Oracle® Business Intelligence Applications

Security Guide

11g Release 1 (11.1.1.8.1)

E51484-01

March 2014

Explains security considerations for Oracle BI Applications.

Oracle Business Intelligence Applications Security Guide, 11g Release 1 (11.1.1.8.1)

E51484-01

Primary Author: P Brownbridge

Contributors: Oracle Business Intelligence development, product management, and quality assurance teams.

Contents

A Configuring Security

Preface

Oracle Business Intelligence Applications is a comprehensive suite of prebuilt solutions that deliver pervasive intelligence across an organization, empowering users at all levels - from front line operational users to senior management - with the key information they need to maximize effectiveness. Intuitive and role-based, these solutions transform and integrate data from a range of enterprise sources and corporate data warehouses into actionable insight that enables more effective actions, decisions, and processes.

Oracle BI Applications is built on Oracle Business Intelligence Suite Enterprise Edition (Oracle BI EE), a comprehensive set of enterprise business intelligence tools and infrastructure, including a scalable and efficient query and analysis server, an ad-hoc query and analysis tool, interactive dashboards, proactive intelligence and alerts, and an enterprise reporting engine.

Audience

This document is intended for BI managers and implementors of Oracle BI Applications who are responsible for managing Oracle BI Applications security. It contains information describing Oracle BI Applications security and its preconfigured implementation.

Documentation Accessibility

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

Access to Oracle Support

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

Related Documentation

See the Oracle Business Intelligence Applications documentation library at `http://docs.oracle.com/cd/E51479_01/index.htm` for a list of related Oracle Business Intelligence Applications documents.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

New Features for Oracle BI Applications Security Administrators

This preface describes new features in Oracle Business Intelligence Applications that relate to security.

New Features for Oracle BI Applications Release 11.1.1.8.1

Endeca Integration

This release supports Endeca. For security setup information relating to Endeca, refer to the Endeca chapter in *Oracle Business Intelligence Applications Administration Guide*.

New Features for Oracle BI Applications Release 11.1.1.7.1

Functional Setup Manager Security Tasks

Security for Offerings in Oracle BI Applications is configured using guidance in informational Functional Setup Manager (FSM) tasks.

1 Integrating Security for Oracle BI Applications

This chapter is aimed at security administrators, and explains how to set up and maintain security for Oracle Business Intelligence Applications.

This chapter contains the following topics:

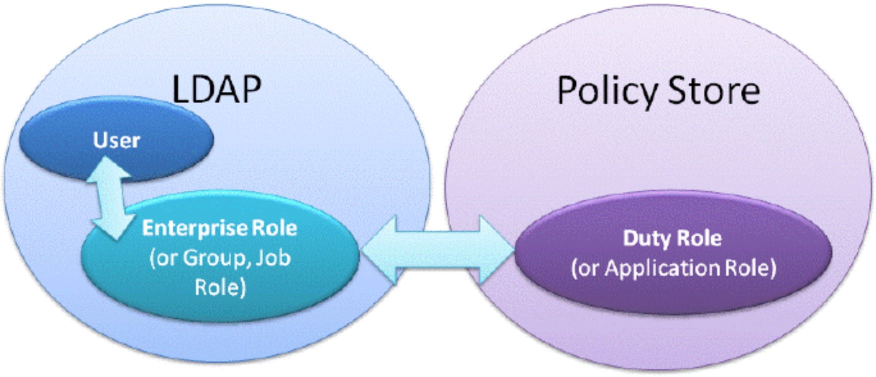
1.1 Introduction

This section contains the following topics:

1.1.1 About Terminology Used In Security

As you familiarize yourself with security concepts across different parts of the BI stack, note the following differences in terminology that are used in software and documentation.

Figure 1–1 Terminology Differences Across The BI Stack



- Enterprise Roles are also referred to as Groups, or Job Roles. For example:

  - the term Enterprise Role is used in this guide, and in Fusion Applications.

  - the term Group is used in Oracle WebLogic Server Administration Console and Oracle BI Administration Tool.

  This guide uses the term Enterprise Role unless referring to tools that use the term Group or Job Role.

- Duty Roles are also referred to as Application Roles. For example:

  - the term Duty Role is used in this guide and in Fusion Applications.

  - the term Application Role is used in Oracle Enterprise Manager Fusion Middleware Control and Oracle Weblogic Server Administration Console.

  This guide uses the term Duty Role unless referring to tools that use the term Application Role.

- Lightweight Directory Access Protocol (LDAP) refers to the Authentication Provider. For example, Oracle WebLogic Server, Oracle Internet Directory (OID), or a proprietary LDAP server and tools.

1.1.2 What Security Components Are Installed By Default?

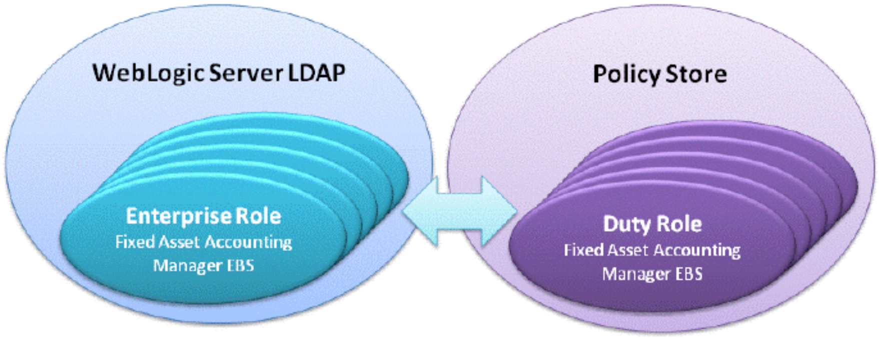
After installing Oracle BI Applications on the Oracle BI EE platform, you get the following ready-to-use security components (as described in Figure 1–2):

- Oracle WebLogic Server LDAP, containing a set of default Enterprise Roles.

  This LDAP also contains system Users that are required for BI components.

- A Policy Store that contains default Duty Roles for all of the Offerings, Functional Areas, and Modules that are available in Oracle BI Applications.

Figure 1–2 Default Weblogic Server LDAP and Policy Store



Using the Default Weblogic Server LDAP and Policy Store

This guide explains how to use the default WebLogic Server LDAP and Policy Store to deploy Oracle BI Applications. For example, you might use the default security components for testing, and then migrate the Users and Enterprise Roles to a different LDAP (for example, Oracle Internet Directory) for production.

Using a Different LDAP and/or Policy Store

If you to deploy a different LDAP, such as Oracle Internet Directory, then you can migrate Users and Enterprise Roles from WebLogic Server LDAP to that LDAP.

1.1.3 High Level Steps for Setting Up Security in Oracle BI Applications

To set up security in Oracle BI Applications, you must do the following:

1. Read the rest of Section 1.1, 'Introduction' to get an overview of security concepts, tools, and terminology.

   In particular, familiarize yourself with Duty Roles and how they control user privileges by reading Section 1.1.6, "Managing Duty Roles in Oracle BI Applications" and Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

   Note: This content in this guide supplements *Oracle Business Intelligence Security Guide*, and contains additional security information that is specific to Oracle BI Applications running on Oracle Business Intelligence Enterprise Edition.

2. During Oracle BI Applications installation, the provisioning process creates a set of default Enterprise Roles in the Oracle WebLogic Server LDAP that is embedded by default, and a set of default Duty Roles in the Policy Store.

3. Create a user account in LDAP for each Oracle BI Applications Configuration Manager, Functional Setup Manager (FSM), and ODI User, and assign an appropriate Duty Role to each User.

   For information about which Duty Roles to use, see Section 1.4.1, "Security Overview of Oracle BI Applications Configuration Manager and Functional Setup Manager".

   For example:

   - A User for administration in FSM must be assigned to an Enterprise Role associated with the Duty Role 'BIA_ADMINISTRATOR_DUTY'.

- A User for Load Plan administration in Oracle BI Applications Configuration Manager must be assigned to an Enterprise Role associated with the Duty Role 'BIA_LOAD_PLAN_DEVELOPER_DUTY'.

- A User for Implementation Plan administration in FSM must be assigned to an Enterprise Role associated with the Duty Role 'BIA_IMPLEMENTATION_MANAGER_DUTY'.

4. Create a user account in LDAP for every BI dashboard and report user (BI Users).
5. Assign each BI User to the appropriate Enterprise Roles.

   To provision BI Users for the Offerings that you are deploying, use Functional Setup Manager (FSM) Tasks to set up security for your Offerings and Functional Areas. For information about using FSM Tasks to configure security, see Section 1.2, "Using Oracle BI Applications Functional Setup Manager Informational Tasks to Set Up Security".

   For each Offering and Functional Area, the FSM Tasks for security typically specify:

   - Init Blocks that you need to enable.

   - Duty Roles that BI Users require.

   - Additional setup steps to perform (where required).

   In addition to the information in the FSM Tasks for security, use *Content Guide for Oracle BI Applications* for a definitive list of default Duty Roles and Enterprise Roles required by BI Users (refer to Tech Note 1639479.1 on My Oracle Support).

   For more information about provisioning BI Users, refer to the following:

   - If you are using FMW provisioning, then refer to Section A.1.13.1, "How to Use Fusion Middleware (FMW) to Provision a BI User", as follows:

     - If you are using the default Oracle WebLogic Server LDAP, then assign each BI User to the appropriate Enterprise Role for the Duty Role that the BI User requires, as described in Section A.1.13.1.1, "How to provision BI Users in the installed Oracle Weblogic Server LDAP".

     - If you are using your own LDAP, then:

       - if required, transfer the default Enterprise Roles from Oracle WebLogic Server LDAP to your LDAP.

       - assign each BI User to an appropriate Enterprise Role, and make sure that this Enterprise Role is associated with the Duty Role that the BI User requires, as described in Section A.1.13.1.2, "How to provision BI Users using your own LDAP".

   - If you are using RPD Initialization Blocks for provisioning, then refer to Section A.1.13.2, "How to Use An RPD Init Block to Provision a BI User".

1.1.4 What Tools Configure Security in Oracle Business Intelligence Applications?

You use the following tools to manage security settings in Oracle Business Intelligence Applications:

- Oracle BI Applications Functional Setup Manager (FSM)

  Use Oracle BI Applications Functional Setup Manager informational tasks to set up security for Oracle BI Applications offerings and modules.

For a summary of how FSM Tasks are used to configure security, see Section 1.2, "Using Oracle BI Applications Functional Setup Manager Informational Tasks to Set Up Security".

- Oracle BI Administration Tool

  Use Oracle BI Administration Tool to perform tasks such as setting permissions for business models, tables, columns, and subject areas; specifying filters to limit data accessibility; and setting authentication options. For detailed information, see *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition*.

- Oracle BI Presentation Services Administration

  Use Oracle BI Presentation Services Administration to perform tasks such as setting permissions to Presentation Catalog objects, including dashboards and dashboard pages. For detailed information, see *Oracle Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition*.

- Oracle Enterprise Manager Fusion Middleware Control

  Use Fusion Middleware Control to manage the policy store, Duty Roles, and permissions for determining functional access. For detailed information, see *Oracle Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition*.

- Oracle WebLogic Server Administration Console

  Use the Administration Console to manage Users and Enterprise Roles/Groups in the Oracle WebLogic Server LDAP. You can also use the Administration Console to manage security realms, and to configure alternative authentication providers. For detailed information, see *Oracle Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition*.

1.1.5 What Security Levels Does Oracle BI Applications Use?

Security in Oracle BI Applications can be classified broadly into the following three levels:

- **Object-level security.** Object-level security controls the visibility to business logical objects based on a user's role. You can set up object-level security for metadata repository objects, such as business models and subject areas, and for Web objects, such as dashboards and dashboard pages, which are defined in the Presentation Catalog. For more information, see Section 1.4.5, "About Object-Level Security."

- **Data-level security.** Data-level security controls the visibility of data (content rendered in subject areas, dashboards, Oracle BI Answers, and so on) based on the user's association to data in the transactional system. For more information, see Section 1.4.6, "About Data-Level Security."

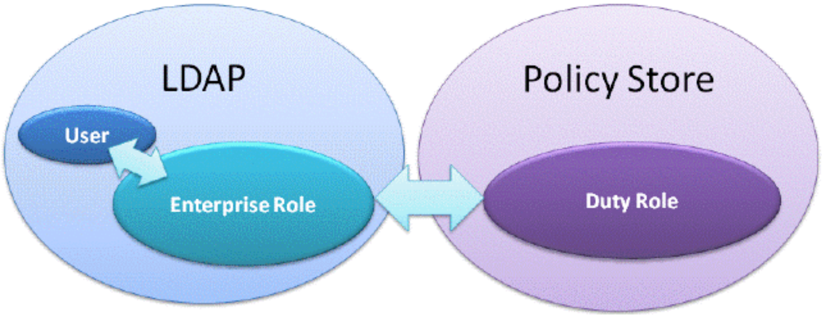
- **User-level security (authentication of users).** User-level security refers to authentication and confirmation of the identity of a user based on the credentials provided. For more information, see Section 1.4.7, "About User-Level Security."

1.1.6 Managing Duty Roles in Oracle BI Applications

Object-level and data-level security are implemented in Oracle BI Applications using Duty Roles in the Policy Store. Duty Roles define a set of permissions granted typically to an Enterprise Role.

Figure 1–3 illustrates how Users are assigned to Enterprise Roles in the LDAP, which are associated with Duty Roles in the Policy Store.

Figure 1–3 Relationship between Users, Enterprise Roles, and Duty Roles



Duty Roles are typically related to either data or object security. For example, the Oracle BI Applications repository (OracleBIAnalyticsApps.rpd) uses the following Duty Roles:

- The *HR Org-based Security* Duty Role is used to control access to human resources data at the data security level.
- The *Human Resources Analyst* Duty Role is used to control Presentation layer object visibility for the Human Resources Analyst role at the object security level.

You can use a number of BI tools to view pre-configured Duty Roles, as follows:

- Oracle BI Administration Tool

  To view pre-configured Duty Roles using Oracle BI Administration Tool, open the RPD, select **Manage**, then select **Identity**. Duty Roles are visible in the Identity Manager dialog in online mode. In offline mode, only Duty Roles that have had permissions, filters, or query limits set for them appear. For this reason, it is recommended that when you work with data access security in the Oracle BI Applications repository, you use online mode.
- Oracle Enterprise Manager Fusion Middleware Control - for details, see Section 1.1.6.1, "How to View Duty Roles for Oracle BI Applications".
- Oracle Authorization Policy Manager - In Oracle APM, navigate to the 'obi' Application and use the Search options to locate Duty Roles prefixed with 'OBIA_'. Select a Duty Role, then click Open to display the <*Application*> | Application Role dialog. Display the External Role Mapping tab, and check that the role list contains the appropriate Enterprise Roles.

The standard hierarchical structure of Duty Roles and users in Oracle BI Applications is typically the following: data security Duty Role, then object security Duty Role, then Enterprise Role (also called Group), then User. It is a best practice to use this structure when setting up security.

Security administrators can view, modify, and create Duty Roles in Oracle Enterprise Manager Fusion Middleware Control.

For example, BI User Fred has Enterprise Role 'Fixed Asset Accounting Manager EBS'. To provision Fred with security access for Fixed Assets Accounting reporting for EBS, you edit the BI Duty Role 'Fixed Asset Accounting Manager EBS' and add Enterprise Role 'Fixed Asset Accounting Manager EBS' as a Member.

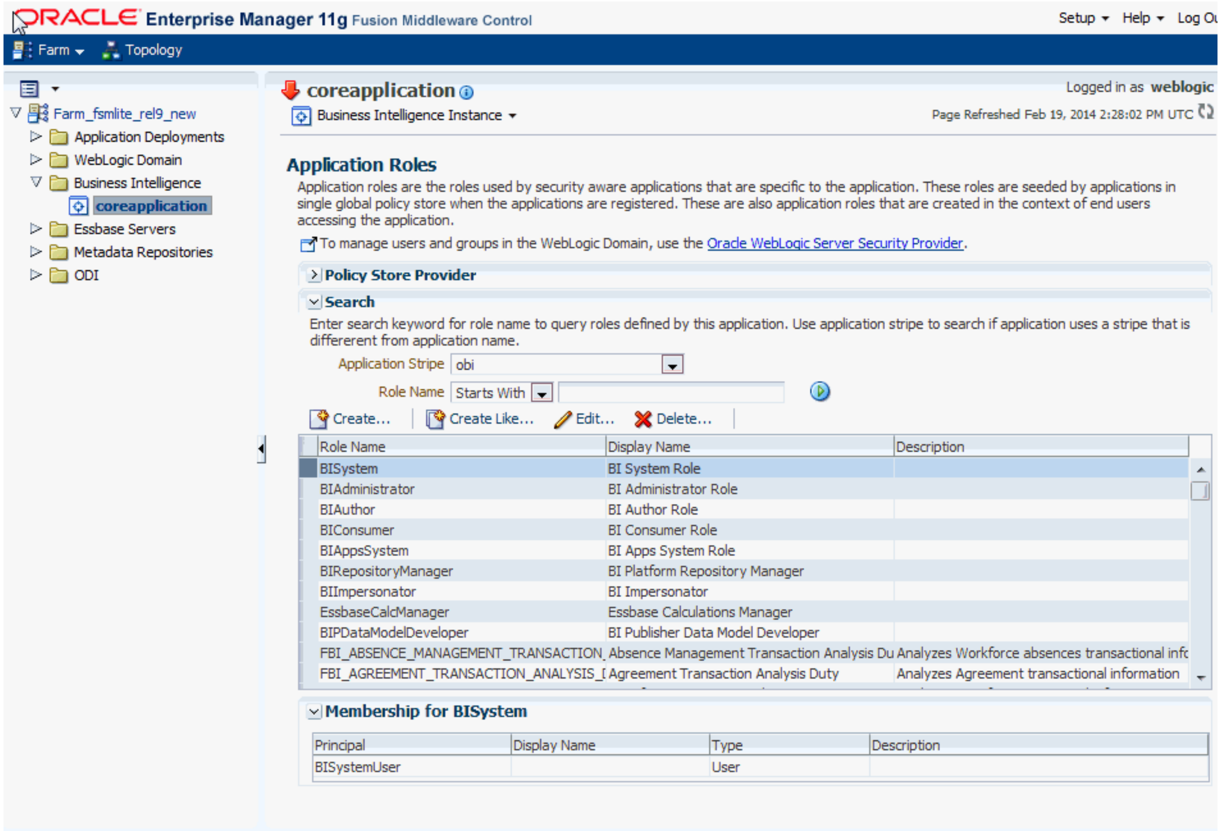
1.1.6.1 How to View Duty Roles for Oracle BI Applications

To view Duty Roles:

1. Log in to Oracle Enterprise Manager Fusion Middleware Control as an administrator.

2. Expand Business Intelligence, right-click coreapplication, and select Security, then Application Roles.

   The available Duty Roles are listed. The **Membership for <Duty Role name>** area displays Enterprise Roles or other Duty Roles that are associated with the selected Duty Role.



Logged in as weblogic

Page Refreshed Feb 19, 2014 2:28:02 PM UTC

Application Roles

Application roles are the roles used by security aware applications that are specific to the application. These roles are seeded by applications in single global policy store when the applications are registered. These are also application roles that are created in the context of end users accessing the application.

To manage users and groups in the WebLogic Domain, use the Oracle WebLogic Server Security Provider.

Enter search keyword for role name to query roles defined by this application. Use application stripe to search if application uses a stripe that is differerent from application name.

Application Stripe: obi

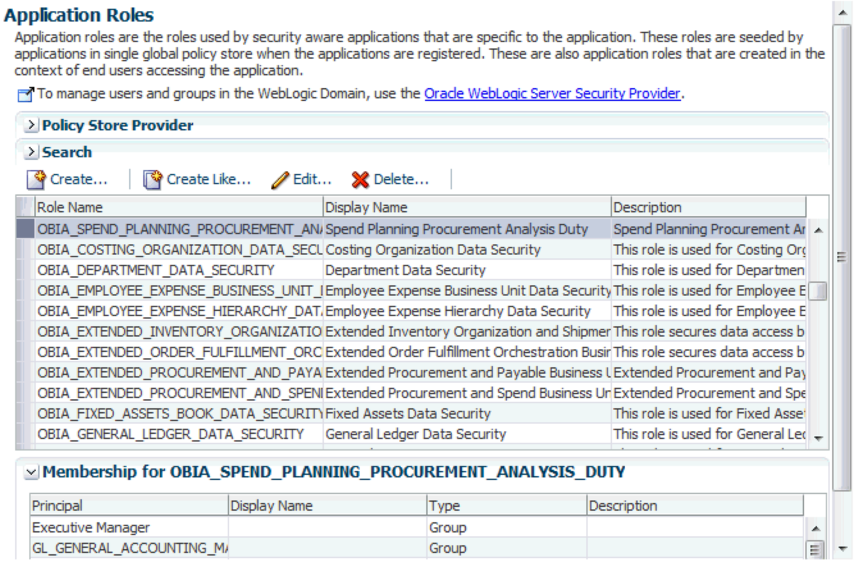
Role Name: Starts With

Role Name	Display Name	Description
BISystem	BI System Role	
BIAdministrator	BI Administrator Role	
BIAuthor	BI Author Role	
BIConsumer	BI Consumer Role	
BIAppsSystem	BI Apps System Role	
BIRepositoryManager	BI Platform Repository Manager	
BIImpersonator	BI Impersonator	
EssbaseCalcManager	Essbase Calculations Manager	
BIPDataModelDeveloper	BI Publisher Data Model Developer	
FBI_ABSENCE_MANAGEMENT_TRANSACTION_	Absence Management Transaction Analysis Du	Analyzes Workforce absences transactional infc
FBI_AGREEMENT_TRANSACTION_ANALYSIS_[	Agreement Transaction Analysis Duty	Analyzes Agreement transactional information

Membership for BISystem

Principal	Display Name	Type	Description
BISystemUser		User	

The screenshot below shows an example of additional pre-defined Duty Roles that are created when Oracle BI Applications is installed. The list of Duty Roles depends on your installation.



Application Roles

Application roles are the roles used by security aware applications that are specific to the application. These roles are seeded by applications in single global policy store when the applications are registered. These are also application roles that are created in the context of end users accessing the application.

To manage users and groups in the WebLogic Domain, use the Oracle WebLogic Server Security Provider.

Role Name	Display Name	Description
OBIA_SPEND_PLANNING_PROCUREMENT_AN/	Spend Planning Procurement Analysis Duty	Spend Planning Procurement Ar
OBIA_COSTING_ORGANIZATION_DATA_SECL	Costing Organization Data Security	This role is used for Costing Or(
OBIA_DEPARTMENT_DATA_SECURITY	Department Data Security	This role is used for Departmen
OBIA_EMPLOYEE_EXPENSE_BUSINESS_UNIT_I	Employee Expense Business Unit Data Security	This role is used for Employee E
OBIA_EMPLOYEE_EXPENSE_HIERARCHY_DAT/	Employee Expense Hierarchy Data Security	This role is used for Employee E
OBIA_EXTENDED_INVENTORY_ORGANIZATIO	Extended Inventory Organization and Shipmer	This role secures data access b
OBIA_EXTENDED_ORDER_FULFILLMENT_ORC	Extended Order Fulfillment Orchestration Busir	This role secures data access b
OBIA_EXTENDED_PROCUREMENT_AND_PAYA	Extended Procurement and Payable Business l	Extended Procurement and Pay
OBIA_EXTENDED_PROCUREMENT_AND_SPENI	Extended Procurement and Spend Business Ur	Extended Procurement and Spe
OBIA_FIXED_ASSETS_BOOK_DATA_SECURITY	Fixed Assets Data Security	This role is used for Fixed Asse
OBIA_GENERAL_LEDGER_DATA_SECURITY	General Ledger Data Security	This role is used for General Le(

Membership for OBIA_SPEND_PLANNING_PROCUREMENT_ANALYSIS_DUTY

Principal	Display Name	Type	Description
Executive Manager		Group	
GL_GENERAL_ACCOUNTING_M/		Group	

1.1.6.2 How to Provision BI Users with Duty Roles

To provision a BI User with a Duty Role, you first assign the User to an Enterprise Role/Group in LDAP, then make sure that the Enterprise Role/Group is associated with the appropriate Duty Role in the Policy Store.

If you are using the default embedded Enterprise Roles in Oracle WebLogic Server LDAP, then these Enterprise Roles are associated with the appropriate Duty Roles by default, and no further configuration is required.

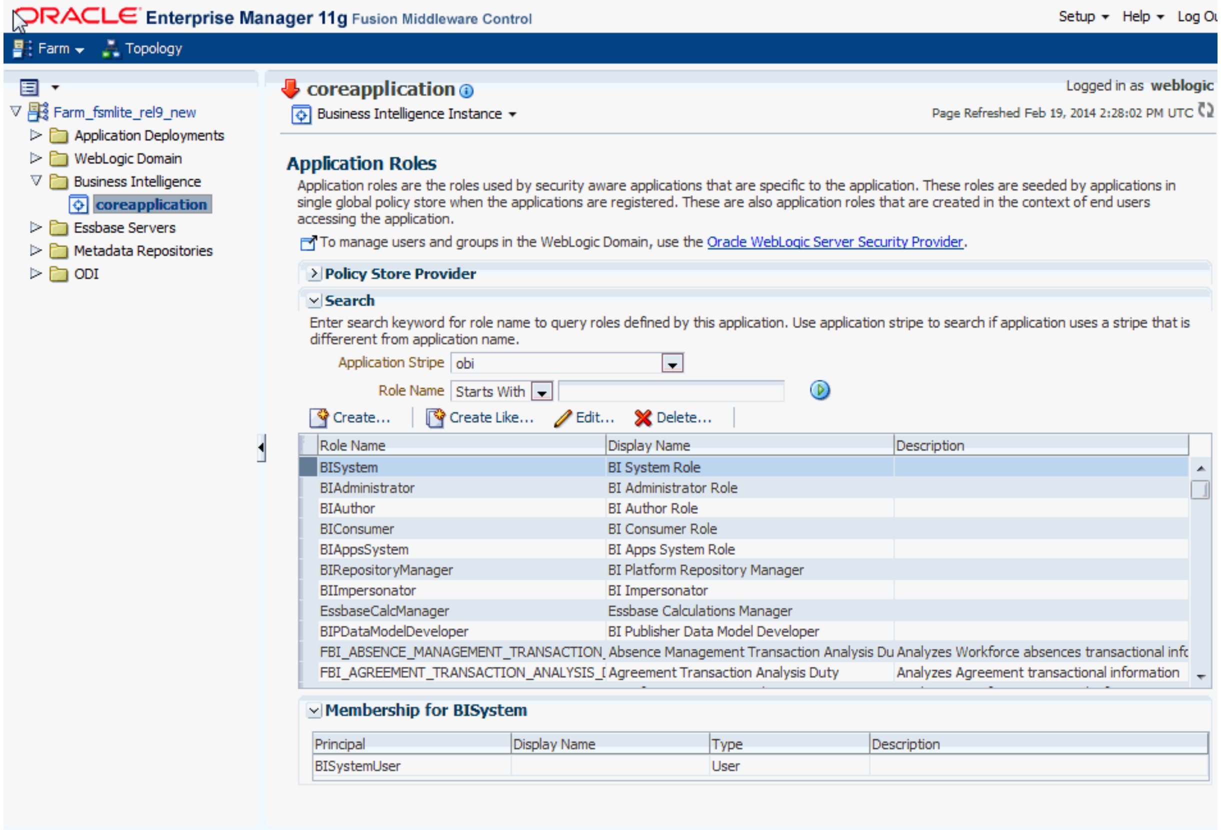
If you are using a different LDAP with your own set of Enterprise Roles, then you need to make sure that these are associated with the appropriate Duty Roles, by following the steps below.

To provision BI Users with Duty Roles:

1. Log in to Oracle Enterprise Manager Fusion Middleware Control as an administrator.

2. Expand Business Intelligence, right-click coreapplication, and select Security, then Application Roles.

   A list of available Duty Roles is displayed.



Application Roles

Application roles are the roles used by security aware applications that are specific to the application. These roles are seeded by applications in single global policy store when the applications are registered. These are also application roles that are created in the context of end users accessing the application.

To manage users and groups in the WebLogic Domain, use the Oracle WebLogic Server Security Provider.

Enter search keyword for role name to query roles defined by this application. Use application stripe to search if application uses a stripe that is differerent from application name.

Application Stripe: obi

Role Name: Starts With

Role Name	Display Name	Description
BISystem	BI System Role	
BIAdministrator	BI Administrator Role	
BIAuthor	BI Author Role	
BIConsumer	BI Consumer Role	
BIAppsSystem	BI Apps System Role	
BIRepositoryManager	BI Platform Repository Manager	
BIImpersonator	BI Impersonator	
EssbaseCalcManager	Essbase Calculations Manager	
BIPDataModelDeveloper	BI Publisher Data Model Developer	
FBI_ABSENCE_MANAGEMENT_TRANSACTION_	Absence Management Transaction Analysis Du	Analyzes Workforce absences transactional infc
FBI_AGREEMENT_TRANSACTION_ANALYSIS_I	Agreement Transaction Analysis Duty	Analyzes Agreement transactional information

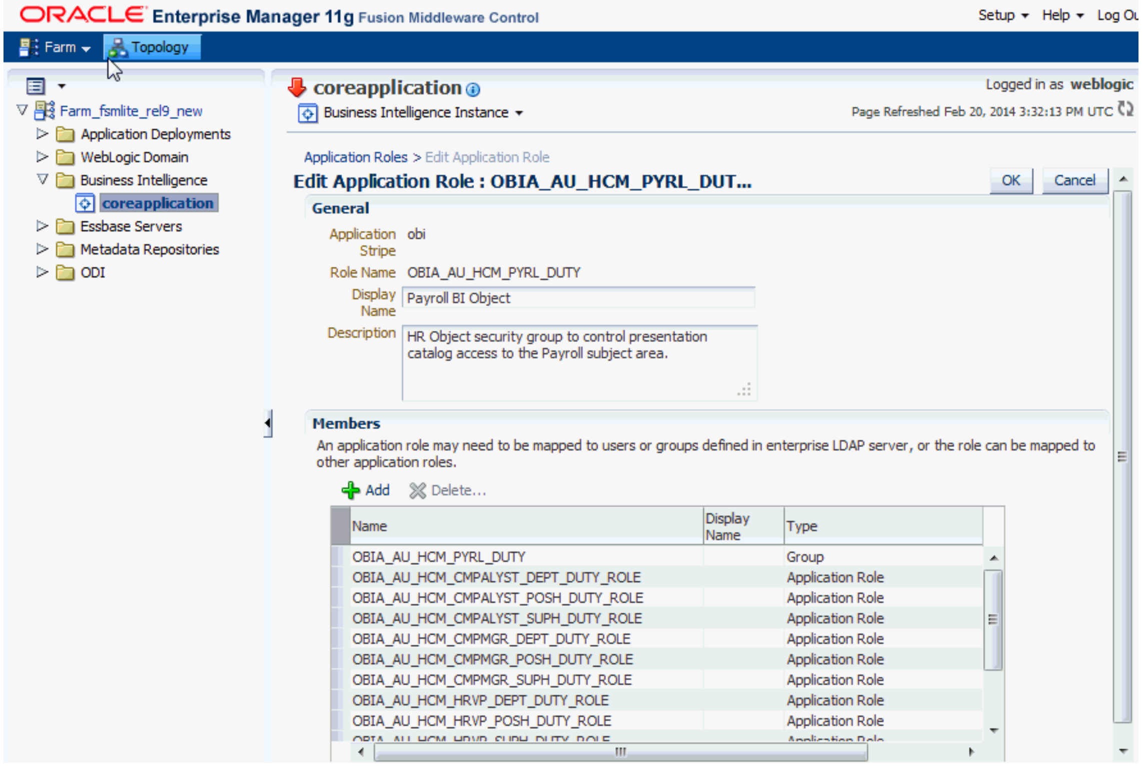
Membership for BISystem

Principal	Display Name	Type	Description
BISystemUser		User	

3. To provision a BI User with a Duty Role:

   a. Select the Duty Role that a BI User requires access to.

   b. Click Edit to display the Edit Application Role dialog.



