder-enabled SSO, general overview:



Note:

The corporate user directories configured with Shared Services must be trusted when SSO from SiteMinder is enabled.

See "Protecting EPM System Products for SSO" on page 30for EPM System resources that should be protected.

Special Considerations

SiteMinder is a Web-only solution. Desktop applications and their add-ins (for example, Microsoft Excel and Report Designer) cannot use authentication through SiteMinder. However, Oracle Hyperion Smart View for Office, Fusion Edition can use SiteMinder authentication.

EPM System products are supported only on NTLM and LDAP-based user directories (including MSAD).

Configuring the SiteMinder Policy Server

A SiteMinder administrator must configure the policy server to enable SSO to EPM System products.

The configuration process:

- Setting up protection for the Web resources of EPM System products.
- Configuring a response that adds a custom header that provides the value of `Login Attribute` to login name to EPM System applications. See `Login Attribute` in Table 8 on page 70.

See the "Responses and Response Groups" topic in the *Netegrity Policy Design Guide* for detailed information. SiteMinder administrators also can configure the header to `SM_USERLOGINNAME` (`SMUSER` for SiteMinder version 6), the user name specified at logon.

Configuring the SiteMinder Web Agent

The Web agent is installed on a Web server that intercepts requests for EPM System application Web resources, such as JSPs, ASPs, and HTML files on the application server. If these Web resources are protected, the Web agent issues a challenge to unauthenticated users. When a user is authenticated, the policy server adds the login name of the authenticated user, which is carried by the header. Thereafter, the HTTP request is passed to the Web resources of EPM System application, and the login name is extracted from headers.

SiteMinder supports SSO across EPM System products running on heterogeneous Web server platforms. If EPM System products use different Web servers, you must ensure that the SiteMinder cookie can be passed among Web servers within the same domain. You do this by specifying the appropriate EPM System application domain as the value of the `Cookiedomain` property in the `WebAgent.conf` file of each Web server.

See the “Configuring Web Agents” chapter in the *Netegrity SiteMinder Agent Guide*.

Note:

Because Shared Services uses basic authentication to protect its content, the Web server that intercepts requests to Shared Services should enable basic authentication to support SSO with SiteMinder.

Enabling SiteMinder in EPM System

Integration with SiteMinder requires that you enable SiteMinder authentication for EPM System products. See the following topics:

- “Configuring Shared Services for SSO” on page 40
- “Configuring EPM Workspace for SSO” on page 41

Kerberos Single Sign-on

- “Overview” on page 35
- “Support Limitations” on page 36
- “Assumptions” on page 36
- “Kerberos SSO Using Oracle Application Server” on page 37
- “Kerberos SSO with WebLogic Server” on page 38
- “Kerberos SSO With WebSphere” on page 39

Overview

EPM System products support Kerberos SSO if the application server that hosts EPM System products is set up for Kerberos authentication.

Kerberos is a trusted authentication service where each Kerberos client trusts the identities of other Kerberos clients (users, network services, and so on) to be valid. Kerberos is centered around its Key Distribution Center (KDC), a database of all users and services in Kerberos realm. KDC maintains details of Kerberos clients and their private keys. Kerberos is based on the concept of tickets. Tickets are data structures that wrap cryptographic keys and some other information. KDC distributes Kerberos tickets to authenticated clients.

Computers on the network are configured to implicitly trust the KDC. Users gain access to network resources by presenting tickets with encrypted information from the KDC, which the server can verify. Because KDC is the only entity that knows every encryption key, it can securely verify the authenticity of users, and because each client trusts the KDC, the entire network is secure as long as the KDC is secure.

Simple and Protected GSSAPI Negotiation Mechanism (SPNEGO) protocol is used to determine the authentication mechanism between client and server. Browsers that are enabled to use

Integrated Windows Authentication use SPNEGO to first try Kerberos 5 protocol for authentication. Application servers provide SPNEGO filters to negotiate authentication with the clients such as browsers. The Generic Security Services API (GSSAPI) provides features such as confidentiality, message integrity, and authentication.

The following steps list what happens when a user accesses an EPM System product:

- From a Windows computer, the user logs in to a Kerberos realm.
- Using a browser that is configured to use Integrated Windows Authentication, the user tries to log into EPM System products running on the application server.
- The application server intercepts the request and gets the SPNEGO token with Kerberos information from the browser's authorization header.
- The application server validates the user's identity from a token against its identity store to pass information about the user to EPM System product. EPM System product validates the user name against an MSAD. EPM System product issues an SSO token that can support SSO across all EPM System products.

Support Limitations

Kerberos SSO is supported for all EPM System products, with the following exceptions.

- Kerberos SSO is not supported for EPM System products deployed on Embedded Java Container (Tomcat).
- Kerberos SSO is not supported for thick clients (including Smart View and Oracle Smart Space, Fusion Edition).
- Kerberos SSO support for IIS-embedded EPM System products (for example, Financial Management) is available only through EPM Workspace. SSO access to Oracle Hyperion Financial Data Quality Management, Fusion Edition, is provided through Financial Management.

Assumptions

This document assumes the following:

- A fully functional Kerberos-enabled network environment.
  - The application server and HTTP server machines that host EPM System products are within the Kerberos realm.
  - The machines from which EPM System products are accessed are part of the Kerberos realm.
  - Browsers used to access EPM System products are configured for Integrated Windows Authentication. For information on enabling Integrated Windows Authentications, see:

    Internet Explorer 6 documentation: on the Microsoft Help and Support Web site.

    Firefox documentation: on the Firefox Support Web site.

- EPM System product users have Kerberos credentials that allow them to log in to client machines in the domain.

Kerberos SSO Using Oracle Application Server

Kerberos SSO for EPM System products uses OSSO to resolve identities between applications and Kerberos. EPM System products are registered as partner applications of OSSO. The OID used by OSSO is considered the identity repository. This OID must be synchronized with the Active Directory that Kerberos uses. OSSO, after resolving the user's identity with Kerberos, passes information about the user to EPM System product, which issues the SSO token that is used by all EPM System products to support SSO.

Assumptions

See "Assumptions" on page 36 for assumptions related to the network environment.

- OSSO is configured and running.
- The Active Directory used by Kerberos is synchronized with the OID used by OSSO. See "Integrating with Microsoft Active Directory" in the *Oracle Identity Management Integration Guide*.

  Make sure that the following modifications are made in the mapping file (`activeCfgImp.map`).

  - ○ `sn` attribute in the mapping file is populated with a value using the rule `SAMAccountName: : :user:sn: : person:`
  - ○ `uid` attribute is mapped to the user name without realm or domain suffixes or prefixes. You can do this by using the rule `userPrincipalName: : :user:uid: :inetorgperson:sAMAccountName`
- OSSO is configured to negotiate with Kerberos to resolve user credentials. See Windows Integration: Configuring the Import Connector in Oracle Security and Identity Management collateral.
- **Optional**: External authentication is configured to allow users to authenticate using their credentials stored in MSAD. See Windows Integration: Configuring External Authentication in Oracle Security and Identity Management collateral.

Configuring EPM System

Integrating Kerberos SSO requires that you enable SSO authentication in EPM System products.

➤ To configure Kerberos SSO using Oracle Application Server:

1 **Configure EPM System for Kerberos SSO. See the following topics:**

- "Configuring Shared Services for SSO" on page 40
- "Configuring EPM Workspace for SSO" on page 41

Note:

You must configure the OID of Oracle Identity Management Infrastructure as an external user directory in Shared Services. See "Configuring OID, MSAD, and Other LDAP-Based User Directories" on page 65.

2. **Provision at least one OID user as Shared Services administrator.**
3. **Restart Shared Services.**
4. **Configure Oracle Application Server instances for SSO.**

   See "Configuring Instances to Use 10.1.4 or 10.1.2 Oracle Identity Management" in the *Oracle Application Server Administrator's Guide* for instructions.
5. **Restart Oracle Identity Management Infrastructure, including OID.**
6. **Restart EPM System products and custom applications that use the Shared Services security APIs.**

Note:

Ensure that the external user directories configured with Shared Services are running before starting EPM System products.

Kerberos SSO with WebLogic Server

Oracle WebLogic Server Kerberos SSO uses the Negotiate Identity Asserter to negotiate and decode SPNEGO tokens to enable SSO with Microsoft clients. WebLogic Server decodes SPNEGO tokens to obtain Kerberos ticket and validates and maps the ticket to a WebLogic Server user. The MSAD Authenticator of WebLogic Server can be used with the Negotiate Identity Asserter to configure MSAD as the user directory for WebLogic Server users.

When the browser requests access to an EPM System product, KDC issues a Kerberos ticket to the browser, which creates a SPNEGO token containing the supported GSS token types. The Negotiate Identity Assertion provider decodes the SPNEGO token and uses GSSAPIs to accept the security context. The identity of the user who initiated the request is mapped to a user name and passed back to WebLogic Server. WebLogic Server also determines the groups to which the user belongs. At this stage, the requested EPM System product is made available to the user.

Note:

The user must use a browser that supports the SPNEGO (for example, Internet Explorer or Firefox) to access the EPM System products running on WebLogic Server. WebLogic Server can run on a UNIX or Windows platform.

Using the user ID derived from the authentication process, the EPM System product authorization process checks for provisioning data. Access to EPM System product is restricted based on the provisioning data.

Assumptions

See “Assumptions” on page 36 for assumptions related to the network environment.

- MSAD security groups and users are available to support WebLogic Server to MSAD hand shake. See “Configuring Single Sign-on with Microsoft Clients” in *Server 9.2 Documentation*.

  The MSAD user must be able to log in to WebLogic Server as a power user, preferably as WebLogic Server Administrator. The user account is updated by selecting these options:

  - `Use DES encryption types for this account`
  - `Do not require Kerberos preauthentication`

    See Microsoft documentation for detailed information.

  The configuration must support the use of Web server DNS name (reverse proxy) as Kerberos Service Principal Name.

- The `myrealm` security realm in the WebLogic Server domain is modified to add MSAD as the authentication provider. See WebLogic Server documentation for detailed information.

Enabling SSO in EPM System

Kerberos SSO using WebLogic Server requires that you enable SSO for EPM System products. See the following topics:

- “Configuring Shared Services for SSO” on page 40
- “Configuring EPM Workspace for SSO” on page 41

Kerberos SSO With WebSphere

The user must use a browser that supports the SPNEGO (for example, Internet Explorer or Firefox) to access EPM System products running on the WebSphere server.

Assumptions

See “Assumptions” on page 36 for assumptions related to the network environment.

- A Kerberos-enabled user directory.
- Fully configured WebSphere installation:
  - A Kerberos-enabled user directory is configured as the identity store for all EPM System product users.

    The configuration must support the use of Web server DNS name (reverse proxy) as Kerberos Service Principal Name.

    An account in the user directory is required to log on to WebSphere after the identity store is configured.
  - Application security is enabled.

- ❍ Trust association is enabled.
- ❍ SPNEGO trust association interceptor is configured.
- ❍ Protected URLs for EPM System products are configured.
- ❍ SSO domain is configured.
- ❍ **Optional:** JVM options for debugging SPNEGO and Kerberos are set.
- ❍ The keytab file was extracted from the domain controller and copied to the WebSphere server machine. The keytab file, an encrypted, local copy of the host's key, is required to decrypt service tickets sent by clients.

Enabling SSO in EPM System

Kerberos SSO using WebSphere requires that you enable SSO for EPM System products. See the following topics:

- "Configuring Shared Services for SSO" on page 40
- "Configuring EPM Workspace for SSO" on page 41

Configuring EPM System for SSO

EPM System products must be configured to support security agent for SSO. The configuration specified in Shared Services determines the following for all EPM System products:

- Whether to accept SSO from a security agent
- The authentication mechanism to accept for SSO

In an SSO-enabled environment, the EPM System product that is first accessed by the user parses the SSO mechanism to retrieve the authenticated user ID contained in it. The EPM System product checks the user ID against the user directories configured in Shared Services to determine that the user is a valid EPM System user. It also issues a token that enables SSO across EPM System products.

See the following topics for setting SSO mechanism for EPM System products.

- "Configuring Shared Services for SSO" on page 40
- "Configuring EPM Workspace for SSO" on page 41

Configuring Shared Services for SSO

The configuration specified in Shared Services enables SSO and determines the authentication mechanism to accept for SSO for all EPM System products. After configuring SSO in Shared Services, you must complete EPM System product configuration for SSO.

➤ To enable SSO from a Web identity management solution:

1 Launch the Shared Services Console. See "Launching Shared Services Console" on page 49. Log in as a Shared Services Administrator.

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

The Defined User Directories screen opens.

3 Verify that the user directories used by the Web identity management solution are configured as external user directories in Shared Services. See Chapter 5, "Configuring User Directories."

4 Select **Security Options.**

Security Options tab opens.

5 Select **Show Advanced Options.**

6 In **Single Sign-on Configuration** in the Defined User Directories screen, perform the following steps.

a. Select **Enable SSO**.

b. From **SSO Provider or Agent**, select a Web identity management solution. Choose **Other** if you are configuring SSO with Kerberos.

The recommended SSO mechanism is automatically selected. See Table 3. See "Supported SSO Methods" on page 26.

Note:

If you are not using the recommended SSO mechanism, you must choose `Other` in SSO Provider or Agent. For example, if you want to use a mechanism other than HTTP Header for SiteMinder, choose `Other` in SSO Provider or Agent and then select the SSO Mechanism you want to use in SSO Mechanism.

Table 3 Preferred SSO Mechanisms for Web Identity Management Solutions

Web Identity Management Solution	Recommended SSO Mechanism
Oracle Access Manager	`Custom HTTP Header`*
Oracle Application Server Single Sign-on (OSSO)	`Get Remote User from HTTP Request`
SiteMinder	`Custom HTTP Header`
Kerberos	Oracle Application Server: `Get Remote User from HTTP Request` WebLogic Server: `Custom HTTP Header` WebSphere: `Custom HTTP Header`

*The default HTTP Header name is `HYPLOGIN`. If you are using a custom HTTP Header, replace the name.

7 Click **OK.**

Configuring EPM Workspace for SSO

EPM Workspace delegates the process of handling SSO to EPM Workspace Core Services. To enable this process, you must configure the settings to establish trust between EPM Workspace and EPM Workspace Core Services. You must complete the following tasks:

- Enter SSO settings in Configuration and Monitoring Console (CMC)

- Define trusted password

Entering SSO settings in CMC

Using CMC, you must configure user name and password policies to enable EPM Workspace to establish trust between EPM Workspace and EPM Workspace Core Services. See *Oracle Enterprise Performance Management Workspace Administrator's Guide* for detailed information on using CMC.

➤ To define SSO settings in CMC:

1 Start CMC and Log in to CMC as an administrator.

2 In **Current View**, select **Web-Application Configuration**.

3 Right-click **Workspace Web-Application**, and select **Properties**.

4 Open **User Interface**.

5 Under **Login**, set the user name and password policy. See the online help for detailed information.

Table 4 Suggested Policy Settings

Security Agent*	Username Policy	Password Policy
OAM	$SECURITY_AGENT$	$TRUSTEDPASS$
OSSO	$REMOTE_USER$	$TRUSTEDPASS$
Kerberos	$REMOTE_USER$	$TRUSTEDPASS$
SiteMinder	$SECURITY_AGENT$	$TRUSTEDPASS$
HTTP (Web server)	$HTTP_USER$	$HTTP_PASSWORD$

*You can use a custom login class in EPM Workspace to check username and password before passing these values to EPM security. See "Using EPM Workspace Custom Login Class" on page 42

6 Click **OK**.

7 Restart EPM Workspace Web application.

Using EPM Workspace Custom Login Class

If you use a custom login class to check the user name and password before passing these values to EPM security, you must configure it in CMC.

➤ To configure custom login class for SSO:

1 Start CMC and Log in to CMC as an administrator.

2 In **Current View**, select **Web-Application Configuration**.

3 Right-click **Workspace Web-Application**, and select **Properties**.

4 Open **User Interface**.

5 Under **Login**, enter information. See Table 5

Table 5 Suggested Settings for Custom Login Class

Field	Description
LoginPolicyClass For	Name of the Java class (fully packaged name without the `.class` extension; for example, `com.oracle.customLogin`) in LoginPolicy class for $CUSTOM_LOGIN$
Username Policy	$CUSTOM_LOGIN$
Password Policy	$CUSTOM_LOGIN$*

*Can be `$TRUSTEDPASS$` or any other.

6 Click **OK.**

7 Restart EPM Workspace Web application.

Defining Trusted Password

Trusted password is used to establish a trust relationship between EPM Workspace Web application and EPM Workspace Core Service.

➤ To define a trusted password:

1 Launch EPM Workspace and log in as administrator.

2 From **Navigate**, select **Administer**, and then select **Authentication.**

3 Select **Enable Trusted Password.**

4 In **Password** and **Confirm Password**, enter the trusted password to use.

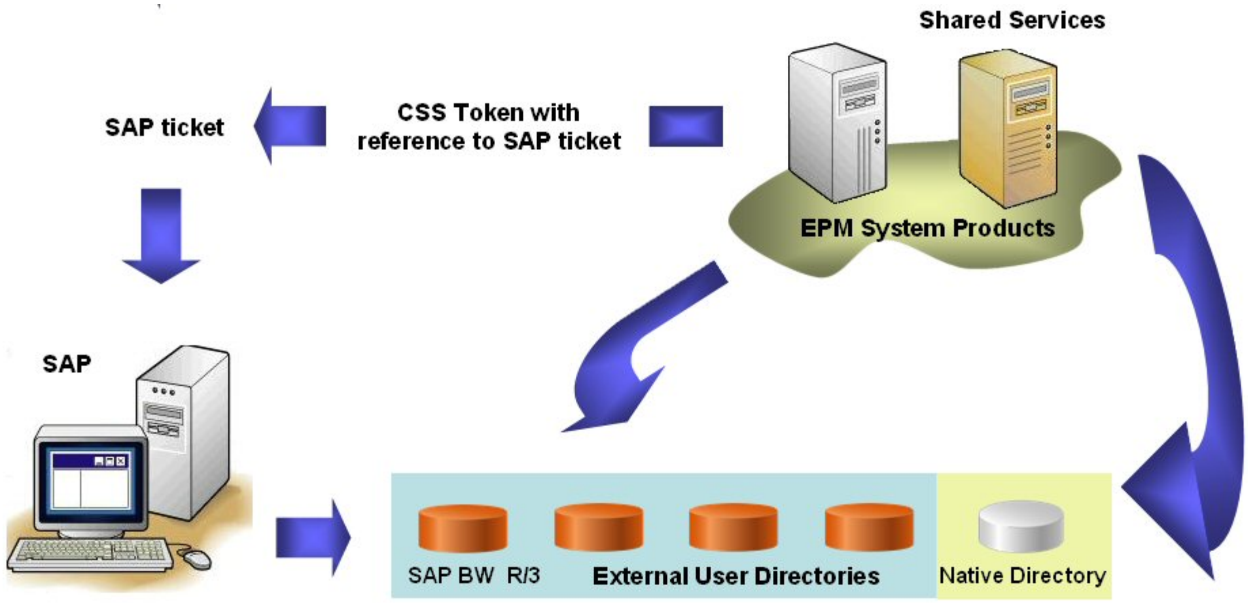
5 Click **OK.**

6 Restart Workspace Core Service.

7 Restart EPM Workspace Web application.

Single Sign-on with SAP Enterprise Portal

EPM System products handle SSO to SAP Enterprise Portal by issuing an SAP logon ticket. This action enables users who log in to EPM System products to navigate seamlessly to SAP applications. The illustrated concept:



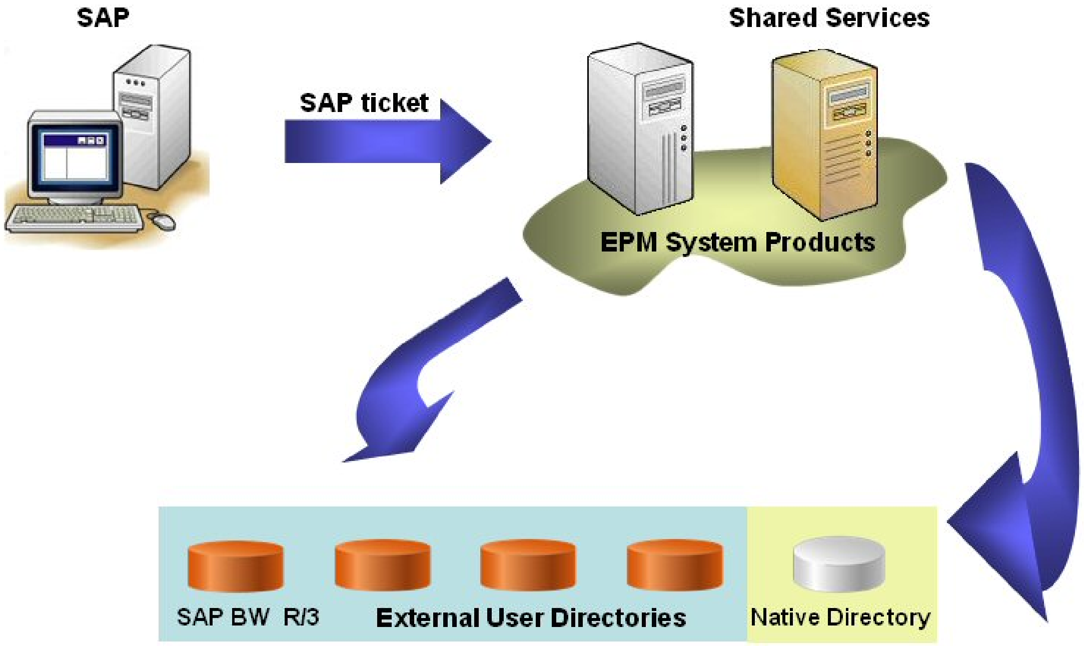
When a user logs in, the EPM System product authenticates the user against configured user directories, including Native Directory, and issues an EPM System logon token. This token enables SSO to EPM System products. It also generates SAP logon ticket.

Note:

For SSO with SAP to work, you must configure SAP native repository as an external user directory on Shared Services.

When the user subsequently navigates to the SAP system or uses an SAP data source, the SAP logon ticket contained in the EPM System token is passed to SAP to enable SSO. The SAP system assumes the responsibility to validate the credentials in the SAP logon ticket.

EPM System products handle SSO from SAP Enterprise Portal by accepting an SAP logon ticket. This action enables users who log in to SAP Enterprise Portal to navigate seamlessly between SAP and EPM System products. The illustrated concept:



When a user logs in to SAP Enterprise Portal, SAP authenticates the user.

When the user navigates to an EPM System product, the SAP ticket is passed to the EPM System product. Using an SAP certificate stored on the Shared Services server machine, the EPM System retrieves the user name, which is trusted as being that of a valid user. The EPM System product queries user directories to determine the user's groups. Using the group information, EPM System product gets provisioning information.

Note:

The SAP provider must be configured as a user directory in Shared Services for this process to work.

Nested SAP Groups

After configuring an SAP user directory, available SAP users and groups are displayed in Shared Services Console. Shared Services considers the SAP roles to be the equivalents of groups created by any corporate directory server. Each role from the SAP user directory is displayed as a distinct group in Shared Services Console. Shared Services, however, does not retrieve the relationships between simple and composite roles within the SAP user directory. If needed, nested groups can be created in Native Directory to mimic the relationship that existed between the simple and composite roles in the SAP user directory. This approach, however, has performance implications and should be avoided, if possible.

Deployment Locations

Deployment location conventions:

- *HYPERION_HOME* denotes the root directory where EPM System products are installed. The location of this directory is specified during the installation process. For example: `C:\Hyperion` (Windows) and `/vol1/Hyperion` (UNIX)
- *HSS_HOME* denotes the Shared Services root directory. For example:

  `C:\Hyperion\deployments\`*App_Server_Name*`\SharedServices9` (Windows) and `/vol1/Hyperion/deployments/`*App_Server_Name*`/SharedServices9` (UNIX)

Prerequisites

- All SAP systems within the SAP landscape must be set up for SSO with the SAP login ticket. User names must be normalized across the SAP landscape so that a user name in one SAP system refers to the same user across all SAP systems. See SAP documentation for more information.
- Copy or download the SAP JCo binaries or shared libraries into *HYPERION_HOME*`/common/SAP/bin` directory.

  JCo binaries and shared libraries are available in your SAP distribution. Registered SAP users can download them from the SAP Web site `https://service.sap.com/connectors`.
- Copy or download the SAP JCo archives (.jar files) and libraries into *HYPERION_HOME*`/common/SAP/lib` directory.

  JCo archives and libraries are available in your SAP distribution. Registered SAP users can download them from the SAP Web site `https://service.sap.com/connectors`.

  The following libraries are required to verify the SAP SSO ticket provided to EPM System products. This step is required only if EPM System products are plugged into SAP Enterprise Portal.

  - `com.sap.security.core.jar`
  - `com.sap.security.api.jar`
  - `sapjco.jar`
  - `sap.logging.jar`
  - `iaik_jce.jar`
  - `iaik_jce_export.jar` (if using the export version of the IAIK-JCE libraries)
- Expand the contents of each SAP .jar file by running `explodejar` available in *HYPERION_HOME*`/common/SAP/lib` directory.
- Using Shared Services Console, configure the SAP native repository as an external user directory in Shared Services. See “Configuring an SAP R3 Native Repository” on page 74 for detailed information.
- Install the SAP Digital Certificate (SAP X509 certificate, `SAP.keystore`) in a convenient location. Oracle recommends that this certificate be installed in *HSS_HOME*`/config`. For example: `C:\Hyperion\deployments\9\SharedServices9\config` (Windows) or `/vol1/Hyperion/deployments/9/SharedServices9/config` (UNIX)

- Using Shared Services Console, provision SAP users and groups to provide them appropriate access rights to EPM System products. See Chapter 9, "Managing Provisioning".

4 Shared Services Console

In This Chapter

Launching Shared Services Console

To launch Shared Services Console:

- Using a browser, access the Shared Services Console URL
- For Windows, select Start, then All Programs, then Oracle EPM System, then Foundation Services, and then Shared Services Console
- Use an EPM System product interface

➤ To launch Shared Services Console from a URL:

1 **Using a browser, access the following URL:**

`http://server_name:port_number/interop`

In the URL, `server_name` indicates the name of the computer where the application server that hosts Shared Services is running, and `port_number` indicates the server port that Shared Services is using; for example, `http://myserver:28080/interop`.

Note:

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

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

Initially, the only user who can access Shared Services Console is `admin` (default password for `admin` is `password`).

3 **Click Log On.**

Note:

Valid SAP users may get a `CSSAuthenticationException` error message during log on if the SAP account is locked. Contact your SAP Administrator to unlock the account.

If you receive Java Virtual Machine (JVM) errors in Shared Services Console while using Microsoft Internet Explorer, ensure that your Internet Explorer installation includes Microsoft XML parser (MSXML) version 4. MSXML is bundled with Internet Explorer 6.0.

To verify that you have the correct MSXML, check for the following file:

```
c:\winnt\system32\msxml4.dll
```

If this file is missing, install Internet Explorer 6.0 or later.

Overview of Shared Services Console

Shared Services Console comprises a View pane and task tabs. When you initially log in, the Shared Services Console displays the View pane and a Browse tab.

The View pane is a navigation frame where you can choose objects (such as user directories, users, groups, roles, projects, and applications). Typically, the details of your current selection in the View pane are displayed in the Browse tab. Additional task tabs open as needed depending on the task that you perform; for example, a Report tab opens when you generate a report, and a Configure tab opens when you configure a user directory.

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

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

Note:

The Oracle Technology Network provides the most recent product documentation for the current release.

Navigating in Shared Services Console

When performing actions on objects in the View pane, you can right-click an object to access a shortcut menu. Options on these menus change dynamically, depending on what you select. The commands displayed in the shortcut menu also are available in 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.

Searching for Users, Groups, Roles, and Delegated Lists

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

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

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

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

1 In the View pane, expand **User Directories.**

2 From the user directory that you want to search, select one of the following:

- Users
- Groups
- Roles
- Delegated List

Note:

Roles and Delegated List options are available only in Native Directory searches.

Available search fields appear in the Browse tab.

3 To search for users:

a. In **User Property**, select a user property that you want to search.

   The user properties that you can select depend on the type of the user directory you selected. For example, you can search user name, first name, last name, description, and e-mail address if you selected an LDAP-based user directory. 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

   Searchable user properties:

   - **LDAP-based user directories**: User name, first name, last name, description, and e-mail address
   - **NTLM:** User name, first name, and last name
   - **SAP and Database providers**: User name

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

c. **Optional**: In **In Group**, specify the groups (in Group1;Group2 format) where the search is to be performed. Use an asterisk (*) as the wildcard in pattern searches. To search multiple groups, use a semicolon to separate group names.

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

e. Click **Search**.

4 To search for groups:

a. In **Group Property** select a property that you want to search. If this property is unspecified in the user directory, the search does not retrieve any records.

Note:

Shared Services considers Oracle, SQL Server, and SAP roles equivalent to groups in user directories. Oracle roles can contain other roles, creating a hierarchy of roles. Shared Services does not display the relationships between database roles in the search results but honors them during provisioning. SQL Server roles cannot be nested. Shared Services does not display groups if you select a DB2 database provider because DB2 does not support roles.

b. In **Group Filter**, type a search filter. 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 that you want to search. If this property is unspecified in Native Directory, the search does not retrieve any records.

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

6 Click **Search.**

7 To search for delegated lists:

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

b. Click **Search**.

5 Configuring User Directories

In This Chapter

Setting up Oracle Internet Directory as the Native Directory

OpenLDAP is automatically configured as the Native Directory when you install and deploy Shared Services. Oracle Internet Directory (OID) is not installed as a part of the Shared Services installation.

Caution!

You cannot use OID as the Native Directory in a mixed environment comprising EPM System 11.1.1.2 and System 9 products. For example, you cannot use OID as the Native Directory if you have an environment where System 9 products (version 9.3.1 or 9.2.x) are registered with Shared Services version 11.1.1.2.

When you configure OID as the Native Directory, Shared Services seeds the Native Directory schema into OID. Because the Native Directory schema is created in a new realm (`dc=css,dc=example,dc=com`) within the root DN of OID, the configuration process does not impact the existing schema.

Note:

If using OID as the Native Directory, you can improve performance by tuning the configuration settings of the OID database. See OID Tuning and Configuration Quick Reference Guide for the recommended minimum configuration settings for OID.

A new password policy is enforced on the Native Directory realm, which the OID administrator can change. This policy applies to `dc=css,dc=example,dc=com` realm only.

See Chapter 8, “Managing Native Directory” for detailed procedures on working with Native Directory.

Migrating an Existing OpenLDAP to OID

If you are upgrading to Shared Services version 11.1.1.2 and plan to use OID as the Native Directory in place of OpenLDAP, follow these steps:

Note:

See *Oracle Hyperion Enterprise Performance Management System Installation and Configuration Guide* for information on upgrading your products.

- Upgrade Shared Services.
- Generate a provisioning report that lists the current provisioning relationships. See “Generating Provisioning Reports” on page 129.
- Use Lifecycle Management Utility to extract data from existing OpenLDAP. See “Migrating Native Directory (Security)” in *Oracle Hyperion Enterprise Performance Management System Lifecycle Management Guide*.
- Modify the Native Directory Configuration to identify OID as the Native Directory. See “Modify the Native Directory Configuration” on page 55.
- Restart Shared Services.
- After Shared Services restart is complete, restart other EPM System products and custom applications that use the Shared Services security APIs.
- Use Lifecycle Management Utility to import data into OID, which is configured as the Native Directory. See “Migrating Native Directory (Security)” in the *Oracle Hyperion Enterprise Performance Management System Lifecycle Management Guide*.

Caution!

Migrating OpenLDAP data into a password-policy-enabled OID will fail if the passwords set in OpenLDAP do not comply with the password policy. To ensure a successful migration of existing OpenLDAP passwords, you must remove the password policy restrictions for Native Directory realm. See Oracle Internet Directory documentation for information on removing password policy restrictions. After completing the migration, restore the password policy for Native Directory.

- Generate a provisioning report that lists all provisioning relationships and compare it against the provisioning report you generated before reconfiguring Native Directory. See "Generating Provisioning Reports" on page 129.

Using OID as Native Directory for New Installations

For new Shared Services version 11.1.1.2 installations, follow these steps to use OID as the Native Directory:

- Modify the Native Directory Configuration to identify OID as the Native Directory. See "Modify the Native Directory Configuration" on page 55.
- Restart Shared Services.
- Restart other EPM System products and custom applications that use the Shared Services security APIs.

Modify the Native Directory Configuration

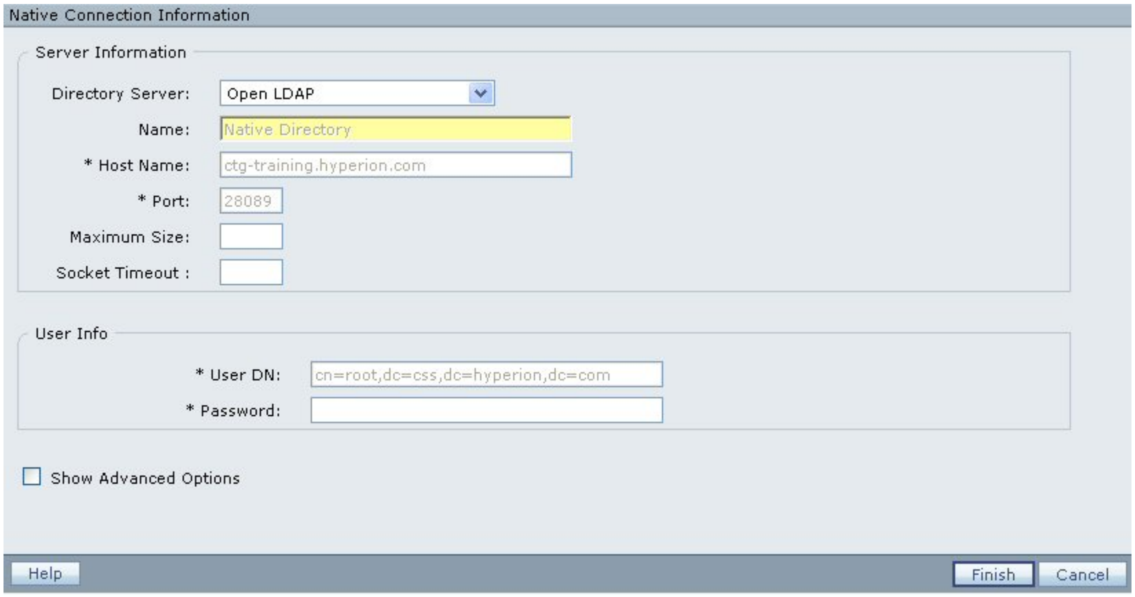
By default, the Native Directory configuration settings point to the OpenLDAP instance that was installed with Shared Services. You must modify the Native Directory configuration so that it points to the OID that you want to use as the Native Directory.

➤ To modify Native Directory settings:

1. Launch the Shared Services Console. See "Launching Shared Services Console" on page 49. Log in as a Shared Services Administrator.
2. Select **Administration**, then **Configure User Directories.**

   The Defined User Directories screen opens.
3. Select **Native Directory.**
4. Click **Edit.**

   The Native Connection Information screen opens.



Native Connection Information

Server Information

Directory Server:	Open LDAP
Name:	Native Directory
* Host Name:	ctg-training.hyperion.com
* Port:	28089
Maximum Size:	
Socket Timeout :	

User Info

* User DN:	cn=root,dc=css,dc=hyperion,dc=com
* Password:	

□ Show Advanced Options

5 **Modify the parameters as indicated in Table 6.**

Table 6 Connection Information for OID

Label	**Description**
Directory Server	Select `Oracle Internet Directory`
Host Name	Name of the server that hosts OID. **Example:** `MyServer`
Port	The server port number where OID is running. **Example:** `13060`
Maximum Size	Maximum number of results that a search for users, groups, and roles can return. Leave this value blank to retrieve all users and groups that meet the search criteria. If you are configuring Shared Services in Delegated Administration mode, set this value to 0.
Socket Time Out	The maximum time that Shared Services will wait for a response from OID.
User DN	The user account that Shared Services should use to establish a connection with OID. Use a user account that can make schema changes in OID. Use of the `orcladmin` or a similar account is recommended. Special characters are not allowed in the User DN value. See “Using Special Characters” on page 88. **Example:** `cn=orcladmin`
Password	Password of the account specified in User DN. **Example:** `UserDNpassword`

6 **Click Save.**

Detailed information about reconfiguring the Native Directory is written to `SharedServices_Security.log`

Import OpenLDAP Data into OID

Note:

This step is needed only if you have previously used OpenLDAP to provision EPM System product users and groups. If this is a new Shared Services deployment, do not perform this task.

Use Lifecycle Management Utility to migrate provisioning information from OpenLDAP to OID. See *Oracle Hyperion Enterprise Performance Management System Lifecycle Management Guide*.

Note:

Importing data into a password-policy-enabled OID will fail if OpenLDAP passwords do not comply with the password policy. To ensure a successful migration of OpenLDAP passwords, remove the password policy restrictions for Native Directory realm.

Restart Shared Services

Restart Shared Services Web application to ensure that all the changes take effect.

Caution!

Ensure that OID is running before restarting Shared Services.

Restart EPM System Products

After Shared Services restart is complete, restart other EPM System products and custom applications that use the Shared Services security APIs.

Using a Custom Authentication Module

EPM System products (thick and thin clients) use a login screen to capture the user name and password, which are used to authenticate users. Instead of using EPM System authentication, you can write a custom authentication module to authenticate users against any system by implementing the `CSSCustomAuthenticationIF`Java interface. The system, which the custom module uses for authenticating users, need not be configured as an external provider in Shared Services.

Note:

The custom module must return a user name that exists in the user directory for which the custom module is enabled. Also, ensure that the user name returned does not contain an * (asterisk).

The custom authentication module uses the information entered in the EPM System login screen. The custom authentication module, if enabled for a user directory, authenticates users using its own code. On successfully authenticating the user, the custom module returns the user name.

The custom authentication module must implement the public interface `CSSCustomAuthenticationIF`. This interface is defined in `com.hyperion.css` package as a part of the standard Shared Services APIs.