Edit Application Role : OBIA_AU_HCM_PYRL_DUT...

General

Application Stripe: obi

Role Name: OBIA_AU_HCM_PYRL_DUTY

Display Name: Payroll BI Object

Description: HR Object security group to control presentation catalog access to the Payroll subject area.

Members

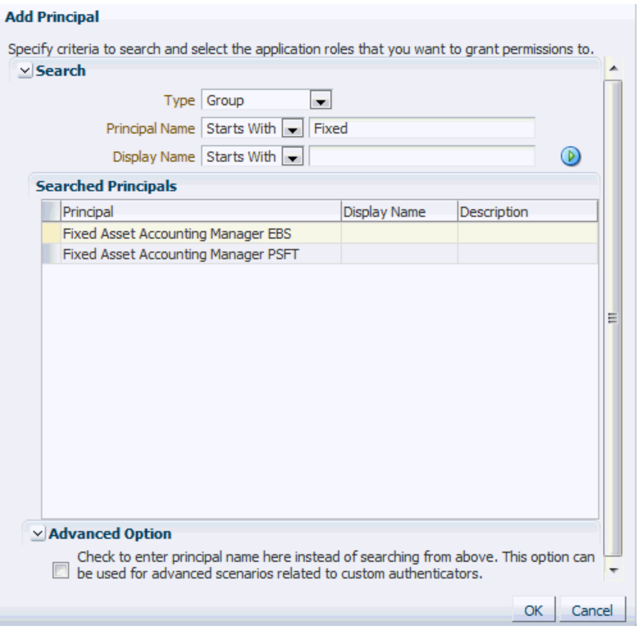
An application role may need to be mapped to users or groups defined in enterprise LDAP server, or the role can be mapped to other application roles.

Name	Display Name	Type
OBIA_AU_HCM_PYRL_DUTY		Group
OBIA_AU_HCM_CMPALYST_DEPT_DUTY_ROLE		Application Role
OBIA_AU_HCM_CMPALYST_POSH_DUTY_ROLE		Application Role
OBIA_AU_HCM_CMPALYST_SUPH_DUTY_ROLE		Application Role
OBIA_AU_HCM_CMPMGR_DEPT_DUTY_ROLE		Application Role
OBIA_AU_HCM_CMPMGR_POSH_DUTY_ROLE		Application Role
OBIA_AU_HCM_CMPMGR_SUPH_DUTY_ROLE		Application Role
OBIA_AU_HCM_HRVP_DEPT_DUTY_ROLE		Application Role
OBIA_AU_HCM_HRVP_POSH_DUTY_ROLE		Application Role
OBIA_AU_HCM_HRVP_SUPH_DUTY_ROLE		Application Role

c. In the Member list, click Add to display the Add Principal dialog.

d. Use the Search area to locate and select the Enterprise Role/Group that the BI User has.

For example, User Fred has Enterprise Role 'Fixed Asset Accounting Manager EBS'. To provision Fred with security access for Fixed Assets Accounting reporting for EBS, you edit the BI Duty Role 'Fixed Asset Accounting Manager EBS' and add Enterprise Role 'Fixed Asset Accounting Manager EBS' as a Member.



Add Principal

Specify criteria to search and select the application roles that you want to grant permissions to.

Search

Type: Group

Principal Name: Starts With | Fixed

Display Name: Starts With

Searched Principals

Principal	Display Name	Description
Fixed Asset Accounting Manager EBS		
Fixed Asset Accounting Manager PSFT		

Advanced Option

□ Check to enter principal name here instead of searching from above. This option can be used for advanced scenarios related to custom authenticators.

e. Click OK.

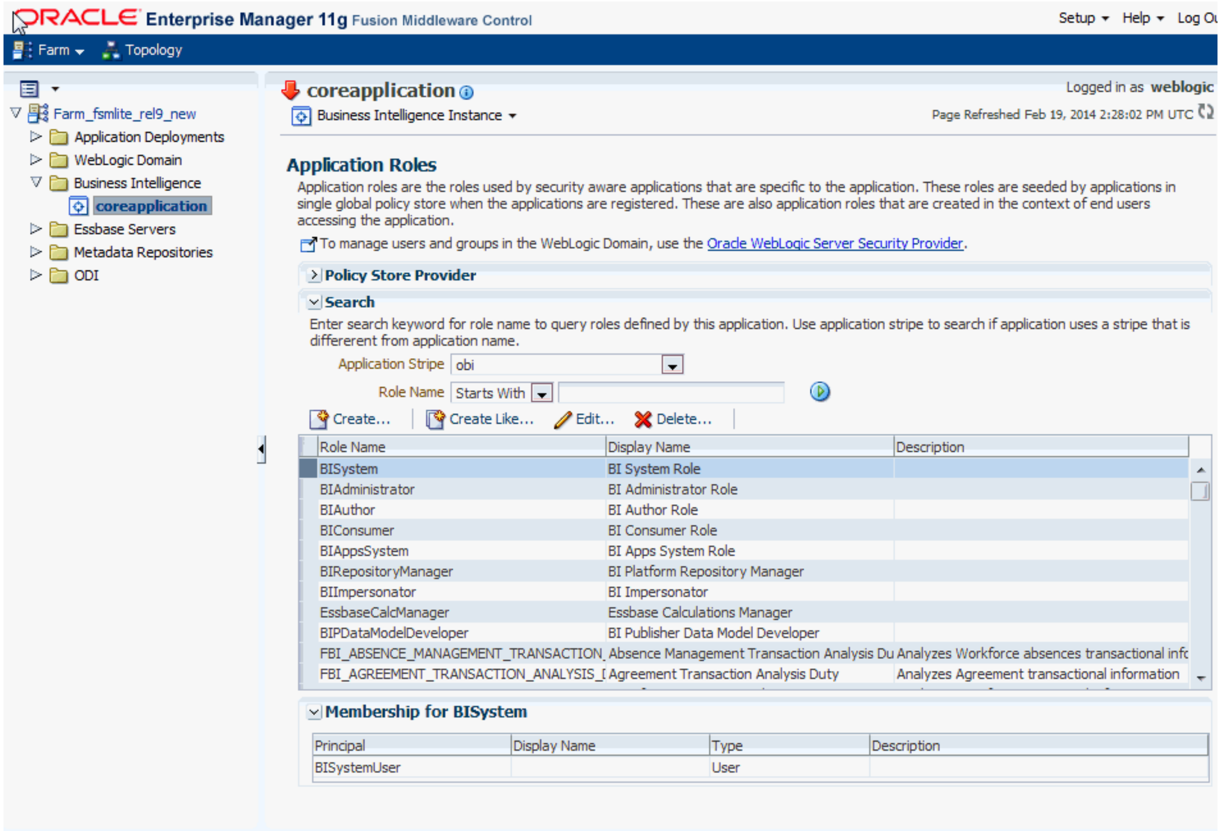
1.1.6.3 How to Edit or Create Duty Roles for Oracle BI Applications

To edit or create Duty Roles:

1. Log in to Oracle Enterprise Manager Fusion Middleware Control as an administrator.

2. Expand Business Intelligence, right-click coreapplication, and select Security, then Application Roles.

   A list of available Duty Roles is displayed.



coreapplication

Logged in as **weblogic**

Page Refreshed Feb 19, 2014 2:28:02 PM UTC

Application Roles

Application roles are the roles used by security aware applications that are specific to the application. These roles are seeded by applications in single global policy store when the applications are registered. These are also application roles that are created in the context of end users accessing the application.

To manage users and groups in the WebLogic Domain, use the Oracle WebLogic Server Security Provider.

Enter search keyword for role name to query roles defined by this application. Use application stripe to search if application uses a stripe that is differerent from application name.

Application Stripe: obi

Role Name: Starts With

Role Name	Display Name	Description
BISystem	BI System Role	
BIAdministrator	BI Administrator Role	
BIAuthor	BI Author Role	
BIConsumer	BI Consumer Role	
BIAppsSystem	BI Apps System Role	
BIRepositoryManager	BI Platform Repository Manager	
BIImpersonator	BI Impersonator	
EssbaseCalcManager	Essbase Calculations Manager	
BIPDataModelDeveloper	BI Publisher Data Model Developer	
FBI_ABSENCE_MANAGEMENT_TRANSACTION_	Absence Management Transaction Analysis Du	Analyzes Workforce absences transactional infc
FBI_AGREEMENT_TRANSACTION_ANALYSIS_[	Agreement Transaction Analysis Duty	Analyzes Agreement transactional information

Membership for BISystem

Principal	Display Name	Type	Description
BISystemUser		User	

3. To edit a Duty Role:

   a. In the **Application Roles** list, select the Duty Role that you want to edit.

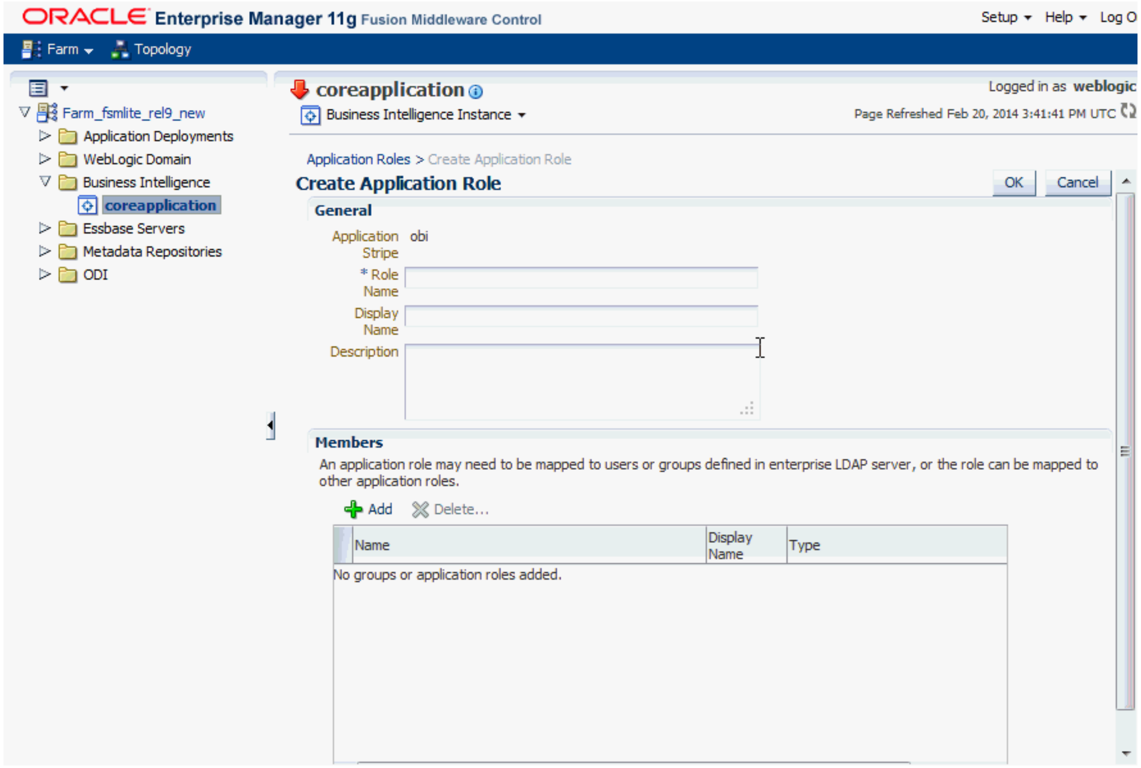
   b. Click **Edit...**

   c. Use the Edit Application Role dialog to change the details, then click OK.

4. To create a Duty Role:

   a. Click **Create...** to display the Create Application Role dialog.

      Alternatively, select a Duty Role similar to the one that you want to create, and click **Create Like**. Using **Create Like** copies the default Members (that is, Enterprise Roles/Groups).



coreapplication

Business Intelligence Instance

Logged in as **weblogic**

Page Refreshed Feb 20, 2014 3:41:41 PM UTC

Application Roles > Create Application Role

Create Application Role

OK Cancel

General

Application Stripe	obi
* Role Name	
Display Name	
Description	

Members

An application role may need to be mapped to users or groups defined in enterprise LDAP server, or the role can be mapped to other application roles.

Add Delete...

Name	Display Name	Type
No groups or application roles added.		

b. Use the General area to specify the details.

c. In the Member list, click **Add** to search for and select the Enterprise Roles/Groups that you want this Duty Role to be associated with.

d. Click OK.

1.1.6.4 Authorizing User Access Using Roles

It is possible to grant multiple Duty Roles to a User; however Oracle recommends that Enterprise Roles are defined so that a User is provisioned with a single Duty Role.

If you have Oracle Business Intelligence Enterprise Edition test servers configured against a test LDAP, and the production servers are configured against the corporate LDAP, but the test LDAP is *not* a fan-out copy of the corporate LDAP directory, then you must refresh the LDAP GUIDs. See "Refreshing User GUIDs" in *Oracle Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition* for more information. Note that while LDAP is required for Fusion Applications environments, it is optional for other source applications.

1.1.7 About Provisioning BI End Users

BI Users are provisioned with BI Duty Roles using Enterprise Roles in the LDAP. To provision users, you typically use either Oracle Fusion Middleware, or RPD initialization blocks.

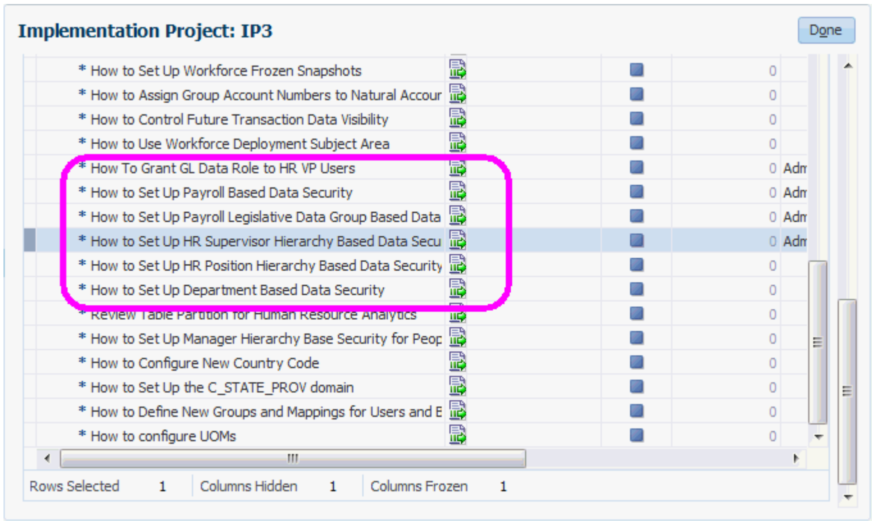
For more information about how to provision BI Users, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

1.2 Using Oracle BI Applications Functional Setup Manager Informational Tasks to Set Up Security

To set up security for Offerings in Oracle BI Applications, you use Functional Setup Manager (FSM) to manage the security tasks. When you create an Implementation Plan in FSM for a particular Functional Area, FSM provides a list of tasks required to configure that Functional Area, including security setup tasks. Security setup tasks typically have the word 'Security' in the task name.

Note: For detailed information about using FSM tasks, see *Oracle Business Intelligence Applications Configuration Guide*.

For example, the screenshot below shows a list of FSM Tasks for a Functional Area in Human Resources. A number of security-related tasks are highlighted, for example, 'How to Set Up Payroll Based Data Security'.



Implementation Project: IP3

* How to Set Up Workforce Frozen Snapshots	■	0	
* How to Assign Group Account Numbers to Natural Accour	■	0	
* How to Control Future Transaction Data Visibility	■	0	
* How to Use Workforce Deployment Subject Area	■	0	
* How To Grant GL Data Role to HR VP Users	■	0	Adm
* How to Set Up Payroll Based Data Security	■	0	Adm
* How to Set Up Payroll Legislative Data Group Based Data	■	0	Adm
* How to Set Up HR Supervisor Hierarchy Based Data Secu	■	0	Adm
* How to Set Up HR Position Hierarchy Based Data Security	■	0	
* How to Set Up Department Based Data Security	■	0	
* Review Table Partition for Human Resource Analytics	■	0	
* How to Set Up Manager Hierarchy Base Security for Peop	■	0	
* How to Configure New Country Code	■	0	
* How to Set Up the C_STATE_PROV domain	■	0	
* How to Define New Groups and Mappings for Users and E	■	0	
* How to configure UOMs	■	0	

Rows Selected 1 Columns Hidden 1 Columns Frozen 1

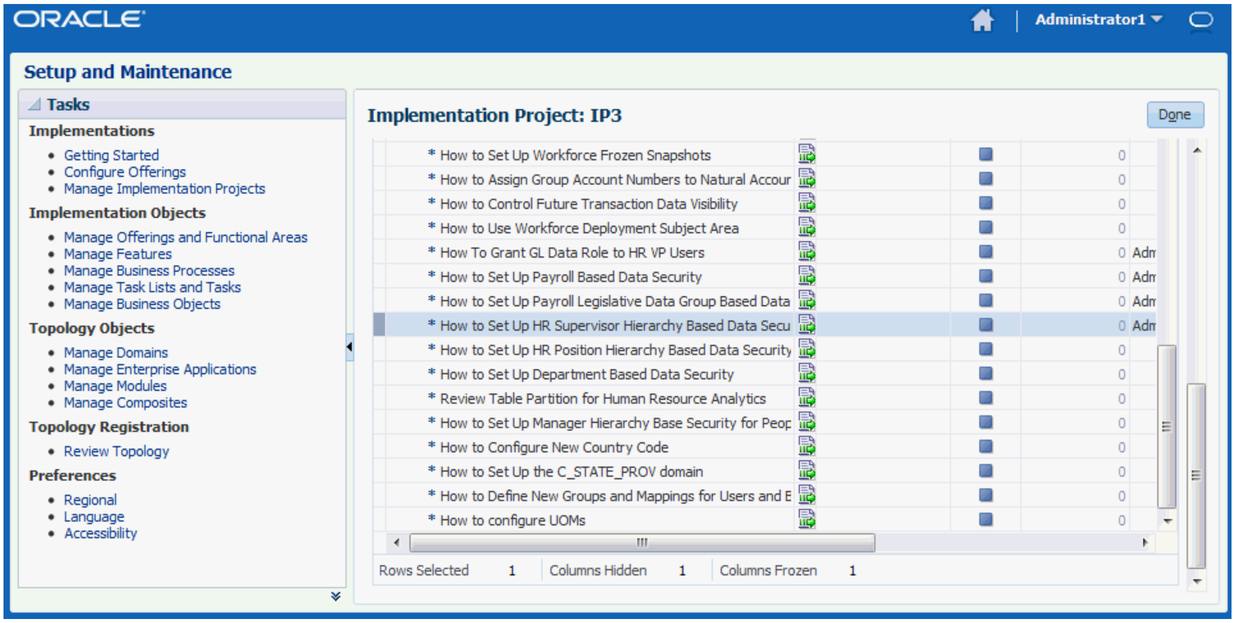
To configure security for a Functional Area:

1. Log into Functional Setup Manager.

2. Navigate to the Implementation Project that has been created to configure a Functional Area.

   If you log in as an Administrator, then you have access to all FSM Tasks. If you log in as a Functional Developer, then the Assigned Implementation Tasks tab provides a list of FSM Tasks that have been assigned to you by the Administrator.

   For example, the screenshot below shows a list of FSM Tasks for a Human Resources module with the Task named 'How to Setup Up HR Supervisor Hierarchy Based Data Security' selected.



Setup and Maintenance

Tasks

Implementations

- Getting Started
- Configure Offerings
- Manage Implementation Projects

Implementation Objects

- Manage Offerings and Functional Areas
- Manage Features
- Manage Business Processes
- Manage Task Lists and Tasks
- Manage Business Objects

Topology Objects

- Manage Domains
- Manage Enterprise Applications
- Manage Modules
- Manage Composites

Topology Registration

- Review Topology

Preferences

- Regional
- Language
- Accessibility

Implementation Project: IP3

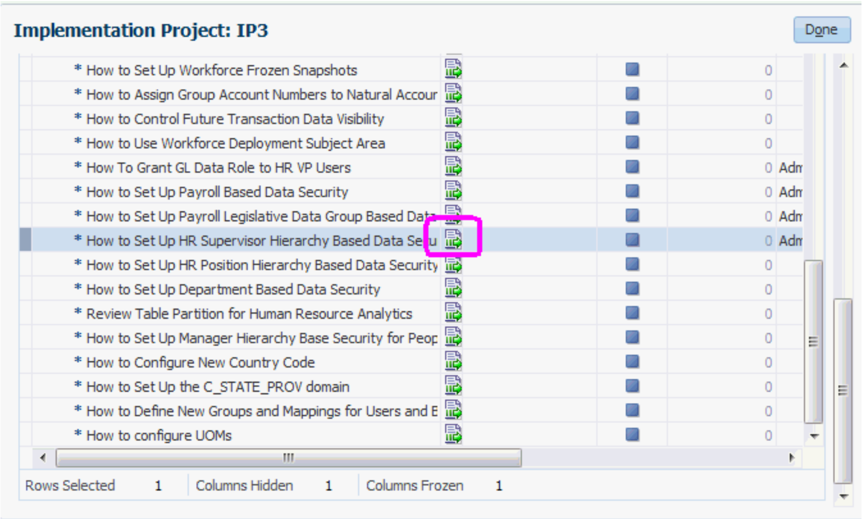
Done

* How to Set Up Workforce Frozen Snapshots		■	0	
* How to Assign Group Account Numbers to Natural Accour		■	0	
* How to Control Future Transaction Data Visibility		■	0	
* How to Use Workforce Deployment Subject Area		■	0	
* How To Grant GL Data Role to HR VP Users		■	0	Adn
* How to Set Up Payroll Based Data Security		■	0	Adn
* How to Set Up Payroll Legislative Data Group Based Data		■	0	Adn
* How to Set Up HR Supervisor Hierarchy Based Data Secu		■	0	Adn
* How to Set Up HR Position Hierarchy Based Data Security		■	0	
* How to Set Up Department Based Data Security		■	0	
* Review Table Partition for Human Resource Analytics		■	0	
* How to Set Up Manager Hierarchy Base Security for Peop		■	0	
* How to Configure New Country Code		■	0	
* How to Set Up the C_STATE_PROV domain		■	0	
* How to Define New Groups and Mappings for Users and E		■	0	
* How to configure UOMs		■	0	

Rows Selected 1 Columns Hidden 1 Columns Frozen 1

3. For each security task, do the following:

   a. Click the Go to Task icon next to the security task.



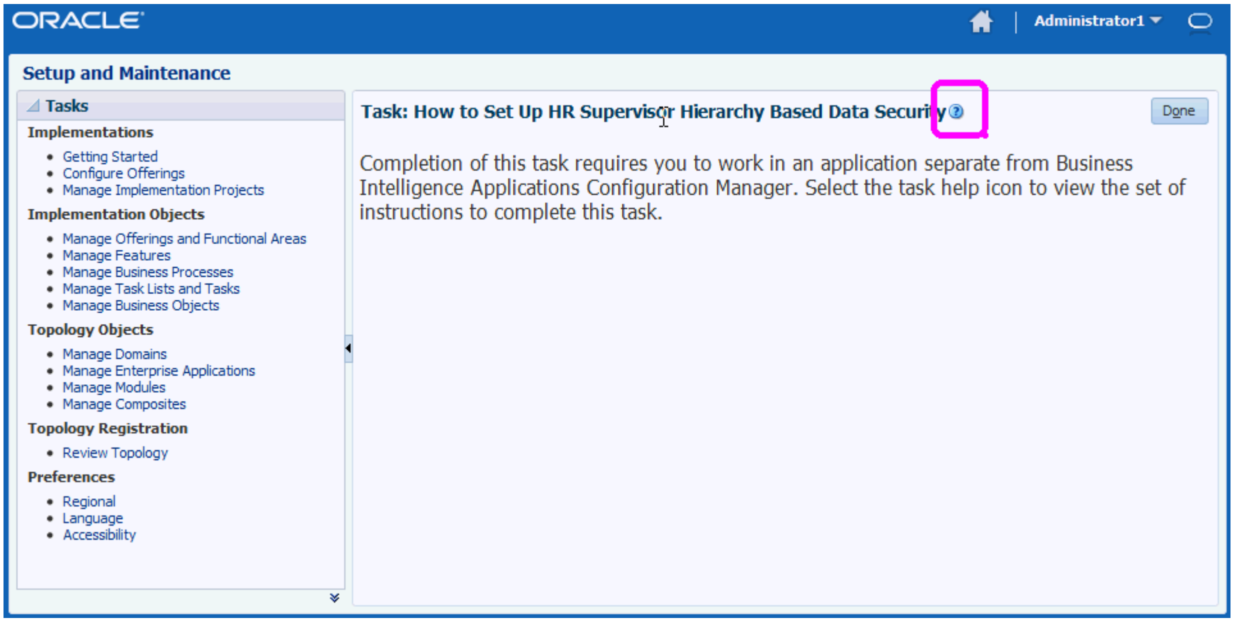
Implementation Project: IP3

Done

* How to Set Up Workforce Frozen Snapshots		■	0	
* How to Assign Group Account Numbers to Natural Accour		■	0	
* How to Control Future Transaction Data Visibility		■	0	
* How to Use Workforce Deployment Subject Area		■	0	
* How To Grant GL Data Role to HR VP Users		■	0	Adn
* How to Set Up Payroll Based Data Security		■	0	Adn
* How to Set Up Payroll Legislative Data Group Based Data		■	0	Adn
* How to Set Up HR Supervisor Hierarchy Based Data Secu		■	0	Adn
* How to Set Up HR Position Hierarchy Based Data Security		■	0	
* How to Set Up Department Based Data Security		■	0	
* Review Table Partition for Human Resource Analytics		■	0	
* How to Set Up Manager Hierarchy Base Security for Peop		■	0	
* How to Configure New Country Code		■	0	
* How to Set Up the C_STATE_PROV domain		■	0	
* How to Define New Groups and Mappings for Users and E		■	0	
* How to configure UOMs		■	0	

Rows Selected 1 Columns Hidden 1 Columns Frozen 1

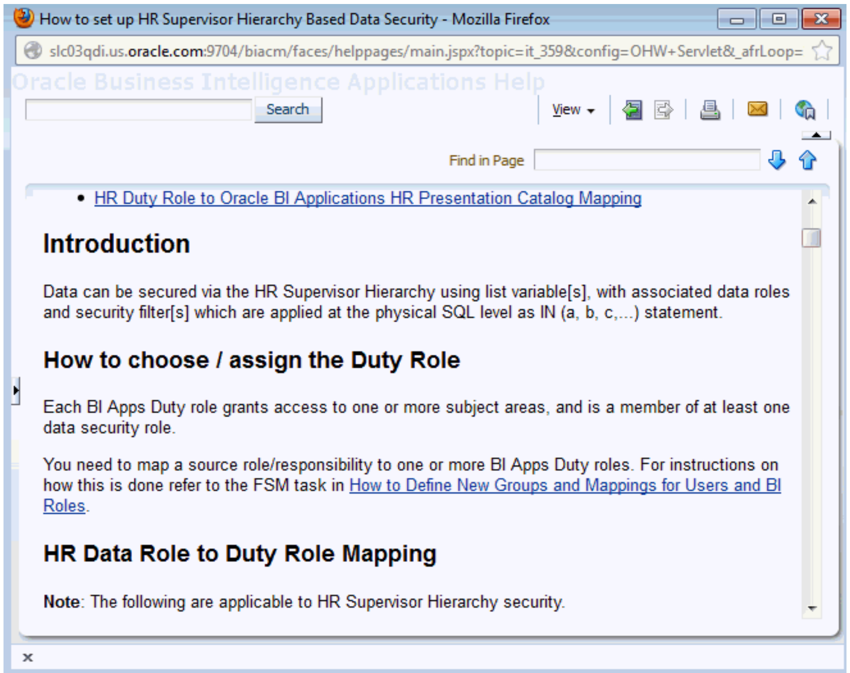
   b. Click the Help icon next to the Task name.



Task: How to Set Up HR Supervisor Hierarchy Based Data Security

Completion of this task requires you to work in an application separate from Business Intelligence Applications Configuration Manager. Select the task help icon to view the set of instructions to complete this task.

The instructions are displayed in a Help topic.


How to set up HR Supervisor Hierarchy Based Data Security - Mozilla Firefox
slc03qdi.us.oracle.com:9704/biacm/faces/helppages/main.jspx?topic=it_359&config=OHW+Servlet&_afrLoop=
Oracle Business Intelligence Applications Help
Search
View
Find in Page

- HR Duty Role to Oracle BI Applications HR Presentation Catalog Mapping

Introduction

Data can be secured via the HR Supervisor Hierarchy using list variable[s], with associated data roles and security filter[s] which are applied at the physical SQL level as IN (a, b, c,...) statement.

How to choose / assign the Duty Role

Each BI Apps Duty role grants access to one or more subject areas, and is a member of at least one data security role.

You need to map a source role/responsibility to one or more BI Apps Duty roles. For instructions on how this is done refer to the FSM task in How to Define New Groups and Mappings for Users and BI Roles.

HR Data Role to Duty Role Mapping

Note: The following are applicable to HR Supervisor Hierarchy security.

c. Follow the instructions in the Help topic.

To complete the task, you typically use one of the security tools such as Oracle Fusion Middleware Control, or Oracle BI Administration Tool.

For example, the steps might involve logging into Oracle WebLogic Server Administration Console to provision a set of users.

d. In FSM, click Done.

e. Set the status of the task to 'Completed'.

1.3 Extending Security in Oracle BI Applications

You can extend the preconfigured Oracle BI Applications security model to match your operational source system. When you extend Oracle BI Applications, you need to ensure that your customizations and any new objects are valid and functional.

The general process for extending data-level security for repository objects is as follows:

1. Extend the physical table by adding the attribute by which the dimension or fact needs to be secured. (This step results in a change to the data model.)
2. Populate the relevant attribute value for each row in the fact or dimension table. (This step results in a change to the ETL mapping.)
3. Use the Oracle BI Administration Tool to create an initialization block to fetch the attribute values and populate them into a session variable when each user logs into Oracle BI Applications. You can create a target session variable for the initialization block if the initialization block is not a row-wise initialization block. (This step results in a change to the Oracle BI repository.) For instructions, see *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition*.
4. Use Fusion Middleware Control to create a Duty Role in the policy store. Then, restart the Oracle BI Server. For instructions, see *Oracle Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition*.
5. Use the Oracle BI Administration Tool in online mode to set up data filters based on the new role for each of the fact and dimension tables that need to be secured by the attribute you added in Step 1. (This step results in a change to the Oracle BI Repository.) For instructions, see *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition*.
6. Use the Oracle BI Administration Tool in online mode to restrict object access based on the Duty Role you created in Step 4. (This step results in a change to the Oracle BI Repository.) For instructions, see *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition*.
7. Use Presentation Services administration to set up Presentation Services catalog privileges based on the Duty Role you created in step 4. For instructions, see *Oracle Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition*.

Note: You can also leverage the existing Oracle BI Applications security objects when extending data-level security. To do this, copy existing security objects for secured dimensions, such as initialization blocks and Duty Roles, and then modify them to apply to the additional dimensions.

For more information on working with security objects like Duty Roles and initialization blocks, see the following resources:

- "Creating and Managing Duty Roles and Application Policies Using Fusion Middleware Control" in *Oracle Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition*
- "Working with Initialization Blocks" in *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition*

1.4 Supplementary Information About Security In Oracle BI Applications

This section contains supplementary and reference information about Oracle BI Applications Security, and contains the following sections:

1.4.1 Security Overview of Oracle BI Applications Configuration Manager and Functional Setup Manager

To access Oracle BI Applications Configuration Manager or Functional Setup Manager (for Oracle BI Applications), a User must be assigned to an Enterprise Role that is associated with one of the following Duty Roles:

- BI Applications Administrator Duty (BIA_ADMINISTRATOR_DUTY)

  Users with the BI Applications Administrator Duty Role have access to all Oracle BI Applications Configuration Manager User Interfaces and all Functional Setup Manager User Interfaces. For Oracle BI Applications Configuration Manager, only users with this Duty Role are able to perform system setup tasks.

- BI Applications Implementation Manager (BIA_IMPLEMENTATION_MANAGER_DUTY)

  Users with the BI Applications Implementation Manager Duty Role have access to Oracle BI Applications Configuration Manager Overview page and the Export and Import of Setup Data. In Functional Setup Manager, these users have access to Configure Offerings and Manage Implementation Projects User Interfaces but cannot execute a setup task.

- BI Applications Functional Developer (BIA_FUNCTIONAL_DEVELOPER_DUTY)

  Users with the BI Applications Functional Developer Duty Role have access to Oracle BI Applications Configuration Manager User Interfaces, except for the System Setup screens. In Functional Setup Manager, these users have access to the list of functional setup tasks assigned to them and have the ability to execute the setup tasks.

- BI Applications Load Plan Developer (BIA_LOAD_PLAN_DEVELOPER_DUTY)

  Users with the BI Applications Load Plan Developer Duty Role have access to the Load Plans page, where they can create, edit, delete, generate, execute and monitor load plans. Users with this role can view and edit fact groups, data load parameters, domains mappings, and schedules associated with a load plan.

- BI Applications Load Plan Operator (BIA_LOAD_PLAN_OPERATORY_DUTY)

Users with the BI Applications Load Plan Operator Duty Role have limited access to the Load Plans page, where they can view the generation status and execution status details of load plans but are not able to modify them.

1.4.2 About Permissions in Oracle BI Applications Configuration Manager and Functional Setup Manager

This section describes permissions in Oracle BI Applications Configuration Manager and Functional Setup Manager, and contains the following sections.

- Section 1.4.2.1, "About Permissions in Oracle BI Applications Configuration Manager"
- Section 1.4.2.2, "About Permissions in Functional Setup Manager"

1.4.2.1 About Permissions in Oracle BI Applications Configuration Manager

Table 1–1 shows the list of Oracle BI Applications Configuration Manager screens visible to each of the Oracle BI Applications Roles.

Table 1–1 List of Oracle BI Applications Configuration Manager Screens Visible to Each Oracle BI Applications Duty Role

Oracle BI Applications Duty Role	Oracle BI Applications Configuration Manager screen	Associated Privilege
BI Applications Administrator	Overview	BIA_OVERVIEW_PRIV
BI Applications Administrator	System Setups - Define Oracle BI Applications Instance	BIA_DEFINE_INSTANCE_PRIV
BI Applications Administrator	System Setups - Manage Oracle BI Applications	BIA_MANAGE_INSTANCE_PRIV
BI Applications Administrator	System Setups - Manage Preferred Currencies	BIA_MANAGE_INSTANCE_PRIV
BI Applications Administrator	Functional Configurations - 'Perform Functional Configurations' link to launch Functional Setup Manager	BIA_FUNCTIONAL_SETUPS_PRIV
BI Applications Administrator	Setup Data Maintenance and Administration - Manage Domains and Mappings	BIA_CONFIGURE_DOMAINS_PRIV
BI Applications Administrator	Setup Data Maintenance and Administration - Manage Data Load Parameters	BIA_CONFIGURE_DATALOAD_PARAMS_PRIV
BI Applications Administrator	Setup Data Maintenance and Administration - Manage Reporting Parameters	BIA_CONFIGURE_RPD_PARAMS_PRIV
BI Applications Administrator	Setup Data Export and Import - Export Setup Data	BIA_EXPORT_SETUPS_PRIV
BI Applications Administrator	Setup Data Export and Import - Import Setup Data	BIA_IMPORT_SETUPS_PRIV
BI Applications Functional Developer	Overview	BIA_OVERVIEW_PRIV

Table 1–1 (Cont.) List of Oracle BI Applications Configuration Manager Screens Visible to Each Oracle BI Applications Duty Role

Oracle BI Applications Duty Role	Oracle BI Applications Configuration Manager screen	Associated Privilege
BI Applications Functional Developer	Functional Configurations - 'Perform Functional Configurations' link to launch Functional Setup Manager	BIA_FUNCTIONAL_ SETUPS_PRIV
BI Applications Functional Developer	Setup Data Maintenance and Administration - Manage Domains and Mappings	BIA_CONFIGURE_ DOMAINS_PRIV
BI Applications Functional Developer	Setup Data Maintenance and Administration - Manage Data Load Parameters	BIA_CONFIGURE_ DATALOAD_PARAMS_PRIV
BI Applications Functional Developer	Setup Data Maintenance and Administration - Manage Reporting Parameters	BIA_CONFIGURE_RPD_ PARAMS_PRIV
BI Applications Functional Developer	Setup Data Export and Import - Export Setup Data	BIA_EXPORT_SETUPS_PRIV
BI Applications Functional Developer	Setup Data Export and Import - Import Setup Data	BIA_IMPORT_SETUPS_PRIV
BI Applications Implementation Manager	Overview	BIA_OVERVIEW_PRIV
BI Applications Implementation Manager	Setup Data Export and Import - Export Setup Data	BIA_EXPORT_SETUPS_PRIV
BI Applications Implementation Manager	Setup Data Export and Import - Import Setup Data	BIA_IMPORT_SETUPS_PRIV

1.4.2.2 About Permissions in Functional Setup Manager

Functional Setup Manager Roles are associated with Oracle BI Applications Roles as follows:

- The BI Applications Administrator role (BIA_ADMINISTRATOR_DUTY) is associated to the following Functional Setup Manager Roles:
  - ASM_FUNCTIONAL_SETUPS_DUTY
  - ASM_IMPLEMENTATION_MANAGER_DUTY
  - ASM_APPLICATION_DEPLOYER_DUTY
  - ASM_APPLICATION_REGISTRATION_DUTY
  - ASM_LOGICAL_ ENTITY_MODELING_DUTY
  - ASM_SETUP_OBJECTS_PROVIDER_DUTY
- The BI Applications Implementation Manager role (BIA_IMPLEMENTATION_ MANAGER_DUTY) is associated to the following Functional Setup Manager duty:
  - ASM_IMPLEMENTATION_MANAGER_DUTY
- The BI Applications Functional Developer role (BIA_FUNCTIONAL_ DEVELOPER_DUTY) is associated to the following Functional Setup Manager duty:

  - ASM_FUNCTIONAL_SETUPS_DUTY

1.4.3 Checking Oracle BI Applications User Responsibilities

Pre-configured Duty Roles match responsibilities and roles in source operational applications, so that after authentication the correct roles can be applied. An administrator can check a user's responsibilities in the following ways:

- In the Siebel or Oracle EBS operational applications, go to the Responsibilities view.
- In PeopleSoft applications, go to the Roles view to check a user's roles.
- In JD Edwards EnterpriseOne applications, go to the User Profiles application (P0092) to check a user's roles.
- Individual users can view the list of Duty Roles to which they are assigned. In the Oracle BI application, click **Signed In As *username*** and select **My Account**. Then, click the Roles and Catalog Groups tab to view the Duty Roles. In Presentation Services, Duty Roles are used to control the ability to perform actions (privileges) within Presentation Services.

For more information, refer to the system administrator for your source system.

1.4.4 About Managing Presentation Services Catalog Privileges in Oracle Business Intelligence

When you add a new catalog privilege to a Duty Role in Oracle BI Presentation Services, the change is not immediately reflected in the Oracle Business Intelligence environment. In order to register the catalog privilege, both the administrator and the user must perform the following tasks:

1. The Oracle BI administrator must reload the Oracle BI Server metadata through Oracle BI Presentation Services. To reload the metadata, in Oracle Business Intelligence Answers, select **Administration**, and then click **Reload Files and Metadata**.

   For more information on managing Presentation Services catalog privileges, see *Oracle Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition*.

2. Users belonging to that Duty Role must log out from the Oracle BI application (or from Siebel or Oracle EBS operational application if the user is looking at Oracle BI dashboards using an embedded application) and then log in again.

1.4.5 About Object-Level Security

This section describes the object-level security features in Oracle BI Applications. It contains the following topics:

- Section 1.4.5.1, "Metadata Object-Level Security in the RPD"
- Section 1.4.5.2, "Metadata Object-Level Security in Presentation Services"

1.4.5.1 Metadata Object-Level Security in the RPD

Duty Roles control access to metadata objects, such as subject areas, tables and columns. For example, users in a particular department can view only the subject areas that belong to their department.

Metadata object security is configured in the Oracle BI Repository, using the Oracle BI Administration Tool. The Everyone Duty Role is denied access to each of the subject areas. Each subject area is configured to give explicit read access to selected related responsibilities. This access can be extended to tables and columns.

Note: By default in Oracle BI Applications, only permissions at the subject area level have been configured.

Note: The Siebel Communications and Financial Analytics industry applications have tables and columns that are industry-specific, and, therefore, hidden from other Duty Roles.

Oracle Business Intelligence supports hierarchies within Duty Roles. In the policy store, there are certain Duty Roles that are parent Duty Roles, which define the behavior of all the child Duty Roles. Inheritance is used to enable permissions to ripple through to child Duty Roles. For more information about parent Duty Roles and the pre-built Duty Role hierarchies, refer to the list of groups, Duty Roles, initialization blocks, and security policies published on My Oracle Support as a document named 'Oracle Business Intelligence Applications Roles and Security'.

1.4.5.2 Metadata Object-Level Security in Presentation Services

Access to Oracle BI Presentation Services objects, such as dashboards, pages, reports, and Web folders, is controlled using Duty Roles. For detailed information about managing object-level security in Presentation Services, see *Oracle Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition*.

1.4.6 About Data-Level Security

This section describes the data-level security features in Oracle BI Applications. It contains the following topics:

- Section 1.4.6.1, "Overview of Data-Level Security in Oracle BI Applications"
- Section 1.4.6.2, "Implementing Data-Level Security in the Oracle BI Repository"
- Section 1.4.6.3, "Initialization Blocks Used for Data-Level Security in Oracle BI Applications"
- Section 1.4.6.4, "About Data-Level Security Design in Oracle BI Applications"

1.4.6.1 Overview of Data-Level Security in Oracle BI Applications

Data-level security defines what a user in an OLTP application can access inside a report. The same report, when run by two different users, can bring up different data. This is similar to how the My Opportunities view in an operational application displays different data for different users. However, the structure of the report is the same for all users, unless a user does not have access to the report subject area, in which case the report displays an error.

For information about the data security policies that are supported in Oracle BI Applications, refer to the list published on My Oracle Support as a document named 'Oracle Business Intelligence Applications Roles and Security'. During installation and configuration, you must make sure the correct Duty Roles and initialization blocks are set up for your environment.

For more information about the use of initialization blocks in Oracle Business Intelligence, see *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition* and *Oracle Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition*.

1.4.6.2 Implementing Data-Level Security in the Oracle BI Repository

Data-level security in Oracle BI Applications is implemented in three major steps, as described below. For instructions on performing these steps, see *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition.*

1. Set up initialization blocks that obtain specific security-related information when a user logs in, for example, the user's hierarchy level in the organization hierarchy, or the user's responsibilities. Initialization blocks obtain DimensionIds for each user session in order to restrict row-level access to factual or dimensional data.

   For a description of the preconfigured initialization blocks, see Section 1.4.6.3, "Initialization Blocks Used for Data-Level Security in Oracle BI Applications."

2. Set up the joins to the appropriate security tables in the metadata physical and logical layers.

   For detailed information about this security feature, see *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition*.

3. Set up the data filters for each Duty Role on each logical table that needs to be secured.

   For detailed information about this security feature, see *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition*.

1.4.6.3 Initialization Blocks Used for Data-Level Security in Oracle BI Applications

Initialization blocks are deployed as part of your configuration using guidance provided in Functional Setup Manager (FSM) tasks.

For a summary of how FSM Tasks are used, see Section 1.2, "Using Oracle BI Applications Functional Setup Manager Informational Tasks to Set Up Security". For detailed information about using FSM tasks, see *Oracle Business Intelligence Applications Configuration Guide*. For information about the initialization blocks prebuilt for Oracle BI Applications, refer to the list published on My Oracle Support as a document named 'Oracle Business Intelligence Applications Roles and Security'.

1.4.6.4 About Data-Level Security Design in Oracle BI Applications

Oracle BI Applications maintains data-level security Duty Roles that are assigned dynamically to every user at the session level. Each Duty Role has a set of filters associated with it that determines the data that each user is allowed to see. A user is assigned a Duty Role through the Authorization initialization block.

The data security design has the following features:

- **Drill down.** The user can drill down on a particular position in the position hierarchy to slice the data by the next position level in the hierarchy. For example, if the initial report is defined as:

  ```
  select Top Level Position, Revenue from RevenueStar
  ```

  then by drilling down on a value of MyPosition in the TopLevelPosition hierarchy, the report will become:

```
Select Level8 Position, Revenue, where TopLevelPosition = 'MyPosition'
```

- **Personalized reports.** Users at different levels of the Position hierarchy can use the same Position-based reports but with each user seeing the data corresponding to his or her level. In such reports, Position is a dynamic column.

  For example, if a report is defined as:

  ```
  select Position, Revenue from RevenueStar
  ```

  the logical query for the user at the top level of the hierarchy will be:

  ```
  select Top Level Position, Revenue from RevenueStar
  ```

  The logical query for the user at the next level of the hierarchy will be:

  ```
  select Level8 Position, Revenue from RevenueStar
  ```

- **CURRENT Position hierarchy columns.** Position hierarchy columns with the prefix CURRENT contain the Current Position hierarchy at any point of time. This feature allows users to see the same data associated with the employee holding the Current Employee position at the time the report runs. This type of Analysis is called As Is.
- **Additional Position hierarchy columns.** The columns EMP_LOGIN and EMPLOYEE_FULL_NAME are used at every level of the Position hierarchy to store additional information about an employee holding a particular position. In the Logical layer, the Employee path and Position path are two drill down paths under the Position hierarchy that allow the user to drill down on a position to see all positions under it. It also allows an employee to see all the employees reporting to him or her.

1.4.7 About User-Level Security

User security concerns the authentication and confirmation of the identity of the user based on the credentials provided, such as username and password. By default, user-level security is set up in the embedded Oracle WebLogic Server LDAP and Policy Store in Oracle Business Intelligence Enterprise Edition. For more information, see *Oracle Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition*.

1.4.8 Additional Sources of Information About Oracle BI Applications Security

When configuring security in Oracle BI Applications, in some circumstances you might need to refer to security in other areas, as follows:

- Oracle Fusion Applications security

  For more information, see:

  – *Oracle Fusion Applications Security Guide*

  – *Oracle Fusion Applications Common Security Reference Manual*

- Oracle Business Intelligence Enterprise Edition security implementation

  For more information, see:

  – *Oracle Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition*

- *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition*

A

Configuring Security

This appendix contains miscellaneous security Help topics. These Help topics are displayed in FSM when a BI security administrator clicks the **Go to Task** icon next to a security task.

A.1 Informational Task Reference - Security

This section contains miscellaneous security Help topics.

A.1.1 How to Implement Accounts Receivable Security for PeopleSoft

Financial Analytics supports security over Billing and Revenue Management Business Unit in Accounts Receivable. This Business Unit is the same as Receivables Business Unit in PeopleSoft, and the list of Receivables Business Unit that a user has access to is determined by the grants in PeopleSoft.

Configuring Accounts Receivable Security

In order for data security filters to be applied, appropriate initialization blocks need to be enabled depending on the deployed source system. To enable Accounts Receivable security for PeopleSoft, enable Oracle PeopleSoft initialization block and make sure the initialization blocks of all other source systems are disabled. The initialization block names relevant to various source systems are given below. If more than one source system is deployed, then you must also enable the initialization blocks of those source systems.

Initialization Blocks

- Oracle Fusion Applications: Receivables Business Unit
- Oracle E-Business Suite: Operating Unit Organizations EBS
- Oracle PeopleSoft: Receivables Organizations

To enable initialization blocks, follow the steps below:

1. In Oracle BI Administration Tool, edit the BI metadata repository (for example, OracleBIAnalyticsApps.rpd).
2. Choose Manage, then Variables to display the Variables dialog
3. Under Session – Initialization Blocks, open the initialization block that you need to enable.
4. Clear the **Disabled** check box.
5. Save the RPD file.

Configuring BI Duty Roles

The following BI Duty Roles are applicable to the Accounts Receivable subject area.

- AR Analyst PSFT
- AR Manager PSFT

These Duty Roles control the subject areas and dashboard content to which the user has access. These Duty Roles also ensure the data security filters are applied to all the queries. For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

A.1.2 How to Setup Accounts Payable Security for Oracle Fusion Applications

Financial Analytics supports security over Payables Invoicing Business Unit in Accounts Payable subject areas. This Business Unit is the same as Business Unit in Oracle Fusion Applications, and the list of Business units that a user has access to is determined by the grants in Oracle Fusion applications.

Configuring Accounts Payable Security

In order for data security filters to be applied, appropriate initialization blocks need to be enabled depending on the deployed source system. The initialization block names relevant to various source systems are given below. Oracle Fusion Applications security is enabled by default so there is no change required in the setup. If more than one source system is deployed, then you must also enable the initialization blocks of those source systems. For example:

- Oracle Fusion Applications: Payables Business Unit
- Oracle E-Business Suite: Operating Unit Organizations EBS
- Oracle PeopleSoft: Payables Organizations

To enable initialization blocks, follow the steps below:

1. In Oracle BI Administration Tool, edit the BI metadata repository (RPD file).
2. Choose Manage, then Variables to display the Variables dialog.
3. Under Session – Initialization Blocks, open the initialization block that you need to enable.
4. Clear the **Disabled** check box.
5. Save the RPD file.

Configuring BI Duty Roles

The following BI Duty Roles are applicable to the Accounts Payable subject area.

- OBIA_ACCOUNTS_PAYABLE_MANAGERIAL_ANALYSIS_DUTY

These Duty Roles control the subject areas and dashboard content to which the user has access. These Duty Roles also ensure the data security filters are applied to all the queries. For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

Optional Drill to Purchase Order Details in Procurement and Spend Analytics

Accounts Payable supports the ability to drill down on Purchase Order Number to the associated Purchase Order Details in Procurement and Spend Analytics. In order for this drill to work, the Procurement and Spend Analytics offering must be licensed and implemented. The Payables user must be granted at least one of the Procurement and Spend BI Duty Roles.

A.1.3 How to Set Up Accounts Payable Security for Oracle E-Business Suite

Financial Analytics supports security over Payables Invoicing Business Unit in Accounts Payable subject areas. This Business Unit is the same as Operating Unit Organizations in E-Business Suite, and the list of Operating Unit Organizations that a user has access to is determined by the grants in E-Business Suite.

Configuring Accounts Payable Security

In order for data security filters to be applied, appropriate initialization blocks need to be enabled depending on the deployed source system. To enable Accounts Payable security for E-Business Suite, enable Oracle E-Business Suite initialization block and make sure the initialization blocks of all other source systems are disabled. The initialization block names relevant to various source systems are given below. If more than one source system is deployed, then you must also enable the initialization blocks of those source systems. For example:

- Oracle Fusion Applications: Payables Business Unit
- Oracle E-Business Suite: Operating Unit Organizations EBS
- Oracle PeopleSoft: Payables Organizations

To enable initialization blocks, follow the steps below:

1. In Oracle BI Administration Tool, edit the BI metadata repository (RPD file).
2. Choose Manage, then Variables to display the Variables dialog.
3. Under Session – Initialization Blocks, open the initialization block that you need to enable.
4. Clear the **Disabled** check box.
5. Save the RPD file.

Configuring BI Duty Roles

The following BI Duty Roles are applicable to the Accounts Payable subject area.

- AP Analyst
- AP Manager

These Duty Roles control the subject areas and dashboard content to which the user has access. These Duty Roles also ensure the data security filters are applied to all the queries. For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

Optional Drill to Purchase Order Details in Procurement and Spend Analytics

Accounts Payable supports the ability to drill down on Purchase Order Number to the associated Purchase Order Details in Procurement and Spend Analytics. In order for this drill to work, the Procurement and Spend Analytics offering must be licensed and implemented. The Payables user must be granted at least one of the Procurement and Spend BI Duty Roles.

A.1.4 How to Setup Accounts Payable Security for PeopleSoft

Financial Analytics supports security over Payables Invoicing Business Unit in Accounts Payable subject areas. This Business Unit is the same as Payables Business Unit in PeopleSoft, and the list of Payables Business Unit that a user has access to is determined by the grants in PeopleSoft.

Configuring Accounts Payable Security

In order for data security filters to be applied, appropriate initialization blocks need to be enabled depending on the deployed source system. To enable Accounts Payable security for PeopleSoft, enable Oracle PeopleSoft initialization block and make sure the initialization blocks of all other source systems are disabled. The initialization block names relevant to various source systems are given below. If more than one source system is deployed, then you must also enable the initialization blocks of those source systems. For example:

- Oracle Fusion Applications: Payables Business Unit
- Oracle E-Business Suite: Operating Unit Organizations EBS
- Oracle PeopleSoft: Payables Organizations

To enable initialization blocks, follow the steps below:

1. In Oracle BI Administration Tool, edit the BI metadata repository (RPD file).
2. Choose Manage, then Variables to display the Variables dialog.
3. Under Session – Initialization Blocks, open the initialization block that you need to enable.
4. Clear the **Disabled** check box.
5. Save the RPD file.

Configuring BI Duty Roles

The following BI Duty Roles are applicable to the Accounts Payable subject area.

- AP Analyst PSFT
- AP Manager PSFT

These Duty Roles control the subject areas and dashboard content to which the user has access. These Duty Roles also ensure the data security filters are applied to all the queries. For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

Optional Drill to Purchase Order Details in Procurement and Spend Analytics

Accounts Payable supports the ability to drill down on Purchase Order Number to the associated Purchase Order Details in Procurement and Spend Analytics.In order for this drill to work, the Procurement and Spend Analytics offering must be licensed and implemented. The Payables user must be granted at least one of the Procurement and Spend BI Duty Roles.

A.1.5 How to Set Up Accounts Receivable Security for Oracle Fusion Applications

Financial Analytics supports security over Billing and Revenue Management Business Unit in Accounts Receivable subject areas. This Business Unit is the same as Business Unit in Oracle Fusion Applications, and the list of Business units that a user has access to is determined by the grants in Oracle Fusion applications.

Configuring Accounts Receivable Security

In order for data security filters to be applied, appropriate initialization blocks need to be enabled depending on the deployed source system. The initialization block names relevant to various source systems are given below. Oracle Fusion Applications security is enabled by default so there is no change required in the setup. If more than one source system is deployed, then you must also enable the initialization blocks of those source systems. For example:

- Oracle Fusion Applications: Receivables Business Unit
- Oracle E-Business Suite: Operating Unit Organizations EBS
- Oracle PeopleSoft: Receivables Organizations

To enable initialization blocks, follow the steps below:

1. In Oracle BI Administration Tool, edit the BI metadata repository (RPD file).
2. Choose Manage, then Variables to display the Variables dialog
3. Under Session – Initialization Blocks, open the initialization block that you need to enable.
4. Clear the **Disabled** check box.
5. Save the RPD file.

Configuring BI Duty Roles

The following BI Duty Roles are applicable to the Accounts Receivable subject area.

- OBIA_ACCOUNTS_RECEIVABLE_MANAGERIAL_ANALYSIS_DUTY

These Duty Roles control the subject areas and dashboard content to which the user has access. These Duty Roles also ensure the data security filters are applied to all the queries. For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

A.1.6 How to Set Up Accounts Receivable Security for Oracle E-Business Suite

Financial Analytics supports security over Billing and Revenue Management Business Unit in Accounts Receivable subject areas. This Business Unit is the same as Operating Unit Organization in E-Business Suite, and the list of Operating Unit Organizations that a user has access to is determined by the grants in E-Business Suite.

Configuring Accounts Receivable Security

In order for data security filters to be applied, appropriate initialization blocks need to be enabled depending on the deployed source system. To enable Accounts Receivable security for E-Business Suite, enable Oracle E-Business Suite initialization block and make sure the initialization blocks of all other source systems are disabled. The initialization block names relevant to various source systems are given below. If more than one source system is deployed, then you must also enable the initialization blocks of those source systems. For example:

- Oracle Fusion Applications: Receivables Business Unit
- Oracle E-Business Suite: Operating Unit Organizations EBS
- Oracle PeopleSoft: Receivables Organizations

To enable initialization blocks, follow the steps below:

1. In Oracle BI Administration Tool, edit the BI metadata repository (RPD file).
2. Choose Manage, then Variables to display the Variables dialog
3. Under Session – Initialization Blocks, open the initialization block that you need to enable.
4. Clear the **Disabled** check box.
5. Save the RPD file.

Configuring BI Duty Roles

The following BI Duty Roles are applicable to the Accounts Receivable subject area.

- AR Analyst
- AR Manager

These Duty Roles control the subject areas and dashboard content to which the user has access. These Duty Roles also ensure the data security filters are applied to all the queries. For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

A.1.7 How to Set Up Fixed Asset Security for Oracle Fusion Applications

Financial Analytics supports security over fixed asset books in Fixed Asset subject areas. The list of asset books that a user has access to is determined by the grants in Oracle Fusion application.

In order for data security filters to be applied, appropriate initialization blocks need to be enabled depending on the deployed source system. The initialization block names relevant to various source systems are given below. Fusion Applications security is enabled by default, therefore no manual configuration is required. If more than one source system is deployed, then you must also enable the initialization blocks of those source systems.

- Oracle Fusion Applications: Fixed Asset Book
- Oracle E-Business Suite: Fixed Asset Book EBS
- Oracle PeopleSoft: Fixed Asset Book PSFT

To enable initialization blocks, follow the steps below:

1. In Oracle BI Administration Tool, edit the BI metadata repository (for example, OracleBIAnalyticsApps.rpd).
2. Choose Manage, then Variables.
3. Under Session – Initialization Blocks, open the initialization block that you need to enable.
4. Clear the **Disabled** check box.
5. Save the metadata repository (RPD file).

Configuring BI Duty Roles

The following BI Duty Role is applicable to the Fixed Asset subject areas for Oracle Fusion Applications:

- OBIA_ASSETS_ACCOUNTING_MANAGERIAL_ANALYSIS_DUTY

These Duty Roles control the subject areas and dashboard content to which the user has access. These Duty Roles also ensure the data security filters are applied to all the queries. For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

A.1.8 How to Set Up Fixed Asset Security for E-Business Suite

In order for data security filters to be applied, appropriate initialization blocks need to be enabled depending on the deployed source system. To enable Fixed Asset security for E-Business Suite, enable Oracle E-Business Suite initialization block and make sure the initialization blocks of all other source systems are disabled. The initialization block names relevant to various source systems are given below. If more than one source system is deployed, then you must also enable the initialization blocks of those source systems.

- Oracle Fusion Applications: Fixed Asset Book
- Oracle E-Business Suite: Fixed Asset Book EBS
- Oracle PeopleSoft: Fixed Asset Book PSFT

To enable initialization blocks, follow the steps below:

1. In Oracle BI Administration Tool, edit the BI metadata repository (for example, OracleBIAnalyticsApps.rpd).
2. Choose Manage, then Variables.
3. Under Session – Initialization Blocks, open the initialization block that you need to enable.
4. Clear the **Disabled** check box.
5. Save the metadata repository (RPD file).

Configuring BI Duty Roles

The following BI Duty Role is applicable to the Fixed Asset subject areas for E-Business Suite:

- Fixed Asset Accounting Manager EBS

These Duty Roles control the subject areas and dashboard content to which the user has access. These Duty Roles also ensure the data security filters are applied to all the queries. For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

A.1.9 How to Set Up Fixed Asset Security for PeopleSoft

Financial Analytics supports security over fixed asset books in Fixed Asset subject areas. The list of asset books that a user has access to is determined by the grants in PeopleSoft.

In order for data security filters to be applied, appropriate initialization blocks need to be enabled depending on the deployed source system. To enable Fixed Asset security for PeopleSoft, enable Oracle PeopleSoft initialization block and make sure the initialization blocks of all other source systems are disabled. The initialization block names relevant to various source systems are given below. If more than one source system is deployed, then you must also enable the initialization blocks of those source systems.

- Oracle Fusion Applications: Fixed Asset Book
- Oracle E-Business Suite: Fixed Asset Book EBS
- Oracle PeopleSoft: Fixed Asset Book PSFT

To enable initialization blocks, follow the steps below:

1. In Oracle BI Administration Tool, edit the BI metadata repository (for example, OracleBIAnalyticsApps.rpd).
2. Choose Manage, then Variables.
3. Under Session – Initialization Blocks, open the initialization block that you need to enable.
4. Clear the **Disabled** check box.
5. Save the metadata repository (RPD file).

Configuring BI Duty Roles

The following BI Duty Role is applicable to the Fixed Asset subject areas for PeopleSoft:

- Fixed Asset Accounting Manager PSFT

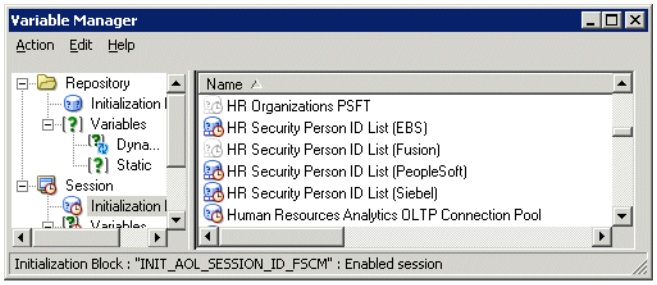
These Duty Roles control the subject areas and dashboard content to which the user has access. These Duty Roles also ensure the data security filters are applied to all the queries. For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

A.1.10 How to Set Up Manager Hierarchy Base Security for Peoplesoft

Note that although the task title mentions PeopleSoft adaptor, it applies to all AU customers who implement manager or resource hierarchy based security.

Manager/Resource hierarchy based security in PS1 is implemented by using the initialization block Manager Hierarchy Level and one or multiple of the initialization blocks HR Security Person ID List (Fusion), HR Security Person ID List (Siebel), HR Security Person ID List (EBS), and HR Security Person ID List (PeopleSoft) that correspond to the adaptors of your choice. Initialization block Manager Hierarchy Level depends on those HR Security Person ID List initialization blocks.