`CSSCustomAuthenticationIF` comprises the `authenticate` method, which accepts the user name and password as input parameters. If the user is authenticated by the custom module, this method returns the user name of authenticated user. If the user is not found, it throws a `java.lang.Exception`. The following is a sample custom authentication Java file.

```
package com.hyperion.css.custom;

import java.util.Map;
import com.hyperion.css.CSSCustomAuthenticationIF;
import org.apache.log4j.Logger; //   imports Log4j's Logger

public class CustomAuthenticationImpl implements CSSCustomAuthenticationIF{

//get the Logger to log exception or debug information
// Log information is written to the security log

static Logger
logger=Logger.getLogger("com.hyperion.css.custom.CustomAuthenticationImpl")
;
public String authenticate(Map context,String userName, String
password)throws Exception{

  try {
  /*  Your custom code goes here. Your code  should do the follwoing:
   // for authenticated users, set authenticationSuccessFlag = true
  // return authenticated userName (return value format can be
userName@providerName
  // if authentication fails, ensure debug is enabled using
logger.isDebugEnabled()
  // log an authentication failure
   // return a null value for userName or throw an exception */

  }catch (Exception e){

  /*  Your custom code goes here. It should
  // catch authentication exception
  // create new exception, set the root cause
  // set any custom error message
  // return the exception to the caller
*/  }
```

```
            return authenticatedUserName;
        }
}
```

The custom authentication class must be included in the classpath. The easiest method for web applications to do this is to add the custom jar file to *HYPERION_HOME*/deployments/*APPLICATION_SERVER*/*PROD_WEB_APP*/webapps/*ROOT_CONTEXT*/WEB-INF/lib directory. For example, for Shared Services deployed on Embedded Java Container, the classpath is *HYPERION_HOME*/deployments/Tomcat5/SharedServices9/webapps/interop/WEB-INF/lib. For EPM System applications that are not deployed on an application server, the easiest method to include custom authentication class in the classpath is to add the custom class to the existing CSS libraries.

Shared Services automatically picks up the custom authentication class file if you use the default class name (CustomAuthenticationImpl) and package (com.hyperion.css.custom). In this scenario, you need not update the Shared Services configuration to specify the custom authentication class.

Caution!

If you are enabling custom authentication for Oracle Essbase, you must specify the fully qualified class name of the custom class even if you use the default class and package name.

If you use a custom class name or package, you must identify the fully qualified Java class name of the custom authentication class in the Shared Services configuration. In Shared Services, custom authentication class is identified at the global level; only one custom authentication module can be used in a deployment. If a custom module class name is not specified at the global level, (in Security options screen), Shared Services looks for CustomAuthenticationImpl within the classpath. If CustomAuthenticationImpl is not found, the default EPM System authentication is used to authenticate users. By default, use of custom authentication module for all external user directories is enabled. You can disable its use for each user directory. If a user directory is not configured to use custom authentication, Shared Services uses default authentication for that directory.

See “Configuring OID, MSAD, and Other LDAP-Based User Directories” on page 65 and “Setting Security Options” on page 86 for detailed procedures to enable custom authentication of users.

Manual steps must be completed for each EPM System product to support custom authentication. These steps are discussed in the following sections:

- “Shared Services Custom Authentication” on page 60
- “EPM Workspace Custom Authentication” on page 60
- “Essbase Custom Authentication” on page 60
- “Planning Custom Authentication” on page 62
- “Financial Management Custom Authentication” on page 63

Shared Services Custom Authentication

Perform these steps to enable Shared Services custom authentication.

➤ To support custom authentication:

1 **Stop Shared Services.**

2 **Create a** `.jar` **file containing the files required for the custom authentication module.**

3 **Copy the custom authentication module's** `.jar` **file into** *`HYPERION_HOME`*`/deployments/`*`APPLICATION_SERVER`*`/SharedServices9/webapps/interop/WEB-INF/lib` **directory.**

Note:

If you are using WebLogic, copy the custom authentication module's `.jar` file into `%TEMP%\`*`USER_NAME`*`\servers\SharedServices9\tmp\_WL_user\interop\`*`SOME_UNIQUE_ID`*`\war\WEB-INF\lib` directory also.

4 **Reconfigure external user directories and Native Directory as needed. See:**

- "Configuring OID, MSAD, and Other LDAP-Based User Directories" on page 65
- "Setting Security Options" on page 86

5 **Start Shared Services.**

EPM Workspace Custom Authentication

Perform these steps to enable EPM Workspace custom authentication.

➤ To enable EPM Workspace custom authentication:

1 **Stop EPM Workspace and Reporting and Analysis Core Services.**

2 **Copy the custom authentication module** `.jar` **file into the following locations:**

- *`HYPERION_HOME`*`/deployments/APPLICATION_SERVER/Workspace/webapps/workspace/WEB-INF/lib`
- *`HYPERION_HOME`*`/common/CSS/9.5.0.0/lib` on the machine where Reporting and Analysis Core Services are deployed.

  Be sure to add the custom authentication module `.jar` file to the classpath.

3 **Start Reporting and Analysis Core Services and EPM Workspace .**

Essbase Custom Authentication

Manual procedures must be completed for Essbase Server and Administration Services.

Essbase Server

To enable custom authentication, you must add the custom authentication class file to the `css-9_5_0.jar` file that Essbase uses.

➤ To enable Essbase custom authentication:

1. **Shut down Essbase server.**
2. **Create a backup copy of** *`HYPERION_HOME`*`/common/CSS/9.5.0.0/lib/css-9_5_0.jar`**.**
3. **Rename** *`HYPERION_HOME`*`/common/CSS/9.5.0.0/lib/css-9_5_0.jar` **as** `css-9_5_0.zip`**.**
4. **Extract the contents of** `css-9_5_0.zip` **into another temporary directory; for example,** `temp1`**.**
5. **Copy the custom authentication module class files into the temporary directory where you extracted the contents of** `css-9_5_0.zip`**.**

   If you have developed a package called `com.yourcompany.customauth` for your custom code , make sure your class is copied in the `com/yourcompany/customauth` folder.
6. **Zip up the contents of the temporary directory** `temp1` **as** `css-9_5_0.zip`
7. **Rename** `css-9_5_0.zip` **as** `css-9_5_0.jar`**.**
8. **Copy** `css-9_5_0.jar` **into** *`HYPERION_HOME`*`/common/CSS/9.5.0.0/lib`**.**
9. **Start Essbase server.**

Administration Services

To enable custom authentication, you must add the custom authentication `.jar` file to the `eas.ear` file and redeploy it to the application server.

➤ To enable Administration Services custom authentication:

1. **Stop Administration Services on the application server, if it is running.**
2. **Create a backup copy of** *`HYPERION_HOME`*`/products/Essbase/eas/server/AppServer/InstallableApps/Common/eas.ear`**.**
3. **Rename** *`HYPERION_HOME`*`/products/Essbase/eas/server/AppServer/InstallableApps/Common/eas.ear` **as** `eas.zip`**.**
4. **Extract the contents of** `eas.zip` **into a temporary directory; for example,** `temp1`**.**
5. **In the temporary directory; for example,** `temp1`**; rename** `eas.war` **to** `eas.zip`**.**
6. **Extract the contents of** `eas.zip` **into another temporary directory; for example,** `temp2`**.**
7. **Copy the** `.jar` **file of the custom authentication module into** `WEB-INF/lib` **directory within** `temp2`**.**
8. **Zip up the contents of** `temp2` **and create** `eas.zip`**.**
9. **Copy** `eas.zip` **into** `temp1` **and rename it** `eas.war`**.**
10. **Zip up the contents of** `temp1` **and create** `eas.zip`**.**

11 Copy `eas.zip` into *HYPERION_HOME*`/products/Essbase/eas/server/AppServer/InstallableApps/Common` and rename it as `eas.ear`.

12 Using Oracle's Hyperion Enterprise Performance Management System Configurator, deploy the updated `eas.ear` to the application server. See *Oracle Hyperion Enterprise Performance Management System Installation and Configuration Guide*.

13 Start Administration Services.

Planning Custom Authentication

To enable custom authentication, you must add the custom authentication `.jar` file to the `planning.ear` file and redeploy it to the application server.

➤ To enable Administration Services custom authentication:

1 Stop Planning on the application server, if it is running.

2 Create backup copies of *HYPERION_HOME*`/products/Planning/config/PlanningSystemDB.properties` and *HYPERION_HOME*`/products/Planning/Offline/lib/HBRServer.properties` files for all Planning servers.

3 Create a backup copy of *HYPERION_HOME*`/products/Planning/AppServer/InstallableApps/Common/HyperionPlanning.ear`.

4 Rename *HYPERION_HOME*`/products/Planning/AppServer/InstallableApps/Common/HyperionPlanning.ear` as `HyperionPlanning.zip`.

5 Extract the contents of `HyperionPlanning.zip` into a temporary directory; for example, `temp1`.

6 In the temporary directory; for example, `temp1`; rename `HyperionPlanning.war` to `HyperionPlanning.zip`.

7 Extract the contents of `HyperionPlanning.zip` into another temporary directory; for example, `temp2`.

8 Copy the `.jar` file of the custom authentication module into `WEB-INF/lib` directory within `temp2`.

9 Zip up the contents of `temp2` and create `HyperionPlanning.zip`.

10 Copy `HyperionPlanning.zip` into `temp1` and rename it `HyperionPlanning.war`.

11 Zip up the contents of `temp1` and create `HyperionPlanning.zip`.

12 Copy `HyperionPlanning.zip` into *HYPERION_HOME*`/products/Planning/AppServer/InstallableApps/Common`.

13 Rename as `HyperionPlanning.zip` to as `HyperionPlanning.ear`.

14 Using EPM System Configurator, deploy the updated `HyperionPlanning.ear` to the application server. See *Oracle Hyperion Enterprise Performance Management System Installation and Configuration Guide*.

Caution!

To ensure that database tables are preserved during the deployment process, select Reuse Existing Tables while specifying database settings.

15 Using the backup copies created in step 2, restore *HYPERION_HOME*/products/Planning/config/PlanningSystemDB.properties and *HYPERION_HOME*/products/Planning/Offline/lib/HBRServer.properties files on all Planning servers.

16 Start Planning.

Financial Management Custom Authentication

➤ To enable custom authentication:

1 Stop all Financial Management processes, especially CASSecurity.exe.

2 Copy the custom authentication module .jar file into*HYPERION_HOME*/common/CSS/9.5.0.0/lib.

3 Add the custom authentication module .jar file to the classpath by adding it in the Windows registry entry for Financial Management (similar to css-9_5_0.jar file).

4 Start all Financial Management processes.

Other Products

The custom authentication class must be included in the classpath. The easiest method for web applications to do this is to add the custom jar file to *HYPERION_HOME*/deployments/*APPLICATION_SERVER*/*PROD_WEB_APP*/webapps/*ROOT_CONTEXT*/WEB-INF/lib directory. For example, for Shared Services deployed on Embedded Java Container, the classpath is *HYPERION_HOME*/deployments/Tomcat5/SharedServices9/webapps/interop/WEB-INF/lib. For EPM System applications that are not deployed on an application server, the easiest method to include custom authentication class in the classpath is to add the custom class to the existing CSS libraries as a .jar file. Alternatively, you may add the .jar file to the classpath.

Operations Related to User Directory Configuration

By default, OpenLDAP is installed and configured as the Native Directory. To use OID as the Native Directory, see "Setting up Oracle Internet Directory as the Native Directory" on page 53.

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

- Configuring user directories:
  - "Configuring OID, MSAD, and Other LDAP-Based User Directories" on page 65
  - "Configuring an SAP R3 Native Repository" on page 74
  - "Configuring Relational Databases as User Directories" on page 76

- “Testing User Directory Connections” on page 78
- “Editing User Directory Settings” on page 79
- “Modifying NTLM External User Directory Configurations” on page 82
- “Deleting User Directory Configurations” on page 84
- “Managing User Directory Search Order” on page 84
- “Setting Security Options” on page 86

MSAD Information

This section explains some MSAD concepts used in this document.

DNS Lookup and Host Name Lookup

You can configure MSAD so that Shared Services can perform a static host name lookup or a DNS lookup to identify MSAD. Static host name lookup does not support MSAD failover without updating the MSAD configuration in Shared Services.

Using the DNS lookup ensures high availability of MSAD in scenarios where MSAD 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 MSAD 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 MSAD objects in a forest. It stores a complete copy of all objects in the directory for its host domain and a partial copy of all objects for all other domains in the forest, which are used in typical user search operations. See Microsoft documentation for information on setting up a global catalog.

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

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

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

Configuring OID, MSAD, and Other LDAP-Based User Directories

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

Note:

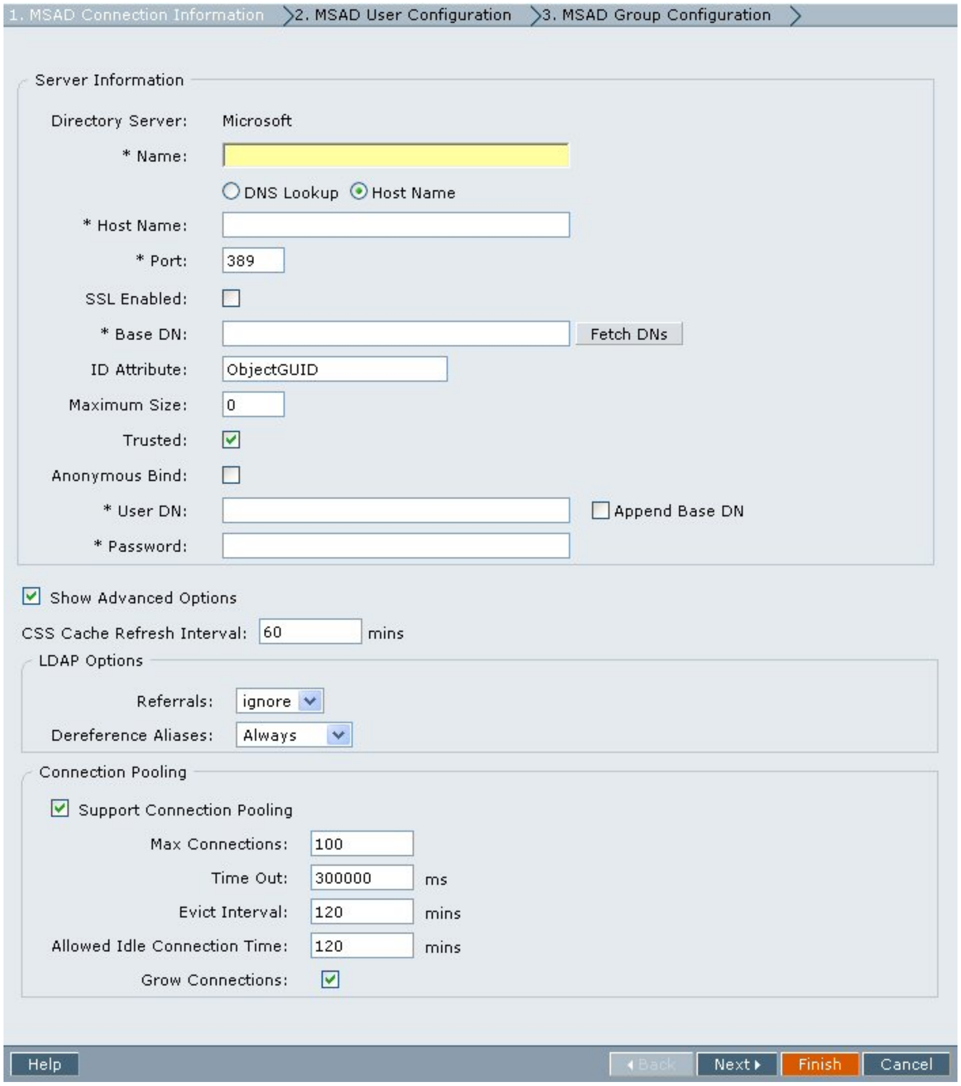
Oracle Virtual Directories that are configured to use a database can be configured in Shared Services as external LDAP-based user directories.

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

1. Launch Shared Services Console. See "Launching Shared Services Console" on page 49.
2. Select **Administration**, then **Configure User Directories.**

   The Defined User Directories screen opens, listing all user directories, including Native Directory, that are already configured.
3. Click **Add.**
4. In **Directory Type**, select an option:
   - **Lightweight Directory Access Protocol** (**LDAP**) to configure an LDAP-based user directory other than MSAD.
   - **Microsoft Active Directory** (**MSAD**) to configure MSAD.
5. Click **Next.**

   The Connection Information screen for the selected user directory type opens.


1. MSAD Connection Information
2. MSAD User Configuration
3. MSAD Group Configuration
Fetch DNs
Help
Back
Next
Finish
Cancel

Server Information

Directory Server: Microsoft

* Name:

○ DNS Lookup ● Host Name

* Host Name:

* Port: 389

SSL Enabled: □

* Base DN:

ID Attribute: ObjectGUID

Maximum Size: 0

Trusted: ☑

Anonymous Bind: □

* User DN: □ Append Base DN

* Password:

☑ Show Advanced Options

CSS Cache Refresh Interval: 60 mins

LDAP Options

Referrals: ignore

Dereference Aliases: Always

Connection Pooling

☑ Support Connection Pooling

Max Connections: 100

Time Out: 300000 ms

Evict Interval: 120 mins

Allowed Idle Connection Time: 120 mins

Grow Connections: ☑

6 Enter the required parameters.

Table 7 Connection Information Screen

Label	Description
Directory Server	Select a user directory. Select `Other` if you are using an LDAP Version 2 (or later) product other than those listed. The **ID Attribute** value changes to the recommended constant identity attribute for the selected product. **Note:** To configure an existing Oracle Virtual Directory that is configured with an underlying database, choose `Other`. **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. **Example:** `MY_OID`
DNS Lookup	**MSAD only:** Select this option to enable DNS lookup. See “DNS Lookup and Host Name Lookup” on page 64.

Label	Description
	Note: Do not select this option if you are configuring a global catalog.
Hostname	**MSAD only:** Select this option to enable static host name lookup. See "DNS Lookup and Host Name Lookup" on page 64.
Host Name	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. If you are using DNS lookup for MSAD, specify the DNS server name. See "DNS Lookup and Host Name Lookup" on page 64. **Note:** If you are configuring an MSAD global catalog, specify the global catalog server host name. See "Global Catalog" on page 64. **Example:** `MyServer`
Port	The port number where the user directory is running. **Note:** If you are configuring an MSAD global catalog, specify the port used by the global catalog server (default is 3268). See "Global Catalog" on page 64. **Example:** `389`
SSL Enabled	The check box that enables Secure Socket Layer (SSL) communication with this user directory. The user directory must be configured for secure communication.
Base DN	The distinguished name (DN) of the node where the search for users and groups should begin. You can also use the Fetch DNs button to list available base DNs and then select the appropriate base DN from the list. **Note:** If you are configuring a global catalog, specify the base DN of the forest. See "Using Special Characters" on page 88 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	A unique user attribute. The recommended value of this attribute is automatically set for OID `orclguid`, SunONE (`nsuniqueid`), IBM Directory Server (`Ibm-entryUuid`), Novell eDirectory (`GUID`), and MSAD (`ObjectGUID`). You may change the default value if necessary. **Example:** `orclguid`
Maximum Size	Maximum number of results that a search can return. If this value is greater than that supported by the user directory settings, the user directory value overrides this value. For LDAP-based user directories other than MSAD, leave this blank to retrieve all users and groups that meet the search criteria. For MSAD, set this value to `0` to retrieve all users and groups that meet the search criteria. If you are configuring Shared Services in Delegated Administration mode, set this value to 0.
Trusted	The check box to indicate that this provider is a trusted SSO source. SSO tokens from trusted sources do not contain the user's password.
Anonymous Bind	The check box to indicate that Shared Services can bind anonymously to the user directory to search for users and groups. Can be used only if the user directory allows anonymous binds. If this option is not selected, you must specify in the User DN an account with sufficient access permissions to search the directory where user information is stored. Oracle recommends that you do not use anonymous bind.

Label	Description
	Note: Anonymous bind is not supported for OID.
User DN	This box is disabled if Anonymous Bind is selected. The distinguished name of the user that Shared Services should use to bind with the user directory. This distinguished name must have read privileges within the Base DN. Special characters are not allowed in the User DN value. See "Using Special Characters" on page 88 for restrictions. **Example:** `cn=admin,dc=example,dc=com`
Append Base DN	The check box for appending the base DN to the User DN. If you are using Directory Manager account as the User DN, do not append Base DN. This check box is disabled if the Anonymous Bind option is selected.
Password	User DN password. This box is disabled if the Anonymous Bind option is selected. **Example:** `UserDNpassword`
Show Advanced Options	The check box to display advanced options.
CSS Cache Refresh Interval	Interval (minutes) for refreshing the Shared Services cache that contains user and group information from the user directory. Provisioning information for newly added users and groups in user directories is available to Shared Services only after the next cache refresh. This may result in new users and members of new groups not getting their provisioned roles for the duration of the refresh interval. **Example:** `75`
Referrals	**MSAD only:** Select `follow` to automatically follow LDAP referrals. Select `ignore` to not use referrals.
Dereference Aliases	Select the method that Shared Services searches should use to dereference aliases in the user directory so that searches retrieve the object to which the DN of the alias points. Select: ● **Always**: Always dereference aliases ● **Never**: Never dereference aliases ● **Finding**: Dereference aliases only during name resolution ● **Searching**: Dereference aliases only after name resolution
Support Connection Pooling	The check box to enable connection pooling for this user directory
Max Connections	Maximum connections in the pool. Default is 100 for LDAP-based directories, including MSAD, and 300 for Native Directory.
TimeOut	Time out to get a connection from the pool. An exception is thrown after this period. Default is 300000 milliseconds (5 minutes).
Evict Interval	**Optional:** The interval for running the eviction process to clean the pool. The eviction process removes idle connections that have exceeded the `Allowed Idle Connection Time`. Default is 60 minutes.

Label	Description
Allowed Idle Connection Time	**Optional:** The time after which the eviction process removes the idle connections in the pool. Default is 120 minutes.
Grow Connections	This option indicates whether the connection pool can grow beyond `Max Connections`. Selected by default. If you do not allow the connection pool to grow, the system throws an error if a connection is not available within the time set for `Time Out`.
Use Authentication Module	The check box to enable the use of a custom authentication module to authenticate users defined in this user directory. The fully qualified Java class name of the authentication module must be specified in the Security Options screen. See “Setting Security Options” on page 86. See “Using a Custom Authentication Module” on page 57.

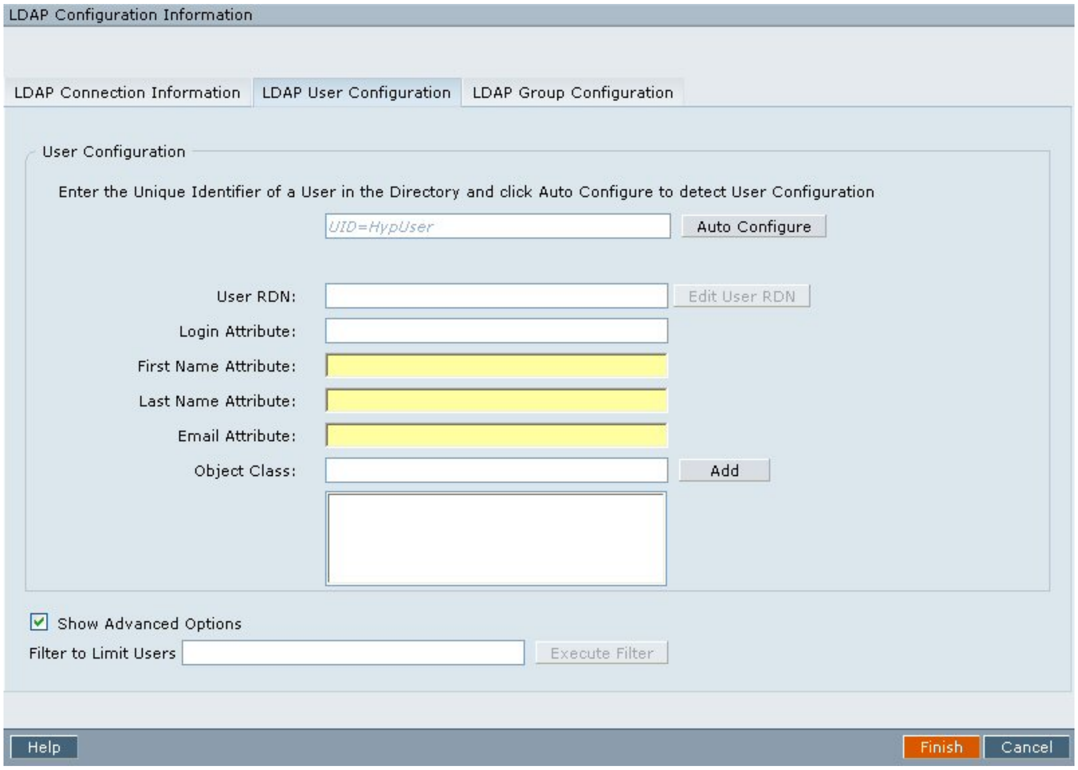
7 Click **Next.**

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

Caution!

User URL should not point to an alias. EPM System security requires that the user URL points to an actual user and not its alias.

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



Enter the Unique Identifier of a User in the Directory and click Auto Configure to detect User Configuration

UID=HypUser

☑ Show Advanced Options

Note:

See "Using Special Characters" on page 88 for a list of special characters that can be used in user configuration.

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

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

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

Note:

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

Table 8 User Configuration Screen

Label	Description
User RDN	The Relative DN of the user. Each component of a DN is called an RDN and represents a branch in the directory tree. The RDN of a user is generally the equivalent of the `uid` or `cn`. See "Using Special Characters" on page 88 for restrictions. **Example:** `ou=People`
Login Attribute	The 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. **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`. **Example:** `uid`
First Name Attribute	The attribute that stores the user's first name. **Example:** `givenName`
Last Name Attribute	The attribute that stores the user's last name. **Example:** `sn`
Email Attribute	**Optional**: The attribute that stores the user's e-mail address. **Example:** `mail`
Object Class	Object classes of the user (the mandatory and optional attributes that can be associated with the user). Shared Services uses the object classes listed in this screen in the search filter. Using these object classes, Shared Services should find all users who should be provisioned. You can manually add additional object classes if needed. To add an object class, enter the object class name into the Object Class box and click Add. To delete object classes, select the object class and click Remove. **Example:** `person, organizationalPerson, inetorgperson`

Label	Description
Show Advanced Options	The check box that enables the use of a filter to retrieve users during search operations.
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 the prefix Hyp. The User Configuration screen validates the User RDN and recommends the use of a user filter, if required. After entering the user filter, click Execute Filter to validate the query by getting a count of the number of users that will be retrieved using the filter. The user filter is used to limit 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.

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 up the search.

Caution!

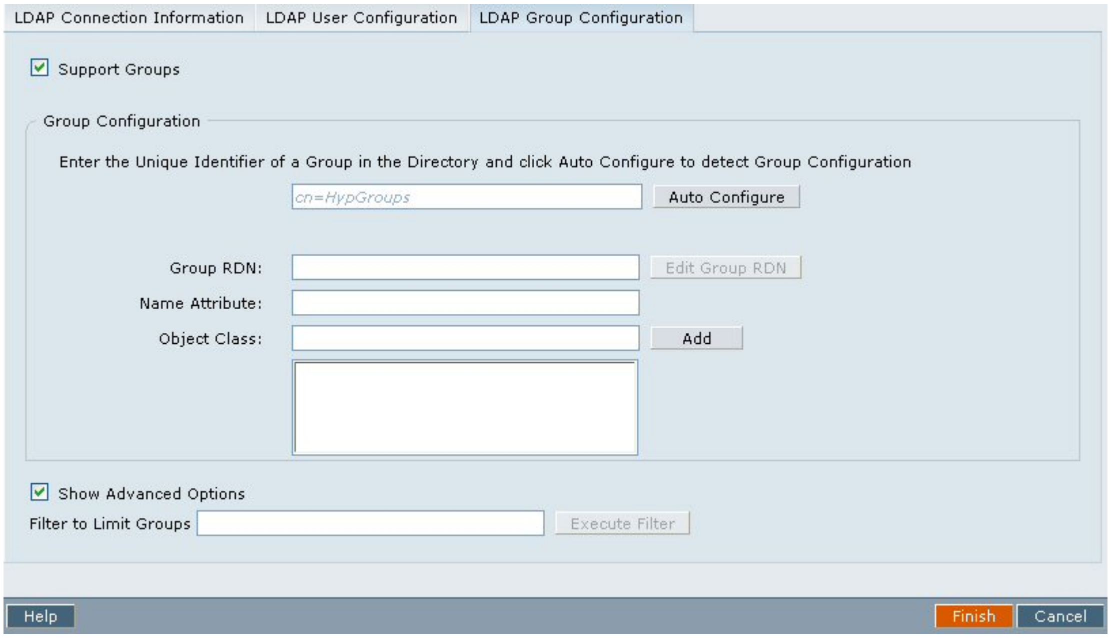
Group URL should not point to an alias. EPM System security requires that the group URL points to an actual group and not its alias.

Caution!

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.



☑ Support Groups

cn=HypGroups

☑ Show Advanced Options

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

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

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

11 **In the Auto Configure text box, enter a unique group identifier, and 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 manually 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 9 Group Configuration Screen

Label	Description
Group RDN	The Relative DN of the group. Each component of a DN is called an RDN and represents a branch in the directory tree. This value, which is 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. The Group RDN has a significant impact on login and search performance. Because it is the starting point for all group searches, you must identify the lowest possible node in which all groups for EPM System products are available. To ensure optimum performance, the number of groups present within the Group RDN should not exceed 10,000. If more groups are present, use a group filter to retrieve only the groups you want to provision. **Note:** Shared Services displays a warning if the number of available groups within the Group URL exceeds 10,000. See "Using Special Characters" on page 88 for restrictions. **Example:** `ou=Groups`
Name Attribute	The attribute that stores the name of the group. **Example:** `cn`
Object class	Object classes of the group. Shared Services uses the object classes listed in this screen in the search filter. Using these object classes, Shared Services should find all groups associated with the user. You can manually add additional object classes if needed. To add an object class, enter the object class name into the Object class text box and click Add. To delete object classes, select the object class and click Remove. **Example:** `groupofuniquenames?uniquemember`
Show Advanced Options	The check box that enables the use of a filter to retrieve groups during search operations.
Filter to Limit Groups	An LDAP query that retrieves only the groups that are to be provisioned with EPM System product roles. For example, the LDAP query `(|(cn=Hyp*)(cn=Admin*))` retrieves only groups whose names start with the prefix Hyp or Admin. After entering the group filter, click Execute Filter to validate the filter by getting a count of the number of groups that will be retrieved by the filter. 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.

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" on page 78.

14 Change the search order assignment, if needed. See "Managing User Directory Search Order" on page 84 for details.

15 Specify security options, if needed. See "Setting Security Options" on page 86 for details.

Configuring an SAP R3 Native Repository

Before starting these procedures, meet all prerequisites in "Prerequisites" on page 46.

By default, the timeout for resolving SAP keystore file is 10 seconds.

➤ To configure an SAP native repository:

1 Launch Shared Services Console. See "Launching Shared Services Console" on page 49.

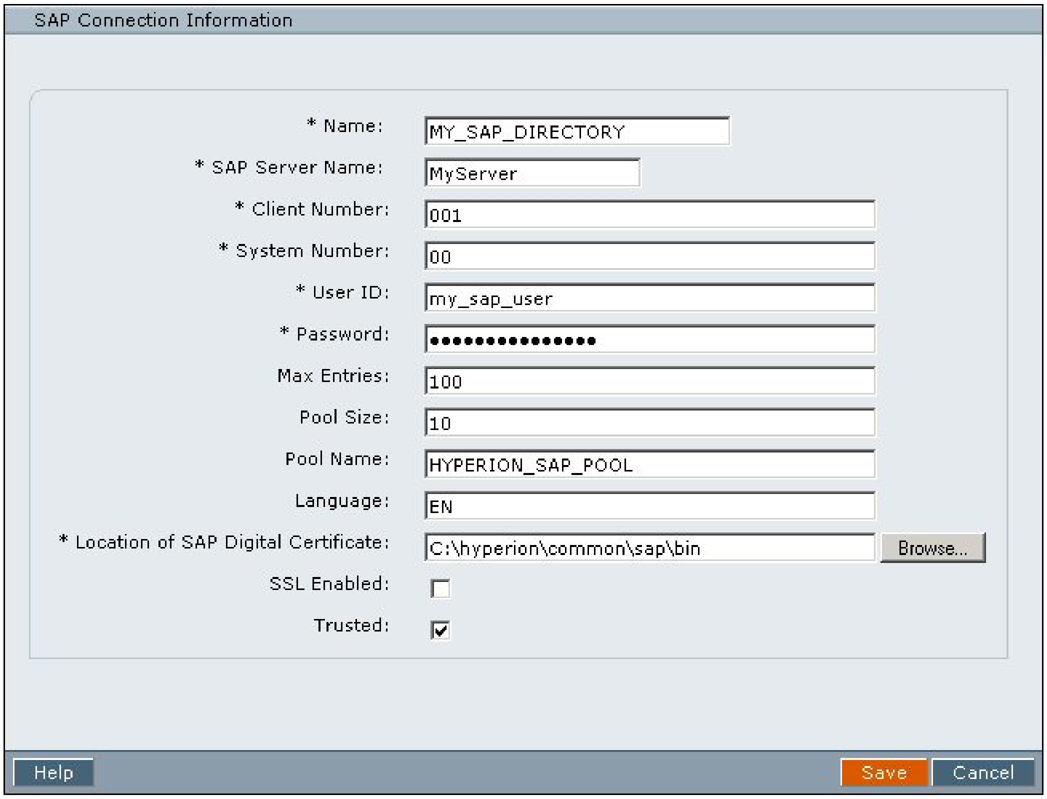
2 Select **Administration**, then **Configure User Directories.**

The Defined User Directories screen opens.

3 Click **Add.**

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

The SAP Connection Information screen opens.



* Name:	MY_SAP_DIRECTORY
* SAP Server Name:	MyServer
* Client Number:	001
* System Number:	00
* User ID:	my_sap_user
* Password:	●●●●●●●●●●●●●●●
Max Entries:	100
Pool Size:	10
Pool Name:	HYPERION_SAP_POOL
Language:	EN
* Location of SAP Digital Certificate:	C:\hyperion\common\sap\bin
SSL Enabled:	☐
Trusted:	☑

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

Table 10 SAP Connection Information Screen

Label	**Description**
Name	A unique configuration name for the SAP provider. You use this name to identify the SAP provider in situations where multiple SAP providers are defined in Shared Services. **Example:** `MY_SAP_DIRECTORY`
SAP Server Name	The host name (or the IP address) of the computer where the SAP Server is running, or the SAP router address.

Label	Description
	Example: `myserver`
Client Number	The client number of the SAP system to which you want to connect. **Example:** `001`
System Number	The system number of the SAP System to which you want to connect. **Example:** `00`
User ID	The user name that Shared Services should use to access SAP. This user must have access permissions to use Remote Function Calls (RFC) to connect to SAP and to access user, activity groups, and their relationship data. **Example:** `my_sap_user`
Password	The password of the user identified in the User ID box. **Example:** `my_sap_password`
Max Entries	The maximum entries that a query to the SAP provider can return. If you are configuring Shared Services in Delegated Administration mode, set this value to 0. **Example:** `100`
Pool Size	The JCo connection pool size. **Example:** `10`
Pool Name	A unique name for the connection pool that should be used to establish a link between Shared Services and SAP. **Example:** `HYPERION_SAP_POOL`
Language	Language for messages, for example error messages, from SAP. By default, this is read from the system locale of the server hosting Shared Services. **Example:** `EN`
Location of SAP Digital Certificate	The SAP X.509 certificate to use. EPM System products use this certificate to parse the SAP login ticket and to extract the user ID needed to support SSO. Required only if EPM System products are plugged into SAP Enterprise Portal. **Example:** `Hyperion/common/SAP/bin/`*`SAP_cert_name`*.
SSL Enabled	Check box that enables you to use Secure Socket Layer (SSL) to communicate between Shared Services and the SAP provider.
Trusted	Check box that enables you to specify that this provider is a trusted SSO source. SSO tokens from trusted sources do not contain the user's password.

6 **Click Save.**

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

7 **Test the SAP native repository configuration. See "Testing User Directory Connections" on page 78.**

8 **Change the search order assignment, if needed. See "Managing User Directory Search Order" on page 84 for details.**

9 **Specify security options, if needed. See "Setting Security Options" on page 86 for details.**

Configuring Relational Databases as User Directories

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

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

Note:

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

➤ To configure database providers:

1 **Launch Shared Services Console. See “Launching Shared Services Console” on page 49.**

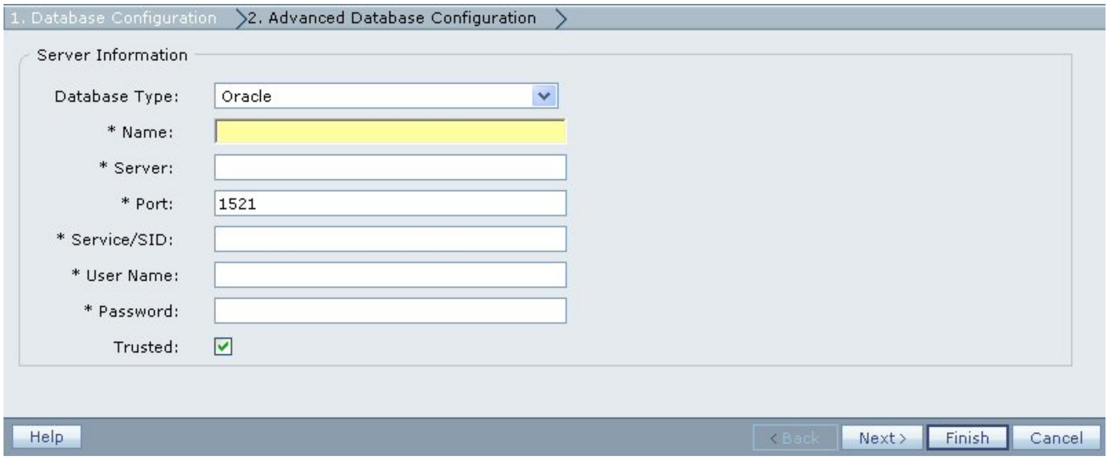
2 **Select Administration, then Configure User Directories.**

The Defined User Directories screen, which lists configured user directories, opens.

3 **Click Add.**

4 **In the Directory Type screen, select Relational Database (Oracle, DB2, SQL Server).**

5 **Click Next.**



Database Type: Oracle

* Port: 1521

Trusted: ☑

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

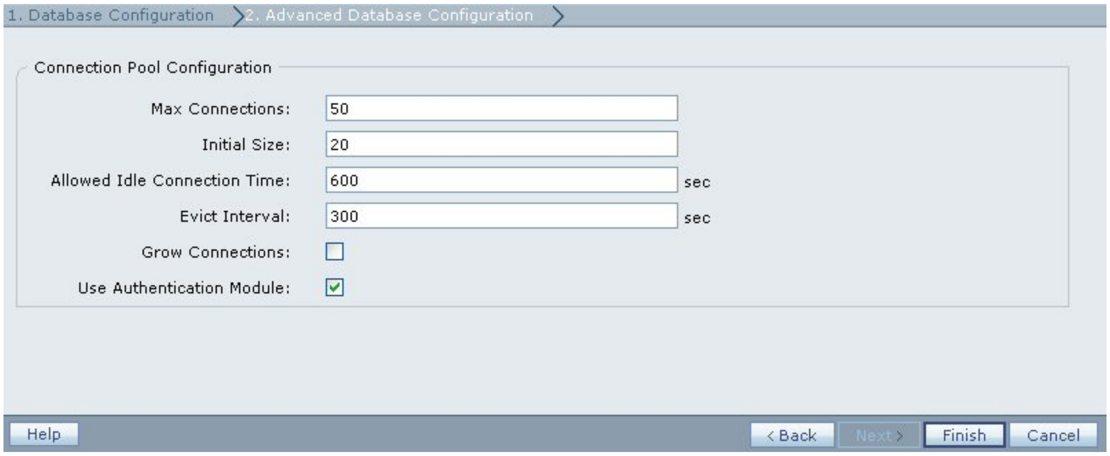
Table 11 Database Configuration Tab

Label	**Description**
Database Type	The relational database provider. Shared Services supports only Oracle, IBM DB2, and SQL Server databases as database providers. **Example:** `Oracle`

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

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

The Advanced Database Configuration tab opens.



Connection Pool Configuration

Max Connections: 50

Initial Size: 20

Allowed Idle Connection Time: 600 sec

Evict Interval: 300 sec

Grow Connections: □

Use Authentication Module: ☑

8 **In Advanced Database Configuration tab, enter connection pool parameters.**

Table 12 Advanced Database Configuration Tab

Label	Description
Max Connections	Maximum connections in the pool. Default is 10.
Initial Size	Available connections when the pool is initialized. Default is 10.
Allowed Idle Connection Time	**Optional:** The time after which the eviction process removes the idle connections in the pool. Default is 300 seconds.
Evict Interval	**Optional:** The interval for running the eviction process to clean up the pool. The eviction process removes idle connections that have exceeded the `Allowed Idle Connection Time`. Default is 60 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 throws an error if a connection is not available within the time set for `Time Out`.

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" on page 78.

12 Change the search order assignment, if needed. See "Managing User Directory Search Order" on page 84 for details.

13 Specify security settings, if needed. See "Setting Security Options" on page 86.

14 Restart Shared Services.

15 After Shared Services restart is complete, restart other EPM System products and custom applications that use the Shared Services security APIs.

Testing User Directory Connections

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

Note:

Establishing a successful test connection does not mean that Shared Services will use the directory. Shared Services uses only the directories that have been assigned a search order.

➤ To test a user directory connection:

1 Launch the Shared Services Console. See "Launching Shared Services Console" on page 49.

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

The Defined User Directories screen opens.

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

4 Click **Test**.

A status message indicating the test results is displayed.

5 Click **OK**.

Editing User Directory Settings

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

Caution!

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

➤ To edit a user directory configuration:

1 Launch the Shared Services Console. See "Launching Shared Services Console" on page 49.

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

3 From **Defined User Directories** screen, select the user directory to edit.

4 Click **Edit**.

5 Modify the configuration settings as needed.

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.

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

- MSAD and other LDAP-based user directories:
  - Table 7, " Connection Information Screen," on page 66
  - Table 8, "User Configuration Screen," on page 70
  - Table 9, "Group Configuration Screen," on page 73
- SAP Native repository: Table 10, " SAP Connection Information Screen," on page 74
- Databases: Table 11, " Database Configuration Tab," on page 76
- NTLM: Table 13, "NTLM Connection Information Screen," on page 83

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

Updating NTLM Configurations

If you upgraded from a release in which Windows NT LAN Manager (NTLM) was configured as external user directory, Shared Services allows you to use NTLM as an external user directory. You can update the parameters of an NTLM configuration; you cannot, however, define a new NTLM configuration.

Under these conditions, you must perform additional prerequisite steps to use NTLM:

- NTLM is to be used to authenticate and provision users where Shared Services and EPM System products are running in a UNIX environment. In this scenario, Oracle's Hyperion® Remote Authentication Module must be deployed on the Windows domain that contains the user accounts.
- Shared Services and EPM System products are running in a Windows environment, but users are in Windows NTLM domains that are not trusted on the domain of the Shared Services host machine. The prerequisite for this scenario is that you deploy Remote Authentication Module on each domain that is not trusted by the domain of the Shared Services host machine.

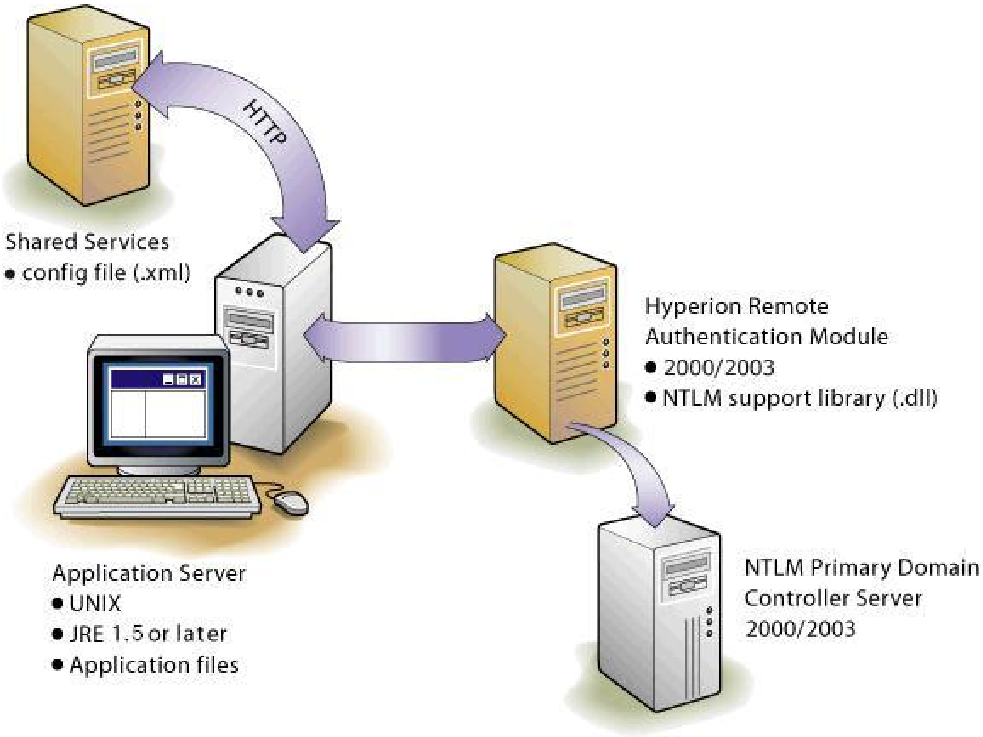
Note:

If you are using Remote Authentication Module, ensure that the `css.jar` file that it uses are identical to those used by Shared Services.

Do not implement Remote Authentication Module if all users belong to the NTLM domain where the Shared Services host machine is installed or if a trust relationship is established between the domain where the Shared Services host machine is installed and the NTLM domains to which users belong.

NTLM with UNIX Application Environments

The following illustration depicts how the Remote Authentication Module enables communication between NTLM and Shared Services running in a UNIX environment.



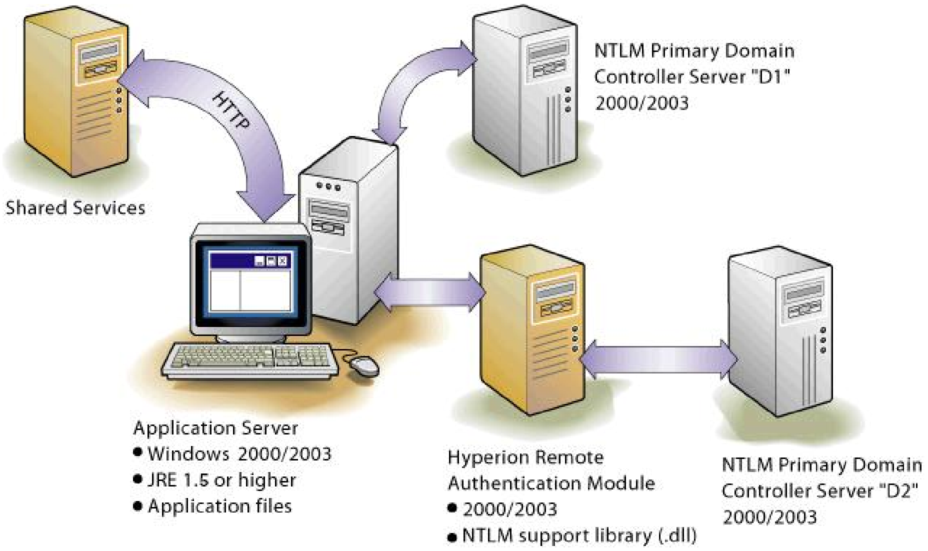
Shared Services configuration information is stored in the Shared Services Registry, and application binaries reside on the application server. For NTLM connectivity, you also need NTLM support library file (`css-9_5_0.dll`) on the machine that hosts Remote Authentication Module in the NTLM domain.

The NTLM Primary Domain Controller and the Remote Authentication Module can be on a Windows 2000 or Windows 2003 server. EPM System does not recommend, however, that you combine the Remote Authentication Module with the NTLM Primary Domain Controller on the same server. The Remote Authentication Module host machine must be in the same domain as the NTLM Primary Domain Controller.

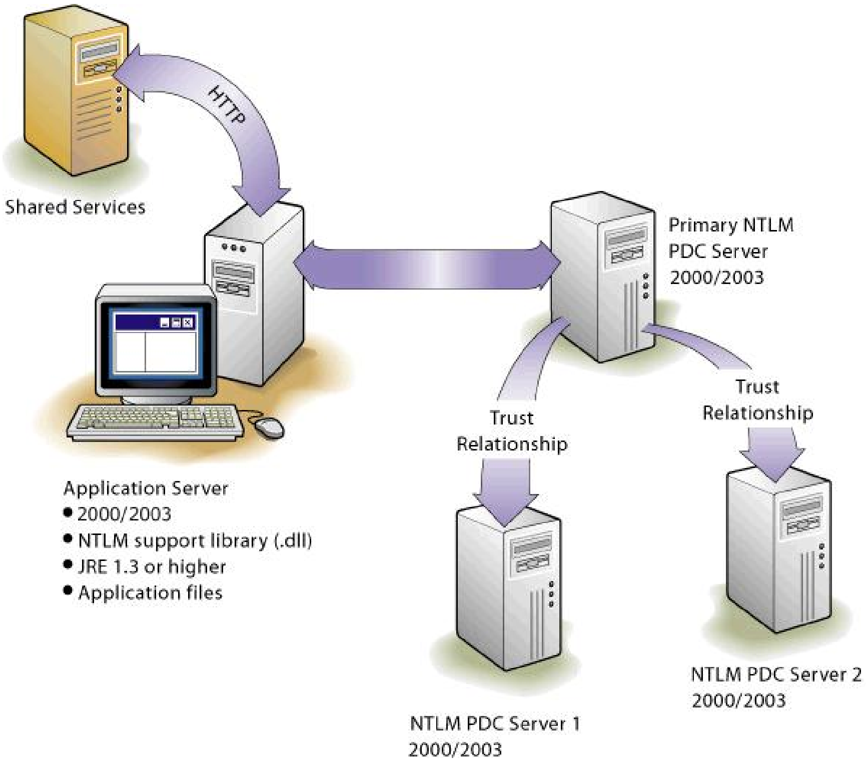
Support for Multiple NTLM Domains

Remote Authentication Module enables an EPM System product to authenticate users belonging to other NTLM domains that are not trusted by the domain where Shared Services is installed.

The following illustration depicts how users spread across multiple NTLM domains can be given access to EPM System products deployed in a Windows environment:



Without Remote Authentication Module, the only way to use multiple NTLM domains for EPM System products is to establish trust relationships between the Shared Services host machine's domain and the NTLM domains where user accounts are available.



Each NTLM domain is configured separately on Shared Services as an external user directory.

Modifying NTLM External User Directory Configurations

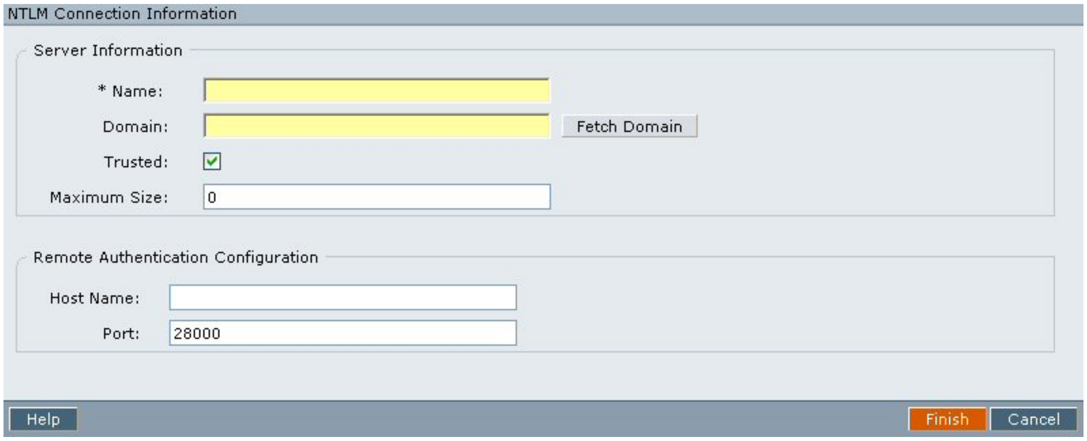
NTLM configurations that existed before upgrading Shared Services are listed in the Defined User Directories screen.

➤ To modify NTLM configuration properties:

1. Launch Shared Services Console. See "Launching Shared Services Console" on page 49.
2. Select **Administration** and then select **Configure User Directories.**

   The Defined User Directories screen opens.
3. From **Provider Configuration**, select the NTLM configuration to modify.
4. Click **Edit.**

   The NTLM Connection Information screen opens.



NTLM Connection Information

Server Information

* Name:

Domain:

Trusted: ☑

Maximum Size: 0

Remote Authentication Configuration

Host Name:

Port: 28000

5. In **NTLM Connection Information**, modify configuration parameters. See Table 13. You can edit all the information in this screen, except the configuration name.

Table 13 NTLM Connection Information Screen

Label	Description
Domain	The name of the NTLM domain. You can use the Fetch Domain button to retrieve the domain name. If the domain is not specified, Shared Services, at runtime, detects and uses all visible domains, which may affect performance. The search order is: local computer, domain of local computer, and trusted domains visible to the local computer. **Note:** Because Shared Services does not detect domains when NTLM is used with Remote Authentication Module, you must specify the domain if Remote Authentication Module is used. **Example:** `MY_DOMAIN`
Trusted	Check box to indicate that this provider is a trusted SSO source. SSO tokens from trusted sources do not contain the user's password.
Maximum Size	Maximum entries that a query to the NTLM can return. If you are configuring Shared Services in Delegated Administration mode, set this value to 0. **Example:** `100`
Hostname	Name of the Windows server where Remote Authentication Module is installed to support SSO to EPM System products running in a UNIX environment. **Example:** `MyHRAMServer`
Port	The port number where Oracle's Hyperion® Remote Authentication Module is running.

Label	Description
	Example: `3891`

6 Click **Finish.**

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

7 Test the configuration. See "Testing User Directory Connections" on page 78.

8 Change the search order assignment, if needed. See "Managing User Directory Search Order" on page 84 for details.

9 Specify additional parameters, if needed, for the NTLM user directory. See "Setting Security Options" on page 86 for details.

Deleting User Directory Configurations

You can delete a user directory configuration anytime. Deleting a directory 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 at a later time, if needed.

➤ To delete a user directory configuration:

1 Launch the Shared Services Console. See "Launching Shared Services Console" on page 49.

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

3 From **Defined User Directories** screen, select the directory.

4 Click **Delete.**

Managing User Directory Search Order

The search order associated with a configured user directory determines the position of the directory in the search order that Shared Services uses to retrieve user and group information. Shared Services automatically adds the configured user directory to the search order and assigns it the next available search sequence. You can remove a configured 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. If a user has multiple accounts within a user directory, Shared Services retrieves the account that the search first encounters.

By default, Native Directory is set as the first directory in the search order. Additional user directories are given the next available sequence number in the search order. You can perform these tasks to manage the search order:

- "Adding a User Directory to the Search Order" on page 85
- "Changing the Search Order" on page 85
- "Removing a Search Order Assignment" on page 86

Adding a User Directory to the Search Order

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

➤ To add a user directory to the search order:

1. Launch Shared Services Console. See "Launching Shared Services Console" on page 49.
2. Select **Administration**, then **Configure User Directories.**
3. From **Defined User Directories** screen, select the directory to add to the search order.
4. Click **Add.**

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

   Shared Services displays a message indicating that the search order was updated.
5. Click **OK** to return to the Defined User Directories screen.

Changing the Search Order

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

➤ To change the search order:

1. Launch the Shared Services Console. See "Launching Shared Services Console" on page 49.
2. Select **Administration**, then **Configure User Directories.**
3. From **Defined User Directories** screen, select the directory whose search order you want to change.
4. Click **Move Up** or **Move Down** as needed.
5. Restart Shared Services for the new search order to take effect.

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

Removing a Search Order Assignment

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

Note:

You cannot remove Native Directory from the search order.

➤ To remove a user directory from the search order:

1 Launch Shared Services Console. See "Launching Shared Services Console" on page 49.

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

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

4 Click **Remove.**

Shared Services displays a confirmation dialog box.

5 Click **OK.**

Shared Services displays a message indicating that the search order was updated.

6 Click **OK** to return to the Defined User Directories screen, which lists user directory status as `Not Used`.

Setting Security Options

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

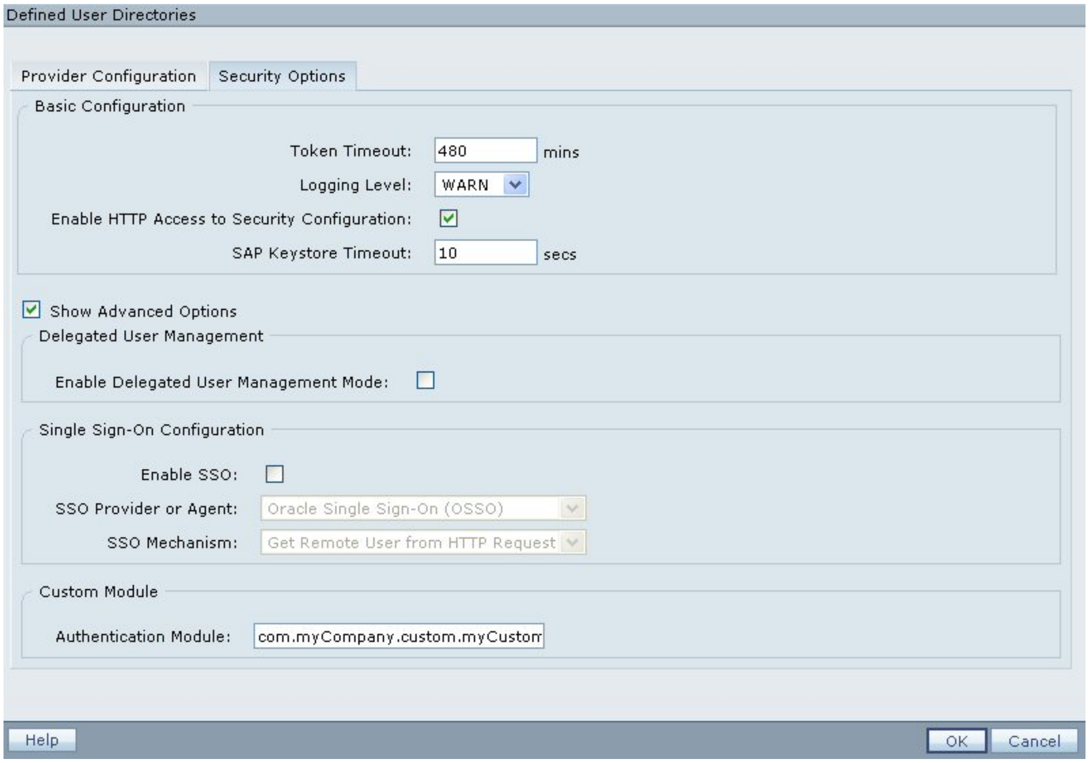
➤ To set security options:

1 Launch Shared Services Console. See "Launching Shared Services Console" on page 49.

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

3 Select **Security Options.**

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



Defined User Directories

Basic Configuration

Token Timeout: 480 mins

Logging Level: WARN

Enable HTTP Access to Security Configuration: ☑

SAP Keystore Timeout: 10 secs

☑ Show Advanced Options

Delegated User Management

Enable Delegated User Management Mode: □

Single Sign-On Configuration

Enable SSO: □

SSO Provider or Agent: Oracle Single Sign-On (OSSO)

SSO Mechanism: Get Remote User from HTTP Request

Custom Module

Authentication Module: com.myCompany.custom.myCustom

Table 14 Security Options for User Directories

Parameter	Description
Token Timeout	Time (in minutes) after which the SSO token issued by EPM System products or the Web identity management solution expires. Users must log in again after this period. Token timeout is set based on the server's system clock. **Note:** Token timeout is not the same as session timeout. **Example:** `480`
Logging Level	Level (`ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`) at which user directory related issues are recorded in the Shared Services security log files. Administrators can change the Shared Services log level on the fly to capture relevant information to debug Shared Services issues. Shared Services application server restart is not required to activate log level change. Log files belonging to EPM System products are stored in *HYPERION_HOME*/`logs`, allowing administrators to easily locate log files to monitor the applications and troubleshoot issues. Product log files are created in a product-specific folder. For example, Shared Services logs are in *HYPERION_HOME*/`logs/SharedServices9`. Existing log files are not moved to the new location. **Example:** `WARN`
Enable HTTP Access to Security Configuration	In a mixed environment comprising EPM System 11.1.1.2 and Hyperion System 9 products, select this option to allow Hyperion System 9 products to use HTTP URL to access the configuration information stored in the Oracle's Hyperion Shared Services Registry. Do not select this option if your environment contains only EPM System 11.1.1.2 products. **Note:** You must select this option to run the Update Native Directory Utility.
SAP Keystore Timeout	The time limit (in seconds) for resolving the SAP keystore file. Default is `10`.

Parameter	Description
	Example: `20`
Show Advanced options	Option that allows you to display options related to Delegated Administration and SSO configuration.
Enable Delegated User Management Mode	Option enabling delegated user management of EPM System products to support the distributed management of provisioning activities. See Chapter 7, "Delegated User Management."
Enable SSO	Option enabling support for SSO from security agents such as Oracle Access Manager.
SSO Provider or Agent	Select the Web identity management solution from which EPM System products should accept SSO. Select Other if your Web identity management solution, for example, Kerberos, is not listed. The preferred SSO method is automatically selected when you select the SSO provider. You can change the name of the HTTP header or custom login class, if required.
SSO Mechanism	The method that the Web identity management solution uses to provide user's login name to EPM System products. For a description of acceptable SSO methods, see "Supported SSO Methods" on page 26.
Authentication Module	If you are using a custom authentication class name or package name, the fully qualified Java class name of the custom authentication module that should be used to authenticate users on all user directories for which custom authentication module is selected. Authentication module is used for a user directory only if the directory configuration has enabled (default) its use. **Note:** If you use the default class name (`CustomAuthenticationImpl`) and package name (`com.hyperion.css.custom`) , you need not update the Shared Services configuration to specify the custom authentication class because Shared Services automatically picks up the custom authentication class. **Caution!** If you are enabling custom authentication for Essbase, you must specify the fully qualified class name of the custom class even if you use the default class and package name. See "Using a Custom Authentication Module" on page 57.

5 Click **OK.**

Using Special Characters

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

Generally, you must use escape characters while specifying any special character used in user directory settings for LDAP-based user directories, including MSAD; for example, user and group URLs and Base DN. Native Directory and NTLM do not require special handling of characters.

Table 15 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. Native Directory and NTLM do not require special handling of characters.

Table 15 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

[*] / (slash) cannot be used in the organization unit names that come within the DN specified for the external user directory.

- Special characters are not permitted in the value of the Login User attribute.
- 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.
- Ampersand (&) can be used without an escape character. For MSAD settings, & must be specified as `&amp;`.
- 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 16 Characters that need not be escaped

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

[*] Must be stated as `&amp`.

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 17 Escape for Special Characters in User Directory Configuration Settings

Special Character	Escape	Sample Setting	Escaped Example
comma (,)	backslash (\)	`ou=test,ou`	`ou=test\,ou`
plus sign (+)	backslash (\)	`ou=test+ou`	`ou=test\+ou`

Special Character	Escape	Sample Setting	Escaped Example
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 (<)	\&lt;	`ou=test<ou`	`ou=test\&lt;ou`
greater than (>)	\&gt;	`ou=test>ou`	`ou=test\&gt;ou`
“ (quotation mark)[*]	\\ (two backslashes)	`ou=test”ou`	`ou=test\\”ou`
\ (backslash)[†]	\\\ (three backslashes)	`ou=test\ou`	`ou=test\\\ou`

[*] In User DNs, quotation mark (“) must be escaped with a single backslash. For example, `ou=test”ou` must be specified as `ou=test\”ou` in User DN.

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

Caution!

If the user URL is not specified, 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.

6

Working with Application Groups and Applications

In This Chapter

Overview

Application groups and applications are two important Shared Services concepts. An application is a reference to a single instance of an EPM System product that is registered with Shared Services. The registration process makes Shared Services aware of the existence of EPM System applications. All provisioning activities are performed against an application, which belongs to an application group.

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

Working with Application Groups

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

Applications that are registered with Shared Services but do not yet belong to an application group are listed under the Default Application Group node in the View pane. You can provision users with roles from applications listed in the Default Application Group node and then move the application to an application group without losing provisioning information.

Topics detailing application group management tasks:

- "Creating Application Groups" on page 92
- "Modifying Application Group Properties" on page 92
- "Deleting Application Groups" on page 93

Note:

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

Creating Application Groups

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

➤ To create an application group:

1 Launch the Shared Services Console. See "Launching Shared Services Console" on page 49.

2 Right-click **Application Groups** in the View pane, and select **New.**

The New Application Group screen opens.

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

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 click **Add.**

The selected applications appear in the Assigned Applications list.

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

5 Click **Finish.**

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

Modifying Application Group Properties

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

Note:

You can also add applications to application groups by moving them from another application group. See "Moving Applications " on page 94.

➤ To modify an application group:

1 Launch the Shared Services Console. See “Launching Shared Services Console” on page 49.

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

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

4 Modify the application group properties as needed. See step 4 on page 92 for information on assigning or removing applications.

5 Click **Save.**

Deleting Application Groups

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

- Default Application Group
- Foundation
- File System

➤ To delete an application group:

1 Launch Shared Services Console. See “Launching Shared Services Console” on page 49.

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

3 Click **OK.**

Managing Applications

Shared Services tracks registered EPM System applications. Registration is completed from individual EPM System applications and not from Shared Services.

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

Topics addressing application management tasks:

- “Assigning Access Permissions to Applications ” on page 94
- “Moving Applications ” on page 94
- “Copying Provisioning Information Across Applications” on page 95
- “Deleting an Application” on page 96

Assigning Access Permissions to Applications

Shared Services Console enables application administrators to perform provisioning tasks, such as assigning access permissions to application-specific objects; for example, reports and calculation scripts. For Essbase applications, for example, users with the appropriate Administration Services permissions can assign filter and calculation script access to selected users and groups.

Some products require that certain security tasks be performed in the product interface, not through Shared Services Console. For example, using the Administration Services interface, you must create filters and calculation scripts. You can then provision these objects by assigning specific users or groups from Shared Services Console. Likewise, you must assign access permission on repository content of Reporting and Analysis from within that product.

You must either be a Shared Services administrator or be provisioned with the appropriate product role (Planning Manager, for example) to assign access permission from Shared Services Console. See the appropriate product appendix at the end of this guide for instructions on assigning access permission for specific products.

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

➤ To assign application-specific access permissions:

1 **Launch Shared Services Console. See "Launching Shared Services Console" on page 49.**

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

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

Assign Preferences tab for the selected application is displayed.

Note:

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

4 **Assign access permissions as needed. Refer to the product appendix at the end of this guide for details.**

Moving Applications

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

Note:

Applications in the Foundation application group cannot be moved.

➤ To move an application:

1. Launch Shared Services Console. See "Launching Shared Services Console" on page 49.
2. From an application group, right-click the application and select **Move To**.
3. On the **Move To** tab, select the destination application group for the application.
4. Click **Save**.

Copying Provisioning Information Across Applications

For multiple applications (for example, multiple Planning applications from EPM System version 11.1.1.2), you can copy provisioning information from one application to another. When you copy provisioning information, all user, group, and role information is copied to the target application. Product-specific access control settings are not copied.

➤ To copy provisioning information across applications:

1. Launch Shared Services Console. See "Launching Shared Services Console" on page 49.
2. In View pane, right-click the application from which you want to copy provisioning information and select **Copy Provisioning**.

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

Deleting Multiple Applications

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

➤ To delete applications:

1. Launch Shared Services Console. See "Launching Shared Services Console" on page 49.
2. In the View pane, right-click **Application Groups** and select **Delete**.

   Delete Applications screen, which lists the applications that can be deleted, opens.
3. Select the applications to delete. To delete all applications within an application group, select the application group.

   Note:

   You cannot delete application groups from this screen. See "Deleting Application Groups" on page 93.
4. Click **Delete**.
5. Click **OK** in the confirmation dialog box.

Deleting an Application

Shared Services administrators can delete applications from application groups. When you delete an application from an application group, all provisioning information for that application is removed.

➤ To delete an application:

1. Launch Shared Services Console. See "Launching Shared Services Console" on page 49.
2. In the View pane, right-click the application and select **Delete**.
3. Click **OK**.

Exploring Applications

You can view, search, migrate, load, export, and import artifacts belonging to the application. The application and repository artifacts are sorted into categories so that artifacts are exposed in an organized manner. This is Lifecycle Management Utility functionality. See the*Oracle Hyperion Enterprise Performance Management System Lifecycle Management Guide*.

7

Delegated User Management

In This Chapter

About Delegated User Management

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

Only users with the Administrator Shared Services role can view all users and groups of EPM System products. 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

The default Shared Services Administrator account (*admin*) is the most powerful account in EPM System products. Oracle recommends that you change the password of this account after you first access Shared Services.

Two tiers of administrators—Shared Services Administrators and Delegated Administrators—exist in delegated administration mode.

Shared Services Administrators

Oracle recommends that you create Shared Services Administrator accounts similar to the default *admin* account to administer Shared Services and other EPM System applications.

You can create Shared Services Administrator accounts by provisioning users and groups with the Shared Services Administrator role, which provides access to all Shared Services functions.

Delegated Administrators

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

The permissions of Delegated Administrators on EPM System products are controlled by the access rights that a Shared Services Administrator has granted them through provisioning. For example, assume that a Delegated Administrator is granted the Directory Manager global role in Shared Services, enabling the user to create users and groups in Native Directory. Without additional roles, this Delegated Administrator cannot view a list of users and groups that other administrators created.

If they have permission to provision users (granted through the Provisioning Manager role), Delegated Administrators can create other Delegated Administrators and provision them to further delegate administrative tasks.

Enabling Delegated User Management Mode

You must enable Delegated User Management mode for Shared Services before you can create delegated administrators. The default Shared Services deployment does not support delegated administration.

Additional screens and menu options become available after you switch to Delegated User Management mode.

In delegated administration 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 restriction 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 will make *del_admin1* an Essbase Provisioning Manager for all users and groups.

➤ To enable Delegated User Management mode:

1. Launch the Shared Services Console. See "Launching Shared Services Console" on page 49.
2. From **Administration**, select **Configure User Directories.**
3. Select **Security Options**, then **Show Advanced Options.**
4. Select **Enable Delegated User Management Mode.**
5. Click **OK.**
6. Restart Shared Services.
7. Restart other EPM System products and custom applications that use the Shared Services security APIs.

Creating Delegated Administrators

Planning Steps

User Accounts for Delegated Administrators

Shared Services Administrators create Delegated Administrators from existing user accounts in the user directories configured on 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 levels of Delegated Administrators needed to effectively administer EPM System products. The plan should identify:

- Users and groups that each Delegated Administrator should manage. This list can be used while creating Delegated Lists. See "Creating Delegated Lists" on page 100.
- Shared Services and EPM System product roles that each Delegated Administrator should be granted.

Provisioning Delegated Administrators

Shared Services Administrators provision Delegated Administrators to grant them roles based on the delegation plan.

Delegated Administrators must be granted Shared Services roles depending on the activities they should perform. See "Shared Services Roles" on page 155.

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

Creating Delegated Lists

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

- 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 whom they manage.
- Search and retrieve only the users and groups that are included in their delegated lists.

Note:

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

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

➤ To create delegated lists:

1. Launch Shared Services Console. See "Launching Shared Services Console" on page 49.
2. In **Native Directory** in View pane, right-click **Delegated List**, and select **New.**

   The Create Delegated List screen opens.
3. In **Name**, enter a unique name for the delegated list.
4. **Optional:** In **Description**, type a list description.
5. **Optional**: To add groups to the list, click **Next.** These are the groups that the Delegated Administrator assigned to this list can administer.

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

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

   c. Click **Go**.

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

   e. Click **Add**.

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

   Note:

   Shared Services considers Oracle and SQL Server database roles as the equivalents of groups in user directories. Oracle database roles can be hierarchical. SQL Server database roles cannot be nested. Because DB2 does not support roles, Shared Services does not display groups if you select a DB2 database provider.

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

6 **Optional: Click Next to add users to the list. These are the users that the Delegated Administrator assigned to this list can administer.**

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

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

c. Click **Go.**

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

e. Click **Add.**

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

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

Note:

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

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

The Managed By tab opens.

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

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

c. Click **Go.**

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

e. Click **Add.**

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

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

Note:

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

8 **Click Finish.**

Modifying Delegated Lists

Delegated Administrators can modify only the lists assigned to them. Users with Shared Services Administrator role can modify all delegated lists.

➤ To modify delegated lists:

1 Launch Shared Services Console. See "Launching Shared Services Console" on page 49.

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

3 Search for the delegated list to modify. See "Searching for Users, Groups, Roles, and Delegated Lists" on page 51.

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

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

The Delegated List Properties screen opens.

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

6 **Optional**: Click **Group Members** to add groups.

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

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

c. Click **Go**.

d. From **Available Groups**, select one or more groups.

e. Click **Add**.

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

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

7 **Optional**: To add users to the list, click **User Members.**

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

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

c. Click **Go**.

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

e. Click **Add**.

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

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

Note:

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

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

The Managed By page opens.

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

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

c. Click **Go**.

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

e. Click **Add**.

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

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

Note:

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

9 Click **Save**.

Deleting Delegated Lists

➤ To delete delegated lists:

1 Launch Shared Services Console. See "Launching Shared Services Console" on page 49.

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

3 Search for the delegated list to modify. See "Searching for Users, Groups, Roles, and Delegated Lists" on page 51.

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

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

5 Click **OK**.

Viewing Delegated Reports

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

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

➤ To view delegated reports:

1 Launch Shared Services Console. See “Launching Shared Services Console” on page 49.

2 In **Native Directory** in **View pane**, right-click **Delegated List**, and select **View Delegated Reports.**

   The View Delegated Report screen opens.

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 wildcard for pattern searches.

5 Click **Create Report.**

6 Click **Cancel** 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.

8 Managing Native Directory

In This Chapter

About Native Directory

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

After the initial logon to an EPM System product, the product directly queries Native Directory for user provisioning information. EPM System products can function normally only if Native Directory is running.

Shared Services Console displays a list of users and groups for each configured user directory, including Native Directory. These lists are used to provision users and groups against application roles.

Shared Services Console is the central administration point for Native Directory, the default user directory installed with Shared Services. Other user directories are administered through their own administration screens.

You can use OID or OpenLDAP as the Native Directory. See:

- "Using OID as Native Directory" on page 106
- "Using OpenLDAP as Native Directory" on page 108

Note:

See the *Oracle Hyperion Enterprise Performance Management System High Availability Guide* for information on setting up OpenLDAP for high availability and failover.

Default Users and Groups in Native Directory

Native Directory, by default, contains one user account (`admin`, with `password` as the default password). Using this account, you can perform all Native Directory and Shared Services administration tasks.

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

Using OID as Native Directory

By default, OpenLDAP is installed as the Native Directory. To use OID as the Native Directory, you must configure an existing OID from Shared Services. See "Setting up Oracle Internet Directory as the Native Directory" on page 53.

Native Directory uses its own realm to create and manage users, groups, and roles. It does not interfere with the normal operation of the corporate OID. Shared Services Console manages only the information contained in the `css` realm.

Managing Native Directory

Use the administration capabilities provided by the Shared Services Console to administer Native Directory.

Related topics:

- "Managing Native Directory Users" on page 109
- "Managing Native Directory Groups" on page 113
- "Managing Roles" on page 117
- "Changing OpenLDAP root User Password" on page 120

If you are using OID as Native Directory, Oracle recommends that you always use the Shared Services Console to administer the `css` realm.