In the security implementation, you must first identify how many of these HR Security Person ID List initialization blocks you have in your BI metadata repository. Note that not all of them might exist in your RPDs depending on the specific Oracle BI Applications products (for example, CRM, HCM, etc) that you are using. In what follows, we assume that all four of them exist in your RPD (but you might just see a subset of them in reality).



HR Organizations PSFT
HR Security Person ID List (EBS)
HR Security Person ID List (Fusion)
HR Security Person ID List (PeopleSoft)
HR Security Person ID List (Siebel)
Human Resources Analytics OLTP Connection Pool

Initialization Block : "INIT_AOL_SESSION_ID_FSCM" : Enabled session

By default (that is, on installation), the initialization block HR Security Person ID List (Fusion) is disabled. As a security best practice, you should disable unused initialization blocks. If unused initialization blocks are not disabled, then they will be run to populate their corresponding variables. Although different AU adaptors have different data structures and formats to store employee information, this might lead to (in very rare cases) more than one eligible employee login ID value to be used in Manager Hierarchy Level, which will in turn impact the security setting.

Specifically:

- if you are implementing EBS, then only HR Security Person ID List (EBS) must be enabled, while HR Security Person ID List (Siebel) and HR Security Person ID List (PeopleSoft) must be disabled.

- if you are implementing PeopleSoft, then only HR Security Person ID List (PeopleSoft) must be enabled, while HR Security Person ID List (EBS) and HR Security Person ID List (Siebel) must be disabled.

- if you are implementing Siebel, then only HR Security Person ID List (Siebel) must be enabled, while HR Security Person ID List (EBS) and HR Security Person ID List (PeopleSoft) must be disabled.

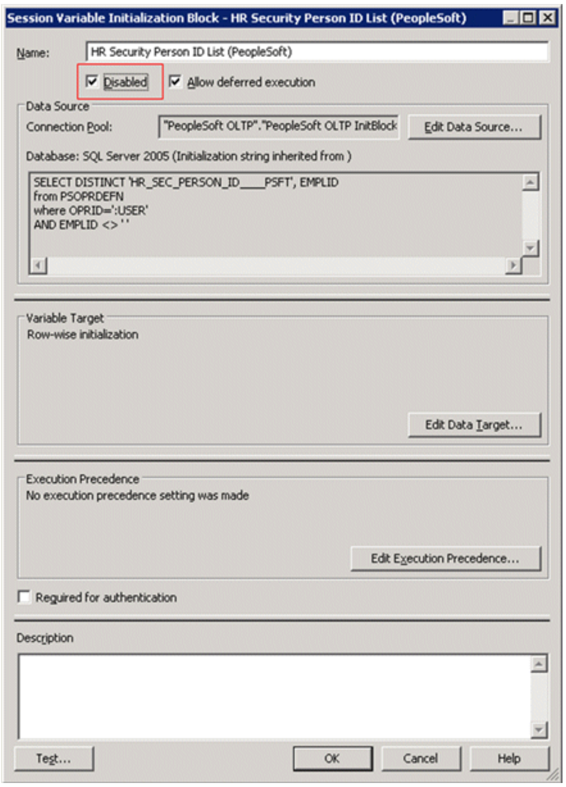
- if you are implementing both EBS and PeopleSoft, then HR Security Person ID List (EBS) and HR Security Person ID List (PeopleSoft) must be enabled, while HR Security Person ID List (Siebel) must be disabled.

- if you are implementing both EBS and Siebel, then HR Security Person ID List (EBS) and HR Security Person ID List (Siebel) must be enabled, while HR Security Person ID List (PeopleSoft) must be disabled.

- if you are implementing both Siebel and PeopleSoft, then HR Security Person ID List (Siebel) and HR Security Person ID List (PeopleSoft) must be enabled, while HR Security Person ID List (EBS) must be disabled.

- if you are implementing all EBS, Siebel and PeopleSoft, then all HR Security Person ID List (EBS), HR Security Person ID List (Siebel) and HR Security Person ID List (PeopleSoft) must be enabled.

The screenshot below shows an example using HR Security Person ID List (PeopleSoft).



Session Variable Initialization Block - HR Security Person ID List (PeopleSoft)

Name: HR Security Person ID List (PeopleSoft)

☑ Disabled ☑ Allow deferred execution

Data Source

Connection Pool: "PeopleSoft OLTP"."PeopleSoft OLTP InitBlock

Database: SQL Server 2005 (Initialization string inherited from)

```
SELECT DISTINCT 'HR_SEC_PERSON_ID____PSFT', EMPLID
from PSOPRDEFN
where OPRID=':USER'
AND EMPLID <> ''
```

Variable Target

Row-wise initialization

Execution Precedence

No execution precedence setting was made

☐ Required for authentication

Description

Click OK after this setting.

Do the same to the initialization blocks corresponding to other AU adaptors that you want to enable/disable.

Save your changes after your setting.

A.1.11 How to Set Up Project Cost and Control Security for PeopleSoft

Overview

Oracle Project Analytics supports security over the following dimensions in Project Costing and Project Control subject areas.

Table A–1 Supported Project Costing and Project Control subject areas

Project Costing and Control Facts Security Entity	Cost	Commitment	Budget	Forecast
Project Business Unit	Y	Y	Y	Y
Project Organization	N	N	N	N
Expenditure Business Unit	N	N	N	N
Contract Business Unit	N	N	N	N
Project	Y	Y	Y	Y
Resource Organization	N	N	N	N
Ledger	N	N	N	N

Configuring Project Cost and Control Security For PeopleSoft

In order for data security filters to be applied, appropriate initialization blocks need to be enabled depending on the deployed source system.

> **Note:** On installation, initialization blocks are enabled for E-Business Suite R12. If you are deploying on a source system other than E-Business Suite R12, then you must enable the appropriate initialization blocks.

To enable data security for Project Cost and Control in PeopleSoft, based on your PeopleSoft security configuration enable PeopleSoft data security initialization blocks listed below and make sure the initialization blocks of all other source systems are disabled. If more than one source system is deployed, then you must also enable the initialization blocks of those source systems.

About Data Security Configuration in PeopleSoft

In PeopleSoft, you access the security configuration pages for securing Project transactions by selecting Main Menu, then Set up Financials/Supply Chain, then Security, then Security Options.

A.1.11.1 Security by Business Unit

Init Blocks:

- Project Business Unit List Budget PSFT
- Project Business Unit List Costing PSFT
- Project Business Unit List Forecast PSFT
- Expenditure Business Unit List PSFT

If you are securing the Project data by Project/Expenditure Business Unit only, then follow the steps below to disable the Project dimension security:

1. In Oracle Enterprise Manager Fusion Middleware Control, select Business Application Instance, then Application Roles, then Select the Oracle BI Applications Stripe, and query for the OBIA_PROJECT_DATA_SECURITY Application Role.

   Note that OBIA_PSFT_PROJECT_DATA_SECURITY is listed as one of the members.

2. Remove OBIA_PSFT_PROJECT_DATA_SECURITY as a member of the OBIA_PROJECT_DATA_SECURITY Duty Role.
3. In Oracle BI Administration Tool, edit the BI metadata repository (for example, OracleBIAnalyticsApps.rpd) in online mode, and select Manage, then Identity, then Action, then Synchronize Application Roles.

A.1.11.2 Security by Project

Init Blocks:

- Project List Budget PSFT
- Project List Costing PSFT
- Project List Forecast PSFT

If you are securing the Project data by Project dimension only, then follow the steps below to disable the Project BU dimension security:

1. Disable Project Business Unit Security, as follows:

   a. In Oracle Enterprise Manager Fusion Middleware Control, select Business Application Instance, then Application Roles, then Select the Oracle BI Applications Stripe, and query for the OBIA_PROJECT_BUSINESS_UNIT_DATA_SECURITY Application Role.

      Note that OBIA_PSFT_PROJECT_DATA_SECURITY is listed as one of the members.

   b. Remove OBIA_PSFT_PROJECT_DATA_SECURITY as a member of the OBIA_PROJECT_BUSINESS_UNIT_DATA_SECURITY Duty Role.

   c. In Oracle BI Administration Tool, edit the BI metadata repository (for example, OracleBIAnalyticsApps.rpd). in online mode, and select Manage, then Identity, then Action, then Synchronize Application Roles.

2. Disable Expenditure Business Unit Security, as follows:

   a. In Oracle Enterprise Manager Fusion Middleware Control, select Business Application Instance, then Application Roles, then Select the Oracle BI Applications Stripe, and query for the OBIA_PROJECT_EXPENDITURE_BUSINESS_UNIT_DATA_SECURITY Application Role.

      Note that OBIA_PSFT_PROJECT_DATA_SECURITY is listed as one of the members.

   b. Remove OBIA_PSFT_PROJECT_DATA_SECURITY as a member of the OBIA_PROJECT_EXPENDITURE_BUSINESS_UNIT_DATA_SECURITY.

   c. In Oracle BI Administration Tool, edit the BI metadata repository (for example, OracleBIAnalyticsApps.rpd) in online mode, and select Manage, then Identity, then Action, then Synchronize Application Roles.

A.1.11.3 Configuring BI Duty Roles

The following BI Duty Roles are applicable to the Project Costing and Control subject area.

- OBIA_PSFT_PROJECT_EXECUTIVE_ANALYSIS_DUTY
- OBIA_PSFT_PROJECT_MANAGEMENT_ANALYSIS_DUTY
- OBIA_PSFT_PROJECT_DATA_SECURITY

These Duty Roles control the subject areas and dashboard content to which the user has access. These Duty Roles also ensure the data security filters are applied to all the queries. For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

A.1.12 How to Set Up Project Billing and Revenue Security for Peoplesoft

Overview

Oracle Project Analytics supports security over the following dimensions in Project Billing and Revenue subject areas.

Table A–2 Supported Project Billing and Revenue subject areas

Project Costing and Control Facts Security Entity	Billing	Revenue	Contract	Funding	Cross Charge-Receiver	Cross Charge - Provider	Cross Charge - Invoice	Cross Charge - Revenue
Project Business Unit	Y	Y	N	Y	Y	N	Y	Y
Project Organization	N	N	N	N	N	N	N	N
Expenditure Business Unit	N	N	N	N	N	Y	N	N
Contract Business Unit	Y	Y	Y	Y	N	N	N	Y
Project	Y	Y	N	Y	Y	Y	Y	Y
Resource Organization	N	N	N	N	N	N	N	N
Ledger	N	N	N	N	N	N	N	N

Configuring Project Billing and Revenue Security for PeopleSoft

In order for data security filters to be applied, appropriate initialization blocks need to be enabled depending on the deployed source system.

> **Note:** On installation, initialization blocks are enabled for E-Business Suite R12. If you are deploying on a source system other than E-Business Suite R12, then you must enable the appropriate initialization blocks.

You must enable data security for Project Billing & Revenue in PeopleSoft, based on your PeopleSoft security configuration. If security by Business Unit has been implemented, then follow the Security by Business Unit Section (ignore Security by Projects section); if security by projects has been implemented, then follow the Security by Projects section (ignore Security by Business Unit section) and enable data security initialization blocks listed in sections below. If only one source system is deployed, then you must make sure that all Project Security initialization blocks for other adapters are disabled. If more than one source system is deployed, then you must also enable the initialization blocks of those source systems.

About Data Security Configuration in PeopleSoft

In PeopleSoft, you access the security configuration pages for securing Project transactions by selecting Main Menu, then Set up Financials/Supply Chain, then Security, then Security Options.

Depending on your security configuration, you need to use any combination of the Project Business Unit or Project dimension that are supported. Based on that, you to change the default installed configuration to match the OLTP security setup.

A.1.12.1 Security by Business Unit

Init Blocks:

- Expenditure Business Unit List PSFT
- Project Business Unit List Funding PSFT
- Project Business Unit List Invoice PSFT

- Project Business Unit List Revenue PSFT
- Project Contract Business Unit List PSFT
- Project Contract Business Unit List Invoice PSFT
- Project Contract Business Unit List Revenue PSFT

If you are securing the Project data by Project /Expenditure/Contract Business Unit only, then follow the steps below to disable the Project dimension security:

1. In Oracle Enterprise Manager Fusion Middleware Control, select Business Application Instance, then Application Roles, then Select the Oracle BI Applications Stripe, and query for the OBIA_PROJECT_DATA_SECURITY Application Role.

   Note that OBIA_PSFT_PROJECT_DATA_SECURITY is listed as one of the members.

2. Remove OBIA_PSFT_PROJECT_DATA_SECURITY as a member of the OBIA_PROJECT_DATA_SECURITY Duty Role.

3. In Oracle BI Administration Tool, edit the BI metadata repository (for example, OracleBIAnalyticsApps.rpd) in online mode, and select Manage, then Identity, then Action, then Synchronize Application Roles.

   Alternatively this step can be performed by restarting all BI Services.

A.1.12.2 Security by Project

Init Blocks:

- Project List Funding PSFT
- Project List Invoice PSFT
- Project List Revenue PSFT

If you are securing the Project data by Project dimension only, then follow the steps below to disable the Project BU dimension security:

1. Disable Project Business Unit Security, as follows:

   a. In Oracle Enterprise Manager Fusion Middleware Control, select Business Application Instance, then Application Roles, then Select the Oracle BI Applications Stripe, and query for the OBIA_PROJECT_BUSINESS_UNIT_DATA_SECURITY Application Role.

      Note that OBIA_PSFT_PROJECT_DATA_SECURITY is listed as one of the members.

   b. Remove OBIA_PSFT_PROJECT_DATA_SECURITY as a member of the OBIA_PROJECT_BUSINESS_UNIT_DATA_SECURITY Duty Role.

   c. In Oracle BI Administration Tool, edit the BI metadata repository (for example, OracleBIAnalyticsApps.rpd) in online mode, and select Manage, then Identity, then Action, then Synchronize Application Roles.

      Alternatively this step can be performed by restarting all BI Services.

2. Disable Expenditure Business Unit Security, as follows:

   a. In Oracle Enterprise Manager Fusion Middleware Control, select Business Application Instance, then Application Roles, then Select the Oracle BI Applications Stripe, and query for the OBIA_PROJECT_EXPENDITURE_BUSINESS_UNIT_DATA_SECURITY Application Role.

Note that OBIA_PSFT_PROJECT_DATA_SECURITY is listed as one of the members.

   b. Remove OBIA_PSFT_PROJECT_DATA_SECURITY as a member of the OBIA_PROJECT_EXPENDITURE_BUSINESS_UNIT_DATA_SECURITY Duty Role.

   c. In Oracle BI Administration Tool, edit the BI metadata repository (for example, OracleBIAnalyticsApps.rpd) in online mode, and select Manage, then Identity, then Action, then Synchronize Application Roles.

3. Disable security filters, as follows:

   a. In Oracle BI Administration Tool, select Manage, then Identity, then OBIA_PROJECT_CONTRACT_BUSINESS_UNIT_DATA_SECURITY, then Permissions, then Data Filters, then Disable data security filters for all facts except Funding and Contract.

A.1.12.3 Configuring BI Duty Roles

The following BI Duty Roles are applicable to the Project Costing and Control subject area.

- OBIA_PSFT_PROJECT_EXECUTIVE_ANALYSIS_DUTY
- OBIA_PSFT_PROJECT_MANAGEMENT_ANALYSIS_DUTY
- OBIA_PSFT_PROJECT_DATA_SECURITY

These Duty Roles control the subject areas and dashboard content to which the user has access. These Duty Roles also ensure the data security filters are applied to all the queries.

For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

A.1.13 How to Define New Groups and Mappings for Users and BI Roles

Note: The following terms are synonymous:

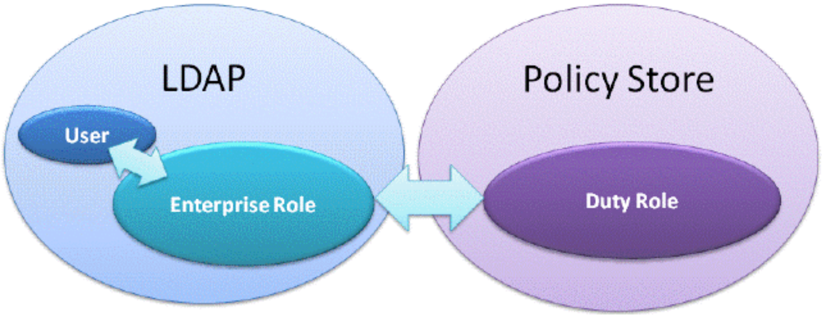
- Enterprise Role

- Job Role

- Group

Oracle BI Applications implements data and object security using a set of BI Duty Roles. BI Users are provisioned with BI Duty Roles via Enterprise Roles in LDAP, as illustrated in the figure below.

Figure A–1 Relationship between Users, Enterprise Roles, and Duty Roles



To simplify security provisioning, each BI Duty Role encapsulates all object and data security access required for a particular BI application area. Therefore, you typically only need to provision a BI User with a single Duty Role in order to enable them to access a specific application area. For example, the BI Duty Role 'Fixed Asset Accounting Manager EBS' provides the encapsulation for EBS Fixed Asset Accounting security.

There are two ways to provision a BI User with a Duty Role:

- Use Fusion Middleware (FMW), as described in Section A.1.13.1, "How to Use Fusion Middleware (FMW) to Provision a BI User".
- Use RPD init block to associate a BI User with a Duty Role, as described in Section A.1.13.2, "How to Use An RPD Init Block to Provision a BI User".

A.1.13.1 How to Use Fusion Middleware (FMW) to Provision a BI User

Overview

To use the FMW provisioning for BI Duty Roles, the BI Users and Enterprise Roles must be present in an LDAP and that LDAP should have been configured as the source for authentication for BI. If your installation has existing Enterprise Roles that you wish to use for BI security, then you might consider using this approach.

In this approach, you can use your own Enterprise Roles to associate BI Duty Roles to BI Users, or you can use the default Enterprise Roles provided with Oracle WebLogic Server LDAP. A BI User with one of the default Enterprise Roles automatically inherits the associated default Duty Roles.

Using Your Own Enterprise Roles with the Default Duty Roles

For example, assume the following scenario:

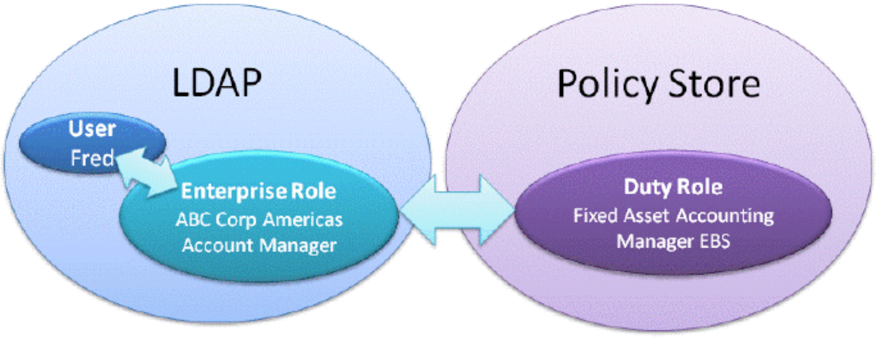
- Your LDAP has Enterprise Role 'ABC Corp Americas Account Manager'.

- BI Users and Enterprise Roles are present in this LDAP.

- This LDAP is used as source for authentication for the BI installation.

Use Oracle Enterprise Manager Fusion Middleware Control in the BI instance and make the Enterprise Role 'ABC Corp Americas Account Manager' a member of BI Duty Role 'Fixed Asset Accounting Manager EBS'.

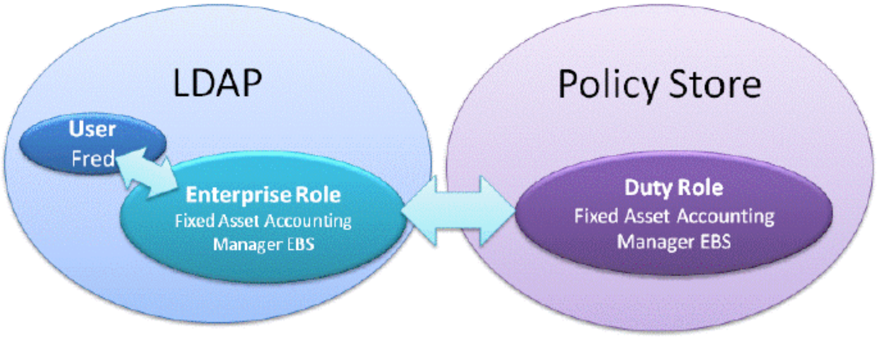
BI Users (for example, Fred) with Enterprise Role 'ABC Corp Americas Account Manager' inherit BI Duty Role 'Fixed Asset Accounting Manager EBS', and have security access for Fixed Assets Accounting reporting for EBS, as illustrated in the diagram below.



Using the Default Enterprise Roles with the Default Duty Roles

Oracle BI Applications provides a sample set of Enterprise Roles (also known as Groups) that inherit the BI Duty Role hierarchy. For example, the default Enterprise Role 'Fixed Asset Accounting Manager EBS' is a member of BI Duty Role 'Fixed Asset Accounting Manager EBS'.

BI Users (for example Fred) with Enterprise Role 'Fixed Asset Accounting Manager EBS' automatically inherit BI Duty Role 'Fixed Asset Accounting Manager EBS', and have security access for Fixed Assets Accounting reporting for EBS, as illustrated in the diagram below.



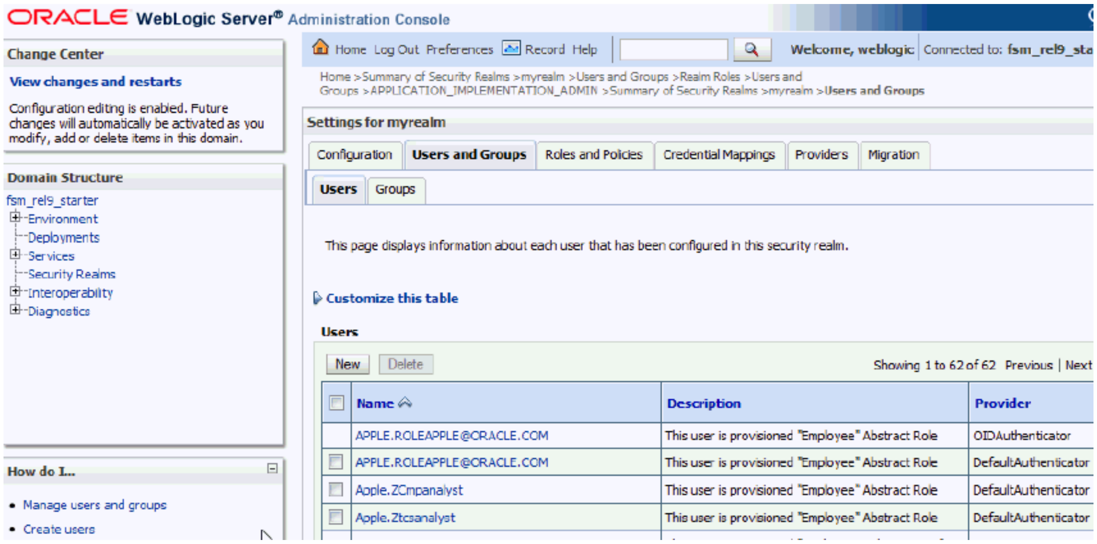
A.1.13.1.1 How to provision BI Users in the installed Oracle Weblogic Server LDAP Use the default installed Oracle Weblogic Server LDAP and default Enterprise Roles.

To provision BI Users:

1. Use the security FSM Tasks for your Offerings to determine the Init Blocks and Duty Roles required by BI Users.

   In addition to the information in the FSM Tasks for security, use *Content Guide for Oracle BI Applications* for a definitive list of default Duty Roles and Enterprise Roles required by BI Users (refer to Tech Note 1639479.1 on My Oracle Support).

2. Use Oracle WebLogic Server Administration Console to assign each BI User to the appropriate Enterprise Role/Group for the Duty Role that the User requires.


ORACLE WebLogic Server® Administration Console
Change Center
View changes and restarts
Home Log Out Preferences Record Help
Welcome, weblogic Connected to: fsm_rel9_sta
Home >Summary of Security Realms >myrealm >Users and Groups >Realm Roles >Users and Groups >APPLICATION_IMPLEMENTATION_ADMIN >Summary of Security Realms >myrealm >Users and Groups
Settings for myrealm
Configuration
Users and Groups
Roles and Policies
Credential Mappings
Providers
Migration
Users
Groups
Domain Structure
fsm_rel9_starter
Environment
Deployments
Services
Security Realms
Interoperability
Diagnostics
Customize this table
Users
New
Delete
Showing 1 to 62 of 62 Previous | Next
How do I...
Manage users and groups
Create users

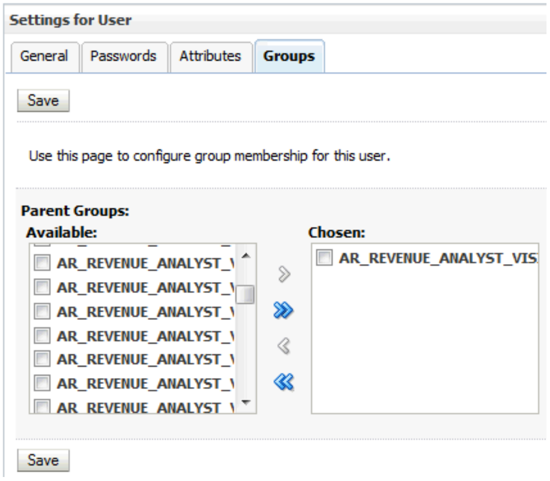
Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

This page displays information about each user that has been configured in this security realm.

	Name	Description	Provider
	APPLE.ROLEAPPLE@ORACLE.COM	This user is provisioned "Employee" Abstract Role	OIDAuthenticator
□	APPLE.ROLEAPPLE@ORACLE.COM	This user is provisioned "Employee" Abstract Role	DefaultAuthenticator
□	Apple.ZCmpanalyst	This user is provisioned "Employee" Abstract Role	DefaultAuthenticator
□	Apple.Ztcsanalyst	This user is provisioned "Employee" Abstract Role	DefaultAuthenticator

For example, if you assign BI User Fred to the Enterprise Role 'Fixed Asset Accounting Manager EBS', then Fred automatically inherits the BI Duty Role 'Fixed Asset Accounting Manager EBS'.

To assign a BI User to an Enterprise Role/Group, select Security Realms, then Users and Groups, then Users, then select a BI User, and use the Groups tab to specify one or more Enterprise Roles/Groups.



Use this page to configure group membership for this user.

Available:
□ AR_REVENUE_ANALYST_\
□ AR_REVENUE_ANALYST_\
□ AR_REVENUE_ANALYST_\
□ AR_REVENUE_ANALYST_\
□ AR_REVENUE_ANALYST_\
□ AR_REVENUE_ANALYST_\
□ AR_REVENUE_ANALYST_\

Chosen:
□ AR_REVENUE_ANALYST_VIS

Refer to the Weblogic Server Administration Console Help for detailed instructions.

A.1.13.1.2 How to provision BI Users using your own LDAP If your installation has an existing LDAP (and you do not wish to use the default Oracle WebLogic Server LDAP) that is being used for authentication, then you can create your own Enterprise Roles, or copy/migrate the Enterprise Roles from the installed Oracle WebLogic Server LDAP to your LDAP.

To provision BI Users:

1. Use the security FSM Tasks for your Offerings to determine the Init Blocks and Duty Roles required by BI Users.

In addition to the information in the FSM Tasks for security, use *Content Guide for Oracle BI Applications* for a definitive list of default Duty Roles and Enterprise Roles required by BI Users (refer to Tech Note 1639479.1 on My Oracle Support).

2. If you want to deploy the default Enterprise Roles/Groups from Oracle WebLogic Server LDAP, then copy or migrate the Enterprise Roles/Groups to your LDAP.
3. Use native LDAP tools to assign each BI User to an appropriate Enterprise Role/Group for the Duty Role that the BI User requires.

   For example, if you assign BI User Fred to the Enterprise Role 'Fixed Asset Accounting Manager EBS', then Fred automatically inherits the BI Duty Role 'Fixed Asset Accounting Manager EBS'.

4.Make sure that each Enterprise Role is associated with the correct Duty Role.

A.1.13.2 How to Use An RPD Init Block to Provision a BI User

For each Offering and Functional Area, FSM Tasks for security typically specify:

- Init Blocks that you need to enable.

- Duty Roles that BI Users require.

Oracle BI Applications provides an Init block named 'Authorization' that queries the roles/responsibilities associated to users in the source system and populates a Oracle BI EE variable called GROUP. Oracle BI EE associates BI Duty Roles to users that are populated in the GROUP variable.

For example, to associate BI Duty Role 'Fixed Asset Accounting Manager EBS' to a user using Init block approach, do the following:

1. In Oracle BI Administration Tool, if the 'Authorization' Init block if disabled, then you must enable it, as follows:
   a. Edit the BI metadata repository (for example, OracleBIAnalyticsApps.rpd).
   b. Navigate to Manage, then Variables, then Session – Initialization Blocks (Inventory Organizations EBS).
   c. Open the initialization block (Inventory Organizations EBS).
   d. Clear the **Disabled** check box.
2. Update the Init block SQL to use the EBS SQL used to populate users' EBS responsibilities.

   Oracle BI Applications provides different SQL statements for E-Business Suite, Siebel, and PeopleSoft for this Init block.
3. Create responsibility 'Fixed Asset Accounting Manager EBS' in the E-Business Suite source system and assign it to the user.
4. When the init block is run for the user, the GROUP variable will be populated with value 'Fixed Asset Accounting Manager EBS'.

   The BI server will then assign BI Duty Role 'Fixed Asset Accounting Manager EBS' to the user (that is, the BI Duty Role of the same name).
5. If the user has multiple responsibilities in the source system, then the GROUP variable will contain the names of all of the responsibilities.

   Oracle BI EE will assign BI Duty Roles that match any names contained in the GROUP variable. If one of the names within the GROUP variable does not matches any BI Duty Role, then Oracle BI EE will ignore that name. For example, if the GROUP variable contains the value (A, B, C, D) and if BI Duty Roles of names

A, B and C exist, then the user will be assigned BI Duty Roles (A, B, C). The value D will be ignored.

A.1.14 How to Set Up Project Billing and Revenue Security For Oracle

Overview

Oracle Project Analytics supports security over the following dimensions in Project Billing and Revenue subject areas.

Table A–3 Supported Project Billing and Revenue subject areas

Project Costing and Control Facts Security Entity	Billing	Reve nue	Contr act	Fund ing	Cros s Char ge-Rece iver	Cros s Char ge - Provi der	Cros s Char ge - Invoi ce	Cros s Char ge - Reve nue
Project Business Unit	Y	Y	N	Y	Y	N	Y	Y
Project Organization	Y	Y	N	Y	Y	N	Y	Y
Expenditure Business Unit	N	N	N	N	N	Y	N	N
Contract Business Unit	Y	Y	Y	Y	N	N	N	Y
Project	Y	Y	N	Y	Y	Y	Y	Y
Resource Organization	N	N	N	N	N	N	N	N
Ledger	N	N	N	N	N	N	N	N

Configuring Project Billing and Revenue Security for Oracle Fusion

In order for data security filters to be applied, ensure that the following initialization blocks are enabled depending on the deployed source system.

> **Note:** On installation, initialization blocks are enabled for E-Business Suite R12. If you are deploying on a source system other than E-Business Suite R12, then you must enable the appropriate initialization blocks.

You must disable Project Security initialization blocks for all other adapters. If more than one source system is deployed, make sure that the initialization blocks of those source systems are enabled.