Administering OID

Because it is a part of the OID Base DN, the following administrative operations are performed using the capabilities provided by OID. Refer to *Oracle Internet Directory Documentation* for information on performing these tasks:

- Starting and stopping Native Directory (OID)
- Clustering and failover
- Backing up Native Directory data (the backup scripts provided in the Shared Services distribution can be used only to back up OpenLDAP)
- Restoring data from backups

Setting up Password Policies

Password polices determine the password syntax and how passwords are used. For example, password policies can determine the period after which a password must be changed, the minimum number of characters in a password, and the use of special characters.

If you are using OID as the Native Directory, you can use the password policy management features of OID to establish password policies for Native Directory users.

Note:

If you are using OpenLDAP, you cannot set or enforce password policies for Native Directory users. Only Administrators and Directory Managers can change Native Directory user passwords.

OID allows you to set policy attributes such as the following:

- `orclpwdIPLockoutDuration`: The period (in seconds) to lock out an account after the threshold of invalid login attempts from one IP address is reached.
- `orclpwdIPMaxFailure`: The number of invalid login attempts after which OID should lock the user account.
- `pwdFailureCountInterval`: The interval (in seconds) after which password failures are purged from the failure counter although no successful authentication occurred.
- `pwdExpireWarning` The period (in seconds) during which a password expiration warning is issued to a user.
- `pwdCheckSyntax`: The option that specifies whether to enable password syntax check.

See the *Oracle Internet Directory Administrator's Guide* for a list of policy attributes and how to use them.

Changing Native Directory User Password

If you are using OID as the Native Directory, Shared Services enforces the OID password policies (see "Setting up Password Policies" on page 107). Shared Services prompts EPM System product users to change their passwords based on these policies.

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

Note:

You can change your Native Directory password anytime by modifying your Native Directory user account. See "Modifying User Accounts" on page 110.

➤ To change a password in Native Directory:

1. In **Current Password**, enter your password.
2. In **New Password** and **Confirm Password**, enter a new password.

   Note:

   The new password must adhere to OID password policies.
3. Click **OK**.

Using OpenLDAP as Native Directory

- "Installation Location" on page 108
- "Starting OpenLDAP in Normal Mode" on page 109
- "Starting OpenLDAP in Debug Mode" on page 109
- "Stopping OpenLDAP" on page 109

Installation Location

By default, OpenLDAP is installed to `*HYPERION_HOME*/products/Foundation/SharedServices/openLDAP`.

Examples:

`C:\Hyperion\products\Foundation\SharedServices\openLDAP` (Windows)

The install location of OpenLDAP is referred to as *OPENLDAP_HOME* throughout this document.

Native Directory data is stored in *OPENLDAP_HOME*`/var/openldap-data`, and utilities are stored in *OPENLDAP_HOME*`/bdb/bin`.

By default, OpenLDAP is deployed to port 28029.

Starting OpenLDAP

By default, OpenLDAP is installed as a service or process.

Starting OpenLDAP in Normal Mode

On Windows, you can start OpenLDAP by starting the OpenLDAP service from the **Services** window, or by executing *OPENLDAP_HOME*/startService.bat.

On UNIX systems, run *OPENLDAP_HOME*/startOpenLDAP script to start the process.

Starting OpenLDAP in Debug Mode

➤ To start OpenLDAP in debug mode:

1 **Using a command prompt window, navigate to** *OPENLDAP_HOME*.

2 **Execute the command:**

```
slapd –d 1.
```

Stopping OpenLDAP

On Windows, you can stop OpenLDAP by stopping the OpenLDAP service from the **Services** window, or by executing *OPENLDAP_HOME*/stopService.bat.

On UNIX systems, run *OPENLDAP_HOME*/stopOpenLDAP script to stop the OpenLDAP process.

Managing Native Directory Users

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

- "Creating Users" on page 110
- "Modifying User Accounts" on page 110
- "Deactivating User Accounts" on page 111
- "Deleting User Accounts " on page 112
- "Provisioning Users and Groups" on page 125
- "Deprovisioning Users and Groups" on page 127
- "Generating Provisioning Reports" on page 129

If you are using OID as Native Directory, Oracle recommends that you always use the Shared Services Console to administer the css realm.

Note:

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

Creating Users

➤ To create users:

1 Launch Shared Services Console. See "Launching Shared Services Console" on page 49.

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

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

Table 18 Create User Screen

Label	**Description**
User Name	A unique user identifier that follows the naming conventions of your organization (for example, first_name initial followed by last name, as in *jyoung*) User names can contain any number or combination of characters. You cannot create identical user names, including names that are differentiated only by number of spaces. For example, you cannot create user names `user 1` (with one space between `user` and `1`) and `user  1` (with two spaces between `user` and `1`).
First Name	User's first name (optional)
Last Name	User's last name (optional)
Description	User's description (optional)
Email Address	User's e-mail address (optional)
Password	Passwords are case-sensitive and can contain any combination of characters.
Confirm Password	Re-enter password.

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

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

b. Click **Go**.

c. From **Available Groups**, select one or more groups.

d. Click **Add**.

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

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

5 Click **Finish**.

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

Modifying User Accounts

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

➤ To modify user accounts:

1 Launch Shared Services Console. See “Launching Shared Services Console” on page 49.

2 In the **Native Directory** node in the View pane, select **Users**.

3 Search for user account. See “Searching for Users, Groups, Roles, and Delegated Lists” on page 51.

A list of users that meet the search criterion is displayed on the Browse tab.

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

The User Properties screen opens.

Note:

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

5 On the **General** tab, modify one or more user properties.

See Table 18 for descriptions of the properties that you can modify.

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

a. Click **Member Of**.

Member Of tab opens.

b. Select `Group Name` or `Description`.

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

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

The selected groups are listed in Assigned Groups.

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

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

8 Click **Save**.

Deactivating User Accounts

You can deactivate user accounts that should not have access to EPM System applications. Account deactivations are, typically, temporary suspensions where the Native Directory administrator hopes to reactivate the accounts in the future.

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

- Inactive user accounts are not displayed on the product-specific access-control screens of items for which access is disabled.
- Inactive user accounts are not deleted from Native Directory.

Note:

The admin account cannot be deactivated.

➤ To deactivate user accounts:

1 Launch Shared Services Console. See “Launching Shared Services Console” on page 49.

2 Search for the **Native Directory** users to deactivate. See “Searching for Users, Groups, Roles, and Delegated Lists” on page 51.

3 Right-click the user account, and select **Deactivate.**

Activating Inactive User Accounts

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

➤ To activate deactivated user accounts:

1 Launch Shared Services Console. See “Launching Shared Services Console” on page 49.

2 Search for **Native Directory** users to reactivate. See “Searching for Users, Groups, Roles, and Delegated Lists” on page 51.

3 Right-click the user account, and select **Activate.**

Deleting User Accounts

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

Note:

The `admin` account cannot be deleted.

➤ To delete user accounts:

1 Launch Shared Services Console. See “Launching Shared Services Console” on page 49.

2 Search for **Native Directory** users to delete. See “Searching for Users, Groups, Roles, and Delegated Lists” on page 51.

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

Managing Native Directory Groups

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

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

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

Tasks performed by Shared Services administrators or directory managers:

- "Creating Groups" on page 114
- "Modifying Groups" on page 115
- "Deleting Groups" on page 117
- "Provisioning Users and Groups" on page 125
- "Deprovisioning Users and Groups" on page 127
- "Generating Provisioning Reports" on page 129

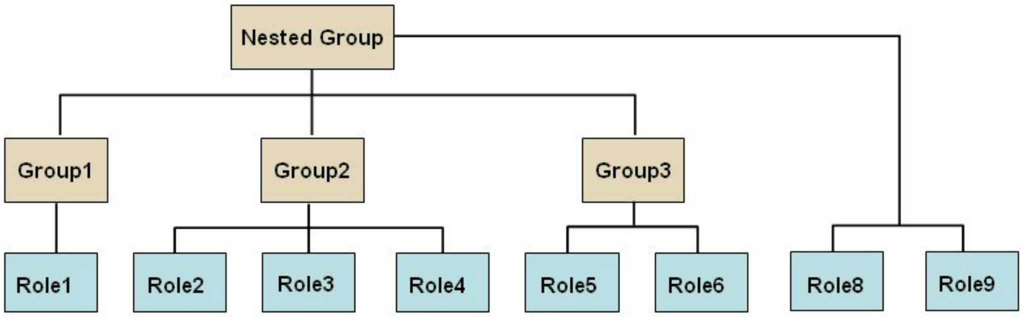
If you are using OID as Native Directory, Oracle recommends that you always use Shared Services Console to administer the css realm.

Note:

Groups on external user directories cannot be managed from Shared Services Console.

Nested Groups

You can use nested groups from external directories to facilitate provisioning. Members of nested groups inherit the roles assigned to the nested group. 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 nested group (Role8 and Role9 in the illustration). For example, the role assignment of Group1 in the illustration is Role1, Role8, and Role9. The nested group does not inherit the groups assigned to component groups.

Note:

Oracle does not recommend the use of nested Native Directory groups, because of their performance impact.

Creating Groups

A Native Directory group contains users and groups from the user directories configured on Shared Services, including Native Directory. Groups that contain other groups are known as *nested groups*. The use of nested Native Directory group is not recommended. See "Nested Groups" on page 113.

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

➤ To create Native Directory groups:

1. Launch Shared Services Console. See "Launching Shared Services Console" on page 49.
2. Right-click **Groups** in the View pane and select **New**.

   Create Group screen opens.
3. In **Name**, enter a unique group name.

   Group names are not case-sensitive.
4. **Optional:** Enter a group description.
5. Perform an action:
   - Click **Finish** to create the group without adding groups or users, and go to step 10.
   - Click **Next** to create a nested group or assign users to the group.

     The Group Members tab is displayed.
6. Create a nested group. To skip this step, click **Next**.

   a. 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.

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

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

   d. Click **Go**.

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

   e. From **Available Groups**, select the groups to nest within the new group.

   f. Click **Add**.

   The selected groups are listed under Assigned Groups list.

   g. **Optional:** Repeat steps a-f to retrieve and assign groups from other user directories.

Shared Services enables you to search the assigned groups to identify the groups that you want to remove. Use the fields above the Assigned Groups list to define the search criteria for searching within assigned groups list. See steps a-d for instructions on searching within assigned groups.

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

7 **Click Finish to create the group without adding users. Click Next to add uses to the group.**

The User Members tab is displayed.

8 **To assign users to the group:**

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

b. Select the user property (**Name**, **First Name**, **Last Name**, or **Description**) that should be searched.

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

d. Click **Go**.

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

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

f. Click **Add**.

The selected user accounts are listed under Assigned Users.

g. **Optional:** Repeat steps a-f to retrieve and assign users from other user directories.

Shared Services enables you to search the assigned users to identify the users that you want to remove. Use the fields above the Assigned Users list to define the search criteria for searching within assigned users list. See steps a-d for instructions on searching within the assigned users list.

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

9 **Click Finish.**

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

Modifying Groups

You can modify the properties of all Native Directory groups except WORLD (the container for all users and groups within Native Directory). 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.

Note:

You cannot modify the settings of the WORLD group.

➤ To modify groups:

1 Launch Shared Services Console. See "Launching Shared Services Console" on page 49.

2 Search for a group. See "Searching for Users, Groups, Roles, and Delegated Lists" on page 51.

A list of groups that meet the search criterion is displayed on the Browse tab.

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

The Group Properties screen is displayed.

Note:

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

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

5 Open the **Group Members** tab and perform one or both actions to modify group assignments:

a. To add groups to the group:

- In **Directory**, select the user directory from which you want to add the nested group. Select **All** to search for groups in all configured directories.
- Select **Group Name** to search based on group names. Select **Description** to search based on group descriptions.
- Enter the criterion for retrieving groups. Use * (asterisk) as the wildcard to retrieve all available groups.
- Click **Go**.
- From **Available Groups**, select one or more groups, and click **Add**.

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

b. To remove assigned groups:

- From **Assigned Groups**, select the group to remove.

  Shared Services enables you to search the assigned groups to identify the groups to remove. Use the fields above the Assigned Groups list to define the search criteria for searching within the assigned groups list.
- Click **Remove**.

  Removed groups are listed in the Available Groups list.
- **Optional:** Click **Reset** to undo the changes you made to **Assigned Groups**.

6 Select the **User Members** tab and perform one or both actions 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 (**Name**, **First Name**, **Last Name**, or **Description**) to search.
- Enter the criterion for retrieving users. Use * (asterisk) as the wildcard to retrieve all available users.
- Click **Go**.
- From **Available Users**, select one or more users to assign to the group.
- Click **Add**.

  The selected users are listed in Assigned Users list.
- **Optional:** Repeat this procedure to retrieve and assign users from other user directories.

b. To remove users from the group:

- From **Assigned Users**, select the users to remove.

  Shared Services enables you to search the assigned users list to identify the users to remove. Use the fields above the Assigned Users list to define the search criteria.
- Click **Remove**.
- **Optional:** Click **Reset** to undo the changes you made to **Assigned Users**.

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

8 Click **Save**.

Deleting Groups

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

➤ To delete groups:

1 Launch Shared Services Console. See "Launching Shared Services Console" on page 49.

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

3 Search for the group to delete. See "Searching for Users, Groups, Roles, and Delegated Lists" on page 51.

Groups that meet the search criterion is displayed on the Browse tab.

4 Right-click the group, and select **Delete**.

Managing Roles

Roles define the operations that users can perform in specific applications.

Application roles from all registered EPM System applications can be viewed but not updated or deleted from Shared Services Console. Tasks performed by Shared Services Administrators:

- "Creating Aggregated Roles" on page 118

- "Modifying Aggregated Roles" on page 119
- "Deleting Aggregated Roles" on page 120
- "Generating Provisioning Reports" on page 129

Note:

You can provision newly created users and groups from LDAP-based user directories, including MSAD. However, the roles provisioned to the new users and groups are available to the users (become effective) only after Shared Services refreshes its cache. By default, the cache refresh interval is 60 minutes, which can be modified by updating the value of `CSS Cache Refresh Interval`. See "Configuring OID, MSAD, and Other LDAP-Based User Directories" on page 65.

Creating Aggregated Roles

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

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

Note:

You can create roles only after at least one EPM System application has been registered with Shared Services.

➤ To create aggregated roles:

1. Launch Shared Services Console. See "Launching Shared Services Console" on page 49.
2. From the **View pane**, right-click **Roles**, and select **New.**

   The Create Role screen is displayed.
3. For **Name**, enter a role name. Role names that contain special characters are not supported. Role names should not start or end with a \ (backslash). See "Using Special Characters" on page 88 for more information.
4. **Optional:** For **Description**, enter a role description.
5. From **Product Name**, select the product for which to create the role.

   This list includes all EPM System applications registered with Shared Services.
6. Click **Next.**
7. On the **Role Members** tab, find the roles to add.
   - Click **Go** to retrieve all roles from the selected application.
   - Enter the role name in **Search for Roles** and click **Go** to search for a role. Use * (asterisk) as the wildcard in pattern searches.

8 From **Available Roles**, select the application roles to assign.

9 Click **Add**.

The selected roles are listed in Assigned Roles list.

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

10 Click **Finish**.

Modifying Aggregated Roles

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

➤ To modify aggregated roles:

1 Launch Shared Services Console. See "Launching Shared Services Console" on page 49.

2 In the **View pane**, select **Roles**.

3 Retrieve an aggregated role. See "Searching for Users, Groups, Roles, and Delegated Lists" on page 51.

4 Right-click the role, and select **Properties**.

The Role Properties screen is displayed.

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

6 If you want to modify role member assignments, open the **Role Members** tab, and perform one or both actions:

a. To add role members:

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

  From Assigned Roles, select one or more roles and click Remove to remove a selected role. Click Reset to undo your actions on this tab.

b. To remove role assignments:

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

7 Click **Save**.

Deleting Aggregated Roles

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

➤ To delete aggregated roles:

1 Launch Shared Services Console. See "Launching Shared Services Console" on page 49.

2 In the **View pane**, select **Roles.**

3 Retrieve an aggregated role.

See "Searching for Users, Groups, Roles, and Delegated Lists" on page 51.

A list of roles that meet the search criterion is displayed on the Browse tab.

4 Right-click a role, and select **Delete.**

5 Click **OK.**

Changing OpenLDAP root User Password

Shared Services Administrators can change the password of the OpenLDAP `root` user account, which provides complete control over OpenLDAP. The default `root` password is hard-coded in a file and is invisible to users. OpenLDAP does not provide an interface to change this password. To improve security, Shared Services provides a screen to change the `root` password. The updated password takes effect after you restart OpenLDAP and Shared Services.

Note:

Only users provisioned with the Shared Services Administrator role can change the `root` password.

➤ To update OpenLDAP `root` password:

1 Launch Shared Services Console. See "Launching Shared Services Console" on page 49.

2 From **Administration**, select **Change Native Directory Password.**

3 In **Current Password**, enter the `root` account password. This field is automatically populated if the default password was not previously changed.

4 In **New Password** and **Confirm Password**, enter the new password for `root` account.

5 Click **Finish.**

6 Restart OpenLDAP.

7 Restart Shared Services.

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

Backing Up OpenLDAP Database

The OpenLDAP database must be backed up periodically to recover from loss of provisioning data due to media failures, user errors, and unforeseen circumstances. Oracle recommends that you regularly back up this database.

See the *Oracle Hyperion Enterprise Performance Management System Backup and Recovery Guide* for information on backing up OpenLDAP database.

Recovering Native Directory Data

The Shared Services database stores information related to product registration while the Native Directory database contains provisioning data for all products. These databases work in tandem to support EPM System products.

Data inconsistencies between these databases impact normal operations. Inconsistencies could occur during manual database update or database upgrades. You should recover Native Directory data if Shared Services does not display registered applications during provisioning. The recovery process uses the Shared Services database as the master database to resolve data inconsistencies. It performs the following activities:

- Creates missing registered applications in Native Directory
- Removes, from Native Directory, stale application entries for which data is not present in the Shared Services database

Caution!

Create a backup copy of the Native Directory data before recovering Native Directory.

Messages (errors as well as information) related to the operation are recorded in the `SharedServices_syncOpenLDAP.log` file. See Chapter 11, "Guidelines for Securing EPM System."

➤ To synchronize the Native Directory database with the Shared Services repository:

1. **Launch Shared Services Console. See "Launching Shared Services Console" on page 49.**
2. **Select Administration, then Recover Native Directory.**

   The Recover Native Directory screen opens.
3. **Click Start Recovery.**

   Status of the recovery process appears.
4. **Optional: Click Refresh to update the status.**
5. **Optional: Click View Log to display a log file that details the operations that were performed.**

Recovering OpenLDAP Data

To enable SSO and provisioning, OpenLDAP must be running. If OpenLDAP fails, causing Native Directory to fail, you must recover the provisioning data before users can access EPM System products, including Shared Services.

➤ To recover provisioning data after an OpenLDAP failure:

1 **Verify that the OpenLDAP is not running.**

2 **Open a command prompt or console.**

3 **Navigate to** `OPENLDAP_HOME/bdb/bin`**. For example,** `HYPERION_HOME/products/Foundation/SharedServices/openLDAP/bdb/bin`**.**

4 **Run the** `db_recover` **utility, using the following command:**

```
db_recover -h Path_OpenLDAP_data_file
```

For example, `db_recover -h ../../var/openldap-data`

Where `openldap-data` indicates the name of OpenLDAP data file.

5 **Monitor the utility to ensure that it runs successfully.**

6 **Restart the OpenLDAP service or process.**

7 **On the application server, restart Shared Services.**

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

Migrating Native Directory

The Native Directory database stores security-related data. You must migrate Native Directory data as a part of migrating Shared Services. Migration is the process of copying an application instance from one operating environment to another; for example, from development to testing or from testing to production.

Information sources:

- See the *Oracle Hyperion Enterprise Performance Management System Lifecycle Management Guide* for information on migrating Native Directory using Lifecycle Management Utility Utility.
- See the *Import/Export Utility Users Guide* for instructions on migrating Native Directory data using the Import/Export Utility. This guide is available in `HYPERION_HOME/common/utilities/CSSImportExportUtility/cssimportexport.zip`.

9

Managing Provisioning

In This Chapter

About Provisioning

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

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

Before Starting the Provisioning Process

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

- Plan how to provision EPM System products. You must:
    - Understand the available roles. See "Shared Services Roles" on page 155 for a list of EPM System product roles.
    - Understand available artifact-level access permissions. Unlike Shared Services, most EPM System products enforce artifact-level access rights using Access Control Lists (ACL) to restrict access to product artifacts. For example, an account is a Planning artifact for which access rights can be set. See the product administrator's guide for information on the product artifacts for which access controls can be set.
    - Configure the external user directories that contain accounts for EPM System users and groups. See Chapter 5, "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 are limited to the delegated lists assigned to them. For example, if user *Admin1* is assigned the Essbase Provisioning Manager role for *DelegatedList1*, *Admin1* can provision only the users from *DelegatedList1*. See Chapter 7, "Delegated User Management."

Overview of Provisioning Steps

All Shared Services provisioning activities must be performed by a Shared Services administrator or provisioning manager. A built-in `admin` account is available to initiate the provisioning process.

Provisioning of users and groups should follow a provisioning plan tailored for your organization. Typically, you should create Shared Services administrators and application specific provisioning managers to provision EPM System product 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 "Shared Services Roles" on page 155 for a discussion of available roles and their access privileges.

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

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

Provisioning Administrative Users

Provisioning of administrative users and groups involves using the Shared Services Console to assign the required EPM System product administrative roles. For example, the Planning Provisioning Manager role enables the recipient to provision users and groups with Planning roles. Other EPM System products have similar administrative roles. Assigning of administrative roles from Shared Services must be done by a Shared Services Administrator.

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

Provisioning EPM System Users

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

You must provision users with product roles to allow them to access other EPM System products. Shared Services administrators and provisioning managers perform the following steps to provision users and groups:

1. From Shared Services Console, identify and select the users (or the groups to which they belong) who need access to the EPM System product. See "Searching for Users, Groups, Roles, and Delegated Lists" on page 51
2. Assign product roles that allow users access to EPM System product. For example, the Server Access role should be assigned to all Essbase users. See "Provisioning Users and Groups" on page 125

   EPM System product roles are described in Appendix A, "Product Roles."
3. Assign application-specific roles that grant access to the functions of the application instances belonging to the EPM System product. For instance, Essbase application `Esb_App1` provides the Calc role which can be assigned to users who need to work with Calc scripts of Esb_App1.

   These roles are assigned on a per application basis. For example, roles from Essbase application `Esb_App1` allows users to access functionalities in `Esb_App1` only.
4. Using a product administration screen, assign access to the artifacts managed by the EPM System application. You can launch the product administration screen from Shared Services Console using these steps:
   a. In the View panel of Shared Services Console, right-click the application to provision.
   b. Select Assign Access Control. A product administration screen, which is not a part of Shared Services Console, opens.
   c. Provision users as needed. See the online help available in the screen for instructions.

   Artifact-level access control allows administrators to fine tune access to application objects. By design, these access privileges are more granular than application roles. These can be used to restrict the access rights that were granted using roles.

   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 roles from EPM System applications to the users and groups that are available in the configured user directories. Provisioning is managed at the user or group levels by Provisioning Managers or Shared Services Administrators assigning one or more EPM System application roles to a user or group. See "Provisioning (Role-based Authorization)" on page 19.

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.

Note:

Essbase Server maintains its own security file containing provisioning data about groups and users who are provisioned to perform operations on the Essbase Server. Because this information is not automatically updated, you must synchronize Essbase security every time the provisioning data of Essbase users or groups is updated or added from Shared Services. For example, newly provisioned users are not recognized by the Essbase Server until synchronization is performed. Similarly, changes to provisioning assignments are recognized by the Essbase Server only after security is synchronized. For information on running a MaxL command to synchronize Essbase security with Shared Services security, see the *Oracle Essbase Technical Reference*. For information on synchronizing Essbase security with Shared Services security from Administration Services, see "Synchronizing Essbase Security with Shared Services Security" on page 170 or the *Administration Services Online Help*.

➤ To provision users or groups:

1 **Launch Shared Services Console. See "Launching Shared Services Console" on page 49.**

2 **Find a user or group to provision.**

See "Searching for Users, Groups, Roles, and Delegated Lists" on page 51.

Note:

Group-based provisioning is not supported for Financial Management taskflows.

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

The Provisioning tab is displayed.

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 one or more roles, and click Add.**

The selected roles are displayed in Selected Roles.

6 **Click Save.**

A dialog box, indicating that the provisioning process is successful, opens.

7 **Click OK.**

Deprovisioning Users and Groups

Deprovisioning removes all the roles the user or group is assigned from an application. Shared Services administrators can deprovision roles from one or more applications. Provisioning managers of applications can deprovision roles from their applications. For example, assume that the group `Sales_West` is provisioned with roles from Planning and Financial Management. If this group is deprovisioned by a Planning Provisioning Manager, only the roles from Planning are removed.

➤ To deprovision users or groups:

1 **Launch Shared Services Console. See "Launching Shared Services Console" on page 49.**

2 **Find a user or group to deprovision.**

See "Searching for Users, Groups, Roles, and Delegated Lists" on page 51.

3 **Right-click the user or group, and select Deprovision.**

The Deprovision tab is displayed.

4 **Select applications, or select Check All to select all applications.**

5 **Click OK.**

6 **In the confirmation dialog box, click OK.**

7 **In the Deprovision Summary screen, click OK.**

Auditing Security Activities and LCM Artifacts

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

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

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

By default, auditing is disabled. You must enable auditing if you want to allow Shared Services Administrators, Directory Managers, and LCM Managers to view audit reports to track the changes that have occurred. See "Generating Audit Reports" on page 130.

Only Shared Services Administrators can enable auditing or change the list of objects and artifacts that are audited at the global level.

- "Purging Audit Data" on page 128
- "Selecting Objects for Application and Application Group-Level Audits" on page 129

➤ To change the auditing configuration:

1. Using Shared Services Administrator credentials, log in to the Shared Services Console. See "Launching Shared Services Console" on page 49.
2. Select **Administration**, then **Configure Auditing**.
3. On the Audit Configuration screen:

   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 retaining the audit data and click **Purge**.

   d. From **Select Tasks**, select the tasks for which audit data is to be preserved. Tasks are categorized based on the applications registered with Shared Services.

   e. Click **OK**.

Purging Audit Data

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

Caution!

Shared Services Administrators must purge the data based on your company's audit data retention policies. Before purging data, be sure to back up the Shared Services database.

➤ To purge audit data:

1. Using Shared Services Administrator credentials, log into the Shared Services Console. See "Launching Shared Services Console" on page 49.
2. Select **Administration**, then **Configure Auditing**.

   The Audit Configuration screen opens.
3. In **Purge Data Older than**, set the number of days for retaining the audit data.
4. Click **Purge**.
5. Click **OK**.

Selecting Objects for Application and Application Group-Level Audits

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

➤ To select objects for auditing:

1. Using Shared Services Administrator credentials, log in to the Shared Services Console. See "Launching Shared Services Console" on page 49.
2. In the View pane, right-click one of the following and select **Configure Auditing**:
   - An application group to enable auditing for all the applications in the application group
   - An application to enable auditing for the application

   Note:

   Configure Auditing option is not enabled at application group and application levels if Allow Global Settings Over-ride is selected in Audit configuration screen. See "Auditing Security Activities and LCM Artifacts" on page 127.
3. From **Select Tasks**, select the tasks for which audit data is to be preserved. Tasks are categorized based on the applications registered with Shared Services.
4. Click **OK**.

Generating Reports

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

- "Generating Provisioning Reports" on page 129
- "Generating Audit Reports" on page 130
- "Generating Migration Status Report" on page 132

Generating Provisioning Reports

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

Provisioning reports enable administrators to review the access rights and permissions granted to users across EPM System applications, making them useful to 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 From the View pane in Shared Services Console, select a user or role. See "Searching for Users, Groups, Roles, and Delegated Lists" on page 51.

2 Select **Administration**, then **View Provisioning Report.**

3 Enter report generation parameters.

Table 19 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 group 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 on only directly assigned roles.
Group By	Select how to group the data in the report. Available grouping criteria depend on the selection in Find All.
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.

4 Click **Create Report.**

The report is displayed on the Provision Report tab.

5 **Optional**: To print the report:

a. Click **Print Preview**.

The report is displayed in View Report window.

b. Click **Print**.

c. Select a printer, and click **Print**.

d. Click **Close**.

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

7 Click **OK.**

Generating Audit Reports

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

Shared Services Administrators, Directory Managers, and LCM Managers can generate and view audit reports to track the changes to the security data that have occurred over time.

Note:

Auditing must be configured before you can generate audit reports. See “Auditing Security Activities and LCM Artifacts” on page 127.

➤ To generate audit reports:

1. Select **Administration**, then **Audit Reports.**
2. Select an option:
   - **Security Reports** to generate Security Audit report.
   - **Artifact Reports** to generate a report on the artifacts that were migrated using Lifecycle Management Utility.
   - **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 all users for the last 30 days.
3. To regenerate the report, select report parameters:
   a. In **Performed By**, select the users for which the report is to be generated.
   b. In **Performed During**, select the period for which the report is to be generated. You can set the period as number of days, or as a date range.
   c. **Optional:** Select **Detailed View** to group the report data based on the attribute that was modified and the new attribute value.
   d. **Optional:** In **Per Page**, select the number of rows of data to display in a report page.
   e. Click **View Report**.
4. To create a CSV file containing the report data, click **Export.**
   a. Select **Save as CSV**.
   b. Click **OK**.
   c. Click **Open** to open the file or **Save** to save the file to the file system. By default, the Security Report file is named `auditsecurityreport.csv`, the Artifact Report is named `AuditArtifactReport.csv`, and the Config Report is named `AuditConfigReport.csv`.
5. Click **Close.**

Generating Migration Status Report

The Migration Status Report contains information on the artifact migrations that were performed using Lifecycle Management Utility Utility. This report presents information such as the user who performed the migration, the package file used, the time the migration was performed, and the number of artifacts migrated.

➤ To generate Migration Status Report:

1 **Select Administration, then Migration Status Report.**

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

2 **To regenerate the report, select report parameters:**

a. 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.

b. In **Status**, select the migration status based on which the report is to be generated. Do not specify the status if you want to generate the report on all migrations.

- Select **Active** to report on only active migrations.
- Select **Success** to report on only successful migrations.

c. **Optional:** In **Per Page**, select the number of rows of data to display in a report page.

3 **Click Refresh.**

4 **Optional: Click Collapse/Expand to hide or show the report parameters.**

Importing and Exporting Native Directory Data

Use the Lifecycle Management Utility to perform the following tasks:

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

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

Note:

If you upgraded to version 11.1.1.2 from version 9.x, and the provisioning data was corrupted, use the Import/Export Utility to import Native Directory data from an existing export file. See the Import/Export Utility documentation (`impexp.pdf`) available in *`HYPERION_HOME`*`/common/utilities/CSSImportExportUtility/cssimportexport.zip`.

10

Using the Update Native Directory Utility

In This Chapter

About the Update Native Directory Utility

The Update Native Directory Utility is used in the following scenarios:

- “Clean Stale Data in Native Directory” on page 133
- “Upgrade Shared Services to Use Unique Identity Attribute” on page 134
- “Migration of Users and Groups Across User Directories” on page 135

Clean Stale Data in Native Directory

The external user directory configuration in Shared Services may use an identity attribute that reflects the location of users and groups (for example, DN). In such cases, moving users and groups across organizational units can cause stale data within Native Directory because EPM System security is not synchronized to be aware of such changes.

When the following actions take place in an LDAP-based user directory including MSAD, the links that Native Directory maintains with the user directory are broken, creating stale data in Native Directory and causing loss of access to EPM System applications.

- Users and groups are moved across organizational units
- Multiple users or groups are assigned identical common name (CN)
- CN of provisioned users or groups are modified

Run the Update Native Directory Utility to synchronize Native Directory data with the data in configured LDAP-based user directories. Running this utility makes the stale provisioning data usable.

➤ To clean stale data from Native Directory:

1 **Create backups of Native Directory and Shared Services repository. See “Backing Up OpenLDAP Database” on page 121.**

2 Install the Update Native Directory Utility. See "Installing the Update Native Directory Utility" on page 138.

3 Run the Update Native Directory Utility to synchronize user and group identities between Native Directory and user directories. See "Running the Update Native Directory Utility" on page 138. See "Operations Performed" on page 137 for actions that the utility performs.

Upgrade Shared Services to Use Unique Identity Attribute

External user directory configuration in Shared Services uses an identity attribute to locate users and groups on configured user directories. While upgrading Shared Services, you can use a unique identity attribute (recommended) that does not reflect the location of users and groups or choose to retain an identifier (for example, DN) that reflects their location.

Because stale provisioning data is created in Native Directory if users and groups are moved across organizational units or if the CN of provisioned users or groups are modified, Oracle recommends the use of the unique identity attribute.

Because migrating to the unique identity attribute affects all EPM System products, plan the migration to minimize application downtime.

Important Considerations

- The unique identity attribute can be set only for LDAP-based user directories, such as OID and MSAD.
- For migration to work, all similar user directories configured on Shared Services must be migrated to the new unique identity attribute. All MSAD user directory configurations must be updated with the unique identity attribute before Shared Services can migrate MSAD users and groups to the new attribute. Similarly, the configuration of all LDAP-based user directories other than MSAD (SunONE, IBM Directory Server, Novell eDirectory, and custom user directories) must be updated to the new identity attribute before Shared Services can migrate users and groups from these user directories to the new attribute.

  For example, assume that three MSAD user directories are configured on Shared Services. Two are configured to use the unique identity attribute `ObjectGUID`, and the third is configured to use `DN` as the attribute. In this scenario, users and groups are not migrated until the third configuration also uses a unique attribute other than `DN`.
- Reverse migration is not supported. After migrating to the new unique identity attribute, you cannot return to the previous identity attribute (`DN`).

  Oracle recommends that you back up Native Directory database before migrating to the new unique identity attribute. If you return to `DN` as the identity attribute, you can restore data from the backup.

Caution!

Do not migrate to the unique identity attribute by using the Update Native Directory Utility if you changed the attribute identified as `loginAttribute` using the `Login` field of the User Configuration screen. If you run the utility, provisioning data of the users whose accounts are defined on the user directory for which the `loginAttribute` is changed is deleted from Native

Directory. You cannot recover the deleted data; however, you can restore it from the latest backup.

Caution!

After you migrate Shared Services users and groups to the unique identity attribute, EPM System products stop working until the user and group information contained in product-specific repositories is updated to reflect the unique identity attribute.

Shared Services and EPM System product migration to the unique identity attribute can take considerable time, depending on the number of users and groups involved. Because EPM System products will not be available during this time, Oracle recommends that you schedule in a way that minimizes downtime.

Upgrade Procedures

➤ To upgrade Shared Services to use a unique identity attribute:

1 Remove stale data, if any, present in the Native Directory. See "Clean Stale Data in Native Directory" on page 133.

2 Back up Native Directory and Shared Services repository. See "Backing Up OpenLDAP Database" on page 121.

3 Install the Update Native Directory Utility. See "Installing the Update Native Directory Utility" on page 138.

4 Update the user directory configuration to use the unique identity attribute. See "Configuring OID, MSAD, and Other LDAP-Based User Directories" on page 65.

5 Restart Shared Services or execute the Update Native Directory Utility. See "Running the Update Native Directory Utility" on page 138. See "Operations Performed" on page 137 for a list of actions that the utility performs.

6 Perform product-specific migration procedures. See the following topics:

- "Essbase" on page 140
- "Planning" on page 141
- "Financial Management" on page 142
- "Reporting and Analysis" on page 142
- "Strategic Finance " on page 143

Migration of Users and Groups Across User Directories

Organizations may retire their corporate user directories and switch to a different user directory, causing the user and group identities of provisioned users maintained by EPM System products to be inaccurate. For example, an organization may replace its NTLM user directory with OID or MSAD. EPM System products become inaccessible if the provisioning information stored by EPM System products is not updated to reflect the identity of the users and groups in the new corporate user directory.

In this discussion, the user directory from which users and groups are migrated is referred to as the source user directory, and the user directory to which users and groups are migrated is referred to as the target user directory.

Assumptions

- If users or groups are moved across organizational units in the source user directory, or if the common name of provisioned users or groups are modified, the Update Native Directory Utility is run to synchronize the provisioning data in the Native Directory with the users and groups in the source user directory. See "Clean Stale Data in Native Directory" on page 133.
- The target user directory contains user and group accounts identical to those maintained in the source directory. The source and target user and group identities must match.
- The source and target user directories are configured in Shared Services.
- **Optional:** If you are not using the unique `identityAttribute`, the user directory search order in Shared Services is changed so that the target user directory is at the top of the search order if other user directories contain user and group accounts similar to those migrated from the source user directory. See "Managing User Directory Search Order" on page 84.

What Happens During Migration

After the migration process is initiated, Shared Services performs the following operations:

- Using the value of the `loginAtttribute` from Native Directory, the process locates the users and groups in a configured user directory. The match found in the source user directory is ignored.
- Upon finding a match in one of the configured user directories, Shared Services stops the search and updates Native Directory so that the provisioning information in the Native Directory is assigned to the matching user or group.
- If a matching entity is found only in the source user directory, the process does not modify the provisioning information in Native Directory.
- If a matching record is not found in the source user directory, the process removes the provisioning information from Native Directory.

Updating Native Directory to Handle User and Group Movement Across User Directories

Create backups of the source and target user directories and Native Directory before starting the migration process. You must also back up EPM System product repositories.

Before migrating users across user directories, perform the following operations. Do not perform these operations with the migration of users and groups across user directories.

- Run the Update Native Directory Utility to handle interorganizational unit moves or changes to the user and group CN. See "Clean Stale Data in Native Directory" on page 133.

➤ To update Native Directory to handle user and group movement across user directories:

1. Back up Native Directory and Shared Services repository. See "Backing Up OpenLDAP Database" on page 121.
2. Install the Update Native Directory Utility. See "Installing the Update Native Directory Utility" on page 138.
3. Run the Update Native Directory Utility. See "Running the Update Native Directory Utility" on page 138. See "Operations Performed" on page 137 for actions that the utility performs.

Post-migration Procedures

After successfully running the Update Native Directory Utility do one of the following:

- Remove the source user directory from the search order. See "Removing a Search Order Assignment" on page 86.
- Delete the source user directory configuration from Shared Services. See "Deleting User Directory Configurations" on page 84.

Operations Performed

The Update Native Directory Utility performs these actions:

- Deletes the user from Native Directory if the user account is not available in the external user directory.
- Deletes user accounts derived from the external user directory if the user directory is removed from the Shared Services search order.
- Updates Native Directory if the CN of the user or group in the external user directory was changed.
- Updates Native Directory if the user or group in the external user directory is moved from one organizational unit to another (the organizational unit to which the user or group is moved must be configured in Shared Services).
- Updates Native Directory if provisioned users and groups have been migrated from one user directory to another.

Note:

After migrating user and group information in Native Directory, you must migrate the user and group information in EPM System product repositories. See "Product-Specific Updates" on page 140 for detailed procedures.

Installing the Update Native Directory Utility

The `UpdateNativeDir.zip` archive containing the Update Native Directory Utility is installed in *`HYPERION_HOME`*`/common/utilities/SyncOpenLdapUtility`.

➤ To install the Update Native Directory Utility:

1. **Extract `UpdateNativeDir.zip` to a convenient location, preferably to *`HYPERION_HOME`*. This creates the `updateNativedir` folder.**
2. **Using a text editor, open `updateNativedir` batch file or script.**
    a. Verify that `JAVA_HOME` points to Sun Java version 1.5 or later (for example, *`HYPERION_HOME`*`/common/JRE/Sun/1.5.0/bin`).

    b. Save and close `updateNativedir`.

Running the Update Native Directory Utility

The Update Native Directory Utility synchronizes the data related to all the external user directories included in Shared Services search order.

Before running the Update Native Directory Utility, back up the following databases:

- Native Directory repository
- Shared Services repository
- Essbase (security file)
- Planning repository
- Financial Management repository
- Reporting and Analysis repository

➤ To run the Update Native Directory Utility:

1. **Using a command prompt or console window, navigate to the directory where the Update Native Directory Utility is installed.**
2. **Execute the following command:**

Note:

Before executing this command, verify that http access to security configuration is allowed in Shared Services. See "Setting Security Options" on page 86.

```
updateNativedir -cssLocation config HTTP URI [-options]
```

Where *`config HTTP URI`* identifies the location where Shared Services configuration information is available. For example: `http://MyServer:port/framework/getCSSConfigFile`, where `MyServer` indicates the name of the application server. If Shared Services is deployed to use SSL, be sure to the secure HTTP URI.

Update Native Directory Utility options are discussed in "Update Native Directory Utility Options" on page 139.

The utility lists the user providers specified in the search order and asks whether to continue with the operation.

3 **Enter `1` to continue running the utility, enter `0` to cancel the operation.**

4 **Monitor the log files to verify progress.**

5 **Restart Shared Services to refresh the cache so that the updates done by the utility are visible to Shared Services.**

Update Native Directory Utility Options

Table 20 Update Native Directory Utility Options

Option	Description
`-nodelete`	**Optional:** Use this option to generate the `CSSMigration-Deleted_`*`time_stamp`*`.log` file that lists the Native Directory users and groups that are candidates for deletion. Users and groups are not deleting from Native Directory. If this option is not set, the utility generates the `CSSMigration-Deleted_`*`time_stamp`*`.log` and automatically deletes the Native Directory users and groups whose identities are not available in external user directories.
`-noprompt`	**Optional:** Use this option to invoke silent mode operation. Used for scheduled jobs because no operator interaction is required. **Example:** `updateNativeDir -cssLocation` *`config HTTP URI`* `-noprompt` updates Native Directory in silent mode.
`-noupdate`	**Optional:** Use this option if you only want to generate the `CSSMigration-Update_`*`time_stamp`*`.log` that lists the users and groups that needs to be updated in Native Directory. User and group information in Native Directory is not updated if you use this option. **Example:** `updateNativeDir -cssLocation` *`config HTTP URI`* `–noupdate` If this option is not set, the utility generates the `CSSMigration-Update_`*`time_stamp`*`.log` and automatically updates the user and group information in Native Directory.

Update Native Directory Utility Log Files

By default, Update Native Directory Utility log files are created in `updateNativedir/logs`. If the utility cannot create `updateNativedir/logs`, the log files are created in `$TMP \Hyperion-logs` or `%TEMP%\Hyperion-logs`.

- `CSSMigration-Ambiguous_`*`time_stamp`*`.log` lists the identities that were not updated because more than one similar identity was detected by the utility. Identities listed in this file must be manually updated.
- `CSSMigration-Deleted_`*`time_stamp`*`.log` lists the deleted external user directory entries that must be deleted from Native Directory. These entries are automatically removed from Native Directory if the `nodelete` option is not set when executing the utility.

- `CSSMigration-Updated_`*`time_stamp`*`.log` lists the Native Directory identities that needs to be updated. If the `-noupdate` option is not set when executing the utility, the utility updates these entries in Native Directory.
- `CSSMigration-ignored_`*`time_stamp`*`.log` lists the entries on which no action was taken because they need not be updated.

Product-Specific Updates

EPM System products must perform steps to update their internal repositories in the following scenarios:

- Stale data in Native Directory is cleaned using Update Native Directory Utility. See "Clean Stale Data in Native Directory" on page 133.
- Shared Services is reconfigured to use the unique identity attribute. See "Upgrade Shared Services to Use Unique Identity Attribute" on page 134.
- Native Directory is updated to handle user and group movement across user directories. See "Migration of Users and Groups Across User Directories" on page 135.

The following EPM System products must update their internal repositories:

- "Essbase" on page 140
- "Planning" on page 141
- "Financial Management" on page 142
- "Reporting and Analysis" on page 142
- "Strategic Finance " on page 143

The following EPM System products need not perform migration procedures:

- Performance Scorecard
- Oracle Essbase Integration Services
- Oracle Hyperion Provider Services

Essbase

Caution!

Oracle recommends that you back up the Essbase security file and the data in Native Directory before starting the migration process. After migrating users and groups to use the new identity attribute, you cannot revert to the previously used identity attribute. To revert, restore user and group data in Native Directory and Essbase from the backups.

Before starting Essbase after the upgrade, edit the `IDMIGRATION` setting in *`HYPERION_HOME`*`\AnalyticServices\bin\essbase.cfg` to indicate whether to migrate to the new identity attribute that Shared Services uses.

On starting up, Essbase checks `essbase.cfg` and performs the action indicated by the `IDMIGRATION` setting.

Table 21 `IDMIGRATION` **Syntax**

Syntax	Description
`CHECKANDMIGRATE`	Default option. Checks for identity attributes that have changed in Shared Services and updates them in Essbase security.
`NOMIGRATION`	Makes no changes in Essbase security.
`FORCEDMIGRATION`	Updates Essbase users and groups without checking whether identity attributes have changed.

Planning

Caution!

Oracle recommends that you back up the user and group data in Native Directory and the Planning repository before starting migration. After migrating users and groups to use the new identity attribute, you cannot revert to the previously used identity attribute. To revert, restore user and group data in Native Directory and Planning repository from the backups.

Note:

After upgrading your system, migrate users and groups to the new identity attribute before performing another operation, such as loading security or changing existing security settings. Such changes may be lost during the migration.

Planning stores information about provisioned users and groups in the Planning repository. If Shared Services was upgraded to use the new identity attribute, you must synchronize the information in the Planning repository with that in the configured user directories by clicking **Migrate Users/Groups**. This button is available in Planning when assigning access to data forms, members, or task lists.

Note:

`HspUserUpdate utility` is no longer used to update users.

Financial Management

Caution!

Oracle recommends that you back up the user and group data in Native Directory and Financial Management before starting migration. After migrating users and groups to use the new identity attribute, you cannot revert to the previously used identity attribute. To revert, restore user and group data in Native Directory and Financial Management repository from the backups.

Financial Management records information about provisioned users and groups in the Financial Management repository. If Shared Services was upgraded to use the new identity attribute, you must synchronize the information in the Financial Management repository with that in the configured user directories.

Note:

After upgrading Financial Management, migrate users and groups to the new identity attribute before performing another operation, such as loading security or changing existing security settings. Such changes may be lost during the migration.

Click the **Migrate Users** button on the Security tab of the Financial Management Configuration Utility to synchronize the information in the Financial Management repository with that in the configured user directories.

Migrating Financial Management users is a onetime operation that must be completed before starting Financial Management after upgrading to Release 11.1.1.2.

Reporting and Analysis

Caution!

Oracle recommends that you back up the user and group data in Native Directory and Reporting and Analysis before starting the migration process. After migrating users and groups to use the new identity attribute, you cannot revert to the previously used identity attribute. To revert, restore user and group data in Native Directory and Reporting and Analysis repository from the backups.

Reporting and Analysis uses the `SyncCSSIdentity_BI` utility to synchronize user and group identities stored in its relational database to reflect the identity attribute set in Shared Services. See “Upgrade Shared Services to Use Unique Identity Attribute” on page 134 and “Running the Update Native Directory Utility” on page 138.

Note:

After upgrading Reporting and Analysis, migrate users and groups to the new identity attribute before performing another operation, such as loading security or changing existing security settings. Such changes may be lost during the migration.

Run the SyncCSSIdentity_BI utility only if Shared Services was upgraded to use the new identity attribute. Do not run the utility if Shared Services does not use the new identity attribute or if you do not have stale data resulting from interorganizational unit moves in the user directories. This utility needs to be run only once after upgrading Shared Services and Reporting and Analysis.

The SyncCSSIdentity_BI utility is installed in *BIPLUS_HOME*/syncCSSId. Execute the utility after upgrading Reporting and Analysis but before starting Reporting and Analysis services.

See *BIPLUS_HOME*/syncCSSId/ReadmeSyncCSSId_BI.txt for detailed instructions to run the SyncCSSIdentity_BI utility. Runtime information from the utility is written into *BIPLUS_HOME*/syncCSSId/BI_Sync.log.

On successfully executing the utility, ConfigurationManager.CSSIdSyncState value in V8_PROP_VALUE table of Reporting and Analysis database is set to 0 (for NO_SYNC). Other possible values for this property are 1 (CHECK_AND_SYNC, which is the default value) and 2 (FORCE_SYNC).

If the synchronization state in the database is not 0 (NO_SYNC), and the system determines that identity synchronization is required, the authentication service writes warning messages to *HYPERION_HOME*/logs/BIPlus/CSSSynchronizer.log. However, Reporting and Analysis services will run normally.

Strategic Finance

Oracle Hyperion Strategic Finance, Fusion Edition automatically migrates users to the unique identity attribute used by Shared Services to resolve issues where domain name or organizational unit changes might result in the loss of provisioning and object access information.

11 Guidelines for Securing EPM System

In This Chapter

Implementing SSL

SSL uses a cryptographic system that encrypts data. SSL creates a secure connection between a client and a server, over which data can be sent securely.

To secure your EPM System environment, configure SSL for your Web applications and LDAPS for user directory communications. See the *Oracle Hyperion Enterprise Performance Management System SSL Configuration Guide*.

Changing the Default Admin Password

The default Native Directory admin user account provides access to all Shared Services functions. You must change the password of this account soon after configuring Shared Services and periodically afterward.

Edit the *admin* user account to change the password. See "Modifying User Accounts" on page 110.

Changing Native Directory Password

Native Directory administrator's password must be changed immediately after configuring Shared Services and periodically afterward.

OpenLDAP

Change the OpenLDAP `root` password. See "Changing OpenLDAP root User Password" on page 120.

OID

➤ To change OID password:

1. **Change the password of the user whose account was used to establish the connection with OID as the Native Directory. See *Oracle Internet Directory Administrator's Guide*.**
2. **Update the Native Directory configuration with the new password. See "Modify the Native Directory Configuration" on page 55.**
3. **Restart all EPM System products.**

Changing the Application Server Administrator Password

EPM System product deployment process uses the default `hyperion` account (password is `hyperion`) to deploy Web applications to WebLogic Server and Oracle Application Server application servers. WebSphere deployment process does not use a password. The default account is not used to deploy Web applications to the Embedded Java Container (Tomcat). The default account is used to administer the WebLogic Server domains and the OC4J containers where EPM System products are deployed.

You must change the password of the default account immediately after completing the deployment and periodically afterward.

Caution!

If you set a password for `hyperion` user on WebSphere, you cannot use the EPM System Configurator to perform any action (deploy, undeploy or redeploy) on the WebSphere installation. To perform these actions using the EPM System Configurator, you must remove the password. Without removing the password, you can perform these actions manually.

➤ To change the password:

1 **Start the application server.**

- **WebLogic**: Execute startWebLogic.cmd (Windows) or startWebLogic.sh (UNIX). Typically, this file is in *HYPERION_HOME*/deployments/WebLogic9/bin.
- **WebSphere**: Execute startServer.bat (Windows) or startServer.sh (UNIX). Typically, this file is in *HYPERION_HOME*/deployments/WebSphere6/bin.

2 **Open the administration console of the application server. The URL to start the administration console is as follows:**

- **WebLogic**: http://*SERVER_NAME*:7001/console; for example, http://myServer:7001/console.
- **WebSphere**: http://*SERVER_NAME*:19060/ibm/console; for example, http://myServer:19060/ibm/console.

3 **Using the application server console, change the password of the hyperion user on the application server. You should change the password in each EPM System product domain (WebLogic Server) and OC4J instance (Oracle Application Server). See your application server documentation for information. See your application server documentation for assistance.**

Note:

WebLogic only:: After changing the password of hyperion user, if you cannot restart the WebLogic Administration Console, delete *HYPERION_HOME*deployments/Weblogic9/boot.properties and then complete the procedures to bypass the prompt for user name and password. After completing the procedure, copy theboot.properties from the WebLogic Administration Server to all managed servers in *HYPERION_HOME*deployments/Weblogic9/servers/*SERVER_NAME*/security/boot.properties.

4 **For WebLogic Server and Oracle Application Server only:** Encrypt the application server password.

a. Open a command prompt and navigate to *HYPERION_HOME*/common/config/9.5.0.0 directory.

b. Execute encryptString.bat using the new application server password of hyperion user as the only parameter.

For example, if myPasswor12 is the new password, use the command encryptString.bat myPasswor12 to encrypt it.

The encrypted password appears in the command prompt window.

Caution!

Enter the password exactly as you specified in the application server. Any deviation will cause a password mismatch.

c. Copy the encrypted password from the command prompt window.

d. Using a text editor, open the property file (.properties or oracle.properties). This file is available in *HYPERION_HOME*/common/config/9.5.0.0/resources/

APP_SERVER/resources folder, where *APP_SERVER* indicates the application server name, or oracle.

e. Replace the existing password with the encrypted password that you copied in step c.

- **Oracle Application Server:** Replace the value of the oc4j.admin.password property.
- **WebLogic Server:** Replace the value of the domain.default.user.password property.

f. Save and close the file.

Regenerating the SSO Encryption Key

Use the SharedServicesHandler Utility to regenerate the SSO encryption key for EPM System products. The SharedServicesHandler Utility generates a new keystore file that can be used to encrypt and decrypt EPM System SSO tokens.

Caution!

Do not run the SharedServicesHandler Utility in a mixed environment that comprises 11.1.1 and 9.x products. Run the SharedServicesHandler Utility if you have only EPM System version 11.1.1 products.

Caution!

Taskflows used by Financial Management, Performance Management Architect, and Profitability and Cost Management are invalidated when you generate a new keystore. After regenerating the keystore, open and save the taskflows to revalidate them.

➤ To run the SharedServicesHandler Utility:

1. **Extract the contents of** *HYPERION_HOME*/common/utilities/SharedServicesHandler/SharedServicesHandler.zip **(Windows) or** *HYPERION_HOME*/common/utilities/SharedServicesHandler/SharedServicesHandler.tar **(UNIX) into a directory on the Shared Services host machine; for example, into** *HYPERION_HOME*/common/utilities/SharedServicesHandler.
2. **Open a command prompt window and navigate to the** bin **directory within the directory where the SharedServicesHandler Utility was extracted; for example,** *HYPERION_HOME*/common/utilities/SharedServicesHandler/bin.
3. **Run** SharedServicesHandler.bat **(Windows) or** SharedServicesHandler.sh **(UNIX).**

   The SharedServicesHandler Utility creates the keystore file ssHandlerTK in *HYPERION_HOME*/common/css.
4. **Copy** *HYPERION_HOME*/common/css/ssHandlerTK **into the** *HYPERION_HOME*/common/CSS **directory on servers that host EPM System products and utilities that uses Shared Services security.**
5. **Restart all EPM System products and custom applications that use Shared Services security APIs.**

Disabling HTTP Access to Security Configuration

If you have only EPM System version 11.1.1.2 products in your environment, disable HTTP Access to Security Configuration. See "Setting Security Options" on page 86.

Changing Database Passwords

Periodically change the password for all EPM System product databases. The procedure for changing the database password in Oracle's Hyperion Shared Services Registry is detailed in this section.

For detailed procedures to change EPM System product database password, see *Oracle Hyperion Enterprise Performance Management System Installation and Configuration Guide*.

➤ To change EPM System product database passwords in Shared Services Registry:

1. **Using the database administration console, change the password of the user whose account was used to configure EPM System product database.**
2. **Stop EPM System products (Web applications, services and processes).**
3. **Using the EPM System Configurator, reconfigure the database using one of the following procedures.**

Shared Services Only:

Note:

In distributed environments where EPM System products are on different machines than Shared Services, you must perform this procedure on all servers.

a. From the Foundation tasks in EPM System Configurator, select **Configure Database**.

b. On the Shared Services and Registry Database Configuration page, select **Connect to a previously configured Shared Services database**.

c. Specify the new password of the user whose account was used to configure Shared Services database. Do not change any of the other settings.

d. Continue the configuration, and click **Finish** when you are done.

EPM System Products Other Than Shared Services:

Note:

Do these steps for the EPM System products deployed on the current server only.

a. From the configuration task list of the product in EPM System Configurator, select **Configure Database**.

b. On the Database Configuration page, select **Perform 1st-time configuration of database**.

c. Specify the new password of the user whose account was used to configure EPM System product database. Do not change any of the other settings.

d. Click **Next**.

A dialog box that prompts you to select one of the following options, is displayed.

- Drop and recreate tables
- Reuse the existing database

e. Select **Reuse the existing database**.

f. Continue the configuration, and click **Finish** when you are done.

See the *Oracle Hyperion Enterprise Performance Management System Installation and Configuration Guide* for detailed instructions.

4 **Start EPM System products and services.**

Securing Cookies

EPM System Web application sets a cookie to track the session. While setting a cookie, especially a session cookie, the server can set the secure flag, which forces the browser to send the cookie over a secure channel. This reduces the risk of session hijacking.

Note:

You should secure cookies only if EPM System products are deployed in an SSL-enabled environment.

WebLogic Server

Modify the WebLogic Server session descriptor to secure Oracle WebLogic Server cookies. Set the value of `cookieSecure` attribute in the `session-param` element to `true`. See http://edocs.bea.com/wls/docs81/webapp/_xml.html for detailed information.

Oracle Application Server

Set the value of `set-secure` to `true` to secure Oracle Application Server cookies. See http://download.oracle.com/docs/cd/B25221_04/web.1013/b14426/xmlfiles.htm#sthref596 for details.

Embedded Java Container

➤ To secure Embedded Java Container (Tomcat) cookies:

1 **Using as text editor, open `server.xml`. If you are using the Embedded Java Container bundled with EPM System, the location of `server.xml` is `*HYPERION_HOME*/common/appServers/Tomcat/5.5.17/conf/`.**

2 **In the HTTP connector definition, set the value of secure attribute to true; for example:**

```
secure="true"
```

3 **Save and close `server.xml`.**

4 **Restart the Embedded Java Container.**

WebSphere

Enable the `Secure` field in session manager properties to secure session cookies. For more information, see WebSphere documentation.

Use OID as Native Directory

Using OID as Native Directory, instead of OpenLDAP, allows you to enforce password policies. See "Setting up Oracle Internet Directory as the Native Directory" on page 53 and "Setting up Password Policies" on page 107.

Reduce SSO Token Timeout

SSO token timeout, by default, is set to 480 minutes. You should reduce the SSO token timeout; for example, to 60 minutes to minimize token reuse if it is exposed. See "Setting Security Options" on page 86.

Review Security Reports

The Security Report contains audit information related to the security tasks for which auditing is configured. Generate and review this report from Shared Services Console on a regular basis, especially to identify failed login attempts across EPM System products and provisioning changes. Select Detailed View as a report generation option to group the report data based on attributes that were modified and the new attribute values. See "Generating Audit Reports" on page 130.

Customize Authentication System for Strong Authentication

You can use a custom authentication module to add strong authentication to EPM System. For example, you can use RSA SecurID two-factor authentication in non-challenge response mode. The custom authentication module is transparent for thin and thick clients, and does not require client side deployment changes. See "Using a Custom Authentication Module" on page 57.

Encrypt UDL File (Financial Management)

While configuring Financial Management, EPM System Configurator creates an unencrypted UDL file by default. This file can be encrypted by selecting an option in the Advanced Database Options page of the EPM System Configurator or by running the EncryptHFMUDL utility after the configuration process is complete.

See "Encrypting UDL Files" in *Oracle Hyperion Enterprise Performance Management System Installation and Configuration Guide* for detailed information.

Disabling EPM Workspace Debug Utilities

For security purposes, administrators can disable the following EPM Workspace features that are primarily used for testing and debugging purposes:

- Configuration Information URL—The following URL presents configuration information about EPM Workspace installation, including Global Service Manager. and Shared Services.
  - `http://`*`hostname`*`:`*`19000`*`/workspace/browse/configInfo` (non-SSL)
  - `https://`*`hostname`*`:`*`19002`*`/workspace/browse/configInfo` (SSL)

  To disable the Configuration Information page, remove or rename *`HYPERION_HOME`*`/deployments/`*`APP_SERVER`*`/Workspace/webapps/workspace/jsp/shared/configInfo.jsp`.
- EPM Workspace test module—`cds.test` contains test cases and debugging utilities that are accessible when EPM Workspace is running in debug mode. To disable this module, rename or delete *`HYPERION_HOME`*`/deployments/`*`APP_SERVER`*`/Workspace/webapps/workspace/modules/com/hyperion/tools/cds/repository/bpm/test`.
- Troubleshooting code—For troubleshooting purposes, EPM Workspace ships with uncrunched JavaScript files. To remove uncrunched JavaScript files from your production environment:
  - Create a backup copy of *`HYPERION_HOME`*`/deployments/`*`APP_SERVER`*`/Workspace/webapps/workspace/js/com/hyperion` directory.
  - Except for the file *`DIRECTORY_NAME`*`.js`, delete the `.js` files from each subdirectory of *`HYPERION_HOME`*`/deployments/`*`APP_SERVER`*`/Workspace/webapps/workspace/js/com/hyperion`.

    Each subdirectory contains a `.js` file that bears the name of the directory. For example, *`HYPERION_HOME`*`/deployments/`*`APP_SERVER`*`/Workspace/webapps/workspace/`

js/com/hyperion/bpm/web/common contains Common.js. Remove all .js files except the one that bears the name of the directory; in this case, Common.js.

- Client-side debug mode—Ensure that EPM Workspace is not in debug mode. If EPM Workspace is in debug mode, use CMC to turn off debugging.

  To turn off debug mode:

  1. Start CMC. Execute startUI.bat (Windows) or startUI.sh (UNIX) to start CMC. Generally, this file is in *HYPERION_HOME*/common/workspacert/5.5.0.0/bin.
  2. Log in to EPM Workspace as administrator.
  3. Select Navigate then Administer, and then Configuration Console to open CMC.
  4. From Current View, select Web-Application Configuration.
  5. In the list of Web applications, right-click Workspace Web-Application and select Properties.
  6. On General tab, change the value of ClientDebugEnabled to No.
  7. Click OK.

Hide Default Apache Information

You can perform some basic hardening of Apache Web server security by updating httpd.conf (generally, located in *HYPERION_HOME*/common/httpServers/Apache/2.0.59/conf/httpd.conf).

- Turn off the Apache banner and version information:
  - ❍ Set ServerTokens to Prod; for example, ServerTokens Prod. The default value is Full.
  - ❍ Set ServerSignature to Off; for example, ServerSignature Off. The default value is On.
- Remove access to Apache documentation by commenting out the following directives for Apache manual:

```
AliasMatch ^/manual(?:/(?:de|en|es|fr|ja|ko|ru))?(/.*)?$ "C:/Hyperion/
common/httpServers/Apache/2.0.59/manual$1"
<Directory "C:/Hyperion/common/httpServers/Apache/2.0.59/manual">
    Options Indexes
    AllowOverride None
    Order allow,deny
    Allow from all
    <Files *.html>
        SetHandler type-map
    </Files>
    SetEnvIf Request_URI ^/manual/(de|en|es|fr|ja|ko|ru)/ prefer-
language=$1
    RedirectMatch 301 ^/manual(?:/(de|en|es|fr|ja|ko|ru)){2,}(/.*)?$ /
manual/$1$2
</Directory>
```

- Disable the indexing module by commenting out the following directives:
  - `LoadModule autoindex_module modules/mod_autoindex.so`
  - `IndexOptions FancyIndexing VersionSort`
  - `ReadmeName README.html`
  - `HeaderName HEADER.html`
  - `IndexIgnore .??* *~ *# HEADER* README* RCS CVS *,v *,t`
- Comment out all the `AddIcon*` directives. These directives are used by `IndexOptions FancyIndexing VersionSort`, which has been commented out. Examples of `AddIcon*` directives iclude `AddIconByType (TXT,/icons/text.gif) text/*` and `AddIcon /icons/tar.gif .tar`.

Change Default Web Server Error Pages

When application servers are not available to accept requests, the Web server plug-in for the back-end application server (for example, apache plug-in for WebLogic) returns a default error page that displays plug-in build information. Web servers display their default error page on other occasions as well. Attackers can use this information to find known vulnerabilities from public web sites.

You should customize the error pages (of Web application server plug-in and Web server) so that they do not contain information about any of your production system components; for example, server version, server type, plug-in build date, and plug-in type. Consult your application server and Web server vendor documentation for more information.

Support for Third-party Software

Oracle acknowledges and supports the backward compatibility assertions made by third-party vendors. Therefore, where vendors assert backward compatibility, subsequent maintenance releases and service packs may be used. If an incompatibility is identified, Oracle will specify a patch release on which the product should be deployed (and remove the incompatible version from the supported matrix) or provide a maintenance release or service fix to the Oracle product.

Server-side Updates: Support for upgrades to third-party server-side components is governed by the Subsequent Maintenance Release Policy. Typically, Oracle supports the upgrading of third-party server-side components to the next maintenance release of service pack of the currently supported release. Upgrades to next major release is not supported. For example, you can upgrade Apache server from version 2.0.61 to 2.0.63. Upgrading from version 2.0.61 to version 2.2 is not supported.

Client-side updates: Oracle supports automatic updates to client components; including updates to the next major release of third-party client components. For example, you can update the browser JRE version from 1.5 to 1.6.

A

Product Roles

In This Appendix

Shared Services Roles

All Shared Services roles are power roles. Typically, these roles are granted to power users who are involved in administering Shared Services and other EPM System products.

Role Name	Description
Administrator	Provides control over all products that integrate with Shared Services. It enables more control over security than any other EPM System product roles and should therefore be assigned sparingly. Administrators can perform all administrative tasks in Shared Services Console and can provision themselves. This role grants broad access to all applications registered with Shared Services. The Administrator role is, by default, assigned to the *admin* Native Directory user, who is the only user available after you deploy Shared Services.
Directory Manager	Creates and manages users and groups within Native Directory. Do not assign to Directory Managers the Provisioning Manager role, because combining these roles allows Directory Managers to provision themselves. The recommended practice is to grant one user the Directory Manager role and another user the Provisioning Manager role.

Role Name	Description
LCM Administrator	Runs Lifecycle Management Utility to promote artifacts or data across product environments and operating systems. In addition to the Provisioning Manager role, the LCM Administrator role comprises Directory Manager and Project Manager roles of Shared Services.
Project Manager	Creates and manages projects within Shared Services
Create Integrations	Creates Shared Services data integrations (the process of moving data between applications) using a wizard. For Performance Management Architect, creates and executes data synchronizations.
Run Integrations	Views and runs Shared Services data integrations. For Performance Management Architect, executes data synchronizations.
Dimension Editor	Creates and manages import profiles for dimension creation. Also creates and manages dimensions manually within the Performance Management Architect user interface or the Classic Application Administration option. Required to access Classic Application Administration options for Financial Management and Planning using Web navigation.
Application Creator ● Analytic Services Application Creator ● Financial Management Application Creator ● Planning Application Creator ● Profitability Application Creator	Creates and deploys Performance Management Architect applications. Users with this role can create applications but can change only the dimensions to which they have access permissions. Required, in addition to the Dimension Editor role, for Financial Management and Planning users to be able to navigate to their product's Classic Application Administration options. When a user with Application Creator role deploys an application from Performance Management Architect, that user automatically becomes the application administrator and provisioning manager for that application. The Application Creator can create all applications. The Analytic Services Application Creator can create Generic applications. The Financial Management Application Creator can create Consolidation applications and Performance Management Architect Generic applications. To create applications, the user must also be a member of the Application Creators group specified in Financial Management Configuration Utility. The Planning Application Creator can create Planning applications and Performance Management Architect Generic applications. The Profitability Application Creator can create Profitability and Cost Management applications and Performance Management Architect generic applications.
Calculation Manager Administrator ● Financial Management Calculation Manager Administrator ● Planning Calculation Manager Administrator	Administers and manages calculation manager functions. Financial Management Calculation Manager Administrator administers calculation manager functions in Financial Management. Planning Calculation Manager Administrator administers calculation manager functions in Planning.

Essbase Roles

The following table describes the roles specific to Essbase. For information on assigning granular access permissions to users and groups for a specific Essbase application or database, see the *Oracle Essbase Database Administrator's Guide*.

Note:

To create Essbase applications, in addition to the Essbase Administrator role, users must be provisioned with the Shared Services Project Manager role.

Role	Description
Server Roles	
Administrator	Full access to administer the server, applications, and databases. **Note:** The Provisioning Manager role is automatically assigned when you migrate Essbase Administrators; however, when you create an Essbase Administrator in Shared Services Console, you must manually assign the Provisioning Manager role.
Create/Delete Application	Creates and deletes applications and databases within applications. Includes Application Manager and Database Manager permissions for the applications and databases created by this user.
Server Access	Accesses any application or database that has a minimum access permission other than the default, which is *None*. **Note:** When assigning security at the Essbase application level, you must assign the user the Server Access role for the Essbase Server that contains the application (unless the user has another Essbase Server level role, for example, Create/Delete Application).
Application Roles	
Application Manager	Creates, deletes, and modifies databases and application settings within the assigned application. Includes Database Manager permissions for databases within the application. **Note:** The Provisioning Manager role is automatically assigned when you migrate Essbase Application Managers; however, when you create an Essbase Application Manager in Shared Services Console, you must manually assign the Provisioning Manager role.
Database Manager	Manages the databases, database artifacts, locks, and sessions within the assigned application.
Start/Stop Application	Starts and stops applications or databases.
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.
Filter	Accesses specific data and metadata according to filter restrictions.
Read	Reads data values.

Essbase Studio Roles

Role	Description
cpAdmin	Administrator* ● Creates, updates, and deletes Oracle Essbase Studio data source connections. ● Creates, updates, and deletes metadata elements in Essbase Studio. ● Performs “view sample” operations in Essbase Studio. ● Deploys cubes from Essbase Studio. ● Executes drill-through reports.
cpDM	Data Modeler* ● Creates, updates, and deletes metadata elements in Essbase Studio. ● Deploys cubes from Essbase Studio. ● Performs “view sample” operations in Essbase Studio. ● Executes drill-through reports. ● Cannot create data source connections.
cpDSAdmin	Data Source Administrator ● Creates, updates, and deletes Essbase Studio data source connections. ● Performs “view sample” operations in Essbase Studio. ● Executes drill-through reports. ● Cannot create metadata elements.
cpViewer	Viewer ● Connects to Essbase Studio for purpose of viewing artifacts, such as hierarchies or dimension elements. ● Executes drill-through reports. ● Cannot delete or modify any Essbase Studio artifacts.

*Additionally, in order to deploy cubes in Essbase Studio, the cpAdmin and cpDM users must be provisioned for, at a minimum, the Shared Services Project Manager role.

Reporting and Analysis Roles

Role	Description
Power Roles	
Reporting and Analysis Administrator	Conditionally accesses all resources (unless the file is locked by “no access”), but not all functionality; accesses the Administer and Impact Manager modules Applies to Financial Reporting, Oracle's Hyperion® Interactive Reporting, Oracle's Hyperion® SQR® Production Reporting, and Web Analysis

Role	Description
Reporting and Analysis Global Administrator	Universally and implicitly accesses all resources and functionality; accesses the Administer and Impact Manager modules **Note:** Reporting and Analysis Global Administrators can never be denied access. Applies to Financial Reporting, Interactive Reporting, Production Reporting, and Web Analysis
Content Manager	Manages imported repository content and execute tasks, with implicit access to all resources (unless the file is locked by "no access"); contains the Data Source Publisher role Applies to Financial Reporting, Interactive Reporting, Production Reporting, and Web Analysis
Data Source Publisher	Imports data source connectivity files Applies to Interactive Reporting and Web Analysis
Favorites Distributor	Pushes content to users' Favorites folders using the Favorites Manager Applies to Financial Reporting, Interactive Reporting, Production Reporting, and Web Analysis
Job Manager*	Creates and manages public job parameters, output directories, and output printer locations Applies to Interactive Reporting and Production Reporting
Schedule Manager	Creates and manages events, calendars, time events, public parameters, and physical resources; creates batches; contains the Scheduler and Job Manager roles Applies to Financial Reporting, Interactive Reporting, and Production Reporting
Interactive Roles	
Analyst	Accesses interactive content using full analytic and reporting functionality Applies to Financial Reporting, Interactive Reporting, and Web Analysis
Content Publisher	Imports, saves, and modifies batches, books, reports, and documents; creates and modifies shortcuts and folders Applies to Financial Reporting, Interactive Reporting, Production Reporting, and Web Analysis
Data Editor	Pushes Web Analysis data to Essbase
Job Publisher*	Imports and modifies documents, jobs, and job output; runs jobs; contains the Smart Form Publisher role Applies to Interactive Reporting and Production Reporting
Personal Page Publisher*	Publishes Personal Pages to the repository, where they can be viewed by other repository users; contains the Personal Page Editor role Applies to Interactive Reporting andProduction Reporting
Report Designer	Accesses authoring studios to create and distribute documents Applies to Financial Reporting and Web Analysis
Scheduler	Schedules jobs and batches using the Schedule module; navigates the repository and assigns access control; contains the Explorer and Job Runner roles Applies to Financial Reporting, Interactive Reporting, and Production Reporting
Smart Form Publisher*	Loads custom forms for programs (forms prompt job runners to enter information used to define jobs) Applies to Production Reporting

Role	Description
	Note: You must have the Job Publisher role to leverage Smart Form Publisher functionality.
View Roles	
Dynamic Viewer*	Views, reprocesses, and prints Interactive Reporting documents.
Explorer	Lists repository content in the Explore module and in context using the Open dialog box; searches, views, and subscribes to content **Note:** Access to the repository does not grant access to individual files and folders, which are secured by file properties and permissions Applies to Financial Reporting, Interactive Reporting, Production Reporting, and Web Analysis
Interactive Reporting Viewer*	Reviews and prints static Interactive Reporting documents
Job Runner*	Runs jobs and views public job parameters and physical resources Applies to Interactive Reporting and Production Reporting
Personal Page Editor*	Creates, modifies, and customizes Personal Pages; copies content from other users' published Personal Pages Applies to Interactive Reporting and Production Reporting
Personal Parameter Editor	Defines points of view and personal parameters on database connections to customize query result sets Applies to Interactive Reporting, Production Reporting, and Web Analysis
Viewer	Reviews EPM Workspace content; content is static and accessible only from the Favorites folder **Note:** This role provides minimal end-user functionality; use it only when no other role assignments are possible. Applies to Financial Reporting, Interactive Reporting, Production Reporting, and Web Analysis
System Roles	
Trusted Application	Enables credentialed client-server communication of Interactive Reporting database connection files (`.oce` extension) that encapsulate connectivity, database type, network address, and database user name information

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

Performance Management Architect Roles

Role	Description
Dimension Editor*	● Dimension Owner for any shared dimension in the Shared Library ● Can be explicitly assigned Dimension Owner, Dimension Writer, or Dimension Reader access to any local dimension in the Shared Library
Application Creators†	● Dimension Owner for all dimensions in undeployed applications ● Can be explicitly assigned Dimension Owner, Dimension Writer, or Dimension Reader access to any dimension in the Shared Library

Role	Description
Application Administrators‡	● Dimension owner for all dimensions in deployed applications ● Can be explicitly assigned Dimension Owner, Dimension Writer, or Dimension Reader access to any dimension in the Shared Library
Calculation Manager Administrator	Dimension reader for all dimensions of appropriate application types

*Only Dimension Editors can create dimensions in the Shared Library.

†Only Application Creators or Application Administrators can create or add dimensions to an application.

‡Only Application Creators or Application Administrators can create or add dimensions to an application.

Financial Management Roles

Additional Shared Services roles are required for Performance Management Architect. See "Shared Services Roles" on page 155.

Role	Description
Power Roles	
Application Administrator	Performs all Financial Management tasks. Access to this role overrides any other access setting for the user.
Load System	Loads rules and member lists
Inter-Company Transaction Admin	Opens and closes periods, locks and unlocks entities, and manages reason codes. Users with the role can also perform all inter-company tasks.
Interactive Roles	
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, accesses running tasks, data tasks, load and extract tasks. Cannot extract metadata or rules.
Journals Manager	Performs all tasks related to journals
Post Journals	Posts and unposts journals
Manage Templates	Grants access to the journals template task in the Setup Journals module
Generate Recurring	Grants access to the generate recurring task in the Setup Journals module
Review Supervisor	Starts process management units and approves and publishes process management data. Can promote or reject process units depending on process level

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

Role	Description
Advanced User	Uses the Browser View and can access Running Tasks
Read Journals	Reads journals
Receive Email Alerts for Process Management	Receives e-mails
Receive Email Alerts for Intercompany	Receives e-mails
Reserved	Not currently used

Planning Roles

Additional Shared Services roles are required for Performance Management Architect. See "Shared Services Roles" on page 155.