Init Blocks:

- Project Business Unit List Funding Fusion
- Project Business Unit List Invoice Fusion
- Project Business Unit List Revenue Fusion
- Project Contract Business Unit List Fusion
- Project Contract Business Unit List Invoice Fusion
- Project Contract Business Unit List Revenue Fusion
- Project List Funding Fusion
- Project List Invoice Fusion

- Project List Revenue Fusion
- Project Organization List Funding Fusion
- Project Organization List Invoice Fusion
- Project Organization List Revenue Fusion

A.1.14.1 Configuring BI Duty Roles

The following BI Duty Roles are applicable to the Project Costing and Control subject area.

- OBIA_PROJECT_EXECUTIVE_ANALYSIS_DUTY
- OBIA_PROJECT_MANAGEMENT_ANALYSIS_DUTY

These Duty Roles control the subject areas and dashboard content to which the user has access. These Duty Roles also ensure the data security filters are applied to all the queries.

For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

A.1.15 How to Set Up Project Cost and Control Security for Oracle Fusion

Overview

Oracle Project Analytics supports security using the following dimensions in Project Costing and Project Control subject areas.

Table A–4 Supported security dimensions in Project Costing and Project Control subject areas

Project Costing and Control Facts Security Entity	Cost	Commitment	Budget	Forecast
Project Business Unit	Y	Y	Y	Y
Project Organization	Y	Y	Y	Y
Expenditure Business Unit	Y	Y	N	N
Contract Business Unit	N	N	N	N
Project	Y	Y	Y	Y
Resource Organization	N	N	N	N
Ledger	N	N	N	N

Configuring Project Cost and Control Security For Oracle Fusion Applications

In order for data security filters to be applied, appropriate initialization blocks need to be enabled depending on the deployed source system.

> **Note:** On installation, initialization blocks are enabled for E-Business Suite R12. If you are deploying on a source system other than E-Business Suite R12, then you must enable the appropriate initialization blocks.

You need to ensure that all Project Security initialization blocks for other adapters are disabled. If more than one source system is deployed, then you must enable the initialization blocks of those source systems.

Init Blocks:

- Expenditure Business Unit List Fusion
- Project Business Unit List Budget Fusion
- Project Business Unit List Costing Fusion
- Project Business Unit List Forecast Fusion
- Project List Budget Fusion
- Project List Costing Fusion
- Project List Forecast Fusion
- Project Organization List Budget Fusion
- Project Organization List Costing Fusion
- Project Organization List Forecast Fusion

A.1.15.1 Configuring BI Duty Roles

The following BI Duty Roles are applicable to the Project Costing and Control subject area.

- OBIA_PROJECT_EXECUTIVE_ANALYSIS_DUTY
- OBIA_PROJECT_MANAGEMENT_ANALYSIS_DUTY

These Duty Roles control the subject areas and dashboard content to which the user has access. These Duty Roles also ensure the data security filters are applied to all the queries.

For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

A.1.16 How to Set Up CRM Primary Organization Based Security for Siebel

Overview

Siebel CRM primary organization based security is applied in partner subject areas. In Siebel partner application, primary organization is basically the partner organization that the partner user belongs to. Primary organization based security gives the partner user access to only the entities of which his partner organization is the primary owner organization.

Configuring Primary Organization Based Security

The session variable ORGANIZATION store the list organization ID that the user belongs to. It is initialized via the Init Block 'Orgs for Org-Based Security' when user logs in and then used as data filter in the primary organization based data security Duty Role.

A.1.16.1 Configuring BI Duty Roles

'Primary Org-Based Security' is the internal BI Duty Role to define data filter for primary organization based data security. And by default, it has the following members:

- Partner Executive Analytics User
- Partner Operations Analytics User
- Partner Sales Manager Analytics User
- Partner Service Manager Analytics User

These Duty Roles control the subject areas and dashboard content to which the user has access. As member of 'Primary Org-Based Security', they also ensure that the primary organization based data security filters are applied.

For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

A.1.17 How to Set Up CRM Primary Employee/Position Hierarchy Based Security for Siebel

Overview

Primary employee/position hierarchy based security is widely used in many CRM subject areas, such as Sales, Marketing and Partner Management. For Siebel data source, CRM BI shares the same concept of Position and Position Hierarchy as they are defined in Siebel application.

Primary Employee/Position Hierarchy Based Security control starts with user's login and the login's level in the position hierarchy. User's login is then compared with the login defined at that particular level in position hierarchy as data filter in queries. By this way, user is granted with data visibility to the transactions as direct owner and the transactions owned by his/her subordinates.

Note: In CRM Siebel Forecasting Analytics, in addition to the position hierarchy, more data visibility is granted to the login user via 'Indirect Sales Hierarchy', which is originally defined in Siebel Forecasting application and brought over to DW by ETL.

Configuring Resource Hierarchy Based Security

There are two session variables used in 'Primary Employee/Position Hierarchy Based Security' for Siebel.

- USER is the OBIEE system session variable, which is populated automatically when an user logs onto BI.
- HIER_LEVEL contains level defined in position hierarchy that the login user belongs to. This variable is initialized via the session Init Block 'User Hierarchy Level'.

A.1.17.1 Configuring BI Duty Roles

All the primary employee and position based security roles should be defined as member of the internal role 'Primary Employee/Position Hierarchy-based Security'. In the default configuration, 'Primary Employee/Position Hierarchy-based Security' has the following members.

- Partner Sales Rep Analytics User

- Partner Service Rep Analytics User
- Pricing Manager
- Primary Owner-Based Security
- Sales Manager Analytics
- Sales Representative Analytics
- Usage Accelerator - Sales Manager

These Duty Roles also control which subject areas and dashboard content the user can get access to.

For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

A.1.18 How to Set Up SIA Student Financial Security for Peoplesoft

The Student Financial module is secured by Business Unit and Academic Institution, (except the Credit history Subject Area, which is only secured by Business Unit). From the object security perspective, the table below shows the default job roles for Student Financial module access.

Table A–5 Role names and Descriptions for Student Financial Analytics

Role Name	Description
Bursar	Manages student receivables, student tuition and fee charges, student billing, student payments and student collections.
Campus Solutions Administrator	Administrator of Campus Solutions.
Student	Student of the Academic Institution.

The table below shows the Duty Roles and data security roles that are used by the Student Financial module.

Table A–6 Role Names and Roles Types for Student Financial Analytics

Role Name	Role Type
OBIA_Student_Accounts_Analysis_Duty	Duty Role
OBIA_SIA_Admin_Analysis_Duty	Duty Role
OBIA_Student_Analysis_Duty	Duty Role
OBIA_STUDENT_INSTITUTION_DATA_SECURITY	Data Security Role
OBIA_STUDENT_BUSINESS_UNIT_DATA_SECURITY	Data Security Role
OBIA_STUDENT_DATA_SECURITY	Data Security Role

To set up SIA Student Financial Security for Peoplesoft:

1. Log into Oracle WebLogic Server Administration Console.
2. Click the 'Lock and Edit' button.
3. Navigate to Security Realms, then myrealm, then Users and Groups, then Users.
4. On the Users tab, create a new user.

Ensure that the same user is present in the Peoplesoft Campus Solution OLTP system.

5. Navigate to Security Realms, then myrealm, then Users and Groups, then Groups.
6. On the Groups tab, create the same group as that available in the JAZN file.

   For example, Bursar, or Admissions Manager.
7. Navigate to Security Realms, then myrealm, then Users and Groups, then Users, and click on the newly created user.
8. Click on the groups tab and associate the user with the appropriate application role along with BIAuthors and BIConsumers roles and save the changes.
9. Click the Release Configuration button.

All role mappings are accomplished inside the JAZN file, which is provided with the Oracle BI Applications installation. Any new role mapping is a part of the customization effort and the JAZN file needs to be updated.

A.1.19 How to Set Up SIA Administration Recruiting Security for Peoplesoft

The Student Financial module is secured by Business Unit and Academic Institution, (except the Credit history Subject Area, which is only secured by Business Unit). From the object security perspective, the table below shows the default job roles for Student Financial module access.

Table A–7 Role names and Descriptions for Student Financial Analytics

Role Name	Description
Admissions Manager	Manages Recruiting processes to meet the enrollment targets.
Campus Solutions Administrator	Administrator of Campus Solutions.

The table below shows the Duty Roles and data security roles that are used by the Admissions and Recruiting module.

Table A–8 Role Names and Role Types for Admissions and Recruiting

Role Name	Role Type
OBIA_Student_Admissions_Analysis_Duty	Duty Role
OBIA_SIA_Admin_Analysis_Duty	Duty Role
OBIA_STUDENT_INSTITUTION_DATA_SECURITY	Data Security Role

To set up SIA Admissions and Recruiting Security for Peoplesoft:

1. Log into Oracle WebLogic Server Administration Console.
2. Click the 'Lock and Edit' button.
3. Navigate to Security Realms, then myrealm, then Users and Groups, then Users.
4. On the Users tab, create a new user.

   Ensure that the same user is present in the Peoplesoft Campus Solution OLTP system.
5. Navigate to Security Realms, then myrealm, then Users and Groups, then Groups.
6. On the Groups tab, create the same group as that available in the JAZN file.

For example, Bursar, or Admissions Manager.

7. Navigate to Security Realms, then myrealm, then Users and Groups, then Users, and click on the newly created user.
8. Click on the groups tab and associate the user with the appropriate application role along with BIAuthors and BIConsumers roles and save the changes.
9. Click the Release Configuration button.

All role mappings are accomplished inside the JAZN file, which is provided with the Oracle BI Applications installation. Any new role mapping is a part of the customization effort and the JAZN file needs to be updated.

A.1.20 How to Set Up SIA Student Records Security for Peoplesoft

The Student Records module is secured by Academic Institution. From the object security perspective, the table below shows the default job roles that have Student Records module access.

Table A–9 Role names and Descriptions for Student Records

Role Name	Description
Registrar	The Registrar is the head of the Student Records Office and is one of the key owners of the Student Information System.
Campus Solutions Administrator	Administrator of Campus Solutions.
Student	Student of the Academic Institution.

Note: The Student does not have access to the following three Subject Areas:

- Institution summary
- Class instructor
- Class meeting pattern

The table below shows the Duty Roles and data security roles that are used by the Student Records module.

Table A–10 Role Names and Roles Types for Student Records

Role Name	Role Type
OBIA_Student_Records_Analysis_Duty	Duty Role
OBIA_SIA_Admin_Analysis_Duty	Duty Role
OBIA_Student_Analysis_Duty	Duty Role
OBIA_STUDENT_INSTITUTION_DATA_SECURITY	Data Security Role
OBIA_STUDENT_DATA_SECURITY	Data Security Role

To set up SIA Student Records for Peoplesoft:

1. Log into Oracle WebLogic Server Administration Console.
2. Click the 'Lock and Edit' button.
3. Navigate to Security Realms, then myrealm, then Users and Groups, then Users.
4. On the Users tab, create a new user.

Ensure that the same user is present in the Peoplesoft Campus Solution OLTP system.

5. Navigate to Security Realms, then myrealm, then Users and Groups, then Groups.
6. On the Groups tab, create the same group as that available in the JAZN file.

   For example, Bursar, or Admissions Manager.
7. Navigate to Security Realms, then myrealm, then Users and Groups, then Users, and click on the newly created user.
8. Click on the groups tab and associate the user with the appropriate application role along with BIAuthors and BIConsumers roles and save the changes.
9. Click the Release Configuration button.

All role mappings are accomplished inside the JAZN file, which is provided with the Oracle BI Applications installation. Any new role mapping is a part of the customization effort and the JAZN file needs to be updated.

A.1.21 How to Implement Security For Order Management Analytics

To implement security for Oracle Order Management Analytics, do the following:

- For EBS:
  - If you are implementing Inventory Org Based Security, then follow the steps in Section A.1.21.1, "How to implement OM Inventory Org Based Security for EBS".
  - If you are implementing Operating Unit Based Security, then follow the steps in Section A.1.21.3, "How to implement OM Operating Unit Org-based Security for EBS".
  - Then, follow the steps in Section A.1.21.5, "How to Grant Cross Functional Access to Order Management Users".
- For Fusion:
  - If you are implementing Inventory Org Based Security, then follow the steps in Section A.1.21.2, "How to implement OM Inventory Org Based Security for Oracle Fusion Applications".
  - If you are implementing Operating Unit Based Security, then follow the steps in Section A.1.21.4, "How to implement OM Operating Unit Org-based Security for Oracle Fusion Applications".
  - Then, follow the steps in Section A.1.21.5, "How to Grant Cross Functional Access to Order Management Users".

A.1.21.1 How to implement OM Inventory Org Based Security for EBS

Overview

Order Management Analytics supports security over Inventory Organizations in OM subject areas. The list of Inventory Organizations that a user has access to is determined by the grants in EBS.

Configuring Inventory Org Based Security

In order for data security filters to be applied, appropriate initialization blocks need to be enabled depending on the deployed source system. To enable Inventory Org Based security for EBS, enable E-Business Suite initialization block and make sure the initialization blocks of all other source systems are disabled. The initialization block names relevant to various source systems are given below. If more than one source system is deployed, then you must also enable the initialization blocks of those source systems.

Oracle Fusion Applications: SCOM_AN: SECURITY: Inv Org Shipments List

E-Business Suite: Inventory Organizations EBS

To enable initialization blocks, follow the steps below:

1. In Oracle BI Administration Tool, edit the BI metadata repository (for example, OracleBIAnalyticsApps.rpd).
2. Open the variable by navigating to: Manage, then Variables, then Session, then Variables, then Non-System, then INV_ORG.
3. Open the initialization block by navigating menu: Manage, then Variables, then Session, then Initialization blocks, then Inventory Organizations EBS.
4. Clear the **Disabled** check box.
5. Save the RPD.

A.1.21.1.1 Configuring BI Duty Roles The following BI Duty Roles are applicable to the Order Management subject area.

- Order Management Analyst
- Order Management Executive
- Order Fulfillment Analyst
- Order Fulfillment Executive

These Duty Roles control the subject areas and dashboard content to which the user has access. These Duty Roles also ensure the data security filters are applied to all the queries.

For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

A.1.21.2 How to implement OM Inventory Org Based Security for Oracle Fusion Applications

Overview

Order Management Analytics supports security over Inventory Organizations in OM subject areas. The list of Inventory Organizations that a user has access to is determined by the grants on the Oracle Fusion Applications

Configuring Inventory Org Based Security

In order for data security filters to be applied, appropriate initialization blocks need to be enabled depending on the deployed source system. To enable Inventory Org Based security for Fusion, enable Oracle Fusion initialization block and make sure the initialization blocks of all other source systems are disabled. The initialization block names relevant to various source systems are given below. If more than one source system is deployed, then you must also enable the initialization blocks of those source systems.

Oracle Fusion Applications: SCOM_AN: SECURITY: Inv Org Shipments List

E-Business Suite: Inventory Organizations EBS

To enable initialization blocks, follow the steps below:

1. In Oracle BI Administration Tool, edit the BI metadata repository (for example, OracleBIAnalyticsApps.rpd).
2. Open the variable by navigating to: Manage, then Variables, then Session, then Variables, then Non-System, then INV_ORG_SHIPMENTS.
3. Open the initialization block by navigating menu: Manage, then Variables, then Session, then Initialization blocks, then SCOM_AN:SECURITY:Inv Org Shipments List.
4. Clear the **Disabled** check box.
5. Save the RPD.

A.1.21.2.1 Configuring BI Duty Roles The following BI Duty Roles are applicable to the Order Management subject area.

- OBIA_SHIPPING_MANAGEMENT_ANALYSIS_DUTY
- OBIA_EXTENDED_SHIPPING_MANAGEMENT_ANALYSIS_DUTY

These Duty Roles control the subject areas and dashboard content to which the user has access. These Duty Roles also ensure the data security filters are applied to all the queries.

For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

A.1.21.3 How to implement OM Operating Unit Org-based Security for EBS

Overview

Order Management Analytics supports security over Operating Unit Organizations in OM subject areas. The list of Operating Unit Organizations that a user has access to is determined by the grants in EBS.

Configuring Inventory Org Based Security

In order for data security filters to be applied, appropriate initialization blocks need to be enabled depending on the deployed source system. To enable Operating Unit Org Based security for EBS, enable E-Business Suite initialization block and make sure the initialization blocks of all other source systems are disabled. The initialization block names relevant to various source systems are given below. If more than one source system is deployed, then you must also enable the initialization blocks of those source systems.

Oracle Fusion Applications: Order Fulfillment Orchestration BU List

E-Business Suite: Operating Unit Organizations EBS

To enable initialization blocks, follow the steps below:

1. In Oracle BI Administration Tool, edit the BI metadata repository (for example, OracleBIAnalyticsApps.rpd).
2. Open the variable by navigating to: Manage, then Variables, then Session, then Variables, then Non-System, then OU_ORG____EBS.

3. Open the initialization block by navigating menu: Manage, then Variables, then Session, then Initialization blocks, then Operating Unit Organizations EBS.
4. Clear the **Disabled** check box.
5. Save the RPD.

A.1.21.3.1 Configuring BI Duty Roles The following BI Duty Roles are applicable to the Order Management subject area.

- Order Management Analyst
- Order Management Executive
- Order Fulfillment Analyst
- Order Fulfillment Executive

These Duty Roles control the subject areas and dashboard content to which the user has access. These Duty Roles also ensure the data security filters are applied to all the queries.

For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

A.1.21.4 How to implement OM Operating Unit Org-based Security for Oracle Fusion Applications

Overview

Order Management Analytics supports security over Operating Unit Organizations in OM subject areas. The list of Operating Unit Organizations that a user has access to is determined by the grants on the Oracle Fusion Applications.

Configuring Operating Unit Org Based Security

In order for data security filters to be applied, appropriate initialization blocks need to be enabled depending on the deployed source system. To enable Operating Unit Org Based security for Fusion, enable Oracle Fusion initialization block and make sure the initialization blocks of all other source systems are disabled. The initialization block names relevant to various source systems are given below. If more than one source system is deployed, then you must also enable the initialization blocks of those source systems.

Oracle Fusion Applications: Order Fulfillment Orchestration BU List

E-Business Suite: Operating Unit Organizations EBS

To enable initialization blocks, follow the steps below:

1. In Oracle BI Administration Tool, edit the BI metadata repository (for example, OracleBIAnalyticsApps.rpd).
2. Open the variable by navigating to: Manage, then Variables, then Session, then Variables, then Non-System, then OM_BU.
3. Open the initialization block by navigating menu: Manage, then Variables, then Session, then Initialization blocks, then Order Fulfillment Orchestration BU List.
4. Clear the **Disabled** check box.
5. Save the RPD.

A.1.21.4.1 Configuring BI Duty Roles The following BI Duty Roles are applicable to the Project Costing and Control subject area.

- OBIA_EXTENDED_ORDER_MANAGEMENT_ANALYSIS_DUTY
- OBIA_ORDER_MANAGEMENT_ANALYSIS_DUTY

For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

A.1.21.5 How to Grant Cross Functional Access to Order Management Users

Overview

Clients are accessing data from across the enterprise and delivering deep insight directly to business users. They perform cross-functional analysis to understand cause and affect relationships between key performance indicators across different departments. Cross functional reporting from a variety of relational databases and data sources is possible too. OBIA is a prepackaged data warehouse enabling historical analysis and cross domain insight. Common Conformed Dimensions ensure cross fact, cross subject areas and federated OBIA reporting.

Order Management enables users to analyze OM data along with data from Inventory, Account Receivable, and GL Revenue. Examples of functional reporting:

Q. How many of my top customers bought products from my worst suppliers?

Q. Which of my top suppliers are also my top customers?

E-Business Suite and JD Edwards EnterpriseOne adapters:

By default, Order Management's security implementation for E-Business Suite and JD Edwards EnterpriseOne adapter is enabled with cross-functional capability. The following BI Duty Roles enable users to access to the Order Management subject areas.

- Order Management Analyst
- Order Management Executive
- Order Fulfillment Analyst
- Order Fulfillment Executive
- Order Management Analyst JDE
- Order Management Executive JDE
- Order Fulfillment Analyst JDE
- Order Fulfillment Executive JDE

Table A–11 Duty Roles and Subject Areas

Duty Role Description	Subject Areas:
Order Fulfillment Executive, Order Fulfillment Executive JDE. This role provides secured access to Sales Order fulfillment managers and supply chain executives with insight into orders, backlogs, shipments and inventory to track fulfillment performance.	Sales - Invoice Lines Sales - Schedule Lines Sales - Backlog Lines Sales - Pick Lines Sales - Sales Revenue Sales - Sales Receivables Sales - Sales Overview Sales - Orders, Backlog and Invoices Sales - Order Process Sales - Order Lines Sales - Customer Activity Sales - Inventory & Backlog Sales - Backlog History
Order Fulfillment Analyst, Order Fulfillment Analyst JDE. This role provides secured access to Sales Order fulfillment analysts with detailed insight into order line, booking line and backlog line details.	Sales - Backlog History Sales - Backlog Lines Sales - Booking Lines Sales - Order Lines Sales - Schedule Lines Sales - Invoice Lines Sales - Pick Lines Sales - Sales Revenue Sales - Sales Receivables Sales - Sales Overview Sales - Orders, Backlog and Invoices Sales - Order Process Sales - Customer Activity Sales - Inventory & Backlog
Order Management Analyst, Order Management Analyst JDE. This role provides secured access to Sales Order management analysts with detailed insight into order lines, booking line and invoice line details.	Sales - Overview Sales - Booking Lines Sales - Invoice Lines Sales - Sales Revenue Sales - Orders and Invoices Sales - Orders, Backlog and Invoices Sales - Order Lines Sales - Customer Activity

Table A–11 (Cont.) Duty Roles and Subject Areas

Duty Role Description	Subject Areas:
Order Management Executive, Order Management Executive JDE. This role provides order management executives with secured access to sales revenue, orders, invoices and backlog details.	Sales - Overview Sales - Booking Lines Sales - Invoice Lines Sales - Sales Revenue Sales - Orders and Invoices Sales - Orders, Backlog and Invoices Sales - Order Lines Sales - Customer Activity

Fusion Adapter:

Order Management's security implementation for Fusion adapter has two modes.

For Fusion embedded BI deployment, use these Duty Roles.

OBIA_ORDER_FULFILLMENT_ORCHESTRATION_BUSINESS_UNIT_DATA_SECURITY,

OBIA_INVENTORY_ORGANIZATION_SHIPMENT_DATA_SECURITY.

For OBIA standalone deployment, which requires cross functional reporting, use these Duty Roles.

OBIA_EXTENDED_ORDER_FULFILLMENT_ORCHESTRATION_BUSINESS_UNIT_DATA_SECURITY,

OBIA_EXTENDED_INVENTORY_ORGANIZATION_SHIPMENT_DATA_SECURITY.

The following table shows the subject areas granted to each Duty Roles. Note that the 'extended' roles have broader access.

Table A–12 Duty Roles and Subject Areas

Duty Role Description	Subject Areas
OBIA_SHIPPING_MANAGEMENT_ANALYSIS_DUTY Description - This BI Duty Role is for Shipping Managers who are responsible for overseeing both processes and people for picking, packing and shipping items. This Duty Role allows Shipping Managers to get insight into Shipping, Backlogs, Inventory Transactions and Inventory Balances Is a member of: OBIA_INVENTORY_ORGANIZATION_SHIPMENT_DATA_SECURITY	Sales - Pick Lines
OBIA_EXTENDED_SHIPPING_MANAGEMENT_ANALYSIS_DUTY Description - This Duty Role provides cross-module access to the shipping manager job role for stand-alone content. Member of - OBIA_EXTENDED_INVENTORY_ORGANIZATION_SHIPMENT_DATA_SECURITY	Sales - Pick Lines Sales - Order Process Sales - Inventory & Backlog

Table A–12 (Cont.) Duty Roles and Subject Areas

Duty Role Description	Subject Areas
OBIA_ORDER_MANAGEMENT_ANALYSIS_DUTY Description - This BI Duty Role is for Order Managers who are responsible for processing orders, managing backlogs and optimizing fulfillment performance. This Duty Role allows Order Managers to analyze Orders, Bookings, Holds, Orchestration Process, Shipping, Backlogs, Invoices and Inventory Is a member of: OBIA_ORDER_FULFILLMENT_ORCHESTRATION_BUSINESS_UNIT_DATA_SECURITY	Sales - Backlog History Sales - Backlog Lines Sales - Booking Lines Sales - Order Lines Sales - Schedule Lines Sales - Order Process DOO Process Instances Sales - Order Holds
OBIA_EXTENDED_ORDER_MANAGEMENT_ANALYSIS_DUTY Description - This Duty Role provides cross-module access to the order manager job role for stand-alone content. The cross-module access will include invoice, inventory, backlog, AR and shipping Is a member of: OBIA_EXTENDED_ORDER_FULFILLMENT_ORCHESTRATION_BUSINESS_UNIT_DATA_SECURITY	Sales - Backlog History Sales - Backlog Lines Sales - Booking Lines Sales - Order Lines Sales - Schedule Lines Sales - Invoice Lines Sales - Pick Lines Sales - Sales Revenue Sales - Sales Receivables Sales - Sales Overview Sales - Orders, Backlog and Invoices Sales - Orders & Invoices Sales - Order Process Sales - Customer Activity Sales - Inventory & Backlog Sales - Order Holds DOO Process Instances

How to Grant Cross Functional Access to Order Management Users

Note: The following section describes a post-installation and optional configuration task.

1. To facilitate OM users (such as Order Manager and Shipping Manager) to perform deeper and cross functional analysis apart from their regular duty, Oracle Supply Chain and Order Management Analytics has configured data and functional security to access cross functional information (such as inventory, backlog, shipping information) through extended Duty Roles. If you would like to provision such a duty to the Order Management users, then follow the instructions in this task.

2. Understanding Extended Duty Roles: Seeded security roles for Oracle BI Applications for Fusion Applications includes the following additional Duty Roles. These extended roles are not mapped to any enterprise job roles by default, but they are pre-configured within Oracle BI Applications to enforce object and data level security for Inventory transactions.

3. 'Extended Order Management Analysis Duty' role (Role name: OBIA_EXTENDED_ORDER_MANAGEMENT_ANALYSIS_DUTY) – This Duty Role

provides cross-module access to the order manager job role for stand-alone Oracle BI Applications content. The cross-module access will include invoice, inventory, backlog, AR and shipping information. Data security on Oracle BI Applications is implemented using OBIA_ORDER_FULFILLMENT_ORCHESTRATION_BUSINESS_UNIT_DATA_SECURITY.

4. 'Extended Shipping Management Analysis Duty' role (Role name: OBIA_EXTENDED_SHIPPING_MANAGEMENT_ANALYSIS_DUTY) – This Duty Role provides cross-module access to the shipping manager job role for stand-alone Oracle BI Applications content. The cross-module access will include inventory, backlog and orders information. Data security on Oracle BI Applications is implemented using 'OBIA_INVENTORY_ORGANIZATION_SHIPMENT_DATA_SECURITY'.

5. Follow the steps below to implement Extended Duty Roles in Supply Chain and Order Management Analytics:

   a. Assign BI duty 'OBIA_EXTENDED_ORDER_MANAGEMENT_ANALYSIS_DUTY' to Fusion Applications job role, 'Order Manager' or similar.

   b. Assign BI duty 'OBIA_EXTENDED_SHIPPING_MANAGEMENT_ANALYSIS_DUTY' to Fusion Applications job role, 'Shipping Manager' or similar.

   c. Assign appropriate Fusion Applications Duty Roles to the job role - 'Order Manager' and assign BU privileges. Data security of 'OBIA_ORDER_MANAGEMENT_ANALYSIS_DUTY' (Oracle BI Applications Duty Role) is controlled by the BUs assigned to the user.

   d. Customize Presentation catalog permissions for subject areas including cross functional content (for example Sales - Inventory and Backlog) and Subject Area permissions as desired for below mentioned roles.

A.1.22 How to set up HR Supervisor Hierarchy Based Data Security

Contents

- Section A.1.22.10, "Human Resource Analyst (secured by HR Supervisor Hierarchy List) AU BI Data"
- Section A.1.22.11, "Human Resource Manager (secured by HR Supervisor Hierarchy List) AU BI Data"
- Section A.1.22.12, "Learning Manager (secured by HR Supervisor Hierarchy List) AU BI Data"
- Section A.1.22.13, "HR Duty Role to Oracle BI Applications HR Presentation Catalog Mapping"

A.1.22.1 Introduction

Data can be secured via the HR Supervisor Hierarchy using list variable[s], with associated data roles and security filter[s] which are applied at the physical SQL level as IN (a, b, c,...) statement.

How to choose / assign the Duty Role

Each Duty Role grants access to one or more subject areas, and is a member of at least one data security role.

You need to map a source role/responsibility to one or more Duty Roles. For instructions on how this is done refer to the FSM task in Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

HR Data Role to Duty Role Mapping

Note: The following are applicable to HR Supervisor Hierarchy security.