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, designates the e-mail server for notifications. Can use the Copy Data function.
Application Owner	Reassigns application ownership.
Mass Allocate	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 Essbase equivalent to their Planning access permissions. Enables users having write access, to change Planning data directly in Essbase using another product such as Financial Reporting or a third-party tool. For more information, see *Write Access to Data in Essbase*.
Interactive Roles	
Interactive User	Creates and maintains data forms, Smart View worksheets, business rules, task lists, Financial Reporting reports, and adapter processes. Manages the budget process. Can create Smart Slices in Smart View, use the Clear Cell Details function, and perform all Planner tasks. Interactive users are typically department heads and business unit managers.
Planner Roles	
Planner	Enters and submits plans for approval, runs business rules and adapter processes. Uses reports that others have created, views and uses task lists, enables e-mail notification for themselves, and creates data using Smart View.
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, Web Analysis, and Smart View). Typical View users are executives who want to see business plans during and at the end of the budget process.

To learn which roles do not apply and should not be assigned to Planning users who access Financial Reporting or Web Analysis, see “Reporting and Analysis Roles” on page 158.

Business Rules Roles

Role	Description
Power Roles	
Administrator	Creates, launches, edits, validates, and manages business rules, sequences, macros, variables, and projects. Assigns access permissions to business rules, sequences, macros, variables, and projects.
Interactive Roles	
Interactive User	Creates business rules, sequences, macros, variables, and projects. Assigns access permissions to business rules, sequences, macros, variables, and projects.
Basic User	Launches business rules and sequences to which the user has access. Views variables and macros, business rules, and sequences to which the users has access. Edits business rules, sequences, macros, variables, and projects for which the user has editing permissions.

Business Modeling Roles

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

Profitability and Cost Management Roles

Role	Description
Power Roles	

Role	Description
Administrator (*admin*)	The Administrator role provides the administrative capability within Profitability and Cost Management to perform these tasks: ● Create and maintain user accounts and security roles, and provision users, using Shared Services ● Generate Essbase databases ● Set up and maintain application preferences ● Build the model database using Performance Management Architect to select the common dimensions and members ● Create and maintain elements within the model, such as stages, drivers, POVs, driver associations, assignments, and application preferences ● Create staging tables in the source database to import model data and metadata from relational databases into Profitability and Cost Management ● Perform POV Copy, calculation, validation, data entry and trace allocations ● Deploy to Essbase and generate calculation scripts ● Import and export data ● Use Lifecycle Management Utility to promote data from one environment, such as development or testing, to another environment, such as production ● Back up and restore Profitability and Cost Management model components ● Monitor changes made to business objects
Power User	The Power User role manages the majority of model functions and can perform these tasks: ● Create and maintain elements within the model, such as stages, drivers, POVs, driver associations, assignments and application preferences ● Perform POV Copy, calculation, validation, data entry and trace allocations. ● Deploy to Essbase and generate calculation scripts ● Import and export data
Interactive Roles	
Interactive User	Can perform these tasks: ● View all modeling screens ● View and modify data in the Data Entry screen
View User	View-only access for these functions: ● Data entry ● Trace allocations ● Application preferences ● Model stages, drivers, and POVs

Transaction Manager Roles

Role	Description
Power Roles	

Role	Description
Administrator	Administers all system resources
Interactive Roles	
Basic User	Views system resources

Performance Scorecard Roles

Role	Description
Power Roles	
Power Manager	Power Manager role provides the administrative capability within an Performance Scorecard environment
Interactive Roles	
Basic User	Grants access to reports, scorecards, measures and initiatives with the additional role of result collection administration
Interactive User	Primarily a designer role, the Interactive User has access to all business objects for creation and modification. These include maps (accountability, strategy, cause and effect) as well as scorecards, initiatives and measures.

Essbase Provider Services Roles

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

Data Integration Management Roles

Oracle's Hyperion® Data Integration Management does not use the security environment established by Shared Services.

If you are upgrading to the current version of Data Integration Management and you used the Shared Services authentication plug-in, you must deregister the Shared Services authentication plug-in and then use Informatica PowerCenter Repository Manager to recreate the users. This version of Data Integration Management supports only native Informatica authentication.

See Data Integration Management documentation for detailed information on securing Oracle's Hyperion® Data Integration Management.

B Shared Services Roles and Permitted Tasks

Table 22 Shared Services User Roles and Tasks Matrix

Tasks	Administrato r	Directory Manager	Project Manager	Provisioning Manager	Create Integrations	Run Integrations
Create users	X	X				
Modify user details	X	X				
Delete users	X	X				
Deactivate and Activate user accounts	X	X				
Create groups	X	X				
Modify group details	X	X				
Delete groups	X	X				
Create projects	X		X			
Modify project details	X		X			
Delete projects	X		X			
Provision users	x			X		
Deprovision users	X			X		
Provision groups				X		
Deprovision groups	X			X		

Tasks	Administrato r	Directory Manager	Project Manager	Provisioning Manager	Create Integrations	Run Integrations
Generate provision reports	X			X		
Assign access to data integrations	X				X	
Create data integrations	X				X	
Edit data integrations					X	
Copy data integrations	X				X	
Delete data integrations	X				X	
Create data integration groups	X				X	
View data integrations	X				X	X
Run, or schedule to run, data integrations	X					X
Run, or schedule to run, data integration groups	X					X

C

Essbase User Provisioning

In This Appendix

Launching Shared Services Console from Essbase

Note:

You can use Shared Services to provide security for Essbase applications, databases, and artifacts. To use Shared Services security, you must migrate the Essbase Server and any existing Essbase users and groups to Shared Services. For detailed information on Essbase security, see the *Oracle Essbase Database Administrator's Guide* and the *Oracle Essbase Administration Services Online Help*.

To manage Essbase users in Shared Services Console, you must log in to Shared Services Console as a user who is provisioned with these Shared Services roles:

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

When you launch Shared Services Console from Administration Services, you automatically log in to Shared Services Console as the Essbase user that established the connection with the Essbase Server you are accessing.

Note:

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

When you launchShared Services Console from a browser, you log in as whatever user is appropriate. For example, you must log in as a Shared Services Administrator in order to provision an Essbase Administrator with the Directory Manager role that allows the Essbase Administrator to manage users.

➤ To launch Shared Services Console from Administration Services:

1 From Enterprise View or a custom view, select an Essbase Server.

2 Under the server node, select the **Security** node.

3 Right-click and select **User Management.**

Shared Services Console launch page is opened in a separate browser window.

Note:

Browser pop-up blockers can prevent Shared Services Console from launching.

4 Click **Launch.**

For information on launching Shared Services Console from MaxL, see the *Oracle Essbase Technical Reference*.

Synchronizing Essbase Security with Shared Services Security

Essbase Server maintains its own security file containing data about users who are provisioned to perform operations on the Essbase Server. Because this information is not automatically updated, you must synchronize Essbase security every time an Essbase Server user's provisioning data is changed from Shared Services.

If Essbase is deployed in Shared Services mode, Shared Services *admin* user account is the only account that can initially synchronize security. Other users who are provisioned with Essbase Server and application roles are recognized by Essbase only after the *admin* refreshes security after completing the provisioning process. For example, newly provisioned users are not recognized by the Essbase Server until synchronization is performed. Similarly, changes to provisioning assignments are recognized by the Essbase Server only after security is synchronized.

Note:

Only `admin` can synchronize security for the first time. Subsequently, users who are provisioned with Essbase Server Administrator role also can synchronize Essbase security with Shared Services security

Tip:

For information on running a MaxL command to synchronize Essbase security with Shared Services security, see the *Oracle Essbase Technical Reference*.

➤ To synchronize Essbase security with Shared Services security:

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

2 In **Enterprise View**, expand **Essbase Severs.**

3 Expand the node representing your Essbase Server.

4 **Right-click Security and select Refresh security from Shared Services.**

Note:

Users with Create/Delete Application or Server Access Essbase Server role can refresh their own security only.

5 **Select All Users in the Refresh Security from Shared Services dialog box. Click Help for assistance.**

6 **Click OK.**

7 **Click Yes to close the message window.**

8 **Click OK in the confirmation window.**

9 **Verify that provisioned users are available in Essbase Server.**

a. Expand the node that represents your Essbase Server.

b. Expand **Security**.

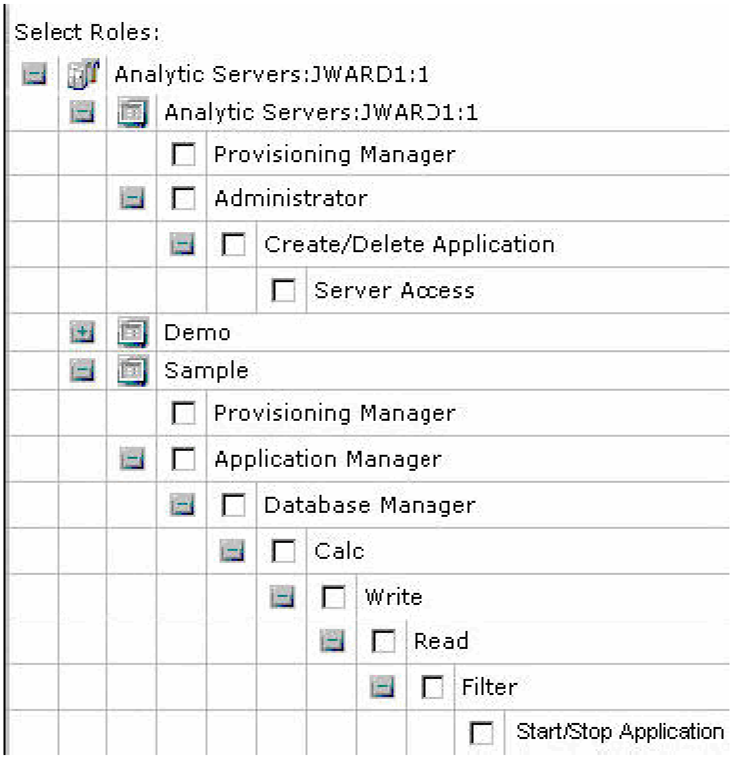
c. Perform an action:

- To list provisioned users, right-click **Users** and select **Display users table**.
- To list provisioned groups, right-click **Groups** and select **Display groups table**.

Essbase Roles

See "Essbase Roles" on page 157 for information on Essbase roles.

Essbase Role Hierarchy



Select Roles:

- Analytic Servers:JWARD1:1
  - Analytic Servers:JWARD1:1
    - □ Provisioning Manager
    - □ Administrator
      - □ Create/Delete Application
        - □ Server Access
  - Demo
  - Sample
    - □ Provisioning Manager
    - □ Application Manager
      - □ Database Manager
        - □ Calc
          - □ Write
            - □ Read
              - □ Filter
                - □ Start/Stop Application

D Essbase Studio Provisioning

In This Appendix

Prerequisites

You use Shared Services to provide security for Essbase Studio artifacts, such as cube schemas and dimension elements. The roles you assign to Essbase Studio users determine their access to these artifacts. For detailed information on Essbase Studio security, see *Oracle Essbase Studio User's Guide*.

To manage Essbase Studio users in Shared Services Console, you must log into Shared Services Console as a user who is provisioned with these Shared Services roles:

- Provisioning Manager role for the appropriate Essbase Studio instance.
- Directory Manager role for the appropriate authentication directory.

Other prerequisites for provisioning users:

- Shared Services must be configured and running.
- The external user directories that store user and group information for Essbase Studio are configured on Shared Services.
- A Essbase Studio instance was created and registered using EPM System Configurator. (Note: Essbase Studio does not need to be running.)

Launching Shared Services Console from Essbase Studio

There is no direct method for launching Shared Services Console from Essbase Studio. To launch Shared Services Console, use either of these methods:

- From the Start menu, select Oracle EPM System, then Foundation Services, then Shared Services Console.
- In a browser, provide the Shared Services Console URL; by default:

```
http://server:port/interop/index.jsp
```

Essbase Studio Roles

See “Essbase Studio Roles” on page 158.

Essbase Studio Role Hierarchy

The roles are listed in descending order by the number of privileges granted to each role, with cpAdmin having the most privileges.

- cpAdmin—Administrator
- cpDM—Data Modeler
- cpDSAdmin—Data SourceAdministrator
- cpViewer—Viewer

Note:

Additionally, in order to deploy cubes in Essbase Studio, the cpAdmin and cpDM users must be provisioned for, at a minimum, the Shared Services Project Manager role.

Essbase Studio Artifact Privileges by Role

Essbase Studio Artifact	cpAdmin	cpDM	cpDSAdmin	cpViewer
Folder	Create Read Update Destroy	Create Read Update Destroy	Read	Read
Data source connection	Create Read Update Destroy	Read	Create Read Update Destroy	Read
Minischema	Create Read Update Destroy	Read	Create Read Update Destroy	Read
Dimension element	Create Read	Create Read	Read	Read

Essbase Studio Artifact	cpAdmin	cpDM	cpDSAdmin	cpViewer
	Update Destroy	Update Destroy		
Hierarchy	Create Read Update Destroy	Create Read Update Destroy	Read	Read
Alias set	Create Read Update Destroy	Create Read Update Destroy	Read	Read
Cube schema	Create Read Update Destroy	Create Read Update Destroy	Read	Read
Essbase model	Create Read Update Destroy	Create Read Update Destroy	Read	Read
Drill-through report	Create Read Update Destroy Execute	Create Read Update Destroy Execute	Read Execute	Read Execute

Note:

Additionally, in order to deploy cubes in Oracle Essbase Studio, the cpAdmin and cpDM users must be provisioned for, at a minimum, the Shared Services Project Manager role.

E

Reporting and Analysis User Provisioning

In This Appendix

Launching Shared Services Console from EPM Workspace

You use Shared Services Console to manage Reporting and Analysis users, groups, and roles. You must be a Shared Services Administrator or Provisioning Manager to provision users or groups. See Chapter 9, "Managing Provisioning."

➤ To launch Shared Services Console from EPM Workspace, select **Navigate**, then **Administer**, and then **User Management**.

Shared Services Console opens in a separate window.

Reporting and Analysis Provisioning

This section presents an overview of the steps you must perform to provision Reporting and Analysis users and groups.

- "Prerequisites" on page 177
- "Provisioning Process" on page 178
- "Setting Access Control for Reporting and Analysis Objects" on page 179

Prerequisites

- "Shared Services" on page 178
- "Essbase" on page 178
- "Reporting and Analysis" on page 178

Shared Services

- Shared Services is running. See "Prerequisites" on page 177 for Shared Services prerequisites.
- The external user directories that store user and group information for Reporting and Analysis applications are configured on Shared Services.
- Shared Services Administrator has created the following power users:
  - Administrators by assigning the Reporting and Analysis Administrator role
  - Provisioning Managers by assigning the Provisioning Manager role
  - Administrators by assigning the Planning Administrator role

Essbase

Essbase Server must be installed and configured. You must have performed these tasks:

- Activated Essbase Server using a valid product deployment ID
- Registered Essbase with Shared Services
- Started Essbase server

Reporting and Analysis

- Reporting and Analysis products are installed and configured.
  - Product activation of Reporting and Analysis products are complete
  - Reporting and Analysis products are configured with Shared Services
  - Reporting and Analysis product servers are running
- EPM Workspace Web application and the Web server are running.

Provisioning Process

The Provisioning Manager role is automatically assigned to the Shared Services Administrator. The deployment process does not create a default Reporting and Analysis user.

Note:

Reporting and Analysis does not maintain a local copy of the provisioning information. It uses the information maintained by Shared Services.

➤ To provision Reporting and Analysis users and groups:

1. Log into EPM Workspace as a user with Reporting and Analysis Provisioning Manager roles.
2. From Navigate, select **Administer**, and then **User Management.** The Shared Services Console opens
3. Provision users and groups with Reporting and Analysis roles.

Setting Access Control for Reporting and Analysis Objects

Reporting and Analysis objects include folders and documents.

➤ To set access control:

1 Log into EPM Workspace as a user with Reporting and Analysis Provisioning Manager and Explorer roles.

2 From Navigate, select **Administer**, and then **User Management.**

3 Under Projects or Application Groups, expand Hyperion System 9 BI+ and select the BI+ application.

Reporting and Analysis Roles

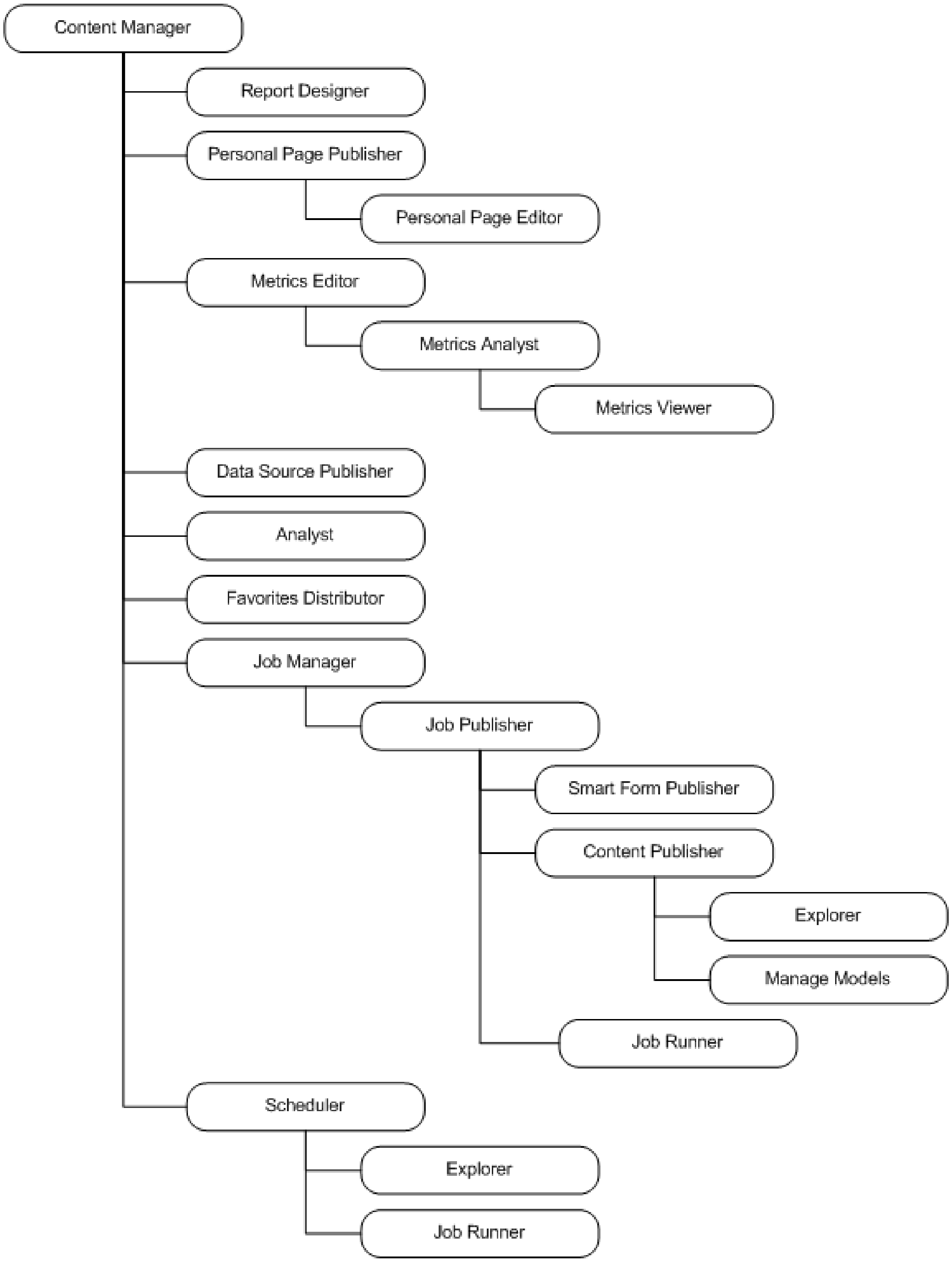
You provision users and groups by assigning combinations of predefined roles (see Appendix A, "Product Roles") to achieve specific product access and functionality.

Reporting and Analysis Role Hierarchy

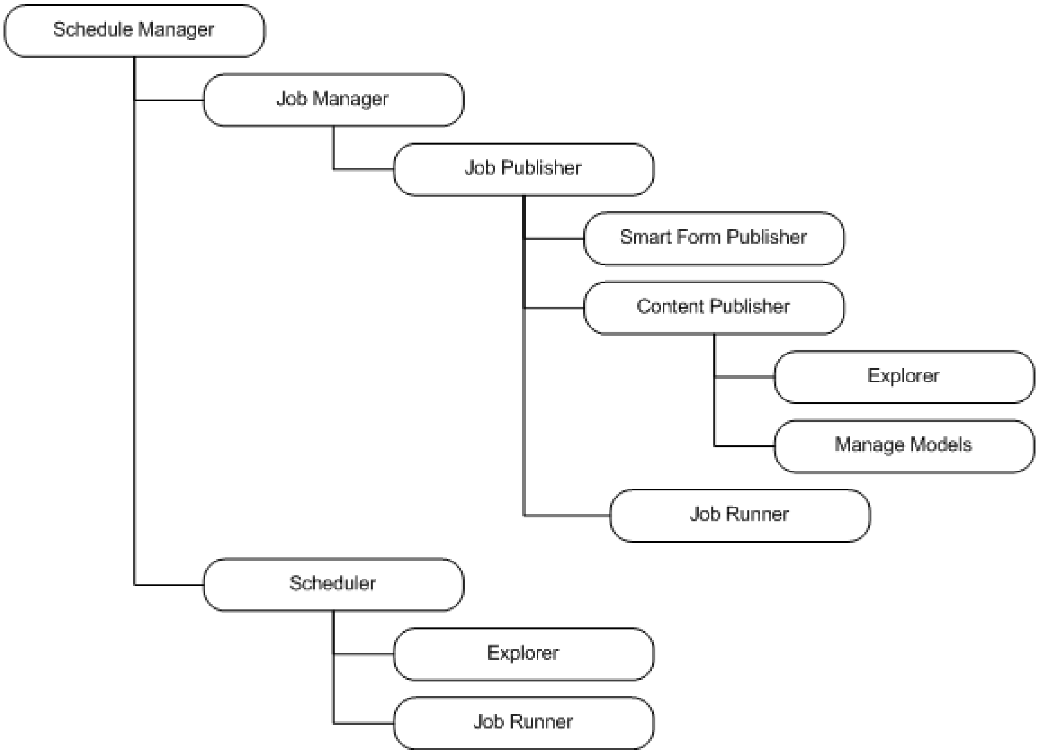
Roles organize into hierarchies that contain other roles. Reporting and Analysis roles aggregate into these branches:

- "Content Manager Branch" on page 180
- "Scheduler Manager Branch" on page 180

Content Manager Branch



Scheduler Manager Branch



Sample Role Combinations

This table provides examples of the access and functionality achieved by assigning combinations of roles.

Combined Role	Tasks	Access Permissions
Explorer + Favorites Distributor + Personal Page Editor + Personal Parameter Editor	● Review interactive Web Analysis and Financial Reporting content in EPM Workspace ● List and subscribe to repository content ● Review accessible interactive content in Oracle's Hyperion® Web Analysis Studio ● Access Personal Page ● Access Favorites Manager ● Define Web Analysis points of view, personal variables, and personal parameters, to customize the query result set	Share interactive content without modifying content or saving changes to the repository
Explorer + Analyst + Content Publisher	● Review interactive Web Analysis, Financial Reporting, and Interactive Reporting content in the EPM Workspace	Iinteractively use document types to edit queries, re-query, and save changes back to the repository

Combined Role	Tasks	Access Permissions
	● List and subscribe to repository content ● Review accessible interactive content in Web Analysis Studio ● Edit queries, re-query and arrange data ● Create Financial Reporting batches and books ● Import, modify and Save As dialog box	
Personal Page Publisher Data Source Publisher + Analyst + Report Designer + Job Manager	● Create and distribute new interactive Web Analysis, Financial Reporting, and Oracle's Hyperion® Interactive Reporting content ● Create and distribute custom Oracle's Hyperion® Web Analysis documents in Oracle's Hyperion® Web Analysis Studio Design Documents interface ● Access Oracle Hyperion Financial Reporting Studio, Fusion Edition ● Access Personal Pages and distribute content to repository users ● Distribute data source connectivity files to repository users ● Distribute batches, books, reports and documents to repository users ● Import and modify Production Reporting files and Oracle's Hyperion® SQR® Production Reporting output ● Create, save and run jobs ● Create and manage output directories	Access most content creation functionality, but not administrator access to resources
Content Manager + Schedule Manager	● Manage all published content in the repository and all content creation functionality ● Create and manage events, calendars, time events, calendars, public parameters, and physical resources	Access all content creation and scheduling functionality, but not administrator access to resources
Reporting and Analysis Administrator + Data Editor	● Conditional access to all resources ● Access the Administer module ● Access the Impact Manager module ● Ability to write edits back to Essbase	Access most functionality and modules, with conditional access to resources

F Performance Management Architect User Provisioning

In This Appendix

Performance Management Architect Roles

You provision users and groups by assigning predefined roles (see Appendix A, "Product Roles").

Performance Management Architect Access Levels

The following table describes common tasks performed in Performance Management Architect and required levels of access. Be aware of the following considerations:

- You can only edit structure for local dimensions within applications or for shared dimensions within the Shared Library.
- You can only copy dimensions if your role also allows you to create dimensions in the target of the copy.
- You can only synchronize dimensions if you have at least reader access to the source dimension and writer access to the target dimension.
- You can only add dimensions to applications if you are an Application Creator or Application Administrator role.

Level of Access	Dimension Level Tasks
Dimension Owner	● Edit dimension structure or properties ● Copy dimensions ● Synchronize dimensions from or to dimensions ● Add dimensions to applications ● Remove dimensions ● Delete dimensions
Dimension Writer	● Edit dimension structure or properties ● Copy dimensions ● Synchronize from or to dimensions

Level of Access	Dimension Level Tasks
	● Add dimensions to applications
Dimension Reader	● Copy dimensions ● Synchronize from dimensions ● Add dimensions to applications

G

User Provisioning in Profitability and Cost Management

In This Appendix

Prerequisites

Before provisioning users, ensure the following are configured and running:

- "EPM Workspace" on page 185
- "Shared Services" on page 185
- "Essbase" on page 185
- "Profitability and Cost Management" on page 186

EPM Workspace

- EPM Workspace and the Web server are running.
- At least one Profitability and Cost Management application is created.

Shared Services

- Shared Services is configured and running.
- The external user directories that store user information for Profitability and Cost Management are configured on Shared Services.
- Shared Services administrator has created these user roles:
  - Profitability and Cost Management Administrator role
  - Profitability and Cost Management Provisioning Manager role

Essbase

Essbase Server must be running.

Profitability and Cost Management

- Profitability and Cost Management is installed and configured, as described in the *Oracle Hyperion Enterprise Performance Management System Installation and Configuration Guide*. This involves these tasks:
  - Product activation
  - Shared Services registration
  - Database configuration
  - Application server deployment
  - Profitability and Cost Management instance registration
  - Data source configuration.
  - Profitability and Cost Management server is running.
- Profitability and Cost Management server is running.
- One or more users have been provisioned as Profitability and Cost Management application creators by assigning the Profitability and Cost Management Application Creator, Dimension Editor, Create Integrations, and Run Integrations Shared Services roles. See "Provisioning Users and Groups" on page 125.
- At least one Profitability and Cost Management application has been created and deployed.
- Profitability and Cost Management applications have been assigned to projects in Shared Services.
- Provisioning Managers for each Profitability and Cost Management application are created by assigning the Provisioning Manager role to the application. See "Provisioning Users and Groups" on page 125.

Launching the Shared Services Consolefrom Profitability and Cost Management

➤ To launch the Shared Services Console:

1. **Ensure the Shared Services server is running.**
2. **Log on to EPM Workspace as an Administrator (*admin*).**
3. **Select Navigate, then Administer, and then User Management.**

   The Shared Services Console is displayed.
4. **Create and provision users and groups. See "Provisioning Users and Groups" on page 125.**

Profitability and Cost Management Roles

In Profitability and Cost Management, each user ID is assigned a security role:

- Administrator (*admin* is the default security role when you log on to Shared Services)
- Power User
- Interactive User
- View User

The assigned security role determines the level of access or privileges available for that user. When an access level is assigned to a group of users, similar security access is granted to all members of that group.

Depending on the access requirements for a particular user, the assigned security may be modified to attach a wider or narrower access.

See "Profitability and Cost Management Roles" on page 164 for a list of default Oracle Hyperion Profitability and Cost Management, Fusion Edition security roles, and a description of their associated access.

H

Financial Management User Provisioning

In This Appendix

Financial Management supports application security enforced through Shared Services provisioning and class access security for metadata and data, including documents. This appendix provides information on provisioning Financial Management users and groups.

Note:

You can also load security files into an application. See the *Oracle Hyperion Financial Management Administrator's Guide*.

Prerequisites for provisioning users:

- Shared Services and Financial Management must be configured and running.
- Shared Services Administrator created the following users:
  - Provisioning Manager. To provision users, you can use the Shared Services Administrator, for which the Provisioning Manager role is automatically assigned, or assign the role to another user.
  - Application creators, by assigning the Financial Management Application Creator role
  - Administrators, by assigning the Financial Management Administrator role
- The external user directories for Financial Management user and group information must be configured on Shared Services.
- Financial Management applications must be registered with Shared Services.

➤ To provision Financial Management users and groups:

1 **Log in to Shared Services as a user with Financial Management Provisioning Manager role.**

2 From Native Directory or one of the configured user directories, select the users or groups to provision with Financial Management roles.

3 Provision users and groups with Financial Management roles. See Appendix A, "Product Roles."

4 Select **Application Groups**.

5 Select the Financial Management application for which you want to provision users and groups.

Note:

If you do not have Lifecycle Management configured, an error message displays that you are unable to connect to the application. To configure Lifecycle Management, see the *Oracle Hyperion Enterprise Performance Management System Installation and Configuration Guide*.

6 Provision users by assigning access to metadata and security roles.

Launching Shared Services Console from EPM Workspace

You use Shared Services Console to manage Financial Management users, groups, and roles. You must be a Shared Services Administrator or Provisioning Manager to provision users or groups.

➤ To launch Shared Services Console from EPM Workspace, select **Navigate**, then **Administer**, and then **User Management**.

Shared Services Console opens in a separate window.

Financial Management Roles

You provision users and groups by assigning combinations of predefined roles (see Appendix A, "Product Roles.") to achieve specific product access and functionality.

The Oracle Hyperion Financial Management, Fusion Edition Provisioning Manager role is automatically assigned to the Shared Services Administrator. You can use this administrator or another user provisioned with that role to provision users and groups.

Assigning Users and Groups to Financial Management Applications

➤ To assign users and groups to applications:

1 From the Shared Services Console, expand **Application Groups**, right-click the application name, select **Assign Access Control**, and then **Select Users and Groups**.

2 Select an option:

- **Show All** to show all users that are provisioned

- **Users** or **Groups**, and in **Search Criteria**, enter the search criteria, and click **Search**.

3 From **Available Users and Groups**, select users and groups to assign to the application and select roles, and use the arrow keys to move them to the Selected Users column.

4 Click **Next.**

Setting Up Security Classes for Financial Management Applications

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

A user's or group's ability to access application elements such as accounts and entities depends on the security classes to which the user or group belong and on the security class associated with the application element.

Creating Security Classes

Note:

Use this procedure if you are using Classic Application Administration. If you are using Performance Management Architect, see the *Enterprise Performance Management Architect Administrator's Guide*.

➤ To create a security class:

1 From the Shared Services Console, expand **Application Groups**, right-click the application name, select **Assign Access Control**, and then **Select Classes.**

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

Note:

The name can contain up to 80 characters.

3 Click **Add.**

Deleting Security Classes

Use this procedure if you are using Classic Application Administration. If you are using Performance Management Architect, see the *Enterprise Performance Management Architect, Fusion Edition Administrator's Guide*.

Caution!

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

You disassociate an entity, account, scenario, report, data form, and journal from a security class by modifying the metadata file. See the *Oracle Hyperion Financial Management Administrator's Guide*, or if you are using Performance Management Architect, see the *Enterprise Performance Management Architect, Fusion Edition Administrator's Guide*.

➤ To delete a security class:

1. From the Shared Services Console, expand **Application Groups**, right-click the application name, select **Assign Access Control**, and then **Select Classes**
2. From **Available Classes**, select the security classes to delete, and click **Delete.**
3. Click **Yes** to confirm deletion.

Selecting Security Classes

➤ To select security classes for an application:

1. From the Shared Services Console, expand **Application Groups**, right-click the application name, select **Assign Access Control**, and then **Select Classes**
2. From **Available Classes**, select the security classes to assign to the application, and use the arrow keys to move them to the Selected Classes column.
3. Click **Next.**

Assigning User Access to Security Classes

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

Note:

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

Table 23 User Access Table

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

You can use the Pivot Table feature to toggle between two views for assigning access. For example, if you have users and groups on rows and security classes on columns and click Pivot Table, users and groups will be on columns and security classes on rows.

➤ To assign user access to security classes:

1. From the Shared Services Console, expand **Application Groups**, right-click the application name, select **Assign Access Control**, and then **Assign Access**.
2. Select cells for which to assign access rights.

   Tip:

   Use the Shift and Ctrl keys to select multiple cells. Select a column or row by clicking in the column or row header.
3. From **Access Rights**, select the access level to assign.
4. Click **Set** to apply the level to the selected cells.
5. **Optional:** To add an e-mail alert, select cells in the table and click **Add Alert**.

   Caution!

   The alerting process uses the e-mail addresses stored in the external authentication files. To set up e-mail alerts, see the *Oracle Hyperion Financial Management Administrator's Guide*.

   Note:

   To remove e-mail alerts, select the cell and click Remove Alert.
6. Click **Save**.
7. Click **Next**.

Running Security Reports for Financial Management Applications

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

Note:

You can format and print the report using HFM-Format, PDF, RTF, HTML, or XLS. See the *Hyperion Financial Management User's Guide*.

➤ To create a security report:

1. From the Shared Services Console, expand **Application Groups**, right-click the application name, select **Assign Access Control**, and then **Security Reports**.
2. Select a report option:
   - Rights
     - Classes by User
     - Roles by User
   - Users by Group
3. Select an option:
   - **Launch Report** to open the report in a new window
   - **Export to File** to save the file as a CSV file.

Migrating Financial Management Users to Shared Services Security

For information on migrating users to Shared Services security, see the *Oracle Hyperion Enterprise Performance Management System Installation and Configuration Guide*.

I

Planning User Provisioning

In This Appendix

Overview to Steps

This section presents an overview of the steps you must perform to provision Planning users and groups. Detailed procedures are available in other sections of this guide and the *Hyperion Planning - System 9 Administration Guide*.

- “Prerequisites” on page 195
- “Provisioning Process” on page 197

Prerequisites

- “Shared Services” on page 195
- “Essbase ” on page 196
- “Reporting and Analysis” on page 196
- “EPM Workspace” on page 196
- “Planning” on page 196

Shared Services

- Shared Services is running.
- The external user directories that store user and group information for Essbase and Planning are configured on Shared Services.
- Shared Services Administrator has created the following power users:
  - Reporting and Analysis Administrators by assigning the Reporting and Analysis Administrator role, which grants access to EPM Workspace

    - Planning Provisioning Managers by assigning the Planning Provisioning Manager and Shared Services Directory Manager roles
    - Administrators by assigning the Planning Administrator role
- A Planning instance was created and registered using EPM System Configurator

Essbase

Essbase Server must be running.

Reporting and Analysis

- Reporting and Analysis products are installed and configured. Reporting and Analysis Common Services, EPM Workspace, and the EPM Workspace Web server are running.
- Planning and Performance Management Architect are enabled in the Reporting and Analysis Web server configuration so that they can be accessed from EPM Workspace.
- Dimension Server is running.

EPM Workspace

- EPM Workspace, the central administration location for Planning, and the Web server are running.
- At least one Planning application is created. Oracle's Hyperion Reporting and Analysis Administrators create Planning applications from Performance Management Architect.

Planning

- Planning is installed and configured.
- Planning server is running.
- One or more users are provisioned as Planning Application Creators by assigning the Planning Application Creator, Dimension Editor, Create Integrations, and Run Integrations Shared Services roles, described in this guide.
- Performance Management Architect is installed, configured, and running.
- Using Performance Management Architect, you created and deployed Planning applications. See *Enterprise Performance Management Architect Administrator's Guide*.

  Only users with Planning Application Creator, Dimension Editor, Create Integrations, and Run Integrations Shared Services roles can create and deploy Planning applications.
- Planning applications are assigned to projects in Shared Services.
- Provisioning Managers for each Planning application are created by assigning the Provisioning Manager role of the application, described in this guide.

Provisioning Process

Users and groups require Planning application roles to access Planning. After provisioning users and groups with roles, you assign their access permissions to dimension members, data forms, folders, task lists, and launch privileges for Calculation Manager business rules—from within Planning or from Shared Services Console. To assign access to application elements in Planning, see the *Oracle Hyperion Planning, Fusion Edition Administrator's Online Help*.

The Planning Provisioning Manager role is automatically assigned to the Shared Services Administrator.

➤ To provision Planning users and groups from Shared Services Console:

1. Log into Shared Services Console as a user with the Planning Administrator or Provisioning Manager role.
2. From Native Directory or a configured user directory, select the users or groups to provision with Planning roles.
3. Select **Administration**, then **Provision**.
4. Expand the Project under which the Planning application is registered.
5. Expand the application to display the available roles.
6. Select the roles and, using the right-arrow, move them to the **Selected Role** pane.
7. Click **Save**.

Note:

Planning synchronizes with Shared Services as described in "Refreshing Users and Groups in Planning" on page 197. After synchronization, Planning users who do not exist in Essbase are automatically created. If users exist in Essbase, their application assignment is updated to reflect access to Planning.

Launching Shared Services Console From EPM Workspace

➤ To launch Shared Services Console from EPM Workspace, select **Navigate**, then **Administer**, then **User Management**.

Shared Services Console opens in a separate window.

Refreshing Users and Groups in Planning

Planning and Oracle's Hyperion® Business Rules get the latest list of users, groups, and roles from Shared Services Console when:

- The application is refreshed with Security Filters selected.
- The `ProvisionUsers` utility is run (see the *Oracle Hyperion Planning Administrator's Guide*).

- Someone logs into the application; Planning synchronizes that user with Shared Services Console.
- Access permissions are assigned in Planning

Migrating User and Group Identities

When you change a user or group's identity or their position in the user directory hierarchy, you must update—or migrate—this information to Planning.