Table A–13 HR Data Role to Duty Role Mapping

Data (Security) Role	Duty Role
Line Manager (secured by HR Supervisor Hierarchy List) AU BI Data	Line Manager (secured by HR Supervisor Hierarchy List) AU BI Duty
Payroll Manager (secured by HR Supervisor Hierarchy List) AU BI Data	Payroll Manager (secured by HR Supervisor Hierarchy List) AU BI Duty
Compensation Analyst (secured by HR Supervisor Hierarchy List) AU BI Data	Compensation Analyst (secured by HR Supervisor Hierarchy List) AU BI Duty
Compensation Manager (secured by HR Supervisor Hierarchy List) AU BI Data	Compensation Manager (secured by HR Supervisor Hierarchy List) AU BI Duty
Recruiting Manager (secured by HR Supervisor Hierarchy List) AU BI Data	Recruiting Manager (secured by HR Supervisor Hierarchy List) AU BI Duty
Recruiting VP (secured by HR Supervisor Hierarchy List) AU BI Data	Recruiting VP (secured by HR Supervisor Hierarchy List) AU BI Duty
Time Collection Manager (secured by HR Supervisor Hierarchy List) AU BI Data	Time Collection Manager (secured by HR Supervisor Hierarchy List) AU BI Duty
Human Resource VP (secured by HR Supervisor Hierarchy List) AU BI Data	Human Resource VP (secured by HR Supervisor Hierarchy List) AU BI Duty
Human Resource Analyst (secured by HR Supervisor Hierarchy List) AU BI Data	Human Resource Analyst (secured by HR Supervisor Hierarchy List) AU BI Duty
Human Resource Manager (secured by HR Supervisor Hierarchy List) AU BI Data	Human Resource Manager (secured by HR Supervisor Hierarchy List) AU BI Duty
Learning Manager (secured by HR Supervisor Hierarchy List) AU BI Data	Learning Manager (secured by HR Supervisor Hierarchy List) AU BI Duty

A.1.22.2 Line Manager (secured by HR Supervisor Hierarchy List) AU BI Data

Initialization Blocks

The Line Manager HR Supervisor Hierarchy list is determined at user sign-on via one or more Initialization Blocks:

Table A–14 Initialization Blocks

Variable Name	Initialization Block Name
HR_SEC_PERSON_ID	Not applicable, this is a multi source variable population see below.
HR_SEC_PERSON_ID____EBS	HR Security Person ID List (EBS)
HR_SEC_PERSON_ID____PSFT	HR Security Person ID List (PeopleSoft)

Data Security Role Filters

The Line Manager HR Supervisor Hierarchy list Security is applied depending on the roles the user is granted, and when it is applied it is supported by the following HR logical facts and dimensions:

Table A–15 Data Security Role Filters

Name	Filter
Dim - HR Supervisor Hierarchy	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Learning Calendar	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Learning Enrollment and Completion	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Learning Enrollment Events	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Absence Event	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Recruitment Event Information	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Workforce Event Information	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Workforce Balance Information	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Accrual Transactions - Event Information	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Accrual Transactions - Balance Information	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)

Table A–15 (Cont.) Data Security Role Filters

Name	Filter
Fact - HR - Time and Labor - Reported Time	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Time and Labor - Processed Time	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Workforce Gains and Losses - Balance Information	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Workforce Gains and Losses - Event Information	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Payroll Balance Summary	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)

A.1.22.3 Payroll Manager (secured by HR Supervisor Hierarchy List) AU BI Data

Initialization Blocks

The Payroll Manager HR Supervisor Hierarchy list is determined at user sign-on via one or more Initialization Blocks:

Table A–16 Initialization Blocks

Variable Name	Initialization Block Name
HR_SEC_PERSON_ID	Not applicable, this is a multi source variable population see below.
HR_SEC_PERSON_ID____EBS	HR Security Person ID List (EBS)
HR_SEC_PERSON_ID____PSFT	HR Security Person ID List (PeopleSoft)

Data Security Role Filters

The Payroll Manager HR Supervisor Hierarchy list Security is applied depending on the roles the user is granted, and when it is applied it is supported by the following HR logical facts and dimensions:

Table A–17 Data Security Role Filters

Name	Filter
Dim - HR Supervisor Hierarchy	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR – Payroll Balance Summary	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Payroll Balance Detail	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)

A.1.22.4 Compensation Analyst (secured by HR Supervisor Hierarchy List) AU BI Data

Initialization Blocks

The Compensation Analyst HR Supervisor Hierarchy list is determined at user sign-on via one or more Initialization Blocks:

Table A–18 Initialization Blocks

Variable Name	Initialization Block Name
HR_SEC_PERSON_ID	Not applicable, this is a multi source variable population see below.
HR_SEC_PERSON_ID____EBS	HR Security Person ID List (EBS)
HR_SEC_PERSON_ID____PSFT	HR Security Person ID List (PeopleSoft)

Data Security Role Filters

The Compensation Analyst HR Supervisor Hierarchy list Security is applied depending on the roles the user is granted, and when it is applied it is supported by the following HR logical facts and dimensions:

Table A–19 Data Security Role Filters

Name	Filter
Dim - HR Supervisor Hierarchy	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Workforce Event Information	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Workforce Balance Information	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR – Payroll Balance Summary	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Payroll Balance Detail	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Workforce Gains and Losses - Balance Information	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Workforce Gains and Losses - Event Information	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)

A.1.22.5 Compensation Manager (secured by HR Supervisor Hierarchy List) AU BI Data

Initialization Blocks

The Compensation Manager HR Supervisor Hierarchy list is determined at user sign-on via one or more Initialization Blocks:

Table A–20 Initialization Blocks

Variable Name	Initialization Block Name
HR_SEC_PERSON_ID	Not applicable, this is a multi source variable population see below.
HR_SEC_PERSON_ID____EBS	HR Security Person ID List (EBS)
HR_SEC_PERSON_ID____PSFT	HR Security Person ID List (PeopleSoft)

Data Security Role Filters

The Compensation Manager HR Supervisor Hierarchy list Security is applied depending on the roles the user is granted, and when it is applied it is supported by the following HR logical facts and dimensions:

Table A–21 Data Security Role Filters

Name	Filter
Dim - HR Supervisor Hierarchy	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Workforce Event Information	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Workforce Balance Information	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR – Payroll Balance Summary	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Payroll Balance Detail	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Workforce Gains and Losses - Balance Information	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Workforce Gains and Losses - Event Information	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)

A.1.22.6 Recruiting Manager (secured by HR Supervisor Hierarchy List) AU BI Data

Initialization Blocks

The Recruiting Manager HR Supervisor Hierarchy list is determined at user sign-on via one or more Initialization Blocks:

Table A–22 Initialization Blocks

Variable Name	Initialization Block Name
HR_SEC_PERSON_ID	Not applicable, this is a multi source variable population see below.
HR_SEC_PERSON_ID____EBS	HR Security Person ID List (EBS)
HR_SEC_PERSON_ID____PSFT	HR Security Person ID List (PeopleSoft)

Data Security Role Filters

The Recruiting Manager HR Supervisor Hierarchy list Security is applied depending on the roles the user is granted, and when it is applied it is supported by the following HR logical facts and dimensions:

Table A–23 Data Security Role Filters

Name	Filter
Dim - HR Supervisor Hierarchy	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Recruitment Event Information	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)

A.1.22.7 Recruiting VP (secured by HR Supervisor Hierarchy List) AU BI Data

Initialization Blocks

The Recruiting VP HR Supervisor Hierarchy list is determined at user sign-on via one or more Initialization Blocks:

Table A–24 Initialization Blocks

Variable Name	Initialization Block Name
HR_SEC_PERSON_ID	Not applicable, this is a multi source variable population see below.
HR_SEC_PERSON_ID____EBS	HR Security Person ID List (EBS)
HR_SEC_PERSON_ID____PSFT	HR Security Person ID List (PeopleSoft)

Data Security Role Filters

The Recruiting VP HR Supervisor Hierarchy list Security is applied depending on the roles the user is granted, and when it is applied it is supported by the following HR logical facts and dimensions:

Table A–25 Data Security Role Filters

Name	Filter
Dim - HR Supervisor Hierarchy	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Recruitment Event Information	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)

A.1.22.8 Time Collection Manager (secured by HR Supervisor Hierarchy List) AU BI Data

Initialization Blocks

The Time Collection Manager HR Supervisor Hierarchy list is determined at user sign-on via one or more Initialization Blocks:

Table A–26 Initialization Blocks

Variable Name	Initialization Block Name
HR_SEC_PERSON_ID	Not applicable, this is a multi source variable population see below.
HR_SEC_PERSON_ID____EBS	HR Security Person ID List (EBS)
HR_SEC_PERSON_ID____PSFT	HR Security Person ID List (PeopleSoft)

Data Security Role Filters

The Time Collection Manager HR Supervisor Hierarchy list Security is applied depending on the roles the user is granted, and when it is applied it is supported by the following HR logical facts and dimensions:

Table A–27 Data Security Role Filters

Name	Filter
Dim - HR Supervisor Hierarchy	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Time and Labor - Reported Time	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Time and Labor - Processed Time	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Workforce Balance Information	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR – Payroll Balance Summary	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)

A.1.22.9 Human Resource VP (secured by HR Supervisor Hierarchy List) AU BI Data

Initialization Blocks

The Human Resource VP HR Supervisor Hierarchy list is determined at user sign-on via one or more Initialization Blocks:

Table A–28 Initialization Blocks

Variable Name	Initialization Block Name
HR_SEC_PERSON_ID	Not applicable, this is a multi source variable population see below.
HR_SEC_PERSON_ID____EBS	HR Security Person ID List (EBS)
HR_SEC_PERSON_ID____PSFT	HR Security Person ID List (PeopleSoft)

Data Security Role Filters

The Human Resource VP HR Supervisor Hierarchy list Security is applied depending on the roles the user is granted, and when it is applied it is supported by the following HR logical facts and dimensions:

Table A–29 Data Security Role Filters

Name	Filter
Dim - HR Supervisor Hierarchy	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Learning Calendar	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Learning Enrollment and Completion	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Learning Enrollment Events	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Absence Event	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Recruitment Event Information	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Workforce Event Information	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Workforce Balance Information	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Accrual Transactions - Event Information	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Accrual Transactions - Balance Information	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR – Payroll Balance Summary	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Payroll Balance Detail	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)

A.1.22.10 Human Resource Analyst (secured by HR Supervisor Hierarchy List) AU BI Data

Initialization Blocks

The Human Resource Analyst HR Supervisor Hierarchy list is determined at user sign-on via one or more Initialization Blocks:

Table A–30 Initialization Blocks

Variable Name	Initialization Block Name
HR_SEC_PERSON_ID	Not applicable, this is a multi source variable population see below.
HR_SEC_PERSON_ID____EBS	HR Security Person ID List (EBS)

Table A–30 (Cont.) Initialization Blocks

Variable Name	Initialization Block Name
HR_SEC_PERSON_ID____PSFT	HR Security Person ID List (PeopleSoft)

Data Security Role Filters

The Human Resource Analyst HR Supervisor Hierarchy list Security is applied depending on the roles the user is granted, and when it is applied it is supported by the following HR logical facts and dimensions:

Table A–31 Data Security Role Filters

Name	Filter
Dim - HR Supervisor Hierarchy	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Workforce Event Information	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Workforce Balance Information	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR – Payroll Balance Summary	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Payroll Balance Detail	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Workforce Gains and Losses - Balance Information	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Workforce Gains and Losses - Event Information	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)

A.1.22.11 Human Resource Manager (secured by HR Supervisor Hierarchy List) AU BI Data

Initialization Blocks

The Human Resource Manager HR Supervisor Hierarchy list is determined at user sign-on via one or more Initialization Blocks:

Table A–32 Initialization Blocks

Variable Name	Initialization Block Name
HR_SEC_PERSON_ID	Not applicable, this is a multi source variable population see below.
HR_SEC_PERSON_ID____EBS	HR Security Person ID List (EBS)
HR_SEC_PERSON_ID____PSFT	HR Security Person ID List (PeopleSoft)

Data Security Role Filters

The Human Resource Manager HR Supervisor Hierarchy list Security is applied depending on the roles the user is granted, and when it is applied it is supported by the following HR logical facts and dimensions:

Table A–33 Data Security Role Filters

Name	Filter
Dim - HR Supervisor Hierarchy	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Learning Calendar	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Learning Enrollment and Completion	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Learning Enrollment Events	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Absence Event	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Recruitment Event Information	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Workforce Event Information	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Workforce Balance Information	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Accrual Transactions - Event Information	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Accrual Transactions - Balance Information	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Workforce Gains and Losses - Balance Information	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Workforce Gains and Losses - Event Information	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)

A.1.22.12 Learning Manager (secured by HR Supervisor Hierarchy List) AU BI Data

Initialization Blocks

The Learning Manager HR Supervisor Hierarchy list is determined at user sign-on via one or more Initialization Blocks:

Table A–34 Initialization Blocks

Variable Name	Initialization Block Name
HR_SEC_PERSON_ID	Not applicable, this is a multi source variable population see below.
HR_SEC_PERSON_ID____EBS	HR Security Person ID List (EBS)
HR_SEC_PERSON_ID____PSFT	HR Security Person ID List (PeopleSoft)

Data Security Role Filters

The Learning Manager HR Supervisor Hierarchy list Security is applied depending on the roles the user is granted, and when it is applied it is supported by the following HR logical facts and dimensions:

Table A–35 Data Security Role Filters

Name	Filter
Dim - HR Supervisor Hierarchy	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Learning Calendar	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Learning Enrollment and Completion	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)
Fact - HR - Learning Enrollment Events	"Core"."Dim - HR Supervisor Hierarchy"."Top Level Source Person ID" = VALUEOF(NQ_SESSION.HR_SEC_PERSON_ID)

A.1.22.13 HR Duty Role to Oracle BI Applications HR Presentation Catalog Mapping

Note: The following are applicable to HR Supervisor Hierarchy security.

Table A–36 HR Duty Role to HR Presentation Catalog Mapping

Duty Role	HR Presentation Catalog Mapping
Line Manager (secured by HR Supervisor Hierarchy List) AU BI Duty	Human Resources - Absence and Leave Accrual Human Resources - Compensation Human Resources - Learning Enrollment and Completion Human Resources - Recruitment Human Resources - Workforce Deployment Human Resources – Time and Labor
Payroll Manager (secured by HR Supervisor Hierarchy List) AU BI Duty	Human Resources – Payroll Human Resources – Time and Labor
Compensation Analyst (secured by HR Supervisor Hierarchy List) AU BI Duty	Human Resources - Compensation Human Resources – Payroll
Compensation Manager (secured by HR Supervisor Hierarchy List) AU BI Duty	Human Resources - Compensation Human Resources – Payroll

Table A–36 (Cont.) HR Duty Role to HR Presentation Catalog Mapping

Duty Role	HR Presentation Catalog Mapping
Recruiting Manager (secured by HR Supervisor Hierarchy List) AU BI Duty	Human Resources – Recruitment
Recruiting VP (secured by HR Supervisor Hierarchy List) AU BI Duty	Human Resources – Recruitment
Time Collection Manager (secured by HR Supervisor Hierarchy List) AU BI Duty	Human Resources – Time and Labor
Human Resource VP (secured by HR Supervisor Hierarchy List) AU BI Duty	Human Resources - Absence and Leave Accrual Human Resources - Compensation Human Resources - Learning Enrollment and Completion Human Resources - Payroll Human Resources - Recruitment Human Resources - Workforce Deployment Human Resources - Workforce Effectiveness
Human Resource Analyst (secured by HR Supervisor Hierarchy List) AU BI Duty	Human Resources - Absence and Leave Accrual Human Resources - Compensation Human Resources - Learning Enrollment and Completion Human Resources - Recruitment Human Resources - Workforce Deployment
Human Resource Manager (secured by HR Supervisor Hierarchy List) AU BI Duty	Human Resources - Absence and Leave Accrual Human Resources - Compensation Human Resources - Learning Enrollment and Completion Human Resources - Recruitment Human Resources - Workforce Deployment
Learning Manager (secured by HR Supervisor Hierarchy List) AU BI Duty	Human Resources - Learning Enrollment and Completion
Fusion Workforce Deployment Analysis Duty	Human Resources - Workforce Deployment
Fusion Compensation Analysis Duty	Human Resources - Compensation Human Resources – Payroll
Fusion Absence and Leave Accrual Analysis Duty	Human Resources - Absence and Leave Accrual

A.1.23 How to set up Department Based Data Security

Contents

A.1.23.1 Introduction

Human Resource Analytics supports data security over Human Resources subject areas / facts via the Department dimension using department list variable[s]; each variable is used by one (or more) data roles, the data roles ensure security filter[s] are applied at the physical SQL level as IN (a, b, c,...) statement.

How to choose / assign the Duty Role

Each Duty Role grants access to one or more subject areas, and is a member of at least one data security role.

You need to map a source role/responsibility to one or more Duty Roles. For instructions on how this is done refer to the FSM task in Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

HR Data Role to Duty Role Mapping

Note: The following are applicable to Department security.

Table A–37 HR Data Role to Duty Role Mapping

Data (Security) Role	Duty Role
Line Manager (secured by Department List) AU BI Data	Line Manager (secured by Department List) AU BI Duty
Payroll Manager (secured by Department List) AU BI Data	Payroll Manager (secured by Department List) AU BI Duty
Compensation Analyst (secured by Department List) AU BI Data	Compensation Analyst (secured by Department List) AU BI Duty
Compensation Manager (secured by Department List) AU BI Data	Compensation Manager (secured by Department List) AU BI Duty

Table A–37 (Cont.) HR Data Role to Duty Role Mapping

Data (Security) Role	Duty Role
Recruiting Manager (secured by Department List) AU BI Data	Recruiting Manager (secured by Department List) AU BI Duty
Recruiting VP (secured by Department List) AU BI Data	Recruiting VP (secured by Department List) AU BI Duty
Time Collection Manager (secured by Department List) AU BI Data	Time Collection Manager (secured by Department List) AU BI Duty
Human Resource VP (secured by Department List) AU BI Data	Human Resource VP (secured by Department List) AU BI Duty
Human Resource Analyst (secured by Department List) AU BI Data	Human Resource Analyst (secured by Department List) AU BI Duty
Human Resource Manager (secured by Department List) AU BI Data	Human Resource Manager (secured by Department List) AU BI Duty
Learning Manager (secured by Department List) AU BI Data	Learning Manager (secured by Department List) AU BI Duty

A.1.23.2 Line Manager (secured by Department List) AU BI Data

Name: OBIA_AU_HCM_LINEMGR_DEPT_DATA_SECURITY.

Initialization Blocks

The Line Manager Department list is determined at user sign-on via one or more Initialization Blocks:

Table A–38 Initialization Blocks

Variable Name	Initialization Block Name
HR_SEC_DEPT_LINEMGR_LIST	Not applicable, this is a multi source variable population see below.
HR_SEC_DEPT_LINEMGR_LIST____EBS	HR - Line Manager - Department List (EBS)
HR_SEC_DEPT_LINEMGR_LIST____PSFT	HR - Line Manager - Department List (PeopleSoft)

Data Security Role Filters

The Line Manager Department list Security is applied depending on the roles the user is granted, and when it is applied it is supported by the following HR logical facts and dimensions:

Table A–39 Data Security Role Filters

Name	Filter
Fact - HR - Learning Enrollment and Completion	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_LINEMGR_LIST)
Fact - HR - Learning Enrollment Events	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_LINEMGR_LIST)
Fact - HR - Absence Event	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_LINEMGR_LIST)

Table A–39 (Cont.) Data Security Role Filters

Name	Filter
Fact - HR - Recruitment Event Information	"Core"."Dim - Requisition Organization"."Requisition Organization Number" = VALUEOF NQ_SESSION.HR_SEC_DEPT_LINEMGR_LIST)
Fact - HR - Workforce - Event Information	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_LINEMGR_LIST)
Fact - HR - Workforce - Balance Information	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_LINEMGR_LIST)
Fact - HR - Accrual Transactions - Event Information	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_LINEMGR_LIST)
Fact - HR - Accrual Transactions - Balance Information	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_LINEMGR_LIST)
Fact - HR - Time and Labor - Reported Time	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_LINEMGR_LIST)
Fact - HR - Time and Labor - Processed Time	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_LINEMGR_LIST)
Dim - Department	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_LINEMGR_LIST)
Dim - Requisition Organization	"Core"."Dim - Requisition Organization"."Requisition Organization Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_LINEMGR_LIST)
Fact - HR - Learning Calendar	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_LINEMGR_LIST)
Fact - HR - Payroll Balance Summary	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_LINEMGR_LIST)

A.1.23.3 Payroll Manager (secured by Department List) AU BI Data

Name: OBIA_AU_HCM_PYRLMGR_DEPT_DATA_SECURITY.

Initialization Blocks

The Payroll Manager Department list is determined at user sign-on via one or more Initialization Blocks:

Table A–40 Initialization Blocks

Variable Name	Initialization Block Name
HR_SEC_DEPT_PYRLMGR_LIST	Not applicable, this is a multi source variable population see below.
HR_SEC_DEPT_PYRLMGR_LIST____EBS	HR - Payroll Manager - Department List (EBS)
HR_SEC_DEPT_PYRLMGR_LIST____PSFT	HR - Payroll Manager - Department List (PeopleSoft)

Data Security Role Filters

The Payroll Manager Department list Security is applied depending on the roles the user is granted, and when it is applied it is supported by the following HR logical facts and dimensions:

Table A–41 Data Security Role Filters

Name	Filter
Dim - Department	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_PYRLMGR_LIST)
Fact - HR - Payroll Balance Detail	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_PYRLMGR_LIST)
Fact - HR - Payroll Balance Summary	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_PYRLMGR_LIST)

A.1.23.4 Compensation Analyst (secured by Department List) AU BI Data

Name: OBIA_AU_HCM_CMPALYST_DEPT_DATA_SECURITY.

Initialization Blocks

The Compensation Analyst Department list is determined at user sign-on via one or more Initialization Blocks:

Table A–42 Initialization Blocks

Variable Name	Initialization Block Name
HR_SEC_DEPT_CMPALYST_LIST	Not applicable, this is a multi source variable population see below.
HR_SEC_DEPT_CMPALYST_LIST____EBS	HR - Compensation Analyst - Department List (EBS)
HR_SEC_DEPT_CMPALYST_LIST____PSFT	HR - Compensation Analyst - Department List (PeopleSoft)

Data Security Role Filters

The Compensation Analyst Department list Security is applied depending on the roles the user is granted, and when it is applied it is supported by the following HR logical facts and dimensions:

Table A–43 Data Security Role Filters

Name	Filter
Dim - Department	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_CMPALYST_LIST)
Fact - HR - Payroll Balance Detail	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_CMPALYST_LIST)
Fact - HR - Payroll Balance Summary	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_CMPALYST_LIST)

Table A–43 (Cont.) Data Security Role Filters

Name	Filter
Fact - HR - Workforce - Event Information	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_CMPALYST_LIST)
Fact - HR - Workforce - Balance Information	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_CMPALYST_LIST)

A.1.23.5 Compensation Manager (secured by Department List) AU BI Data

Name: OBIA_AU_HCM_CMPMGR_DEPT_DATA_SECURITY.

Initialization Blocks

The Compensation Manager Department list is determined at user sign-on via one or more Initialization Blocks:

Table A–44 Initialization Blocks

Variable Name	Initialization Block Name
HR_SEC_DEPT_CMPMGR_LIST	Not applicable, this is a multi source variable population see below.
HR_SEC_DEPT_CMPMGR_LIST____EBS	HR - Compensation Manager - Department List (EBS)
HR_SEC_DEPT_CMPMGR_LIST____PSFT	HR - Compensation Manager - Department List (PeopleSoft)

Data Security Role Filters

The Compensation Manager Department list Security is applied depending on the roles the user is granted, and when it is applied it is supported by the following HR logical facts and dimensions:

Table A–45 Data Security Role Filters

Name	Filter
Dim - Department	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_CMPMGR_LIST)
Fact - HR - Payroll Balance Detail	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_CMPMGR_LIST)
Fact - HR - Payroll Balance Summary	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_CMPMGR_LIST)
Fact - HR - Workforce - Event Information	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_CMPMGR_LIST)
Fact - HR - Workforce - Balance Information	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_CMPMGR_LIST)

A.1.23.6 Recruiting Manager (secured by Department List) AU BI Data

Name: OBIA_AU_HCM_RCRTMTMGR_DEPT_DATA_SECURITY.

Initialization Blocks

The Recruiting Manager Department list is determined at user sign-on via one or more Initialization Blocks:

Table A–46 Initialization Blocks

Variable Name	Initialization Block Name
HR_SEC_DEPT_RCRTMTMGR_LIST	Not applicable, this is a multi source variable population see below.
HR_SEC_DEPT_RCRTMTMGR_LIST ____ EBS	HR - Recruiting Manager - Department List (EBS)
HR_SEC_DEPT_RCRTMTMGR_LIST____ PSFT	HR - Recruiting Manager - Department List (PeopleSoft)

Data Security Role Filters

The Recruiting Manager Department list Security is applied depending on the roles the user is granted, and when it is applied it is supported by the following HR logical facts and dimensions:

Table A–47 Data Security Role Filters

Name	Filter
Dim - Department	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_RCRTMTVP_ LIST)
Dim - Requisition Organization	"Core"."Dim - Requisition Organization"."Requisition Organization Number" = VALUEOF(NQ_SESSION.HR_ SEC_DEPT_RCRTMTMGR_LIST)
Fact - HR - Recruitment Event Information	"Core"."Dim - Requisition Organization"."Requisition Organization Number" = VALUEOF(NQ_SESSION.HR_ SEC_DEPT_RCRTMTMGR_LIST)

A.1.23.7 Recruiting VP (secured by Department List) AU BI Data

Name: OBIA_AU_HCM_RCRTMTVP_DEPT_DATA_SECURITY.

Initialization Blocks

The Recruiting VP Department list is determined at user sign-on via one or more Initialization Blocks:

Table A–48 Initialization Blocks

Variable Name	Initialization Block Name
HR_SEC_DEPT_RCRTMTVP_LIST	Not applicable, this is a multi source variable population see below.
HR_SEC_DEPT_RCRTMTVP_LIST____EBS	HR - Recruiting VP - Department List (EBS)
HR_SEC_DEPT_RCRTMTVP_LIST____PSFT	HR - Recruiting VP - Department List (PeopleSoft)

Data Security Role Filters

The Recruiting VP Department list Security is applied depending on the roles the user is granted, and when it is applied it is supported by the following HR logical facts and dimensions:

Table A–49 Data Security Role Filters

Name	Filter
Dim - Department	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_RCRTMTVP_LIST)
Dim - Requisition Organization	"Core"."Dim - Requisition Organization"."Requisition Organization Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_RCRTMTVP_LIST)
Fact - HR - Recruitment Event Information	"Core"."Dim - Requisition Organization"."Requisition Organization Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_RCRTMTVP_LIST)

A.1.23.8 Time Collection Manager (secured by Department List) AU BI Data

Name: OBIA_AU_HCM_TLBRMGR_DEPT_DATA_SECURITY.

Initialization Blocks

The Time Collection Manager Department list is determined at user sign-on via one or more Initialization Blocks:

Table A–50 Initialization Blocks

Variable Name	Initialization Block Name
HR_SEC_DEPT_TLBRMGR_LIST	Not applicable, this is a multi source variable population see below.
HR_SEC_DEPT_TLBRMGR_LIST____EBS	HR - Time Collection Manager - Department List (EBS)
HR_SEC_DEPT_TLBRMGR_LIST____PSFT	HR - Time Collection Manager - Department List (PeopleSoft)

Data Security Role Filters

The Time Collection Manager Department list Security is applied depending on the roles the user is granted, and when it is applied it is supported by the following HR logical facts and dimensions:

Table A–51 Data Security Role Filters

Name	Filter
Dim - Department	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_TLBRMGR_LIST)
Fact - HR - Time and Labor - Reported Time	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_TLBRMGR_LIST)
Fact - HR - Time and Labor - Processed Time	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_TLBRMGR_LIST)
Fact - HR - Workforce Balance Information	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_TLBRMGR_LIST)

Table A–51 (Cont.) Data Security Role Filters

Name	Filter
Fact - HR – Payroll Balance Summary	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_TLBRMGR_LIST)

A.1.23.9 Human Resource VP (secured by Department List) AU BI Data

Name: OBIA_AU_HCM_HRVP_DEPT_DATA_SECURITY.

Initialization Blocks

The Human Resource VP Department list is determined at user sign-on via one or more Initialization Blocks:

Table A–52 Initialization Blocks

Variable Name	Initialization Block Name
HR_SEC_DEPT_HRVP_LIST	Not applicable, this is a multi source variable population see below.
HR_SEC_DEPT_HRVP_LIST____EBS	HR - Human Resource VP - Department List (EBS)
HR_SEC_DEPT_HRVP_LIST____PSFT	HR - Human Resource VP - Department List (PeopleSoft)

Data Security Role Filters

The Human Resource VP Department list Security is applied depending on the roles the user is granted, and when it is applied it is supported by the following HR logical facts and dimensions:

Table A–53 Data Security Role Filters

Name	Filter
Dim - Department	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_HRVP_LIST)
Fact - HR - Learning Calendar	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_HRVP_LIST)
Fact - HR - Learning Enrollment and Completion	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_HRVP_LIST)
Fact - HR - Learning Enrollment Events	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_HRVP_LIST)
Fact - HR - Absence Event	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_HRVP_LIST)
Fact - HR - Recruitment Event Information	"Core"."Dim - Requisition Organization"."Requisition Organization Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_HRVP_LIST)
Fact - HR - Workforce - Event Information	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_HRVP_LIST)
Fact - HR - Workforce - Balance Information	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_HRVP_LIST)
Fact - HR - Accrual Transactions - Event Information	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_HRVP_LIST)

Table A–53 (Cont.) Data Security Role Filters

Name	Filter
Fact - HR - Accrual Transactions - Balance Information	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_HRVP_LIST)
Fact - HR - Payroll Balance Detail	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_HRVP_LIST)
Fact - HR - Payroll Balance Summary	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_HRVP_LIST)
Fact - HR - Time and Labor - Reported Time	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_HRVP_LIST)
Fact - HR - Time and Labor - Processed Time	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_HRVP_LIST)
Dim - Requisition Organization	"Core"."Dim - Requisition Organization"."Requisition Organization Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_HRVP_LIST)

A.1.23.10 Human Resource Analyst (secured by Department List) AU BI Data

Name: OBIA_AU_HCM_HRALYST_DEPT_DATA_SECURITY

Initialization Blocks

The Human Resource Analyst Department list is determined at user sign-on via one or more Initialization Blocks:

Table A–54 Initialization Blocks

Variable Name	Initialization Block Name
HR_SEC_DEPT_HRALYST_LIST	Not applicable, this is a multi source variable population see below.
HR_SEC_DEPT_HRALYST_LIST____EBS	HR - Human Resource Analyst - Department List (EBS)
HR_SEC_DEPT_HRALYST_LIST ____PSFT	HR - Human Resource Analyst - Department List (PeopleSoft)

Data Security Role Filters

The Human Resource Analyst Department list Security is applied depending on the roles the user is granted, and when it is applied it is supported by the following HR logical facts and dimensions:

Table A–55 Data Security Role Filters

Name	Filter
Fact - HR - Learning Enrollment and Completion	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_HRALYST_LIST)
Fact - HR - Learning Enrollment Events	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_HRALYST_LIST)
Fact - HR - Absence Event	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_HRALYST_LIST)
Fact - HR - Recruitment Event Information	"Core"."Dim - Requisition Organization"."Requisition Organization Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_HRALYST_LIST)

Table A–55 (Cont.) Data Security Role Filters

Name	Filter
Fact - HR - Workforce - Event Information	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_HRALYST_LIST)
Fact - HR - Workforce - Balance Information	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_HRALYST_LIST)
Fact - HR - Accrual Transactions - Event Information	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_HRALYST_LIST)
Fact - HR - Accrual Transactions - Balance Information	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_HRALYST_LIST)
Dim - Department	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_HRALYST_LIST)
Dim - Requisition Organization	"Core"."Dim - Requisition Organization"."Requisition Organization Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_HRALYST_LIST)
Fact - HR - Learning Calendar	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_HRALYST_LIST)

A.1.23.11 Human Resource Manager (secured by Department List) AU BI Data

Name: OBIA_AU_HCM_HRMGR_DEPT_DATA_SECURITY.