➤ To migrate changed user and group identities from Shared Services Console to Planning:

1 Take an action:

- Select **Administration**, then **Manage Data Forms** and select a data form folder or data form.
- Select **Administration**, then **Dimensions** and select a dimension member.
- Select **Administration**, then **Manage Task Lists** and select a task list.
- Select **Administration**, then **Business Rule Security** and select a business rule folder or business rule.

2 Click **Assign Access.**

3 Click **Migrate Identities.**

Note:

You can also use the `UpdateUsers` utility, described in *Oracle Hyperion Planning, Fusion Edition Administrator's Online Help*, to migrate identities.

Roles in Planning

Subject to the applicable license for the software and users, Planning supports the roles described in this guide.

Write Access to Data in Essbase

All administrators have write access to Planning data in Essbase. By default, security filters that Planning generates in Essbase for planners and interactive users are read-only. However, you can grant planners and interactive users the same access permissions they have in Planning to data in Essbase by assigning them the Essbase Write Access role. Using another product such as Financial Reporting, Essbase Excel Add-in, or third-party tools, they can then change Planning data—to which they have write access in Planning—directly in Essbase.

Note:

Security filters are always read-only for view users.

Roles Between Planning and Business Rules

To allow users to launch business rules from Classic Planning applications, a Business Rules administrator must grant access rights to business rules created with Business Rules. For Oracle Hyperion EPM Architect, Fusion Edition Planning applications, a Planning administrator can assign launch access permissions from within Planning.

Table 24 Roles in Planning and Business Rules

Planning Role	Business Rules Role	Tasks Performed
Administrator	Administrator	● Designs business rules ● Launches business rules for a Planning application
Interactive user	Interactive user	● Designs business rules ● Launches rules that have been assigned Launch permissions by an administrator
Planner	Basic user	Launches business rules that have been assigned Launch permissions by an administrator
View user	None	None

If a Planning user has different roles across Planning applications, the user's highest role is used in Business Rules. For example, if a user is an administrator in one application and a planner in another application, the user becomes an administrator in Business Rules.

Note:

See Appendix A for information on the Calculation Manager roles.

Access Permissions Between Planning and Essbase

After security filters are updated in the Essbase database, a Planning user's access in Essbase depends on the user type that establishes the connection.

Table 25 Access Permissions Between Planning and Essbase

User Type for Connection	View User	Planner	Interactive User	Administrator
Named User	Filter Access	Calculate	Calculate	Database Designer*

*Not reflected in Application Manager.

About Connection Types and Planning

Planning establishes a connection to the Essbase database using the appropriate user type.

Table 26 Connection Types and Planning

Program Used to Log on to Planning Application	Essbase Connection
Planning and Oracle Hyperion Smart View for Office, Fusion Edition client through the Oracle Hyperion Planning, Fusion Edition provider	Pool of supervisor user connections
Oracle Hyperion Financial Reporting, Fusion Edition, Business Rules, and third-party tools	Named user

J

Business Rules User Provisioning

In This Appendix

This appendix provides information on provisioning Business Rules users and groups.

Provisioning Overview

Here is an overview of the process of provisioning Business Rules users.

1. An administrator migrates native Administration Services and Business Rules users to Shared Services using the Externalize Users utility in Administration Services. See *Oracle Hyperion Enterprise Performance Management System Installation and Configuration Guide*.
2. An administrator uses Oracle's Hyperion Enterprise Performance Management System Configurator to deploy Shared Services. Native Directory is configured when Shared Services is deployed. See *Oracle Hyperion Enterprise Performance Management System Installation and Configuration Guide*.
3. An administrator configures the external user directories that store user and group information for Business Rules. See Chapter 5, "Configuring User Directories.".
4. An administrator registers Administration Services (of whichBusiness Rules is a component) with Shared Services. See *Oracle Hyperion Enterprise Performance Management System Installation and Configuration Guide*.
5. Shared Services stores product registration information in the database.
6. An administrator assigns Business Rules roles to users and groups defined in Native Directory and external user directories. See Chapter 9, "Managing Provisioning."

   Shared Services stores provisioning information in Native Directory.
7. A user logs onto Administration Services, and the application authenticates the user against the external user directory.

Launching Shared Services Console

Shared Services Console provides a centralized user interface where you can perform user provisioning tasks for Oracle Hyperion Enterprise Performance Management System products. For instructions on launching Shared Services Console, see "Launching Shared Services Console" on page 49.

Business Rules User Roles

Subject to the applicable license for the software and users, Business Rules supports three predefined user roles that you can assign to users and groups: administrator, interactive user, and basic user. These roles determine what tasks users and groups can perform on Business Rules repository objects. For information on Business Rules roles, see "Business Rules Roles" on page 164. For information on assigning roles to users and groups, see "Provisioning Users and Groups" on page 125.

After you assign roles to users and groups in Shared Services, you assign them access permissions to repository objects in Business Rules. For example, you might want to assign a user access permissions to edit all of the business rules in a Business Rules application group. See the *Hyperion Business Rules Administrator's Guide* or the *Oracle Essbase Administration Services Online Help*.

Migrating Business Rules Users to Shared Services Security

If you are upgrading Business Rules, you may need to migrate native Administration Services and Oracle's Hyperion® Business Rules users to Shared Services by running the Externalize Users utility in Administration Services. See *Oracle Hyperion Enterprise Performance Management System Upgrade Guide* for detailed information.

K

Performance Scorecard Provisioning

In This Appendix

Overview

You can provision users and groups for Performance Scorecardusing the following items:

- Security roles provided by Shared Services as described in this guide.
- Security roles that you create in Performance Scorecard that determine scorecards, measures, initiatives, and Web pages access. See “Custom Security Roles” on page 205.
- Custom domains that you create in Performance Scorecard to represent geographically or functionally distinct areas in your organization. This determines the data users can access. See “Domains” on page 206.

You can also perform these tasks based on your setup and previous use of Shared Services:

- Perform a bulk synchronization between users and groups provisioned with Performance Scorecard roles in Shared Services against those provisioned in Performance Scorecard.
- Identify the accounts that you must create in Shared Services to accommodate new employees created in Performance Scorecard.

See Chapter 2 of the *Oracle Hyperion Performance Scorecard Administrator's Guide*.

Requirements

To provision Performance Scorecard user and group accounts, ensure that your account has the following roles:

- Provisioning manager
- BI+ Administrative\Global Administrative
- HPS Power Manager
- Administrator

Assigning Security

➤ To provision Performance Scorecard accounts:

1. Launch the Shared Services Console by selecting **Administer**, then **User Management**.
2. Ensure that your account provides the necessary access. See "Requirements" on page 203.
3. In the Shared Services Console create and provision accounts as described in this guide.
4. Select the **Application Groups** explorer to the left.
5. Select **Scorecard**, right-click **Performance Scorecard**, and then select **Assign Security** from the shortcut menu.

   The Select User or Group page is displayed.

6. Select the account and click **Next**.

   The Manage Properties page is displayed. Any domains or security roles that you created in Performance Scorecard are available. Domains are not available for group accounts.

7. To associate a Performance Scorecardemployee with the account, perform these tasks:

   a. Click **Select**.

   b. On the Select Employee box is displayed, click **Search** to view all employees.

   c. Select the employee and click **Apply**.

   See "Sample Role Combinations" on page 181.

8. From **Primary Domain**, select the domain that represents a distinct geographical or functional area in your organization with which to associate the account. This grants the user access to all data in the domain.

   See "Domains" on page 206.

9. In **Security Roles**, select the provided or custom security roles that determines the data that the user can access and the tasks that they can perform.

   See "Provided Security Roles" on page 204

   For information about creating your own Performance Scorecard security roles that determine measure, scorecard, initiative, and Web page permissions, see Chapter 2 of the *Oracle Hyperion Performance Scorecard Administrator's Guide*.

10. Click **Finish**.

Provided Security Roles

The following table identify the tasks that users can perform depending on the role you assign to their account.

Table 27 Provided Security Roles

Security Role	Privilege Description
user	Enables users to perform these tasks: ● View maps and drill down into map elements

Security Role	Privilege Description
	● Access data about objects to which they have access and use notes ● Access all reports and, if authorized, enter data on reports. ● Create and subscribe to alerts ● Create, edit or delete annotations **Note:** This restricts access to measures and scorecards unless the user meets certain criteria. **Do not apply** this role to employees who must access all business objects, regardless of their association with objects.
designer	Enable users to perform these tasks: ● Create all application objects such as those listed above, but with the additional ability to place these objects in a domain. ● View maps and drill down into map elements ● Use all reports and, if authorized, enter data such as measure results and target values. ● Create and subscribe to alerts
generic domain designer	Enables users to perform the steps granted by the designer (Interactive) role, but also to associate objects such as measures and maps with domains; enabling them to build domain-specific applications.
administrator	Enable users to perform these tasks: ● Create custom security roles that provide conditional access to Performance Scorecard data such as measures and scorecards. ● Create, modify or delete domains ● Synchronize security with Shared Services ● Track changes made to business objects ● Generate Star Schema and multidimensional Essbase databases of application data ● Promote application data to another environment ● Configure the Alerter, enabling users to send and receive alert notifications ● Monitor user activity

Custom Security Roles

You can create security roles in Performance Scorecard to determine the Performance Scorecard data that users can access. This enables you to specify the measures, scorecards, and initiatives that users can access, and restrict particular pages and reports. To make access to data conditional, you can determine permissions that provide access to measures, scorecards, and initiatives only if the user meets certain criteria. For example, you could restrict access to scorecards unless the scorecard contains measures that the user owns. .

Security role that you create are automatically available in Shared Services for use in provisioning. For information about creating security roles, see Chapter 2 of the *Oracle Hyperion Performance Scorecard Administrator's Guide*.

Domains

Create domains to represent geographically or functionally distinct areas in your organization with which to associate users. Because application designers can associate objects such as maps, measures, and scorecards, with domains, assigning domains to accounts determines the data users can access, and enables data partitioning. The domains you create in Performance Scorecard are automatically available for use in Shared Services for account provisioning, enabling you to associate accounts with domains.

For information about creating domains, see Chapter 2 of the *Oracle Hyperion Performance Scorecard Administrator's Guide*.

Employees

Employees represent any Performance Scorecard user responsible for performing tasks related to the objects with which they are associated, such as entering measure results and working on strategy elements. Assigning an employee to a user account therefore enables the person using the account to access the objects that the employee uses and the data that they are authorized to access.

To identify the accounts that need to be provisioned in Shared Services for Oracle Hyperion Performance Scorecard, Fusion Edition employees, perform a Synchronize User Accounts With Employees command as described in Chapter 2 of the *Oracle Hyperion Performance Scorecard Administrator's Guide*. If you have the designer security role, you can also create and assign employees to empty accounts.

L

Provider Services User Provisioning

In This Appendix

Provisioning the Administrator Role in Shared Services

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

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

➤ To provision the Administrator role:

1 **Log into Shared Services Shared Services Console at:** `http://sharedservices_server:28080/interop/index.jsp`.

   For example, `http://myServer:28080/interop/index.jsp`.

2 **In Logon, enter the administrator username (default is `admin`) and password (default is `password`).**

3 **Click Log on.**

4 **In the navigation pane, expand Projects and APS 11.1.0 Servers.**

   Provider Services is listed.

5 **To create a user to provision:**

   a. In the navigation pane, expand **User Directories** and a directory, such as **Native Directory**.

   b. Select **Users** and right-click, then select **New**.

   c. Fill in the information to create a new user.

   d. Click **Next** to add the user to one or more existing groups, or click **Finish**.

   e. Click **OK** to add the user, or click **Create Another** to continue adding users.

6 **To select an existing user to provision:**

a. In the navigation pane, expand **User Directories** and a directory, such as **Native Directory**.

b. Select **Users**, right-click, then select **Show All**.

7 To search for a particular user, enter the user ID in the **User** box, then click **Search.**

8 From the list, select a user ID and select **Provision.**

9 In **Provision Users or Groups**, expand **APS 11.1.0 Servers** and expand the name of Provider Services.

10 Select **Administrator** and select ⇥ to select the role.

11 Click **Save.**

The user is provisioned as an Provider Services administrator. Log into Oracle Essbase Administration Services Console with the administrator user name and password to create and manage Analytic Server clusters.

12 In **Provision Summary**, review the provisioning information and click **OK.**

Migrating Analytic Provider Services Users to Shared Services

Because Oracle Hyperion Provider Services has no other users, migration to Shared Services is unnecessary.

M

FDM

In This Appendix

FDM does not fully utilize the security environment provided by Shared Services. Using the Shared Services Console, you can add FDM users. However, you cannot use the Shared Services Console to manage users, groups, and or roles in FDM. Groups and roles are provisioned only from within FDM by the FDM administrator or other FDM power users.

Launching the Shared Services Console from EPM Workspace

Use the Shared Services Console to add users to FDM. You must be a Oracle's Hyperion® Shared Services Administrator or Provisioning Manager to add users. See Chapter 9, "Managing Provisioning."

➤ To launch Shared Services Console:

1. Log into Oracle Enterprise Performance Management Workspace, Fusion Edition
2. Select **Navigate**, then **Administer**, and then **User Management.**

   The Oracle's Hyperion® Shared Services Console opens in a separate window.

FDM Roles

You provision users and groups from within Oracle Hyperion Financial Data Quality Management, Fusion Edition. See Chapter 5 of the *Oracle Hyperion Financial Data Quality Management Administrator's Guide* for information about assigning specific product access and functionality.

Glossary

! *See bang character (!).*

#MISSING *See missing data (#MISSING).*

access permissions A set of operations that a user can perform on a resource.

accessor Input and output data specifications for data mining algorithms.

account blocking The process by which accounts accept input data in the consolidated file. Blocked accounts do not receive their value through the additive consolidation process.

account eliminations Accounts which have their values set to zero in the consolidated file during consolidation.

account type How an account's value flows over time, and its sign behavior. Account type options can include expense, income, asset, liability, and equity.

accountability map A visual, hierarchical representation of the responsibility, reporting, and dependency structure of the accountability teams (also known as critical business areas) in an organization.

accounts dimension A dimension type that makes accounting intelligence available. Only one dimension can be defined as Accounts.

active service A service whose Run Type is set to Start rather than Hold.

activity-level authorization Defines user access to applications and the types of activities they can perform on applications, independent of the data that will be operated on.

ad hoc report An online analytical query created on-the-fly by an end user.

adapter Software that enables a program to integrate with data and metadata from target and source systems.

adaptive states Interactive Reporting Web Client level of permission.

adjustment *See journal entry (JE).*

Advanced Relational Access The integration of a relational database with an Essbase multidimensional database so that all data remains in the relational database and is mapped to summary-level data residing in the Essbase database.

agent An Essbase server process that starts and stops applications and databases, manages connections from users, and handles user-access security. The agent is referred to as ESSBASE.EXE.

aggregate cell A cell comprising several cells. For example, a data cell that uses Children(Year) expands to four cells containing Quarter 1, Quarter 2, Quarter 3, and Quarter 4 data.

aggregate function A type of function, such as sum or calculation of an average, that summarizes or performs analysis on data.

aggregate limit A limit placed on an aggregated request line item or aggregated metatopic item.

aggregate storage database The database storage model designed to support large-scale, sparsely distributed data which is categorized into many, potentially large dimensions. Upper level members and formulas are dynamically calculated, and selected data values are aggregated and stored, typically with improvements in overall aggregation time.

aggregate view A collection of aggregate cells based on the levels of the members within each dimension. To reduce calculation time, values are pre-aggregated and stored as aggregate views. Retrievals start from aggregate view totals and add up from there.

aggregation The process of rolling up and storing values in an aggregate storage database; the stored result of the aggregation process.

aggregation script In aggregate storage databases only, a file that defines a selection of aggregate views to be built into an aggregation.

alias An alternative name. For example, for a more easily identifiable column descriptor you can display the alias instead of the member name.

alias table A table that contains alternate names for members.

alternate hierarchy A hierarchy of shared members. An alternate hierarchy is based upon an existing hierarchy in a database outline, but has alternate levels in the dimension. An alternate hierarchy allows the same data to be seen from different points of view.

ancestor A branch member that has members below it. For example, the members Qtr2 and 2006 are ancestors of the member April.

appender A Log4j term for destination.

application (1) A software program designed to run a specific task or group of tasks such as a spreadsheet program or database management system. (2) A related set of dimensions and dimension members that are used to meet a specific set of analytical and/or reporting requirements.

application currency The default reporting currency for the application.

area A predefined set of members and values that makes up a partition.

arithmetic data load A data load that performs operations on values in the database, such as adding 10 to each value.

artifact An individual application or repository item; for example, scripts, forms, rules files, Interactive Reporting documents, and financial reports. Also known as an object.

assemblies Installation files for EPM System products or components.

asset account An account type that stores values that represent a company's assets.

assignment The association of a source and destination in the allocation model that controls the direction of allocated costs or revenue flow within Profitability and Cost Management.

attribute Characteristic of a dimension member. For example, Employee dimension members may have attributes of Name, Age, or Address. Product dimension members can have several attributes, such as a size and flavor.

attribute association A relationship in a database outline whereby a member in an attribute dimension describes a characteristic of a member of its base dimension. For example, if product 100-10 has a grape flavor, the product 100-10 has the Flavor attribute association of grape. Thus, the 100-10 member of the Product dimension is associated with the Grape member of the Flavor attribute dimension.

Attribute Calculations dimension A system-defined dimension that performs these calculation operations on groups of members: Sum, Count, Avg, Min, and Max. This dimension is calculated dynamically and is not visible in the database outline. For example, using the Avg member, you can calculate the average sales value for Red products in New York in January.

attribute dimension A type of dimension that enables analysis based on the attributes or qualities of dimension members.

attribute reporting A reporting process based on the attributes of the base dimension members. *See also base dimension*.

attribute type A text, numeric, Boolean, date, or linked-attribute type that enables different functions for grouping, selecting, or calculating data. For example, because the Ounces attribute dimension has the type numeric, the number of ounces specified as the attribute of each product can be used to calculate the profit per ounce for that product.

authentication Verification of identity as a security measure. Authentication is typically based on a user name and password. Passwords and digital signatures are forms of authentication.

authentication service A core service that manages one authentication system.

auto-reversing journal A journal for entering adjustments that you want to reverse in the next period.

automated stage A stage that does not require human intervention, for example, a data load.

axis (1) A straight line that passes through a graphic used for measurement and categorization. (2) A report aspect used to arrange and relate multidimensional data, such as filters, pages, rows, and columns. For example, for a data query in Simple Basic, an axis can define columns for values for Qtr1, Qtr2, Qtr3, and Qtr4. Row data would be retrieved with totals in the following hierarchy: Market, Product.

backup A duplicate copy of an application instance.

balance account An account type that stores unsigned values that relate to a particular point in time.

balanced journal A journal in which the total debits equal the total credits.

bang character (!) A character that terminates a series of report commands and requests information from the database. A report script must be terminated with a bang character; several bang characters can be used within a report script.

bar chart A chart that can consist of one to 50 data sets, with any number of values assigned to each data set. Data sets are displayed as groups of corresponding bars, stacked bars, or individual bars in separate rows.

base currency The currency in which daily business transactions are performed.

base dimension A standard dimension that is associated with one or more attribute dimensions. For example, assuming products have flavors, the Product dimension is the base dimension for the Flavors attribute dimension.

base entity An entity at the bottom of the organization structure that does not own other entities.

batch calculation Any calculation on a database that is done in batch; for example, a calculation script or a full database calculation. Dynamic calculations are not considered to be batch calculations.

batch file An operating system file that can call multiple ESSCMD scripts and run multiple sessions of ESSCMD. On Windows-based systems, batch files have BAT file extensions. On UNIX, batch files are written as a shell script.

batch loader An FDM component that enables the processing of multiple files.

batch POV A collection of all dimensions on the user POV of every report and book in the batch. While scheduling the batch, you can set the members selected on the batch POV.

batch processing mode A method of using ESSCMD to write a batch or script file that can be used to automate routine server maintenance and diagnostic tasks. ESSCMD script files can execute multiple commands and can be run from the operating system command line or from within operating system batch files. Batch files can be used to call multiple ESSCMD scripts or run multiple instances of ESSCMD.

block The primary storage unit which is a multidimensional array representing the cells of all dense dimensions.

block storage database The Essbase database storage model categorizing and storing data based on the sparsity of data values defined in sparse dimensions. Data values are stored in blocks, which exist only for sparse dimension members for which there are values.

Blocked Account An account that you do not want calculated in the consolidated file because you want to enter it manually.

book A container that holds a group of similar Financial Reporting documents. Books may specify dimension sections or dimension changes.

book POV The dimension members for which a book is run.

bookmark A link to a reporting document or a Web site, displayed on a personal page of a user. The two types of bookmarks are My Bookmarks and image bookmarks.

bounding rectangle The required perimeter that encapsulates the Interactive Reporting document content when embedding Interactive Reporting document sections in a personal page, specified in pixels for height and width or row per page.

broadcast message A simple text message sent by an administrator to a user who is logged on to a Planning application. The message displays information to the user such as system availability, notification of application refresh, or application backups.

budget administrator A person responsible for setting up, configuring, maintaining, and controlling an application. Has all application privileges and data access permissions.

build method A method used to modify database outlines. Choice of a build method is based on the format of data in data source files.

business process A set of activities that collectively accomplish a business objective.

business rules Logical expressions or formulas that are created within an application to produce a desired set of resulting values.

cache A buffer in memory that holds data temporarily.

calc script A set of commands that define how a database is consolidated or aggregated. A calculation script may also contain commands that specify allocation and other calculation rules separate from the consolidation process.

calculated member in MaxL DML A member designed for analytical purposes and defined in the optional WITH section of a MaxL DML query.

calculated member in MaxL DML A member designed for analytical purposes and defined in the optional WITH section of a MaxL DML query.

calculation The process of aggregating data, or of running a calculation script on a database.

Calculation Manager A module of Performance Management Architect that Planning and Financial Management users can use to design, validate, and administrate business rules in a graphical environment.

calculation status A consolidation status that indicates that some values or formula calculations have changed. You must reconsolidate to get the correct values for the affected entity.

calendar User-defined time periods and their relationship to each other. Q1, Q2, Q3, and Q4 comprise a calendar or fiscal year.

cascade The process of creating multiple reports for a subset of member values.

Catalog pane Displays a list of elements available to the active section. If Query is the active section, a list of database tables is displayed. If Pivot is the active section, a list of results columns is displayed. If Dashboard is the active section, a list of embeddable sections, graphic tools, and control tools are displayed.

categories Groupings by which data is organized. For example, Month.

cause and effect map Depicts how the elements that form your corporate strategy relate and how they work together to meet your organization's strategic goals. A Cause and Effect map tab is automatically created for each Strategy map.

CDF *See custom-defined function (CDF).*

CDM *See custom-defined macro (CDM).*

cell (1) The data value at the intersection of dimensions in a multidimensional database; the intersection of a row and a column in a worksheet. (2) A logical group of nodes belonging to one administrative domain.

cell note A text annotation for a cell in an Essbase database. Cell notes are a type of LRO.

CHANGED status Consolidation status that indicates data for an entity has changed.

chart A graphical representation of spreadsheet data. The visual nature expedites analysis, color-coding, and visual cues that aid comparisons.

chart template A template that defines the metrics to display in Workspace charts.

child A member with a parent above it in the database outline.

choice list A list of members that a report designer can specify for each dimension when defining the report's point of view. A user who wants to change the point of view for a dimension that uses a choice list can select only the members specified in that defined member list or those members that meet the criteria defined in the function for the dynamic list.

clean block A data block that where the database is fully calculated, if a calculation script calculates all dimensions at once, or if the SET CLEARUPDATESTATUS command is used in a calculation script.

cluster An array of servers or databases that behave as a single resource which share task loads and provide failover support; eliminates one server or database as a single point of failure in a system.

clustered bar charts Charts in which categories are viewed side-by-side; useful for side-by-side category analysis; used only with vertical bar charts.

code page A mapping of bit combinations to a set of text characters. Different code pages support different sets of characters. Each computer contains a code page setting for the character set requirements of the language of the computer user. In the context of this document, code pages map characters to bit combinations for non-Unicode encodings. *See also encoding*.

column A vertical display of information in a grid or table. A column can contain data from one field, derived data from a calculation, or textual information.

committed access An Essbase Kernel Isolation Level setting that affects how Essbase handles transactions. Under committed access, concurrent transactions hold long-term write locks and yield predictable results.

computed item A virtual column (as opposed to a column that is physically stored in the database or cube) that can be calculated by the database during a query, or by Interactive Reporting Studio in the Results section. Computed items are calculations of data based on functions, data items, and operators provided in the dialog box and can be included in reports or reused to calculate other data.

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

connection file *See Interactive Reporting connection file (.oce)*.

consolidated file (Parent) A file into which all of the business unit files are consolidated; contains the definition of the consolidation.

consolidation The process of aggregating data from dependent entities to parent entities. For example, if the dimension Year consists of the members Qtr1, Qtr2, Qtr3, and Qtr4, its consolidation is Year.

consolidation file (*.cns) The consolidation file is a graphical interface that enables you to add, delete or move Strategic Finance files in the consolidation process using either a Chart or Tree view. It also enables you to define and modify the consolidation.

consolidation rule Identifies the rule that is executed during the consolidation of the node of the hierarchy. This rule can contain customer specific formulas appropriate for the correct consolidation of parent balances. Elimination processing can be controlled within these rules.

content Information stored in the repository for any type of file.

content browser A Component that allows users to Browse and select content to be placed in a Workspace Page .

context variable A variable that is defined for a particular task flow to identify the context of the taskflow instance.

contribution The value added to a parent from a child entity. Each child has a contribution to its parent.

controls group Used in FDM to maintain and organize certification and assessment information, especially helpful for meeting Sarbanes-Oxley requirements.

conversion rate *See exchange rate*.

cookie A segment of data placed on your computer by a Web site.

correlated subqueries Subqueries that are evaluated once for every row in the parent query; created by joining a topic item in the subquery with a topic in the parent query.

critical business area (CBA) An individual or a group organized into a division, region, plant, cost center, profit center, project team, or process; also called accountability team or business area.

critical success factor (CSF) A capability that must be established and sustained to achieve a strategic objective; owned by a strategic objective or a critical process and is a parent to one or more actions.

crosstab reporting Categorizes and summarizes data in table format. The table cells contain summaries of the data that fit within the intersecting categories. For example, a crosstab report of product sales information could show size attributes, such as Small and Large, as column headings and color attributes, such as Blue and Yellow, as row headings. The cell in the table where Large and Blue intersect could contain the total sales of all Blue products that are sized Large.

cube A block of data that contains three or more dimensions. An Essbase database is a cube.

cube deployment In Essbase Studio, the process of setting load options for a model to build an outline and load data into an Essbase application and database.

cube schema In Essbase Studio, the metadata elements, such as measures and hierarchies, representing the logical model of a cube.

currency conversion A process that converts currency values in a database from one currency into another. For example, to convert one U. S. dollar into the European euro, the exchange rate (for example, 0.923702) is multiplied with the dollar (1* 0.923702). After conversion, the European euro amount is .92.

Currency Overrides In any input period, the selected input method can be overridden to enable input of that period's value as Default Currency/Items. To override the input method, enter a pound sign (#) either before or after the number.

currency partition A dimension type that separates local currency members from a base currency, as defined in an application. Identifies currency types, such as Actual, Budget, and Forecast.

custom calendar Any calendar created by an administrator.

custom dimension A dimension created and defined by users. Channel, product, department, project, or region could be custom dimensions.

custom property A property of a dimension or dimension member that is created by a user.

custom report A complex report from the Design Report module, composed of any combination of components.

custom-defined function (CDF) Essbase calculation functions developed in Java and added to the standard Essbase calculation scripting language using MaxL. *See also custom-defined macro (CDM)*.

custom-defined macro (CDM) Essbase macros written with Essbase calculator functions and special macro functions. Custom-defined macros use an internal Essbase macro language that enables the combination of calculation functions and they operate on multiple input parameters. *See also custom-defined function (CDF)*.

cycle through To perform multiple passes through a database while calculating it.

dashboard A collection of metrics and indicators that provide an interactive summary of your business. Dashboards enable you to build and deploy analytic applications.

data cache A buffer in memory that holds uncompressed data blocks.

data cell *See cell*.

data file cache A buffer in memory that holds compressed data (PAG) files.

data form A grid display that enables users to enter data into the database from an interface such as a Web browser, and to view and analyze data or related text. Certain dimension member values are fixed, giving users a specific view into the data.

data function That computes aggregate values, including averages, maximums, counts, and other statistics, that summarize groupings of data.

data load location In FDM, a reporting unit responsible for submitting source data into the target system. Typically, there is one FDM data load location for each source file loaded to the target system.

data load rules A set of criteria that determines how to load data from a text-based file, a spreadsheet, or a relational data set into a database.

data lock Prevents changes to data according to specified criteria, such as period or scenario.

data mining The process of searching through an Essbase database for hidden relationships and patterns in a large amount of data.

data model A representation of a subset of database tables.

data value *See cell*.

database connection File that stores definitions and properties used to connect to data sources and enables database references to be portable and widely used.

date measure In Essbase, a member tagged as “Date” in the dimension where measures are represented. The cell values are displayed as formatted dates. Dates as measures can be useful for types of analysis that are difficult to represent using the Time dimension. For example, an application may need to track acquisition dates for a series of capital assets, but the acquisition dates span too large a period to allow for feasible Time dimension modeling. *See also* typed measure.

Default Currency Units Define the unit scale of data. For example, if you select to define your analysis in Thousands, and enter “10”, this is interpreted as “10,000”.

dense dimension In block storage databases, a dimension likely to contain data for every combination of dimension members. For example, time dimensions are often dense because they can contain all combinations of all members. *Contrast with* sparse dimension.

dependent entity An entity that is owned by another entity in the organization.

derived text measure In Essbase Studio, a text measure whose values are governed by a predefined rule expressed as a range. For example, a derived text measure, called "Sales Performance Index," based on a measure Sales, could consist of the values "High," "Medium," and "Low." This derived text measure is defined to display "High," "Medium," and "Low" depending on the range in which the corresponding sales values fall. *See also* text measure.

descendant Any member below a parent in the database outline. In a dimension that includes years, quarters, and months, the members Qtr2 and April are descendants of the member Year.

Design Report An interface in Web Analysis Studio for designing custom reports, from a library of components.

destination Within a Profitability and Cost Management assignment, the destination is the receiving point for allocated values.

destination currency The currency to which balances are converted. You enter exchange rates and convert from the source currency to the destination currency. For example, when you convert from EUR to USD, the destination currency is USD.

detail chart A chart that provides the detailed information that you see in a Summary chart. Detail charts appear in the Investigate Section in columns below the Summary charts. If the Summary chart shows a Pie chart, then the Detail charts below represent each piece of the pie.

dimension A data category used to organize business data for retrieval and preservation of values. Dimensions usually contain hierarchies of related members grouped within them. For example, a Year dimension often includes members for each time period, such as quarters and months.

dimension build The process of adding dimensions and members to an Essbase outline.

dimension build rules Specifications, similar to data load rules, that Essbase uses to modify an outline. The modification is based on data in an external data source file.

dimension tab In the Pivot section, the tab that enables you to pivot data between rows and columns.

dimension table (1) A table that includes numerous attributes about a specific business process. (2) In Essbase Integration Services, a container in the OLAP model for one or more relational tables that define a potential dimension in Essbase.

dimension type A dimension property that enables the use of predefined functionality. Dimensions tagged as time have a predefined calendar functionality.

dimensionality In MaxL DML, the represented dimensions (and the order in which they are represented) in a set. For example, the following set consists of two tuples of the same dimensionality because they both reflect the dimensions (Region, Year): { (West, Feb), (East, Mar) }

direct rate A currency rate that you enter in the exchange rate table. The direct rate is used for currency conversion. For example, to convert balances from JPY to USD, In the exchange rate table, enter a rate for the period/scenario where the source currency is JPY and the destination currency is USD.

dirty block A data block containing cells that have been changed since the last calculation. Upper level blocks are marked as dirty if their child blocks are dirty (that is, they have been updated).

display type One of three Web Analysis formats saved to the repository: spreadsheet, chart, and pinboard.

dog-ear The flipped page corner in the upper right corner of the chart header area.

domain In data mining, a variable representing a range of navigation within data.

drill-down Navigation through the query result set using the dimensional hierarchy. Drilling down moves the user perspective from aggregated data to detail. For example, drilling down can reveal hierarchical relationships between years and quarters or quarters and months.

drill-through The navigation from a value in one data source to corresponding data in another source.

driver A driver is an allocation method that describes the mathematical relationship between the sources that utilize the driver, and the destinations to which those sources allocate cost or revenue.

duplicate alias name A name that occurs more than once in an alias table and that can be associated with more than one member in a database outline. Duplicate alias names can be used with duplicate member outlines only.

duplicate member name The multiple occurrence of a member name in a database, with each occurrence representing a different member. For example, a database has two members named "New York." One member represents New York state and the other member represents New York city.

duplicate member outline A database outline containing duplicate member names.

Dynamic Calc and Store members A member in a block storage outline that Essbase calculates only upon the first retrieval of the value. Essbase then stores the calculated value in the database. Subsequent retrievals do not require calculating.

Dynamic Calc members A member in a block storage outline that Essbase calculates only at retrieval time. Essbase discards calculated values after completing the retrieval request.

dynamic calculation In Essbase, a calculation that occurs only when you retrieve data on a member that is tagged as Dynamic Calc or Dynamic Calc and Store. The member's values are calculated at retrieval time instead of being precalculated during batch calculation.

dynamic hierarchy In aggregate storage database outlines only, a hierarchy in which members are calculated at retrieval time.

dynamic member list A system-created named member set that is based on user-defined criteria. The list is refreshed automatically whenever it is referenced in the application. As dimension members are added and deleted, the list automatically reapplies the criteria to reflect the changes.

dynamic reference A pointer in the rules file to header records in a data source.

dynamic report A report containing data that is updated when you run the report.

Dynamic Time Series A process that performs period-to-date reporting in block storage databases.

dynamic view account An account type indicating that account values are calculated dynamically from the data that is displayed.

Eliminated Account An account that does not appear in the consolidated file.

elimination The process of zeroing out (eliminating) transactions between entities within an organization.

employee A user responsible for, or associated with, specific business objects. Employees need not work for an organization; for example, they can be consultants. Employees must be associated with user accounts for authorization purposes.

encoding A method for mapping bit combinations to characters for creating, storing, and displaying text. Each encoding has a name; for example, UTF-8. Within an encoding, each character maps to a specific bit combination; for example, in UTF-8, uppercase A maps to HEX41. *See also* *code page* and *locale*.

ending period A period enabling you to adjust the date range in a chart. For example, an ending period of "month", produces a chart showing information through the end of the current month.

Enterprise View An Administration Services feature that enables management of the Essbase environment from a graphical tree view. From Enterprise View, you can operate directly on Essbase artifacts.

entity A dimension representing organizational units. Examples: divisions, subsidiaries, plants, regions, products, or other financial reporting units.

Equity Beta The riskiness of a stock, measured by the variance between its return and the market return, indicated by an index called "beta". For example, if a stock's return normally moves up or down 1.2% when the market moves up or down 1%, the stock has a beta of 1.2.

essbase.cfg An optional configuration file for Essbase. Administrators may edit this file to customize Essbase Server functionality. Some configuration settings may also be used with Essbase clients to override Essbase Server settings.

EssCell A function entered into a cell in Essbase Spreadsheet Add-in to retrieve a value representing an intersection of specific Essbase database members.

ESSCMD A command-line interface for performing Essbase operations interactively or through batch script files.

ESSLANG The Essbase environment variable that defines the encoding used to interpret text characters. *See also encoding*.

ESSMSH *See MaxL Shell*.

exceptions Values that satisfy predefined conditions. You can define formatting indicators or notify subscribing users when exceptions are generated.

exchange rate A numeric value for converting one currency to another. For example, to convert 1 USD into EUR, the exchange rate of 0.8936 is multiplied with the U.S. dollar. The European euro equivalent of $1 is 0.8936.

exchange rate type An identifier for an exchange rate. Different rate types are used because there may be multiple rates for a period and year. Users traditionally define rates at period end for the average rate of the period and for the end of the period. Additional rate types are historical rates, budget rates, forecast rates, and so on. A rate type applies to one point in time.

expense account An account that stores periodic and year-to-date values that decrease net worth if they are positive.

Extensible Markup Language (XML) A language comprising a set of tags used to assign attributes to data that can be interpreted between applications according to a schema.

external authentication Logging on to Oracle's Hyperion applications with user information stored outside the applications, typically in a corporate directory such as MSAD or NTLM.

externally triggered events Non-time-based events for scheduling job runs.

Extract, Transform, and Load (ETL) Data source-specific programs for extracting data and migrating it to applications.

extraction command An Essbase reporting command that handles the selection, orientation, grouping, and ordering of raw data extracted from a database; begins with the less than (<) character.

fact table The central table in a star join schema, characterized by a foreign key and elements drawn from a dimension table. This table typically contains numeric data that can be related to all other tables in the schema.

Favorites gadget Contains links to Reporting and Analysis documents and URLs.

field An item in a data source file to be loaded into an Essbase database.

file delimiter Characters, such as commas or tabs, that separate fields in a data source.

filter A constraint on data sets that restricts values to specific criteria; for example, to exclude certain tables, metadata, or values, or to control access.

flow account An unsigned account that stores periodic and year-to-date values.

folder A file containing other files for the purpose of structuring a hierarchy.

footer Text or images at the bottom of report pages, containing dynamic functions or static text such as page numbers, dates, logos, titles or file names, and author names.

format Visual characteristics of documents or report objects.

format string In Essbase, a method for transforming the way cell values are displayed.

formula A combination of operators, functions, dimension and member names, and numeric constants calculating database members.

frame An area on the desktop. There are two main areas: the navigation and Workspace frames.

free-form grid An object for presenting, entering, and integrating data from different sources for dynamic calculations.

free-form reporting Creating reports by entering dimension members or report script commands in worksheets.

function A routine that returns values or database members.

gadget Simple, specialized, lightweight applications that provide easy viewing of EPM content and enable access to core Reporting and Analysis functionality.

genealogy data Additional data that is optionally generated after allocation calculations. This data enables reporting on all cost or revenue flows from start to finish through all allocation steps.

generation A layer in a hierarchical tree structure that defines member relationships in a database. Generations are ordered incrementally from the top member of the dimension (generation 1) down to the child members. Use the unique generation name to identify a layer in the hierarchical tree structure.

generic jobs Non-SQR Production Reporting or non-Interactive Reporting jobs.

global report command A command in a running report script that is effective until replaced by another global command or the file ends.

grid POV A means for specifying dimension members on a grid without placing dimensions in rows, columns, or page intersections. A report designer can set POV values at the grid level, preventing user POVs from affecting the grid. If a dimension has one grid value, you put the dimension into the grid POV instead of the row, column, or page.

group A container for assigning similar access permissions to multiple users.

GUI Graphical user interface

head up display A mode that shows your loaded Smart Space desktop including the background image above your Windows desktop.

highlighting Depending on your configuration, chart cells or ZoomChart details may be highlighted, indicating value status: red (bad), yellow (warning), or green (good).

Historical Average An average for an account over a number of historical periods.

holding company An entity that is part of a legal entity group, with direct or indirect investments in all entities in the group.

host A server on which applications and services are installed.

host properties Properties pertaining to a host, or if the host has multiple Install_Homes, to an Install_Home. The host properties are configured from the CMC.

Hybrid Analysis An analysis mapping low-level data stored in a relational database to summary-level data stored in Essbase, combining the mass scalability of relational systems with multidimensional data.

hyperlink A link to a file, Web page, or an intranet HTML page.

Hypertext Markup Language (HTML) A programming language specifying how Web browsers display data.

identity A unique identification for a user or group in external authentication.

image bookmarks Graphic links to Web pages or repository items.

IMPACTED status Indicates changes in child entities consolidating into parent entities.

implied share A member with one or more children, but only one is consolidated, so the parent and child share a value.

import format In FDM, defines the structure of the source file which enables the loading of a source data file to an FDM data load location.

inactive group A group for which an administrator has deactivated system access.

inactive service A service suspended from operating.

INACTIVE status Indicates entities deactivated from consolidation for the current period.

inactive user A user whose account has been deactivated by an administrator.

income account An account storing periodic and year-to-date values that, if positive, increase net worth.

index (1) A method where Essbase uses sparse-data combinations to retrieve data in block storage databases. (2) The index file.

index cache A buffer containing index pages.

index entry A pointer to an intersection of sparse dimensions. Index entries point to data blocks on disk and use offsets to locate cells.

index file An Essbase file storing block storage data retrieval information, residing on disk, and containing index pages.

index page A subdivision in an index file. Contains pointers to data blocks.

input data Data loaded from a source rather than calculated.

Install_Home A variable for the directory where EPM System products are installed. Refers to one instance of an EPM System product when multiple applications are installed on the same computer.

integration Process that is run to move data between EPM System products using Shared Services. Data integration definitions specify the data moving between a source application and a destination application, and enable the data movements to be grouped, ordered, and scheduled.

intelligent calculation A calculation method tracking updated data blocks since the last calculation.

Interactive Reporting connection file (.oce) Files encapsulating database connection information, including: the database API (ODBC, SQL*Net, etc.), database software, the database server network address, and database user name. Administrators create and publish Interactive Reporting connection files (.oce).

intercompany elimination *See elimination.*

intercompany matching The process of comparing balances for pairs of intercompany accounts within an application. Intercompany receivables are compared to intercompany payables for matches. Matching accounts are used to eliminate intercompany transactions from an organization's consolidated totals.

intercompany matching report A report that compares intercompany account balances and indicates if the accounts are in, or out, of balance.

interdimensional irrelevance A situation in which a dimension does not intersect with other dimensions. Because the data in the dimension cannot be accessed from the non-intersecting dimensions, the non-intersecting dimensions are not relevant to that dimension.

intersection A unit of data representing the intersection of dimensions in a multidimensional database; also, a worksheet cell.

intrastage assignment Assignments in the financial flow that are assigned to objects within the same stage.

introspection A deep inspection of a data source to discover hierarchies based on the inherent relationships in the database. *Contrast with scraping.*

Investigation *See drill-through.*

isolation level An Essbase Kernel setting that determines the lock and commit behavior of database operations. Choices are: committed access and uncommitted access.

iteration A "pass" of the budget or planning cycle in which the same version of data is revised and promoted.

Java Database Connectivity (JDBC) A client-server communication protocol used by Java based clients and relational databases. The JDBC interface provides a call-level API for SQL-based database access.

job output Files or reports produced from running a job.

jobs Documents with special properties that can be launched to generate output. A job can contain Interactive Reporting, SQR Production Reporting, or generic documents.

join A link between two relational database tables or topics based on common content in a column or row. A join typically occurs between identical or similar items within different tables or topics. For example, a record in the Customer table is joined to a record in the Orders table because the Customer ID value is the same in each table.

journal entry (JE) A set of debit/credit adjustments to account balances for a scenario and period.

JSP Java Server Pages.

KeyContacts gadget Contains a group of Smart Space users and provides access to Smart Space Collaborator. For example, you can have a KeyContacts gadget for your marketing team and another for your development team.

latest A Spreadsheet key word used to extract data values from the member defined as the latest time period.

layer (1) The horizontal location of members in a hierarchical structure, specified by generation (top down) or level (bottom up). (2) Position of objects relative to other objects. For example, in the Sample Basic database, Qtr1 and Qtr4 are in the same layer, so they are also in the same generation, but in a database with a ragged hierarchy, Qtr1 and Qtr4 might not be in same layer, though they are in the same generation.

layout area Used to designate an area on a Workspace Page where content can be placed.

legend box A box containing labels that identify the data categories of a dimension.

level A layer in a hierarchical tree structure that defines database member relationships. Levels are ordered from the bottom dimension member (level 0) up to the parent members.

level 0 block A data block for combinations of sparse, level 0 members.

level 0 member A member that has no children.

liability account An account type that stores "point in time" balances of a company's liabilities. Examples of liability accounts include accrued expenses, accounts payable, and long term debt.

life cycle management The process of managing application information from inception to retirement.

Lifecycle Management Utility A command-line utility for migrating applications and artifacts.

line chart A chart that displays one to 50 data sets, each represented by a line. A line chart can display each line stacked on the preceding ones, as represented by an absolute value or a percent.

line item detail The lowest level of detail in an account.

lineage The relationship between different metadata elements showing how one metadata element is derived from one or more other metadata elements, ultimately tracing the metadata element to its physical source. In Essbase Studio, a lineage viewer displays the relationships graphically. *See also traceability*.

link (1) A reference to a repository object. Links can reference folders, files, shortcuts, and other links. (2) In a task flow, the point where the activity in one stage ends and another begins.

link condition A logical expression evaluated by the taskflow engine to determine the sequence of launching taskflow stages.

linked data model Documents that are linked to a master copy in a repository.

linked partition A shared partition that enables you to use a data cell to link two databases. When a user clicks a linked cell in a worksheet, Essbase opens a new sheet displaying the dimensions in the linked database. The user can then drill down those dimensions.

linked reporting object (LRO) A cell-based link to an external file such as cell notes, URLs, or files with text, audio, video, or pictures. (Only cell notes are supported for Essbase LROs in Financial Reporting.) *Contrast with local report object*.

local currency An input currency type. When an input currency type is not specified, the local currency matches the entity's base currency.

local report object A report object that is not linked to a Financial Reporting report object in Explorer. *Contrast with linked reporting object (LRO)*.

local results A data model's query results. Results can be used in local joins by dragging them into the data model. Local results are displayed in the catalog when requested.

locale A computer setting that specifies a location's language, currency and date formatting, data sort order, and the character set encoding used on the computer. Essbase uses only the encoding portion. *See also encoding* and *ESSLANG*.

locale header record A text record at the beginning of some non-Unicode-encoded text files, such as scripts, that identifies the encoding locale.

location alias A descriptor that identifies a data source. The location alias specifies a server, application, database, user name, and password. Location aliases are set by DBAs at the database level using Administration Services Console, ESSCMD, or the API.

locked A user-invoked process that prevents users and processes from modifying data.

locked data model Data models that cannot be modified by a user.

LOCKED status A consolidation status indicating that an entity contains data that cannot be modified.

Log Analyzer An Administration Services feature that enables filtering, searching, and analysis of Essbase logs.

logic group In FDM, contains one or more logic accounts that are generated after a source file is loaded into FDM. Logic accounts are calculated accounts that are derived from the source data.

LRO *See linked reporting object (LRO).*

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

manual stage A stage that requires human intervention to complete.

Map File Used to store the definition for sending data to or retrieving data from an external database. Map files have different extensions (.mps to send data; .mpr to retrieve data).

Map Navigator A feature that displays your current position on a Strategy, Accountability, or Cause and Effect map, indicated by a red outline.

Marginal Tax Rate Used to calculate the after-tax cost of debt. Represents the tax rate applied to the last earned income dollar (the rate from the highest tax bracket into which income falls) and includes federal, state and local taxes. Based on current level of taxable income and tax bracket, you can predict marginal tax rate.

Market Risk Premium The additional rate of return paid over the risk-free rate to persuade investors to hold "riskier" investments than government securities. Calculated by subtracting the risk-free rate from the expected market return. These figures should closely model future market conditions.

master data model An independent data model that is referenced as a source by multiple queries. When used, "Locked Data Model" is displayed in the Query section's Content pane; the data model is linked to the master data model displayed in the Data Model section, which an administrator may hide.

mathematical operator A symbol that defines how data is calculated in formulas and outlines. Can be any of the standard mathematical or Boolean operators; for example, +, -, *, /, and %.

MaxL The multidimensional database access language for Essbase, consisting of a data definition language (MaxL DDL) and a data manipulation language (MaxL DML). *See also MaxL DDL, MaxL DML,* and *MaxL Shell.*

MaxL DDL Data definition language used by Essbase for batch or interactive system-administration tasks.

MaxL DML Data manipulation language used in Essbase for data query and extraction.

MaxL Perl Module A Perl module (essbase.pm) that is part of Essbase MaxL DDL. This module can be added to the Perl package to provide access to Essbase databases from Perl programs.

MaxL Script Editor A script-development environment in Administration Services Console. MaxL Script Editor is an alternative to using a text editor and the MaxL Shell for administering Essbase with MaxL scripts.

MaxL Shell An interface for passing MaxL statements to Essbase Server. The MaxL Shell executable file is located in the Essbase bin directory (UNIX: essmsh, Windows: essmsh.exe).

MDX (multidimensional expression) The language that give instructions to OLE DB for OLAP- compliant databases, as SQL is used for relational databases. When you build the OLAPQuery section's Outliner, Interactive Reporting Clients translate requests into MDX instructions. When you process the query, MDX is sent to the database server, which returns records that answer your query. *See also SQL spreadsheet.*

measures Numeric values in an OLAP database cube that are available for analysis. Measures are margin, cost of goods sold, unit sales, budget amount, and so on. *See also fact table.*

member A discrete component within a dimension. A member identifies and differentiates the organization of similar units. For example, a time dimension might include such members as Jan, Feb, and Qtr1.

member list A named group, system- or user-defined, that references members, functions, or member lists within a dimension.

member load In Integration Services, the process of adding dimensions and members (without data) to Essbase outlines.

member selection report command A type of Report Writer command that selects member ranges based on outline relationships, such as sibling, generation, and level.

member-specific report command A type of Report Writer formatting command that is executed as it is encountered in a report script. The command affects only its associated member and executes the format command before processing the member.

merge A data load option that clears values only from the accounts specified in the data load file and replaces them with values in the data load file.

metadata A set of data that defines and describes the properties and attributes of the data stored in a database or used by an application. Examples of metadata are dimension names, member names, properties, time periods, and security.

metadata elements Metadata derived from data sources and other metadata that is stored and cataloged for Essbase Studio use.

metadata sampling The process of retrieving a sample of members in a dimension in a drill-down operation.

metadata security Security set at the member level to restrict users from accessing certain outline members.

metaoutline In Integration Services, a template containing the structure and rules for creating an Essbase outline from an OLAP model.

metric A numeric measurement computed from business data to help assess business performance and analyze company trends.

migration The process of copying applications, artifacts, or users from one environment or computer to another; for example, from a testing environment to a production environment.

migration audit report A report generated from the migration log that provides tracking information for an application migration.

migration definition file (.mdf) A file that contains migration parameters for an application migration, enabling batch script processing.

migration log A log file that captures all application migration actions and messages.

migration snapshot A snapshot of an application migration that is captured in the migration log.

MIME Type (Multipurpose Internet Mail Extension) An attribute that describes the data format of an item, so that the system knows which application should open the object. A file's mime type is determined by the file extension or HTTP header. Plug-ins tell browsers what mime types they support and what file extensions correspond to each mime type.

mining attribute In data mining, a class of values used as a factor in analysis of a set of data.

minireport A report component that includes layout, content, hyperlinks, and the query or queries to load the report. Each report can include one or more minireports.

minischema A graphical representation of a subset of tables from a data source that represents a data modeling context.

missing data (#MISSING) A marker indicating that data in the labeled location does not exist, contains no value, or was never entered or loaded. For example, missing data exists when an account contains data for a previous or future period but not for the current period.

model (1) In data mining, a collection of an algorithm's findings about examined data. A model can be applied against a wider data set to generate useful information about that data. (2) A file or content string containing an application-specific representation of data. Models are the basic data managed by Shared Services, of two major types: dimensional and non-dimensional application objects. (3) In Business Modeling, a network of boxes connected to represent and calculate the operational and financial flow through the area being examined.

monetary A money-related value.

multidimensional database A method of organizing, storing, and referencing data through three or more dimensions. An individual value is the intersection point for a set of dimensions. *Contrast with relational database*.

multiload An FDM feature that allows the simultaneous loading of multiple periods, categories, and locations.

My Workspace Page A page created with content from multiple sources including documents, URL, and other content types. Enables a user to aggregate content from Oracle and non-Oracle sources.

named set In MaxL DML, a set with its logic defined in the optional WITH section of a MaxL DML query. The named set can be referenced multiple times in the query.

native authentication The process of authenticating a user name and password from within the server or application.

nested column headings A report column heading format that displays data from multiple dimensions. For example, a column heading that contains Year and Scenario members is a nested column. The nested column heading shows Q1 (from the Year dimension) in the top line of the heading, qualified by Actual and Budget (from the Scenario dimension) in the bottom line of the heading.

NO DATA status A consolidation status indicating that this entity contains no data for the specified period and account.

non-dimensional model A Shared Services model type that includes application objects such as security files, member lists, calculation scripts, and Web forms.

non-unique member name *See duplicate member name*.

note Additional information associated with a box, measure, scorecard or map element.

Notifications gadget Shows notification message history received from other users or systems.

null value A value that is absent of data. Null values are not equal to zero.

numeric attribute range A feature used to associate a base dimension member that has a discrete numeric value with an attribute that represents a value range. For example, to classify customers by age, an Age Group attribute dimension can contain members for the following age ranges: 0-20, 21-40, 41-60, and 61-80. Each Customer dimension member can be associated with an Age Group range. Data can be retrieved based on the age ranges rather than on individual age values.

ODBC Open Database Connectivity. A database access method used from any application regardless of how the database management system (DBMS) processes the information.

OK status A consolidation status indicating that an entity has already been consolidated, and that data has not changed below it in the organization structure.

OLAP Metadata Catalog In Integration Services, a relational database containing metadata describing the nature, source, location, and type of data that is pulled from the relational data source.

OLAP model In Integration Services, a logical model (star schema) that is created from tables and columns in a relational database. The OLAP model is then used to generate the structure of a multidimensional database.

online analytical processing (OLAP) A multidimensional, multiuser, client-server computing environment for users who analyze consolidated enterprise data in real time. OLAP systems feature drill-down, data pivoting, complex calculations, trend analysis, and modeling.

Open Database Connectivity (ODBC) Standardized application programming interface (API) technology that allows applications to access multiple third-party databases.

organization An entity hierarchy that defines each entity and their relationship to others in the hierarchy.

origin The intersection of two axes.

outline The database structure of a multidimensional database, including all dimensions, members, tags, types, consolidations, and mathematical relationships. Data is stored in the database according to the structure defined in the outline.

outline synchronization For partitioned databases, the process of propagating outline changes from one database to another database.

P&L accounts (P&L) Profit and loss accounts. Refers to a typical grouping of expense and income accounts that comprise a company's income statement.

page A display of information in a grid or table often represented by the Z-axis. A page can contain data from one field, derived data from a calculation, or text.

page file Essbase data file.

page heading A report heading type that lists members represented on the current page of the report. All data values on the page have the members in the page heading as a common attribute.

page member A member that determines the page axis.

palette A JASC compliant file with a .PAL extension. Each palette contains 16 colors that complement each other and can be used to set the dashboard color elements.

parallel calculation A calculation option. Essbase divides a calculation into tasks and calculates some tasks simultaneously.

parallel data load In Essbase, the concurrent execution of data load stages by multiple process threads.

parallel export The ability to export Essbase data to multiple files. This may be faster than exporting to a single file, and it may resolve problems caused by a single data file becoming too large for the operating system to handle.

parent adjustments The journal entries that are posted to a child in relation to its parent.

parents The entities that contain one or more dependent entities that report directly to them. Because parents are both entities and associated with at least one node, they have entity, node, and parent information associated with them.

partition area A sub cube within a database. A partition is composed of one or more areas of cells from a portion of the database. For replicated and transparent partitions, the number of cells within an area must be the same for the data source and target to ensure that the two partitions have the same shape. If the data source area contains 18 cells, the data target area must also contain 18 cells to accommodate the number of values.

partitioning The process of defining areas of data that are shared or linked between data models. Partitioning can affect the performance and scalability of Essbase applications.

pattern matching The ability to match a value with any or all characters of an item entered as a criterion. Missing characters may be represented by wild card values such as a question mark (?) or an asterisk (*). For example, “Find all instances of apple” returns apple, but “Find all instances of apple*” returns apple, applesauce, applecranberry, and so on.

percent consolidation The portion of a child's values that is consolidated to its parent.

percent control Identifies the extent to which an entity is controlled within the context of its group.

percent ownership Identifies the extent to which an entity is owned by its parent.

performance indicator An image file used to represent measure and scorecard performance based on a range you specify; also called a status symbol. You can use the default performance indicators or create an unlimited number of your own.

periodic value method (PVA) A process of currency conversion that applies the periodic exchange rate values over time to derive converted results.

permission A level of access granted to users and groups for managing data or other users and groups.

persistence The continuance or longevity of effect for any Essbase operation or setting. For example, an Essbase administrator may limit the persistence of user name and password validity.

personal pages A personal window to repository information. You select what information to display and its layout and colors.

personal recurring time events Reusable time events that are accessible only to the user who created them.

personal variable A named selection statement of complex member selections.

perspective A category used to group measures on a scorecard or strategic objectives within an application. A perspective can represent a key stakeholder (such as a customer, employee, or shareholder/financial) or a key competency area (such as time, cost, or quality).

pie chart A chart that shows one data set segmented in a pie formation.

pinboard One of the three data object display types. Pinboards are graphics, composed of backgrounds and interactive icons called pins. Pinboards require traffic lighting definitions.

pins Interactive icons placed on graphic reports called pinboards. Pins are dynamic. They can change images and traffic lighting color based on the underlying data values and analysis tools criteria.

pivot The ability to alter the perspective of retrieved data. When Essbase first retrieves a dimension, it expands data into rows. You can then pivot or rearrange the data to obtain a different viewpoint.

planner Planners, who comprise the majority of users, can input and submit data, use reports that others create, execute business rules, use task lists, enable e-mail notification for themselves, and use Smart View.

planning unit A data slice at the intersection of a scenario, version, and entity; the basic unit for preparing, reviewing, annotating, and approving plan data.

plot area The area bounded by X, Y, and Z axes; for pie charts, the rectangular area surrounding the pie.

plug account An account in which the system stores any out of balance differences between intercompany account pairs during the elimination process.

post stage assignment Assignments in the allocation model that are assigned to locations in a subsequent model stage.

POV (point of view) A feature for setting data focus by selecting members that are not already assigned to row, column, or page axes. For example, selectable POVs in FDM could include location, period, category, and target category. In another example, using POV as a filter in Smart View, you could assign the Currency dimension to the POV and select the Euro member. Selecting this POV in data forms displays data in Euro values.

precalculation Calculating the database prior to user retrieval.

precision Number of decimal places displayed in numbers.

predefined drill paths Paths used to drill to the next level of detail, as defined in the data model.

presentation A playlist of Web Analysis documents, enabling reports to be grouped, organized, ordered, distributed, and reviewed. Includes pointers referencing reports in the repository.

preserve formulas User-created formulas kept within a worksheet while retrieving data.

primary measure A high-priority measure important to your company and business needs. Displayed in the Contents frame.

process monitor report Displays a list of locations and their positions within the FDM data conversion process. You can use the process monitor report to monitor the status of the closing process. The report is time-stamped. Therefore, it can be used to determine to which locations at which time data was loaded.

product In Shared Services, an application type, such as Planning or Performance Scorecard.

Production Reporting *See SQR Production Reporting.*

project An instance of EPM System products grouped together in an implementation. For example, a Planning project may consist of a Planning application, an Essbase cube, and a Financial Reporting server instance.

property A characteristic of an artifact, such as size, type, or processing instructions.

provisioning The process of granting users and groups specific access permissions to resources.

proxy server A server acting as an intermediary between workstation users and the Internet to ensure security.

public job parameters Reusable, named job parameters created by administrators and accessible to users with requisite access privileges.

public recurring time events Reusable time events created by administrators and accessible through the access control system.

PVA *See periodic value method (PVA).*

qualified name A member name in a qualified format that differentiates duplicate member names in a duplicate member outline. For example, [Market].[East].[State].[New York] or [Market].[East].[City].[New York]

query Information requests from data providers. For example, used to access relational data sources.

query governor An Essbase Integration server parameter or Essbase server configuration setting that controls the duration and size of queries made to data sources.

range A set of values including upper and lower limits, and values falling between limits. Can contain numbers, amounts, or dates.

reciprocal assignment An assignment in the financial flow that also has the source as one of its destinations.

reconfigure URL URL used to reload servlet configuration settings dynamically when users are already logged on to the Workspace.

record In a database, a group of fields making up one complete entry. For example, a customer record may contain fields for name, address, telephone number, and sales data.

recurring template A journal template for making identical adjustments in every period.

recurring time event An event specifying a starting point and the frequency for running a job.

redundant data Duplicate data blocks that Essbase retains during transactions until Essbase commits updated blocks.

regular journal A feature for entering one-time adjustments for a period. Can be balanced, balanced by entity, or unbalanced.

Related Accounts The account structure groups all main and related accounts under the same main account number. The main account is distinguished from related accounts by the first suffix of the account number.

relational database A type of database that stores data in related two-dimensional tables. *Contrast with multidimensional database*.

replace A data load option that clears existing values from all accounts for periods specified in the data load file, and loads values from the data load file. If an account is not specified in the load file, its values for the specified periods are cleared.

replicated partition A portion of a database, defined through Partition Manager, used to propagate an update to data mastered at one site to a copy of data stored at another site. Users can access the data as though it were part of their local database.

Report Extractor An Essbase component that retrieves report data from the Essbase database when report scripts are run.

report object In report designs, a basic element with properties defining behavior or appearance, such as text boxes, grids, images, and charts.

report script A text file containing Essbase Report Writer commands that generate one or more production reports.

Report Viewer An Essbase component that displays complete reports after report scripts are run.

reporting currency The currency used to prepare financial statements, and converted from local currencies to reporting currencies.

repository Stores metadata, formatting, and annotation information for views and queries.

resources Objects or services managed by the system, such as roles, users, groups, files, and jobs.

restore An operation to reload data and structural information after a database has been damaged or destroyed, typically performed after shutting down and restarting the database.

restructure An operation to regenerate or rebuild the database index and, in some cases, data files.

result frequency The algorithm used to create a set of dates to collect and display results.

review level A Process Management review status indicator representing the process unit level, such as Not Started, First Pass, Submitted, Approved, and Published.

Risk Free Rate The rate of return expected from “safer” investments such as long-term U.S. government securities.

role The means by which access permissions are granted to users and groups for resources.

roll-up *See consolidation.*

root member The highest member in a dimension branch.

RSC services Services that are configured with Remote Service Configurator, including Repository Service, Service Broker, Name Service, Event Service, and Job Service.

runtime prompt A variable that users enter or select before a business rule is run.

sampling The process of selecting a representative portion of an entity to determine the entity's characteristics. *See also metadata sampling.*

saved assumptions User-defined Planning assumptions that drive key business calculations (for example, the cost per square foot of office floor space).

scaling Scaling determines the display of values in whole numbers, tens, hundreds, thousands, millions, and so on.

scenario A dimension for classifying data (for example, Actuals, Budget, Forecast1, and Forecast2).

scope The area of data encompassed by any Essbase operation or setting; for example, the area of data affected by a security setting. Most commonly, scope refers to three levels of granularity, where higher levels encompass lower levels. From highest to lowest, these levels are as follows: the entire system (Essbase Server), applications on Essbase servers, or databases within Essbase server applications. *See also persistence.*

score The level at which targets are achieved, usually expressed as a percentage of the target.

scorecard Business object that represents the progress of an employee, strategy element, or accountability element toward goals. Scorecards ascertain this progress based on data collected for each measure and child scorecard added to the scorecard.

scraping An inspection of a data source to derive the most basic metadata elements from it. *Contrast with introspection.*

Search gadget Searches the Reporting and Analysis repository. The Search gadget looks for a match in the document keywords and description, which are set when you import a document.

secondary measure A low-priority measure, less important than primary measures. Secondary measures do not have Performance reports but can be used on scorecards and to create dimension measure templates.

security agent A Web access management provider (for example, Netegrity SiteMinder) that protects corporate Web resources.

security platform A framework enabling EPM System products to use external authentication and single sign-on.

serial calculation The default calculation setting. Divides a calculation pass into tasks and calculates one task at a time.

services Resources that enable business items to be retrieved, changed, added, or deleted. Examples: Authorization and Authentication.

servlet A piece of compiled code executable by a Web server.

Servlet Configurator A utility for configuring all locally installed servlets.

shared member A member that shares storage space with another member of the same name, preventing duplicate calculation of members that occur multiple times in an Essbase outline.

Shared Services Registry Part of the Shared Services database, the Shared Services Registry stores and re-uses information for most installed EPM System products, including installation directories, database settings, deployment settings, computer names, ports, servers, URLs, and dependent service data.

Shared Workspace Page Workspace Pages shared across an organization which are stored in a special System folder and can be accessed by authorized users from the Shared Workspace Pages Navigate menu.

sibling A child member at the same generation as another child member and having the same immediate parent. For example, the members Florida and New York are children of East and each other's siblings.

single sign-on Ability to access multiple EPM System products after a single login using external credentials.

smart slice In Smart View, a reusable perspective of a data source that contains a restricted set of dimensions or dimension members.

Smart Space client software Runs on the client's computer and provides gadgets, instant collaboration and access to the Reporting and Analysis repository. It is composed of the Smart Space framework and gadgets.

Smart Space Collaborator A service that enables users or systems to send messages and share Reporting and Analysis repository content. The message can take many forms, including instant message style discussions, meetings, and toast messages.

smart tags Keywords in Microsoft Office applications that are associated with predefined actions available from the Smart Tag menu. In EPM System products, smart tags can also be used to import Reporting and Analysis content, and access Financial Management and Essbase functions.

SmartBook gadget Contains documents from the Reporting and Analysis repository or URLs. All documents are loaded when the SmartBook is opened so you can access all content immediately.

SmartCut A link to a repository item, in URL form.

snapshot Read-only data from a specific time.

source currency The currency from which values originate and are converted through exchange rates to the destination currency.

sparse dimension In block storage databases, a dimension unlikely to contain data for all member combinations when compared to other dimensions. For example, not all customers have data for all products. *Contrast with dense dimension*.

SPF files Printer-independent files created by an SQR Production Reporting server, containing a representation of the actual formatted report output, including fonts, spacing, headers, footers, and so on.

Spotlighter A tool that enables color coding based on selected conditions.

SQL spreadsheet A data object that displays the result set of a SQL query.

SQR Production Reporting A specialized programming language for data access, data manipulation, and creating SQR Production Reporting documents.

stage A task description that forms one logical step within a taskflow, usually performed by an individual. A stage can be manual or automated.

stage action For automated stages, the invoked action that executes the stage.

staging area A database that you create to meet the needs of a specific application. A staging area is a snapshot or restructured version of one or more RDBMSs.

standard dimension A dimension that is not an attribute dimension.

standard journal template A journal function used to post adjustments that have common adjustment information for each period. For example, you can create a standard template that contains the common account IDs, entity IDs, or amounts, then use the template as the basis for many regular journals.

Status bar The status bar at the bottom of the screen displays helpful information about commands, accounts, and the current status of your data file.

stored hierarchy In aggregate storage databases outlines only. A hierarchy in which the members are aggregated according to the outline structure. Stored hierarchy members have certain restrictions, for example, they cannot contain formulas.

strategic objective (SO) A long-term goal defined by measurable results. Each strategic objective is associated with one perspective in the application, has one parent, the entity, and is a parent to critical success factors or other strategic objectives.

Strategy map Represents how the organization implements high-level mission and vision statements into lower-level, constituent strategic goals and objectives.

structure view Displays a topic as a simple list of component data items.

Structured Query Language A language used to process instructions to relational databases.

Subaccount Numbering A system for numbering subaccounts using non-sequential, whole numbers.

subscribe Flags an item or folder to receive automatic notification whenever the item or folder is updated.

Summary chart In the Investigates Section, rolls up detail charts shown below in the same column, plotting metrics at the summary level at the top of each chart column.

super service A special service used by the startCommonServices script to start the RSC services.

supervisor A user with full access to all applications, databases, related files, and security mechanisms for a server.

supporting detail Calculations and assumptions from which the values of cells are derived.

suppress rows Excludes rows containing missing values, and underscores characters from spreadsheet reports.

symmetric multiprocessing (SMP) A server architecture that enables multiprocessing and multithreading. Performance is not significantly degraded when a large number of users connect to an single instance simultaneously.

sync Synchronizes Shared Services and application models.

synchronized The condition that exists when the latest version of a model resides in both the application and in Shared Services. *See also model*.

system extract Transfers data from an application's metadata into an ASCII file.

tabs Navigable views of accounts and reports in Strategic Finance.

target Expected results of a measure for a specified period of time (day, quarter, and so on).

task list A detailed status list of tasks for a particular user.

taskflow The automation of a business process in which tasks are passed from one taskflow participant to another according to procedural rules.

taskflow definition Represents business processes in the taskflow management system. Consists of a network of stages and their relationships; criteria indicating the start and end of the taskflow; and information about individual stages, such as participants, associated applications, associated activities, and so on.

taskflow instance Represents a single instance of a taskflow including its state and associated data.

taskflow management system Defines, creates, and manages the execution of a taskflow including: definitions, user or application interactions, and application executables.

taskflow participant The resource who performs the task associated with the taskflow stage instance for both manual and automated stages.

Taxes - Initial Balances Strategic Finance assumes that the Initial Loss Balance, Initial Gain Balance and the Initial Balance of Taxes Paid entries have taken place in the period before the first Strategic Finance time period.

TCP/IP *See Transmission Control Protocol/Internet Protocol (TCP/IP)*.

template A predefined format designed to retrieve particular data consistently.

text list In Essbase, an object that stores text values mapped to numeric identifiers. Text Lists enable the use of text measures.

text measure A data type that allows measure values to be expressed as text. In Essbase, a member tagged as “Text” in the dimension where measures are represented. The cell values are displayed as predefined text. For example, the text measure "Satisfaction Index" may have the values Low, Medium, and High. *See also typed measure*, *text list*, *derived text measure*.

time dimension Defines the time period that the data represents, such as fiscal or calendar periods.

time events Triggers for execution of jobs.

time line viewer An FDM feature that allows a user to view dates and times of completed process flow steps for specific locations.

time scale Displays metrics by a specific period in time, such as monthly or quarterly.

time series reporting A process for reporting data based on a calendar date (for example, year, quarter, month, or week).

Title bar Displays the Strategic Finance name, the file name, and the scenario name Version box.

toast message Messages that appear in the lower right corner of the screen and fade in and out.

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

top and side labels Column and row headings on the top and sides of a Pivot report.

top-level member A dimension member at the top of the tree in a dimension outline hierarchy, or the first member of the dimension in sort order if there is no hierarchical relationship among dimension members. The top-level member name is generally the same as the dimension name if a hierarchical relationship exists.

trace allocations A feature of Profitability and Cost Management that enables you to visually follow the flow of financial data, either forwards or backwards, from a single intersection throughout the model.

trace level Defines the level of detail captured in the log file.

traceability The ability to track a metadata element to its physical source. For example, in Essbase Studio, a cube schema can be traced from its hierarchies and measure hierarchies, to its dimension elements, date/time elements, and measures, and ultimately, to its physical source elements.

traffic lighting Color-coding of report cells, or pins based on a comparison of two dimension members, or on fixed limits.

transformation (1) Transforms artifacts so that they function properly in the destination environment after application migration. (2) In data mining, modifies data (bidirectionally) flowing between the cells in the cube and the algorithm.

translation *See currency conversion.*

Transmission Control Protocol/Internet Protocol (TCP/IP) A standard set of communication protocols linking computers with different operating systems and internal architectures. TCP/IP utilities are used to exchange files, send mail, and store data to various computers that are connected to local and wide area networks.

transparent login Logs in authenticated users without launching the login screen.

transparent partition A shared partition that enables users to access and change data in a remote database as though it is part of a local database

triangulation A means of converting balances from one currency to another via a third common currency. In Europe, this is the euro for member countries. For example, to convert from French franc to Italian lira, the common currency is defined as European euro. Therefore, in order to convert balances from French franc to Italian lira, balances are converted from French franc to European euro and from European euro to Italian lira.

triggers An Essbase feature whereby data is monitored according to user-specified criteria which when met cause Essbase to alert the user or system administrator.

trusted password A password that enables users authenticated for one product to access other products without reentering their passwords.

trusted user Authenticated user.

tuple MDX syntax element that references a cell as an intersection of a member from each dimension. If a dimension is omitted, its top member is implied. Examples: (Jan); (Jan, Sales); ([Jan], [Sales], [Cola], [Texas], [Actual])

two-pass An Essbase property that is used to recalculate members that are dependent on the calculated values of other members. Two-pass members are calculated during a second pass through the outline.

typed measure In Essbase, a member tagged as “Text” or “Date” in the dimension where measures are represented. The cell values are displayed as predefined text or dates.

unary operator A mathematical indicator (+, -, *, /, %) associated with an outline member. The unary operator defines how the member is calculated during a database roll-up.

Unicode-mode application An Essbase application wherein character text is encoded in UTF-8, enabling users with computers set up for different languages to share application data.

Uniform Resource Locator The address of a resource on the Internet or an intranet.

unique member name A non-shared member name that exists only once in a database outline.

unique member outline A database outline that is not enabled for duplicate member names.

upgrade The process of replacing an earlier software release with a current release or replacing one product with another.

upper-level block A type of data block wherein at least one of the sparse members is a parent-level member.

user directory A centralized location for user and group information. Also known as a repository or provider.

user variable Dynamically renders data forms based on a user's member selection, displaying only the specified entity. For example, user variable named Department displays specific departments and employees.

user-defined attribute (UDA) User-defined attribute, associated with members of an outline to describe a characteristic of the members. Users can use UDAs to return lists of members that have the specified UDA associated with them.

user-defined member list A named, static set of members within a dimension defined by the user.

validation A process of checking a business rule, report script, or partition definition against the outline to make sure that the object being checked is valid. For example, in FDM, validation rules ensure that certain conditions are met after data is loaded from FDM to the target application.

value dimension Used to define input value, translated value, and consolidation detail.

variance Difference between two values (for example, planned and actual value).

varying attribute An attribute association that changes over one or more dimensions. It can be used to track a value in relation to these dimensions; for example, the varying attribute Sales Representative, associated with the Product dimension, can be used to track the value Customer Sales of several different sales representatives in relation to the Time dimension. Varying attributes can also be used for member selection, such as finding the Products that a Sales Representative was responsible for in May.

version Possible outcome used within the context of a scenario of data. For example, Budget - Best Case and Budget - Worst Case where Budget is scenario and Best Case and Worst Case are versions.

view Representation of either a year-to-date or periodic display of data.

visual cue A formatted style, such as a font or a color, that highlights specific types of data values. Data values may be dimension members; parent, child, or shared members; dynamic calculations; members containing a formula; read only data cells; read and write data cells; or linked objects.

Web server Software or hardware hosting intranet or Internet Web pages or Web applications.

weight Value assigned to an item on a scorecard that indicates the relative importance of that item in the calculation of the overall scorecard score. The weighting of all items on a scorecard accumulates to 100%. For example, to recognize the importance of developing new features for a product, the measure for New Features Coded on a developer's scorecard would be assigned a higher weighting than a measure for Number of Minor Defect Fixes.

wild card Character that represents any single character or group of characters (*) in a search string.

WITH section In MaxL DML, an optional section of the query used for creating re-usable logic to define sets or members. Sets or custom members can be defined once in the WITH section, and then referenced multiple times during a query.

work flow The steps required to process data from start to finish in FDM. The workflow consists of Import (loading data from the GL file), Validate (ensures all members are mapped to a valid account), Export (loads the mapped members to the target application), and Check (verifies accuracy of data by processing data with user-defined validation rules).

workbook An entire spreadsheet file with many worksheets.

Workspace Page A page created with content from multiple sources including documents, URL, and other content types. Enables a user to aggregate content from Oracle and non-Oracle sources.

write-back The ability for a retrieval client, such as a spreadsheet, to update a database value.

ws.conf A configuration file for Windows platforms.

wsconf_platform A configuration file for UNIX platforms.

XML *See Extensible Markup Language (XML).*

XOLAP An Essbase multidimensional database that stores only the outline metadata and retrieves all data from a relational database at query time. XOLAP supports aggregate storage databases and applications that contain duplicate member names.

Y axis scale Range of values on Y axis of charts displayed in Investigate Section. For example, use a unique Y axis scale for each chart, the same Y axis scale for all Detail charts, or the same Y axis scale for all charts in the column. Often, using a common Y axis improves your ability to compare charts at a glance.

Zero Administration Software tool that identifies version number of the most up-to-date plug-in on the server.

zoom Sets the magnification of a report. For example, magnify a report to fit whole page, page width, or percentage of magnification based on 100%.

ZoomChart Used to view detailed information by enlarging a chart. Enables you to see detailed numeric information on the metric that is displayed in the chart.

Index