Initialization Blocks

The Human Resource Manager - Department list is determined at user sign-on via one or more Initialization Blocks:

Table A–56 Initialization Blocks

Variable Name	Initialization Block Name
HR_SEC_DEPT_HRMGR_LIST	Not applicable, this is a multi source variable population see below.
HR_SEC_DEPT_HRMGR_LIST____EBS	HR - Human Resources Manager - Department List (EBS)
HR_SEC_DEPT_HRMGR_LIST____PSFT	HR - Human Resources Manager - Department List (PeopleSoft)

Data Security Role Filters

The Human Resource Manager - Department list Security is applied depending on the roles the user is granted, and when it is applied it is supported by the following HR logical facts and dimensions:

Table A–57 Data Security Role Filters

Name	Filter
Fact - HR - Learning Enrollment and Completion	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_HRMGR_LIST)
Fact - HR - Learning Enrollment Events	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_HRMGR_LIST)
Fact - HR - Absence Event	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_HRMGR_LIST)

Table A–57 (Cont.) Data Security Role Filters

Name	Filter
Fact - HR - Recruitment Event Information	"Core"."Dim - Requisition Organization"."Requisition Organization Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_HRMGR_LIST)
Fact - HR - Workforce - Event Information	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_HRMGR_LIST)
Fact - HR - Workforce - Balance Information	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_HRMGR_LIST)
Fact - HR - Accrual Transactions - Event Information	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_HRMGR_LIST)
Fact - HR - Accrual Transactions - Balance Information	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_HRMGR_LIST)
Dim - Department	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_HRMGR_LIST)
Dim - Requisition Organization	"Core"."Dim - Requisition Organization"."Requisition Organization Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_HRMGR_LIST)
Fact - HR - Learning Calendar	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_HRMGR_LIST)

A.1.23.12 Learning Manager (secured by Department List) AU BI Data

Name: OBIA_AU_HCM_LRNGMGR_DEPT_DATA_SECURITY

Initialization Blocks

The Learning Manager Department list is determined at user sign-on via one or more Initialization Blocks:

Table A–58 Initialization Blocks

Variable Name	Initialization Block Name
HR_SEC_DEPT_LRNGMGR_LIST	Not applicable, this is a multi source variable population see below.
HR_SEC_DEPT_LRNGMGR_LIST____EBS	HR - Learning Manager - Department List (EBS)
HR_SEC_DEPT_LRNGMGR_LIST ____PSFT	HR - Learning Manager - Department List (PeopleSoft)

Data Security Role Filters

The Learning Manager Department list Security is applied depending on the roles the user is granted, and when it is applied it is supported by the following HR logical facts and dimensions:

Table A–59 Data Security Role Filters

Name	Filter
Fact - HR - Learning Enrollment and Completion	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_LRNGMGR_LIST)

Table A–59 (Cont.) Data Security Role Filters

Name	Filter
Fact - HR - Learning Enrollment Events	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_LRNGMGR_LIST)
Dim - Department	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_LRNGMGR_LIST)
Fact - HR - Learning Calendar	"Core"."Dim - Department"."Department Number" = VALUEOF(NQ_SESSION.HR_SEC_DEPT_LRNGMGR_LIST)

A.1.23.13 HR Duty Role to Oracle BI Applications HR Presentation Catalog Mapping

Note: The following are applicable to Department security.

Table A–60 HR Duty Role to HR Presentation Catalog Mapping

BI Duty Roles	HR Presentation Catalog Mapping
Line Manager (secured by Department List) AU BI Duty	Human Resources - Absence and Leave Accrual Human Resources - Compensation Human Resources - Learning Enrollment and Completion Human Resources - Recruitment Human Resources - Workforce Deployment Human Resources - Time and Labor
Payroll Manager (secured by Department List) AU BI Duty	Human Resources - Payroll Human Resources - Time and Labor
Compensation Analyst (secured by Department List) AU BI Duty	Human Resources - Compensation Human Resources - Payroll
Compensation Manager (secured by Department List) AU BI Duty	Human Resources - Compensation Human Resources - Payroll
Recruiting Manager (secured by Department List) AU BI Duty	Human Resources - Recruitment
Recruiting VP (secured by Department List) AU BI Duty	Human Resources - Recruitment
Time Collection Manager (secured by Department List) AU BI Duty	Human Resources - Time and Labor
Human Resource VP (secured by Department List) AU BI Duty	Human Resources - Absence and Leave Accrual Human Resources - Compensation Human Resources - Learning Enrollment and Completion Human Resources - Payroll Human Resources - Recruitment Human Resources - Workforce Deployment Human Resources - Workforce Effectiveness

Table A–60 (Cont.) HR Duty Role to HR Presentation Catalog Mapping

BI Duty Roles	HR Presentation Catalog Mapping
Human Resource Analyst (secured by Department List) AU BI Duty	Human Resources - Absence and Leave Accrual Human Resources - Compensation Human Resources - Learning Enrollment and Completion Human Resources - Recruitment Human Resources - Workforce Deployment
Human Resource Manager (secured by Department List) AU BI Duty	Human Resources - Absence and Leave Accrual Human Resources - Compensation Human Resources - Learning Enrollment and Completion Human Resources - Recruitment Human Resources - Workforce Deployment
Learning Manager (secured by Department List) AU BI Duty	Human Resources - Learning Enrollment and Completion

A.1.24 How to Set Up Price Analytics Security for EBS

There is no row-level security applied to Price Analytics reports and metrics. Users who can access Price Analytics Subject areas can view all Order and Quote data in the related reports without any data-security filter.

Configuring BI Duty Roles

The table below lists BI Duty Roles that can be assigned to users in order to give them access to Price Analytics Subject Areas.

Table A–61 BI Duty Roles and Subject Areas

BI Duty Roles	Subject areas
Price Administrator	Sales – CRM Price Waterfall
Price Order Analytics	Sales – CRM Price Waterfall - Orders
Price Quote Analytics (Member E-Business Suite responsibility : Quoting User, Quoting Sales Agent, Quoting Sales Manager)	Sales – CRM Price Waterfall - Quotes

For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

A.1.25 How to set up HR Position Hierarchy Based Data Security

Contents

- Section A.1.25.4, "Compensation Analyst (secured by HR Position Hierarchy List) AU BI Data"
- Section A.1.25.5, "Compensation Manager (secured by HR Position Hierarchy List) AU BI Data"
- Section A.1.25.6, "Recruiting Manager (secured by HR Position Hierarchy List) AU BI Data"
- Section A.1.25.7, "Recruiting VP (secured by HR Position Hierarchy List) AU BI Data"
- Section A.1.25.8, "Time Collection Manager (secured by HR Position Hierarchy List) AU BI Data"
- Section A.1.25.9, "Human Resource VP (secured by HR Position Hierarchy List) AU BI Data"
- Section A.1.25.10, "Human Resource Analyst (secured by HR Position Hierarchy List) AU BI Data"
- Section A.1.25.11, "Human Resource Manager (secured by HR Position Hierarchy List) AU BI Data"
- Section A.1.25.12, "Learning Manager (secured by HR Position Hierarchy List) AU BI Data"
- Section A.1.25.13, "HR Duty Role to Oracle BI Applications HR Presentation Catalog Mapping"

A.1.25.1 Introduction

Data can be secured via the HR Position Hierarchy using list variable[s], with associated data roles and security filter[s] which are applied at the physical SQL level as JOIN statement with the variables.

How to choose / assign the Duty Role

Each Duty Role grants access to one or more subject areas, and is a member of at least one data security role.

You need to map a source role/responsibility to one or more Duty Roles. For instructions on how this is done refer to the FSM task in Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

HR Data Role to Duty Role Mapping

Note: The following are applicable to HR Position Hierarchy security.

Table A–62 HR Data Role to Duty Role Mapping

Data (Security) Role	Duty Role
Line Manager (secured by HR Position Hierarchy List) AU BI Data	Line Manager (secured by HR Position Hierarchy List) AU BI Duty
Payroll Manager (secured by HR Position Hierarchy List) AU BI Data	Payroll Manager (secured by HR Position Hierarchy List) AU BI Duty
Compensation Analyst (secured by HR Position Hierarchy List) AU BI Data	Compensation Analyst (secured by HR Position Hierarchy List) AU BI Duty
Compensation Manager (secured by HR Position Hierarchy List) AU BI Data	Compensation Manager (secured by HR Position Hierarchy List) AU BI Duty

Table A–62 (Cont.) HR Data Role to Duty Role Mapping

Data (Security) Role	Duty Role
Recruiting Manager (secured by HR Position Hierarchy List) AU BI Data	Recruiting Manager (secured by HR Position Hierarchy List) AU BI Duty
Recruiting VP (secured by HR Position Hierarchy List) AU BI Data	Recruiting VP (secured by HR Position Hierarchy List) AU BI Duty
Time Collection Manager (secured by HR Position Hierarchy List) AU BI Data	Time Collection Manager (secured by HR Position Hierarchy List) AU BI Duty
Human Resource VP (secured by HR Position Hierarchy List) AU BI Data	Human Resource VP (secured by HR Position Hierarchy List) AU BI Duty
Human Resource Analyst (secured by HR Position Hierarchy List) AU BI Data	Human Resource Analyst (secured by HR Position Hierarchy List) AU BI Duty
Human Resource Manager (secured by HR Position Hierarchy List) AU BI Data	Human Resource Manager (secured by HR Position Hierarchy List) AU BI Duty
Learning Manager (secured by HR Position Hierarchy List) AU BI Data	Learning Manager (secured by HR Position Hierarchy List) AU BI Duty

A.1.25.2 Line Manager (secured by HR Position Hierarchy List) AU BI Data

Initialization Blocks

The Line Manager HR Position Hierarchy list is determined at user sign-on via one or more Initialization Blocks:

Table A–63 Initialization Blocks

Variable Name	Initialization Block Name
HR_SEC_POS_LIST	Not applicable, this is a multi source variable population see below.
HR_SEC_POS_HIER_VER	Not applicable, this is a multi source variable population see below.
HR_SEC_POS_HIER_ID	Not applicable, this is a multi source variable population see below.
HR_SEC_POS_LIST____EBS	HR Position Hierarchy ID Version and Position List (EBS).
HR_SEC_POS_LIST____PSFT	HR Position Hierarchy ID Version and Position List (PeopleSoft).
HR_SEC_POS_LIST____FUSN	HR Position Hierarchy ID Version and Position List (Fusion).
HR_SEC_POS_HIER_VER____EBS	HR Position Hierarchy ID Version and Position List (EBS).
HR_SEC_POS_HIER_VER____PSFT	HR Position Hierarchy ID Version and Position List (PeopleSoft).
HR_SEC_POS_HIER_VER____FUSN	HR Position Hierarchy ID Version and Position List (Fusion).
HR_SEC_POS_HIER_ID____EBS	HR Position Hierarchy ID Version and Position List (EBS).
HR_SEC_POS_HIER_ID____PSFT	HR Position Hierarchy ID Version and Position List (PeopleSoft).
HR_SEC_POS_HIER_ID____FUSN	HR Position Hierarchy ID Version and Position List (Fusion).

Table A–63 (Cont.) Initialization Blocks

Variable Name	Initialization Block Name
HR_SEC_POS_HIER_LVL_POS_ID	HR Position Hierarchy Fixed Hier Level.

Data Security Role Filters

The Line Manager HR Position Hierarchy list Security is applied depending on the roles the user is granted, and when it is applied it is supported by the following HR logical facts and dimensions:

Table A–64 Data Security Role Filters

Name	Filter
Dim - HR Position Hierarchy	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Learning Calendar	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Learning Enrollment and Completion	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Learning Enrollment Events	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Absence Event	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))

Table A–64 (Cont.) Data Security Role Filters

Name	Filter
Fact - HR - Recruitment Event Information	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Workforce Event Information	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Workforce Balance Information	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Accrual Transactions - Event Information	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Accrual Transactions - Balance Information	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Time and Labor - Reported Time	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Time and Labor - Processed Time	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))

A.1.25.3 Payroll Manager (secured by HR Position Hierarchy List) AU BI Data

Initialization Blocks

The Payroll Manager HR Position Hierarchy list is determined at user sign-on via one or more Initialization Blocks:

Table A–65 Initialization Blocks

Variable Name	Initialization Block Name
HR_SEC_POS_LIST	Not applicable, this is a multi source variable population see below.
HR_SEC_POS_HIER_VER	Not applicable, this is a multi source variable population see below.
HR_SEC_POS_HIER_ID	Not applicable, this is a multi source variable population see below.
HR_SEC_POS_LIST____EBS	HR Position Hierarchy ID Version and Position List (EBS).
HR_SEC_POS_LIST____PSFT	HR Position Hierarchy ID Version and Position List (PeopleSoft).
HR_SEC_POS_LIST____FUSN	HR Position Hierarchy ID Version and Position List (Fusion).
HR_SEC_POS_HIER_VER____EBS	HR Position Hierarchy ID Version and Position List (EBS).
HR_SEC_POS_HIER_VER____PSFT	HR Position Hierarchy ID Version and Position List (PeopleSoft).
HR_SEC_POS_HIER_VER____FUSN	HR Position Hierarchy ID Version and Position List (Fusion).
HR_SEC_POS_HIER_ID____EBS	HR Position Hierarchy ID Version and Position List (EBS).
HR_SEC_POS_HIER_ID____PSFT	HR Position Hierarchy ID Version and Position List (PeopleSoft).
HR_SEC_POS_HIER_ID____FUSN	HR Position Hierarchy ID Version and Position List (Fusion).
HR_SEC_POS_HIER_LVL_POS_ID	HR Position Hierarchy Fixed Hier Level.

Data Security Role Filters

The Payroll Manager HR Position Hierarchy list Security is applied depending on the roles the user is granted, and when it is applied it is supported by the following HR logical facts and dimensions:

Table A–66 Data Security Role Filters

Name	Filter
Dim - HR Position Hierarchy	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))

Table A–66 (Cont.) Data Security Role Filters

Name	Filter
Fact - HR – Payroll Balance Summary	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Payroll Balance Detail	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))

A.1.25.4 Compensation Analyst (secured by HR Position Hierarchy List) AU BI Data

Initialization Blocks

The Compensation Analyst HR Position Hierarchy list is determined at user sign-on via one or more Initialization Blocks:

Table A–67 Initialization Blocks

Variable Name	Initialization Block Name
HR_SEC_POS_LIST	Not applicable, this is a multi source variable population see below.
HR_SEC_POS_HIER_VER	Not applicable, this is a multi source variable population see below.
HR_SEC_POS_HIER_ID	Not applicable, this is a multi source variable population see below.
HR_SEC_POS_LIST____EBS	HR Position Hierarchy ID Version and Position List (EBS).
HR_SEC_POS_LIST____PSFT	HR Position Hierarchy ID Version and Position List (PeopleSoft).
HR_SEC_POS_LIST____FUSN	HR Position Hierarchy ID Version and Position List (Fusion).
HR_SEC_POS_HIER_VER____EBS	HR Position Hierarchy ID Version and Position List (EBS).
HR_SEC_POS_HIER_VER____PSFT	HR Position Hierarchy ID Version and Position List (PeopleSoft).
HR_SEC_POS_HIER_VER____FUSN	HR Position Hierarchy ID Version and Position List (Fusion).
HR_SEC_POS_HIER_ID____EBS	HR Position Hierarchy ID Version and Position List (EBS).
HR_SEC_POS_HIER_ID____PSFT	HR Position Hierarchy ID Version and Position List (PeopleSoft).
HR_SEC_POS_HIER_ID____FUSN	HR Position Hierarchy ID Version and Position List (Fusion).

Table A–67 (Cont.) Initialization Blocks

Variable Name	Initialization Block Name
HR_SEC_POS_HIER_LVL_POS_ ID	HR Position Hierarchy Fixed Hier Level.

Data Security Role Filters

The Compensation Analyst HR Position Hierarchy list Security is applied depending on the roles the user is granted, and when it is applied it is supported by the following HR logical facts and dimensions:

Table A–68 Data Security Role Filters

Name	Filter
Dim - HR Position Hierarchy	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_ SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_ HIER_ID))
Fact - HR – Payroll Balance Summary	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_ SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_ HIER_ID))
Fact - HR - Payroll Balance Detail	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_ SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_ HIER_ID))
Fact - HR - Workforce Event Information	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_ SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_ HIER_ID))
Fact - HR - Workforce Balance Information	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_ SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_ HIER_ID))

A.1.25.5 Compensation Manager (secured by HR Position Hierarchy List) AU BI Data

Initialization Blocks

The Compensation Manager HR Position Hierarchy list is determined at user sign-on via one or more Initialization Blocks:

Table A–69 Initialization Blocks

Variable Name	Initialization Block Name
HR_SEC_POS_LIST	Not applicable, this is a multi source variable population see below.
HR_SEC_POS_HIER_VER	Not applicable, this is a multi source variable population see below.
HR_SEC_POS_HIER_ID	Not applicable, this is a multi source variable population see below.
HR_SEC_POS_LIST____EBS	HR Position Hierarchy ID Version and Position List (EBS).
HR_SEC_POS_LIST____PSFT	HR Position Hierarchy ID Version and Position List (PeopleSoft).
HR_SEC_POS_LIST____FUSN	HR Position Hierarchy ID Version and Position List (Fusion).
HR_SEC_POS_HIER_VER____EBS	HR Position Hierarchy ID Version and Position List (EBS).
HR_SEC_POS_HIER_VER____PSFT	HR Position Hierarchy ID Version and Position List (PeopleSoft).
HR_SEC_POS_HIER_VER____FUSN	HR Position Hierarchy ID Version and Position List (Fusion).
HR_SEC_POS_HIER_ID____EBS	HR Position Hierarchy ID Version and Position List (EBS).
HR_SEC_POS_HIER_ID____PSFT	HR Position Hierarchy ID Version and Position List (PeopleSoft).
HR_SEC_POS_HIER_ID____FUSN	HR Position Hierarchy ID Version and Position List (Fusion).
HR_SEC_POS_HIER_LVL_POS_ID	HR Position Hierarchy Fixed Hier Level.

Data Security Role Filters

The Compensation Manager HR Position Hierarchy list Security is applied depending on the roles the user is granted, and when it is applied it is supported by the following HR logical facts and dimensions:

Table A–70 Data Security Role Filters

Name	Filter
Dim - HR Position Hierarchy	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))

Table A–70 (Cont.) Data Security Role Filters

Name	Filter
Fact - HR – Payroll Balance Summary	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Payroll Balance Detail	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Workforce Event Information	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Workforce Balance Information	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))

A.1.25.6 Recruiting Manager (secured by HR Position Hierarchy List) AU BI Data

Initialization Blocks

The Recruiting Manager HR Position Hierarchy list is determined at user sign-on via one or more Initialization Blocks:

Table A–71 Initialization Blocks

Variable Name	Initialization Block Name
HR_SEC_POS_LIST	Not applicable, this is a multi source variable population see below.
HR_SEC_POS_HIER_VER	Not applicable, this is a multi source variable population see below.
HR_SEC_POS_HIER_ID	Not applicable, this is a multi source variable population see below.
HR_SEC_POS_LIST____EBS	HR Position Hierarchy ID Version and Position List (EBS).
HR_SEC_POS_LIST____PSFT	HR Position Hierarchy ID Version and Position List (PeopleSoft).

Table A–71 (Cont.) Initialization Blocks

Variable Name	Initialization Block Name
HR_SEC_POS_LIST____FUSN	HR Position Hierarchy ID Version and Position List (Fusion).
HR_SEC_POS_HIER_VER____EBS	HR Position Hierarchy ID Version and Position List (EBS).
HR_SEC_POS_HIER_VER____PSFT	HR Position Hierarchy ID Version and Position List (PeopleSoft).
HR_SEC_POS_HIER_VER____FUSN	HR Position Hierarchy ID Version and Position List (Fusion).
HR_SEC_POS_HIER_ID____EBS	HR Position Hierarchy ID Version and Position List (EBS).
HR_SEC_POS_HIER_ID____PSFT	HR Position Hierarchy ID Version and Position List (PeopleSoft).
HR_SEC_POS_HIER_ID____FUSN	HR Position Hierarchy ID Version and Position List (Fusion).
HR_SEC_POS_HIER_LVL_POS_ID	HR Position Hierarchy Fixed Hier Level.

Data Security Role Filters

The Recruiting Manager HR Position Hierarchy list Security is applied depending on the roles the user is granted, and when it is applied it is supported by the following HR logical facts and dimensions:

Table A–72 Data Security Role Filters

Name	Filter
Dim - HR Position Hierarchy	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Recruitment Event Information	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))

A.1.25.7 Recruiting VP (secured by HR Position Hierarchy List) AU BI Data

Initialization Blocks

The Recruiting VP HR Position Hierarchy list is determined at user sign-on via one or more Initialization Blocks:

Table A–73 Initialization Blocks

Variable Name	Initialization Block Name
HR_SEC_POS_LIST	Not applicable, this is a multi source variable population see below.
HR_SEC_POS_HIER_VER	Not applicable, this is a multi source variable population see below.
HR_SEC_POS_HIER_ID	Not applicable, this is a multi source variable population see below.
HR_SEC_POS_LIST____EBS	HR Position Hierarchy ID Version and Position List (EBS).
HR_SEC_POS_LIST____PSFT	HR Position Hierarchy ID Version and Position List (PeopleSoft).
HR_SEC_POS_LIST____FUSN	HR Position Hierarchy ID Version and Position List (Fusion).
HR_SEC_POS_HIER_VER____EBS	HR Position Hierarchy ID Version and Position List (EBS).
HR_SEC_POS_HIER_VER____PSFT	HR Position Hierarchy ID Version and Position List (PeopleSoft).
HR_SEC_POS_HIER_VER____FUSN	HR Position Hierarchy ID Version and Position List (Fusion).
HR_SEC_POS_HIER_ID____EBS	HR Position Hierarchy ID Version and Position List (EBS).
HR_SEC_POS_HIER_ID____PSFT	HR Position Hierarchy ID Version and Position List (PeopleSoft).
HR_SEC_POS_HIER_ID____FUSN	HR Position Hierarchy ID Version and Position List (Fusion).
HR_SEC_POS_HIER_LVL_POS_ID	HR Position Hierarchy Fixed Hier Level.

Data Security Role Filters

The Recruiting VP HR Position Hierarchy list Security is applied depending on the roles the user is granted, and when it is applied it is supported by the following HR logical facts and dimensions:

Table A–74 Data Security Role Filters

Name	Filter
Dim - HR Position Hierarchy	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))

Table A–74 (Cont.) Data Security Role Filters

Name	Filter
Fact - HR - Recruitment Event Information	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))

A.1.25.8 Time Collection Manager (secured by HR Position Hierarchy List) AU BI Data

Initialization Blocks

The Time Collection Manager HR Position Hierarchy list is determined at user sign-on via one or more Initialization Blocks:

Table A–75 Initialization Blocks

Variable Name	Initialization Block Name
HR_SEC_POS_LIST	Not applicable, this is a multi source variable population see below.
HR_SEC_POS_HIER_VER	Not applicable, this is a multi source variable population see below.
HR_SEC_POS_HIER_ID	Not applicable, this is a multi source variable population see below.
HR_SEC_POS_LIST____EBS	HR Position Hierarchy ID Version and Position List (EBS).
HR_SEC_POS_LIST____PSFT	HR Position Hierarchy ID Version and Position List (PeopleSoft).
HR_SEC_POS_LIST____FUSN	HR Position Hierarchy ID Version and Position List (Fusion).
HR_SEC_POS_HIER_VER____EBS	HR Position Hierarchy ID Version and Position List (EBS).
HR_SEC_POS_HIER_VER____PSFT	HR Position Hierarchy ID Version and Position List (PeopleSoft).
HR_SEC_POS_HIER_VER____FUSN	HR Position Hierarchy ID Version and Position List (Fusion).
HR_SEC_POS_HIER_ID____EBS	HR Position Hierarchy ID Version and Position List (EBS).
HR_SEC_POS_HIER_ID____PSFT	HR Position Hierarchy ID Version and Position List (PeopleSoft).
HR_SEC_POS_HIER_ID____FUSN	HR Position Hierarchy ID Version and Position List (Fusion).
HR_SEC_POS_HIER_LVL_POS_ID	HR Position Hierarchy Fixed Hier Level.

Data Security Role Filters

The Time Collection Manager HR Position Hierarchy list Security is applied depending on the roles the user is granted, and when it is applied it is supported by the following HR logical facts and dimensions:

Table A–76 Data Security Role Filters

Name	Filter
Dim - HR Position Hierarchy	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Time and Labor - Reported Time	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Time and Labor - Processed Time	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Workforce Balance Information	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR – Payroll Balance Summary	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))

A.1.25.9 Human Resource VP (secured by HR Position Hierarchy List) AU BI Data

Initialization Blocks

The Human Resource VP HR Position Hierarchy list is determined at user sign-on via one or more Initialization Blocks:

Table A–77 Initialization Blocks

Variable Name	Initialization Block Name
HR_SEC_POS_LIST	Not applicable, this is a multi source variable population see below.
HR_SEC_POS_HIER_VER	Not applicable, this is a multi source variable population see below.

Table A–77 (Cont.) Initialization Blocks

Variable Name	Initialization Block Name
HR_SEC_POS_HIER_ID	Not applicable, this is a multi source variable population see below.
HR_SEC_POS_LIST____EBS	HR Position Hierarchy ID Version and Position List (EBS).
HR_SEC_POS_LIST____PSFT	HR Position Hierarchy ID Version and Position List (PeopleSoft).
HR_SEC_POS_LIST____FUSN	HR Position Hierarchy ID Version and Position List (Fusion).
HR_SEC_POS_HIER_VER____EBS	HR Position Hierarchy ID Version and Position List (EBS).
HR_SEC_POS_HIER_VER____PSFT	HR Position Hierarchy ID Version and Position List (PeopleSoft).
HR_SEC_POS_HIER_VER____FUSN	HR Position Hierarchy ID Version and Position List (Fusion).
HR_SEC_POS_HIER_ID____EBS	HR Position Hierarchy ID Version and Position List (EBS).
HR_SEC_POS_HIER_ID____PSFT	HR Position Hierarchy ID Version and Position List (PeopleSoft).
HR_SEC_POS_HIER_ID____FUSN	HR Position Hierarchy ID Version and Position List (Fusion).
HR_SEC_POS_HIER_LVL_POS_ID	HR Position Hierarchy Fixed Hier Level.

Data Security Role Filters

The Human Resource VP HR Position Hierarchy list Security is applied depending on the roles the user is granted, and when it is applied it is supported by the following HR logical facts and dimensions:

Table A–78 Data Security Role Filters

Name	Filter
Dim - HR Position Hierarchy	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Learning Calendar	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))

Table A–78 (Cont.) Data Security Role Filters

Name	Filter
Fact - HR - Learning Enrollment and Completion	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Learning Enrollment Events	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Absence Event	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Recruitment Event Information	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Workforce Event Information	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Workforce Balance Information	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Accrual Transactions - Event Information	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))

Table A–78 (Cont.) Data Security Role Filters

Name	Filter
Fact - HR - Accrual Transactions - Balance Information	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Time and Labor - Reported Time	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Time and Labor - Processed Time	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))

A.1.25.10 Human Resource Analyst (secured by HR Position Hierarchy List) AU BI Data

Initialization Blocks

The Human Resource Analyst HR Position Hierarchy list is determined at user sign-on via one or more Initialization Blocks:

Table A–79 Initialization Blocks

Variable Name	Initialization Block Name
HR_SEC_POS_LIST	Not applicable, this is a multi source variable population see below.
HR_SEC_POS_HIER_VER	Not applicable, this is a multi source variable population see below.
HR_SEC_POS_HIER_ID	Not applicable, this is a multi source variable population see below.
HR_SEC_POS_LIST____EBS	HR Position Hierarchy ID Version and Position List (EBS).
HR_SEC_POS_LIST____PSFT	HR Position Hierarchy ID Version and Position List (PeopleSoft).
HR_SEC_POS_LIST____FUSN	HR Position Hierarchy ID Version and Position List (Fusion).
HR_SEC_POS_HIER_VER____EBS	HR Position Hierarchy ID Version and Position List (EBS).
HR_SEC_POS_HIER_VER____PSFT	HR Position Hierarchy ID Version and Position List (PeopleSoft).

Table A–79 (Cont.) Initialization Blocks

Variable Name	Initialization Block Name
HR_SEC_POS_HIER_VER____FUSN	HR Position Hierarchy ID Version and Position List (Fusion).
HR_SEC_POS_HIER_ID____EBS	HR Position Hierarchy ID Version and Position List (EBS).
HR_SEC_POS_HIER_ID____PSFT	HR Position Hierarchy ID Version and Position List (PeopleSoft).
HR_SEC_POS_HIER_ID____FUSN	HR Position Hierarchy ID Version and Position List (Fusion).
HR_SEC_POS_HIER_LVL_POS_ID	HR Position Hierarchy Fixed Hier Level.

Data Security Role Filters

The Human Resource Analyst HR Position Hierarchy list Security is applied depending on the roles the user is granted, and when it is applied it is supported by the following HR logical facts and dimensions:

Table A–80 Data Security Role Filters

Name	Filter
Dim - HR Position Hierarchy	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Learning Calendar	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Learning Enrollment and Completion	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Learning Enrollment Events	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))

Table A–80 (Cont.) Data Security Role Filters

Name	Filter
Fact - HR - Absence Event	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Recruitment Event Information	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Workforce Event Information	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Workforce Balance Information	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Accrual Transactions - Event Information	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Accrual Transactions - Balance Information	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Payroll Balance Summary	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))

A.1.25.11 Human Resource Manager (secured by HR Position Hierarchy List) AU BI Data

Initialization Blocks

The Human Resource Manager HR Position Hierarchy list is determined at user sign-on via one or more Initialization Blocks:

Table A–81 Initialization Blocks

Variable Name	Initialization Block Name
HR_SEC_POS_LIST	Not applicable, this is a multi source variable population see below.
HR_SEC_POS_HIER_VER	Not applicable, this is a multi source variable population see below.
HR_SEC_POS_HIER_ID	Not applicable, this is a multi source variable population see below.
HR_SEC_POS_LIST____EBS	HR Position Hierarchy ID Version and Position List (EBS).
HR_SEC_POS_LIST____PSFT	HR Position Hierarchy ID Version and Position List (PeopleSoft).
HR_SEC_POS_LIST____FUSN	HR Position Hierarchy ID Version and Position List (Fusion).
HR_SEC_POS_HIER_VER____EBS	HR Position Hierarchy ID Version and Position List (EBS).
HR_SEC_POS_HIER_VER____PSFT	HR Position Hierarchy ID Version and Position List (PeopleSoft).
HR_SEC_POS_HIER_VER____FUSN	HR Position Hierarchy ID Version and Position List (Fusion).
HR_SEC_POS_HIER_ID____EBS	HR Position Hierarchy ID Version and Position List (EBS).
HR_SEC_POS_HIER_ID____PSFT	HR Position Hierarchy ID Version and Position List (PeopleSoft).
HR_SEC_POS_HIER_ID____FUSN	HR Position Hierarchy ID Version and Position List (Fusion).
HR_SEC_POS_HIER_LVL_POS_ID	HR Position Hierarchy Fixed Hier Level.

Data Security Role Filters

The Human Resource Manager HR Position Hierarchy list Security is applied depending on the roles the user is granted, and when it is applied it is supported by the following HR logical facts and dimensions:

Table A–82 Data Security Role Filters

Name	Filter
Dim - HR Position Hierarchy	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Learning Calendar	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Learning Enrollment and Completion	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Learning Enrollment Events	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Absence Event	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Recruitment Event Information	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Workforce Event Information	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))

Table A–82 (Cont.) Data Security Role Filters

Name	Filter
Fact - HR - Workforce Balance Information	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Accrual Transactions - Event Information	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Accrual Transactions - Balance Information	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))

A.1.25.12 Learning Manager (secured by HR Position Hierarchy List) AU BI Data

Initialization Blocks

The Learning Manager HR Position Hierarchy list is determined at user sign-on via one or more Initialization Blocks:

Table A–83 Initialization Blocks

Variable Name	Initialization Block Name

Data Security Role Filters

The Learning Manager HR Position Hierarchy list Security is applied depending on the roles the user is granted, and when it is applied it is supported by the following HR logical facts and dimensions:

Table A–84 Data Security Role Filters

Name	Filter
Dim - HR Position Hierarchy	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))

Table A–84 (Cont.) Data Security Role Filters

Name	Filter
Fact - HR - Learning Calendar	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Learning Enrollment and Completion	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))
Fact - HR - Learning Enrollment Events	"Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Based Position Id" = VALUEOF(NQ_SESSION.HR_SEC_POS_LIST) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy Version" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_VER)) AND "Core"."Dim - HR Position Hierarchy"."Sec Filter Col - Hierarchy ID" = (VALUEOF(NQ_SESSION.HR_SEC_POS_HIER_ID))

A.1.25.13 HR Duty Role to Oracle BI Applications HR Presentation Catalog Mapping

Note: The following are applicable to security.

Table A–85 HR Duty Role to Oracle BI Applications HR Presentation Catalog Mapping

BI Duty Roles	HR Presentation Catalog Mapping
Line Manager (secured by HR Position Hierarchy List) AU BI Duty	Human Resources - Absence and Leave Accrual Human Resources - Compensation Human Resources - Learning Enrollment and Completion Human Resources - Recruitment Human Resources - Workforce Deployment Human Resources – Time and Labor
Payroll Manager (secured by HR Position Hierarchy List) AU BI Duty	Human Resources – Payroll Human Resources – Time and Labor
Compensation Analyst (secured by HR Position Hierarchy List) AU BI Duty	Human Resources - Compensation Human Resources – Payroll
Compensation Manager (secured by HR Position Hierarchy List) AU BI Duty	Human Resources - Compensation Human Resources – Payroll
Recruiting Manager (secured by HR Position Hierarchy List) AU BI Duty	Human Resources – Recruitment
Recruiting VP (secured by HR Position Hierarchy List) AU BI Duty	Human Resources – Recruitment

Table A–85 (Cont.) HR Duty Role to Oracle BI Applications HR Presentation Catalog

BI Duty Roles	HR Presentation Catalog Mapping
Time Collection Manager (secured by HR Position Hierarchy List) AU BI Duty	Human Resources – Time and Labor
Human Resource VP (secured by HR Position Hierarchy List) AU BI Duty	Human Resources - Absence and Leave Accrual Human Resources - Compensation Human Resources - Learning Enrollment and Completion Human Resources - Payroll Human Resources - Recruitment Human Resources - Workforce Deployment Human Resources - Workforce Effectiveness
Human Resource Analyst (secured by HR Position Hierarchy List) AU BI Duty	Human Resources - Absence and Leave Accrual Human Resources - Compensation Human Resources - Learning Enrollment and Completion Human Resources - Recruitment Human Resources - Workforce Deployment
Human Resource Manager (secured by HR Position Hierarchy List) AU BI Duty	Human Resources - Absence and Leave Accrual Human Resources - Compensation Human Resources - Learning Enrollment and Completion Human Resources - Recruitment Human Resources - Workforce Deployment
Learning Manager (secured by HR Position Hierarchy List) AU BI Duty	Human Resources - Learning Enrollment and Completion

A.1.26 How to set up Payroll Based Data Security

There is no topic for this FSM Task.

A.1.27 How to Set Up Project GL Reconciliation Security for Peoplesoft

Overview

Project Analytics supports security over following dimensions in Project GL Recon. In the Oracle Business Intelligence Applications solution, the 'Business Unit' entity refers to 'Operating Unit Organizations' in EBS. The list of Business Units that a user has access to, is determined by E-Business Suite grants.

Table A–86 Project Costing and Control Facts

Security Entity	GL Recon Cost Fact	GL Recon Revenue Fact
Project Business Unit	N	N
Project Organization	N	N
Expenditure Business Unit	N	N
Contract Business Unit	N	N
Project	N	N

Table A–86 (Cont.) Project Costing and Control Facts

Security Entity	GL Recon Cost Fact	GL Recon Revenue Fact
Resource Organization	N	N
Ledger	Y	Y

Configuring PROJECT GL REC FOR E-Business Suite

In order for data security filters to be applied, appropriate initialization blocks need to be enabled depending on the deployed source system.

> **Note:** On installation, initialization blocks are enabled for E-Business Suite R12. If you are deploying on a source system other than E-Business Suite R12, then you must enable the appropriate initialization blocks.

You must enable data security for Project GL Reconciliation in E-Business Suite by enabling E-Business Suite data security initialization block listed below. If only one source system is deployed, then you must make sure that all Project Security initialization blocks for other adapters are disabled. If more than one source system is deployed, then you must also enable the initialization blocks of those source systems.

Init Blocks

EBS: Project GL Recon Ledger List EBS

To Set Up Project GL Reconcilliation Security for EBS

1. In Oracle BI Administration Tool, edit the BI metadata repository (for example, OracleBIAnalyticsApps.rpd) in online mode, and select Manage, then Identity, then Application Roles.
2. Double click on OBIA_PROJECT_LEDGER_DATA_SECURITY, navigate to Permissions, then Data Filters, and enable all data security filters.
3. Save the metadata repository.

A.1.27.1 Configuring BI Duty Roles

The following BI Duty Roles are applicable to the Project GL Recon subject area.

- OBIA_EBS_PROJECT_EXECUTIVE_ANALYSIS_DUTY
- OBIA_EBS_PROJECT_MANAGEMENT_ANALYSIS_DUTY
- OBIA_EBS_PROJECT_DATA_SECURITY

These Duty Roles control the subject areas and dashboard content to which the user has access. These Duty Roles also ensure the data security filters are applied to all the queries. For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

A.1.28 How to Set Up Project Resource Management Security for Peoplesoft

Overview

Project Analytics supports security using following dimensions in Project Resource Management subject areas.

Table A–87 Supported Project Resource Management Security subject areas

Project Resource Management Facts Securing Entity	Resource Availability	Resource Requirement	Resource Utilization Assignment	Resource Utilization Capacity	Resource Utilization Expected	Employee Job/Competency
Project Business Unit	N	Y	Y	N	Y	N
Project Organization	N	N	N	N	N	N
Expenditure Business Unit	N	N	N	N	N	N
Contract Business Unit	N	N	N	N	N	N
Project	N	Y	Y	N	Y	N
Resource Organization	N	N	N	N	N	N
Ledger	N	N	N	N	N	N

Configuring Project Resource Management For PeopleSoft

In order for data security filters to be applied, appropriate initialization blocks need to be enabled depending on the deployed source system.

> **Note:** On installation, initialization blocks are enabled for E-Business Suite R12. If you are deploying on a source system other than E-Business Suite R12, then you must enable the appropriate initialization blocks.

Enable data security for Project Resource Management in PeopleSoft based on your PeopleSoft security configuration. That is, if security by Business Unit has been implemented, then you must follow the Security by Business Unit Section (ignore Security by Projects section); if security by projects has been implemented, then you must follow the Security by Projects section (ignore Security by Business Unit section) and enable data security initialization blocks listed in sections below. You must disable Project Security initialization blocks for other adapters. If more than one source system is deployed, then you must also enable the initialization blocks of those source systems.

About Data Security Configuration in PeopleSoft

In PeopleSoft, you access the security configuration pages for securing Project transactions by selecting Main Menu, then Set up Financials/Supply Chain, then Security, then Security Options.

Depending on your security configuration, you need to use any combination of either Project Business Unit or Project dimension. Based on that, you need to change the default configuration to match the OLTP security setup.

A.1.28.1 Security by Business Unit

Init Blocks:

- Project Business Unit List RM PSFT

If you are securing the Project data by Project BU only, then follow the steps below to disable the Project dimension security:

1. In Oracle BI Administration Tool, edit the BI metadata repository (for example, OracleBIAnalyticsApps.rpd) in online mode, and select Manage, then Identity.
2. Double click on OBIA_PROJECT_BUSINESS_UNIT_DATA_SECURITY, navigate to Permissions, then Data Filters, and enable all data security filters that are disabled.

   This activates Project BU Security, which is required for the Resource Management Module in PeopleSoft.
3. In Oracle Enterprise Manager Fusion Middleware Control, select Business Application Instance, then Application Roles, then Select the Oracle BI Applications Stripe, and query for the OBIA_PROJECT_DATA_SECURITY Application Role.

   Note that OBIA_PSFT_PROJECT_DATA_SECURITY is listed as one of the members.
4. Remove OBIA_PSFT_PROJECT_DATA_SECURITY as a member of the OBIA_PROJECT_DATA_SECURITY Duty Role.
5. In Oracle BI Administration Tool, edit the BI metadata repository (for example, OracleBIAnalyticsApps.rpd) in online mode, and select Manage, then Identity, then Action, then Synchronize Application Roles.

A.1.28.2 Security by Project

Init Blocks:

- Project List RM PSFT

If you are securing the Project data by Project dimension only, then follow the steps below to disable the Project BU dimension security:

1. In Oracle BI Administration Tool, edit the BI metadata repository (for example, OracleBIAnalyticsApps.rpd) in online mode, and select Manage, then Identity.
2. Double click on OBIA_PROJECT_DATA_SECURITY, navigate to Permissions, then Data Filters, and enable all data security filters that are disabled.

   This activates Project based Security, which is required for the Resource Management Module in PeopleSoft.
3. In Oracle Enterprise Manager Fusion Middleware Control, select Business Application Instance, then Application Roles, then Select the Oracle BI Applications Stripe, and query for the OBIA_PROJECT_BUSINESS_UNIT_DATA_SECURITY Application Role.

   Note that OBIA_PSFT_PROJECT_DATA_SECURITY is listed as one of the members.
4. Remove OBIA_PSFT_PROJECT_DATA_SECURITY as a member of the OBIA_PROJECT_BUSINESS_UNIT_DATA_SECURITY Duty Role.
5. In Oracle BI Administration Tool, select Manage, then Identity, then Action, then Synchronize Application Roles.

Note: Tree based Project Security type queries are not supported in the default application.

A.1.28.3 Configuring BI Duty Roles

The following BI Duty Roles are applicable to the Project Resource Management subject area.

- OBIA_PSFT_PROJECT_EXECUTIVE_ANALYSIS_DUTY
- OBIA_PSFT_PROJECT_MANAGEMENT_ANALYSIS_DUTY
- OBIA_PSFT_PROJECT_DATA_SECURITY

These Duty Roles control the subject areas and dashboard content to which the user has access. These Duty Roles also ensure the data security filters are applied to all the queries. For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

A.1.29 How to Set Up General Ledger Security for Peoplesoft

Overview

Financial Analytics supports a combination of the following security mechanisms for GL subject areas:

- Security using Ledgers
- Security using PeopleSoft Chartfields

A.1.29.1 Configuring Ledger Security

In order for data security filters to be applied, appropriate initialization blocks need to be enabled depending on the deployed source system. To enable Ledger Security for PeopleSoft, enable PeopleSoft initialization block and make sure the initialization blocks of all other source systems are disabled. The initialization block names relevant to various source systems are given below. If more than one source system is deployed, then you must also enable the initialization blocks of those source systems.

- E-Business Suite 11i: Ledgers EBS11
- E-Business Suite R12: Ledgers EBS12
- Oracle PeopleSoft: Ledgers PeopleSoft

To enable initialization blocks, follow the steps below:

1. In Oracle BI Administration Tool, edit the BI metadata repository (for example, OracleBIAnalyticsApps.rpd).
2. Choose Manage, then Variables.
3. Under Session – Initialization Blocks, open the initialization block that you need to enable.
4. Clear the **Disabled** check box.
5. Save the metadata repository (RPD file).

A.1.29.2 Configuring GL Segment Security using PeopleSoft Chartfields

Note: This section is applicable only if you have enabled Commitment Control in PeopleSoft. If you do not have Commitment Control, then you can skip this section.

This section gives an overview of the segment security using PeopleSoft Chartfields and supported scenarios in BI Applications.

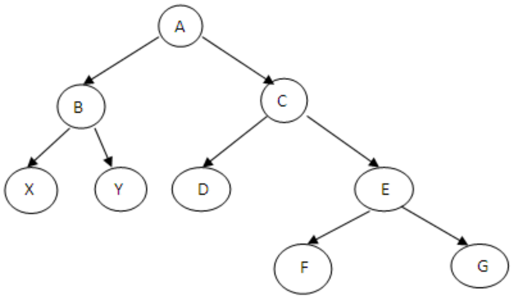
There are various options using which you can setup security rules in the Commitment Control module in PeopleSoft. Oracle BI Applications supports only the following two security rules:

- Security rules setup using the 'Allow' access attribute.
- Security rules setup using the 'Tree Node' parameter.

A user can have two different types of access for each chartfield:

- Partial Access - User has access to specific values within the tree defined for a chartfield. The node, for which the user has access to, is defined using the 'Allow' and the 'Tree Node' parameter in PeopleSoft. When the user is given access to a node within the tree, it means that the user has access to that node and all its child nodes.

  For example, if a user is granted access to node C, then the user has access to nodes C, D, E, F and G.



- Full Access – The user has complete access to all the SETIDs for that chartfield.

A.1.29.3 Configuring GL Segment Security

GL Segment Security can be applied on the qualified GL Segment Dimensions: 'Dim – Cost Center', 'Dim – Natural Account' & 'Dim – Balancing Segment', as well as the 10 generic dimensions 'Dim – GL Segment1 to 'Dim – GL Segment 10' which are configurable to be any of the chartfields.

Before setting up the security, you need to first identify which of these segment dimensions you need to apply security on depending on your security requirements and the security setup in the Commitment Control module. Once that is determined the following steps to configure the RPD metadata need to be repeated for each of the securing segment dimension.

Initialization Blocks and Session Variables

1. Create a 'row wise' session initialization block and a corresponding session variable to get all the parent nodes the user has access to in a tree. Use the SQL queries and session variable names as given in the table below depending on the dimension that is secured.

Table A–88 Initialization Blocks and Session Variables

<table>
<tr><th>Dimension</th><th>SQL</th><th>Variable Name</th></tr>
<tr><td>Dim – Cost Center</td><td>SELECT DISTINCT 'GL_SEC_COSTCENTER_FILTEREDACCESS____PSFT', 'Department'||'~'||DEFN.SETID||'~'||DEFN.TREE_NAME||'~'||DEFN.TREE_NODE FROM PS_KSEC_RULES RULES, PS_KSEC_RULES_DEFN DEFN, PS_KSEC_RULES_EVEN EVENTS, PS_KSEC_OPR_RULES OPR WHERE OPR.KSEC_RULE=EVENTS.KSEC_RULE AND EVENTS.KSEC_RULE=RULES.KSEC_RULE AND RULES.KSEC_RULE=DEFN.KSEC_RULE AND EVENTS.KSEC_EVENT='INQUIRE' AND RULES.KSEC_ATTRIB='A' AND DEFN.KSEC_RULE_PARAM='TRE' AND DEFN.CHARTFIELD='DEPTID' AND OPR.OPRID = 'VALUEOF(NQ_SESSION.USER)'
UNION
SELECT DISTINCT 'GL_SEC_COSTCENTER_FILTEREDACCESS____PSFT', 'Department'||'~'||DEFN.SETID||'~'||DEFN.TREE_NAME||'~'||DEFN.TREE_NODE FROM PS_KSEC_RULES RULES, PS_KSEC_RULES_DEFN DEFN,PS_KSEC_RULES_EVEN EVENTS, PS_KSEC_CLSS_RULES CLSS, PSOPRDEFN OP, PSROLEUSER ORL, PSROLECLASS RCL WHERE CLSS.OPRCLASS = RCL.CLASSID AND OP.OPRID = ORL.ROLEUSER AND ORL.ROLENAME = RCL.ROLENAME AND CLSS.KSEC_RULE=EVENTS.KSEC_RULE AND EVENTS.KSEC_RULE=RULES.KSEC_RULE AND RULES.KSEC_RULE=DEFN.KSEC_RULE AND EVENTS.KSEC_EVENT='INQUIRE' AND RULES.KSEC_ATTRIB='A' AND DEFN.KSEC_RULE_PARAM='TRE' AND DEFN.CHARTFIELD='DEPTID' AND OP.OPRID = 'VALUEOF(NQ_SESSION.USER)</td><td>GL_SEC_COSTCENTER_FILTEREDACCESS____PSFT</td></tr>
</table>

Table A–88 (Cont.) Initialization Blocks and Session Variables

<table>
<tr><th>Dimension</th><th>SQL</th><th>Variable Name</th></tr>
<tr><td>Dim – Natural Account</td><td>SELECT DISTINCT 'GL_SEC_ACCOUNT_FILTEREDACCESS____PSFT', 'Account'||'~'||DEFN.SETID||'~'||DEFN.TREE_NAME||'~'||DEFN.TREE_NODE FROM PS_KSEC_RULES RULES, PS_KSEC_RULES_DEFN DEFN, PS_KSEC_RULES_EVEN EVENTS, PS_KSEC_OPR_RULES OPR WHERE OPR.KSEC_RULE=EVENTS.KSEC_RULE AND EVENTS.KSEC_RULE=RULES.KSEC_RULE AND RULES.KSEC_RULE=DEFN.KSEC_RULE AND EVENTS.KSEC_EVENT='INQUIRE' AND RULES.KSEC_ATTRIB='A' AND DEFN.KSEC_RULE_PARAM='TRE' AND DEFN.CHARTFIELD='ACCOUNT' AND OPR.OPRID = 'VALUEOF(NQ_SESSION.USER)'
UNION
SELECT DISTINCT 'GL_SEC_ACCOUNT_FILTEREDACCESS____PSFT', 'Account'||'~'||DEFN.SETID||'~'||DEFN.TREE_NAME||'~'||DEFN.TREE_NODE FROM PS_KSEC_RULES RULES, PS_KSEC_RULES_DEFN DEFN,PS_KSEC_RULES_EVEN EVENTS, PS_KSEC_CLSS_RULES CLSS, PSOPRDEFN OP, PSROLEUSER ORL, PSROLECLASS RCL WHERE CLSS.OPRCLASS = RCL.CLASSID AND OP.OPRID = ORL.ROLEUSER AND ORL.ROLENAME = RCL.ROLENAME AND CLSS.KSEC_RULE=EVENTS.KSEC_RULE AND EVENTS.KSEC_RULE=RULES.KSEC_RULE AND RULES.KSEC_RULE=DEFN.KSEC_RULE AND EVENTS.KSEC_EVENT='INQUIRE' AND RULES.KSEC_ATTRIB='A' AND DEFN.KSEC_RULE_PARAM='TRE' AND DEFN.CHARTFIELD='ACCOUNT' AND OP.OPRID = 'VALUEOF(NQ_SESSION.USER)'</td><td>GL_SEC_ACCOUNT_FILTEREDACCESS____PSFT</td></tr>
</table>

Table A–88 (Cont.) Initialization Blocks and Session Variables

Dimension	SQL	Variable Name

Dim – Balancing Segment	SELECT DISTINCT 'GL_SEC_BALANCING_FILTEREDACCESS____PSFT', 'Fund Code'||'~'||DEFN.SETID||'~'||DEFN.TREE_NAME||'~'||DEFN.TREE_NODE FROM PS_KSEC_RULES RULES, PS_KSEC_RULES_DEFN DEFN, PS_KSEC_RULES_EVEN EVENTS, PS_KSEC_OPR_RULES OPR WHERE OPR.KSEC_RULE=EVENTS.KSEC_RULE AND EVENTS.KSEC_RULE=RULES.KSEC_RULE AND RULES.KSEC_RULE=DEFN.KSEC_RULE AND EVENTS.KSEC_EVENT='INQUIRE' AND RULES.KSEC_ATTRIB='A' AND DEFN.KSEC_RULE_PARAM='TRE' AND DEFN.CHARTFIELD='FUND_CODE' AND OPR.OPRID = 'VALUEOF(NQ_SESSION.USER)'
	UNION
	SELECT DISTINCT 'GL_SEC_BALANCING_FILTEREDACCESS____PSFT', 'Fund Code'||'~'||DEFN.SETID||'~'||DEFN.TREE_NAME||'~'||DEFN.TREE_NODE FROM PS_KSEC_RULES RULES, PS_KSEC_RULES_DEFN DEFN,PS_KSEC_RULES_EVEN EVENTS, PS_KSEC_CLSS_RULES CLSS, PSOPRDEFN OP, PSROLEUSER ORL, PSROLECLASS RCL WHERE CLSS.OPRCLASS = RCL.CLASSID AND OP.OPRID = ORL.ROLEUSER AND ORL.ROLENAME = RCL.ROLENAME AND CLSS.KSEC_RULE=EVENTS.KSEC_RULE AND EVENTS.KSEC_RULE=RULES.KSEC_RULE AND RULES.KSEC_RULE=DEFN.KSEC_RULE AND EVENTS.KSEC_EVENT='INQUIRE' AND RULES.KSEC_ATTRIB='A' AND DEFN.KSEC_RULE_PARAM='TRE' AND DEFN.CHARTFIELD='FUND_CODE' AND OP.OPRID = 'VALUEOF(NQ_SESSION.USER)'
		GL_SEC_BALANCING_FILTEREDACCESS____PSFT

Table A–88 (Cont.) Initialization Blocks and Session Variables

<table>
<tr><th>Dimension</th><th>SQL</th><th>Variable Name</th></tr>
<tr><td>Dim – GL Segment<n></td><td>SELECT DISTINCT 'GL_SEC_SEGMENT<n>_FILTEREDACCESS____PSFT', '<ChartfieldString>'||'~'||DEFN.SETID||'~'||DEFN.TREE_NAME||'~'||DEFN.TREE_NODE FROM PS_KSEC_RULES RULES, PS_KSEC_RULES_DEFN DEFN, PS_KSEC_RULES_EVEN EVENTS, PS_KSEC_OPR_RULES OPR WHERE OPR.KSEC_RULE=EVENTS.KSEC_RULE AND EVENTS.KSEC_RULE=RULES.KSEC_RULE AND RULES.KSEC_RULE=DEFN.KSEC_RULE AND EVENTS.KSEC_EVENT='INQUIRE' AND RULES.KSEC_ATTRIB='A' AND DEFN.KSEC_RULE_PARAM='TRE' AND DEFN.CHARTFIELD='<ChartfieldCode>' AND OPR.OPRID = 'VALUEOF(NQ_SESSION.USER)'
UNION
SELECT DISTINCT 'GL_SEC_SEGMENT<n>_FILTEREDACCESS____PSFT', '<ChartfieldString>'||'~'||DEFN.SETID||'~'||DEFN.TREE_NAME||'~'||DEFN.TREE_NODE FROM PS_KSEC_RULES RULES, PS_KSEC_RULES_DEFN DEFN,PS_KSEC_RULES_EVEN EVENTS, PS_KSEC_CLSS_RULES CLSS, PSOPRDEFN OP, PSROLEUSER ORL, PSROLECLASS RCL WHERE CLSS.OPRCLASS = RCL.CLASSID AND OP.OPRID = ORL.ROLEUSER AND ORL.ROLENAME = RCL.ROLENAME AND CLSS.KSEC_RULE=EVENTS.KSEC_RULE AND EVENTS.KSEC_RULE=RULES.KSEC_RULE AND RULES.KSEC_RULE=DEFN.KSEC_RULE AND EVENTS.KSEC_EVENT='INQUIRE' AND RULES.KSEC_ATTRIB='A' AND DEFN.KSEC_RULE_PARAM='TRE' AND DEFN.CHARTFIELD='<ChartfieldCode>' AND OP.OPRID = 'VALUEOF(NQ_SESSION.USER)'</td><td>GL_SEC_SEGMENT<n>_FILTEREDACCESS____PSFT</td></tr>
</table>

Connection Pool: "PeopleSoft OLTP"."PeopleSoft OLTP DbAuth Connection Pool"

Notes:

- For the Dim – GL Segment<n> init blocks, use the appropriate chartfield string and the chartfield code based on the chartfield you are securing. You can get the chartfield code from the PeopleSoft source system and the chartfield string should match the names used in file_glacct_segment_config_psft.csv file.

- Use the default value for these variables as 'Default'.

- All the variables created above should end with ____PSFT (4 '_' followed by the string PSFT). This is for multi source implementation where the same variable can be initialized using multiple SQL statements for multiple source systems.

2. Create a 'row wise' session initialization block and a corresponding session variable to get the level in the hierarchy the above nodes fall in a tree. Use the SQL queries and session variable names as given in the table below depending on the dimension that is secured.

Table A–89 Initialization Blocks and Session Variables

Dimension	SQL	Variable Name
Dim – Cost Center	SELECT DISTINCT 'GL_SEC_COSTCENTER_FILTEREDACCESSLEVELS____PSFT', FIXED_HIER_LEVEL FROM W_COST_CENTER_DH WHERE LEVEL0_SECURITY_ID IN (VALUELISTOF(NQ_SESSION.GL_SEC_COSTCENTER_FILTEREDACCESS____ PSFT)) AND CURRENT_FLG='Y'	GL_SEC_COSTCENTER_FILTEREDACCESSLEVELS____PSFT
Dim – Natural Account	SELECT DISTINCT 'GL_SEC_ACCOUNT_FILTEREDACCESSLEVELS____ PSFT', FIXED_HIER_LEVEL FROM W_NATURAL_ACCOUNT_DH WHERE LEVEL0_SECURITY_ID IN (VALUELISTOF(NQ_SESSION.GL_SEC_ ACCOUNT_FILTEREDACCESS____ PSFT)) AND CURRENT_FLG='Y'	GL_SEC_ACCOUNT_FILTEREDACCESSLEVELS____PSFT
Dim – Balancing Segment	SELECT DISTINCT 'GL_SEC_BALANCING_FILTEREDACCESSLEVELS____ PSFT', FIXED_HIER_LEVEL FROM W_BALANCING_SEGMENT_DH WHERE LEVEL0_SECURITY_ID IN (VALUELISTOF(NQ_SESSION.GL_SEC_ BALANCING_FILTEREDACCESS____ PSFT)) AND CURRENT_FLG='Y'	GL_SEC_BALANCING_FILTEREDACCESSLEVELS____PSFT
Dim – GL Segment<n>	SELECT DISTINCT 'GL_SEC_SEGMENT<n>_FILTEREDACCESSLEVELS___PSFT, FIXED_HIER_LEVEL FROM W_GL_SEGMENT_DH WHERE LEVEL0_SECURITY_ID IN (VALUELISTOF(NQ_SESSION.GL_SEC_SEGMENT<n>_FILTEREDACCESS____ PSFT)) AND CURRENT_FLG='Y'	GL_SEC_SEGMENT<n>_FILTEREDACCESSLEVELS____PSFT

Connection Pool: "Oracle Data Warehouse"."Oracle Data Warehouse Repository Initblocks Connection Pool"

Notes:

- The 2nd highlighted variable name in the SQL comes from the variable names defined in Step 1. Make sure you use the same names.

- Use the default value for these variables as 0.

- All the variables created above should end with ____PSFT (4 '_' followed by the string PSFT). This is for multi source implementation where the same variable can be initialized using multiple SQL statements for multiple source systems.

3. Create a 'row wise' session initialization block and a corresponding session variable to get all the SETIDs to which user has partial access for a given segment. Use the SQL queries and session variable names as given in the table below depending on the dimension that is secured.

Table A–90 Initialization Blocks and Session Variables

Dimension	SQL	Variable Name

Dim – Cost Center	SELECT DISTINCT 'GL_SEC_COSTCENTER_FILTEREDACCESSVALUESETS____PSFT', 'Department' || '~' || DEFN.SETID FROM PS_KSEC_RULES RULES, PS_KSEC_RULES_DEFN DEFN, PS_KSEC_RULES_EVEN EVENTS, PS_KSEC_OPR_RULES OPR WHERE OPR.KSEC_RULE=EVENTS.KSEC_RULE AND EVENTS.KSEC_RULE=RULES.KSEC_RULE AND RULES.KSEC_RULE=DEFN.KSEC_RULE AND EVENTS.KSEC_EVENT='INQUIRE' AND RULES.KSEC_ATTRIB='A' AND DEFN.KSEC_RULE_PARAM='TRE' AND DEFN.CHARTFIELD='DEPTID' AND OPR.OPRID = 'VALUEOF(NQ_SESSION.USER)'
	UNION
	SELECT DISTINCT 'GL_SEC_COSTCENTER_FILTEREDACCESSVALUESETS____PSFT', 'Department' || '~' || DEFN.SETID FROM PS_KSEC_RULES RULES, PS_KSEC_RULES_DEFN DEFN,PS_KSEC_RULES_EVEN EVENTS, PS_KSEC_CLSS_RULES CLSS, PSOPRDEFN OP, PSROLEUSER ORL, PSROLECLASS RCL WHERE CLSS.OPRCLASS = RCL.CLASSID AND OP.OPRID = ORL.ROLEUSER AND ORL.ROLENAME = RCL.ROLENAME AND CLSS.KSEC_RULE=EVENTS.KSEC_RULE AND EVENTS.KSEC_RULE=RULES.KSEC_RULE AND RULES.KSEC_RULE=DEFN.KSEC_RULE AND EVENTS.KSEC_EVENT='INQUIRE' AND RULES.KSEC_ATTRIB='A' AND DEFN.KSEC_RULE_PARAM='TRE' AND DEFN.CHARTFIELD='DEPTID' AND OP.OPRID = 'VALUEOF(NQ_SESSION.USER)'
		GL_SEC_COSTCENTER_FILTEREDACCESSVALUESETS____PSFT

Table A–90 (Cont.) Initialization Blocks and Session Variables

Dimension	SQL	Variable Name

Dim – Natural Account	SELECT DISTINCT 'GL_SEC_ACCOUNT_FILTEREDACCESSVALUESETS____PSFT', 'Account'||'~'||DEFN.SETID FROM PS_KSEC_RULES RULES, PS_KSEC_RULES_DEFN DEFN, PS_KSEC_RULES_EVEN EVENTS, PS_KSEC_OPR_RULES OPR WHERE OPR.KSEC_RULE=EVENTS.KSEC_RULE AND EVENTS.KSEC_RULE=RULES.KSEC_RULE AND RULES.KSEC_RULE=DEFN.KSEC_RULE AND EVENTS.KSEC_EVENT='INQUIRE' AND RULES.KSEC_ATTRIB='A' AND DEFN.KSEC_RULE_PARAM='TRE' AND DEFN.CHARTFIELD='ACCOUNT' AND OPR.OPRID = 'VALUEOF(NQ_SESSION.USER)'
	UNION
	SELECT DISTINCT 'GL_SEC_ACCOUNT_FILTEREDACCESSVALUESETS____PSFT', 'Account'||'~'||DEFN.SETID FROM PS_KSEC_RULES RULES, PS_KSEC_RULES_DEFN DEFN,PS_KSEC_RULES_EVEN EVENTS, PS_KSEC_CLSS_RULES CLSS, PSOPRDEFN OP, PSROLEUSER ORL, PSROLECLASS RCL WHERE CLSS.OPRCLASS = RCL.CLASSID AND OP.OPRID = ORL.ROLEUSER AND ORL.ROLENAME = RCL.ROLENAME AND CLSS.KSEC_RULE=EVENTS.KSEC_RULE AND EVENTS.KSEC_RULE=RULES.KSEC_RULE AND RULES.KSEC_RULE=DEFN.KSEC_RULE AND EVENTS.KSEC_EVENT='INQUIRE' AND RULES.KSEC_ATTRIB='A' AND DEFN.KSEC_RULE_PARAM='TRE' AND DEFN.CHARTFIELD='ACCOUNT' AND OP.OPRID = 'VALUEOF(NQ_SESSION.USER)'
		GL_SEC_ACCOUNT_FILTEREDACCESSVALUESETS____PSFT

Table A–90 (Cont.) Initialization Blocks and Session Variables

Dimension	SQL	Variable Name

Dim – Balancing Segment	SELECT DISTINCT 'GL_SEC_BALANCING_FILTEREDACCESSVALUESETS____PSFT', 'Fund Code'||'~'||DEFN.SETID FROM PS_KSEC_RULES RULES, PS_KSEC_RULES_DEFN DEFN, PS_KSEC_RULES_EVEN EVENTS, PS_KSEC_OPR_RULES OPR WHERE OPR.KSEC_RULE=EVENTS.KSEC_RULE AND EVENTS.KSEC_RULE=RULES.KSEC_RULE AND RULES.KSEC_RULE=DEFN.KSEC_RULE AND EVENTS.KSEC_EVENT='INQUIRE' AND RULES.KSEC_ATTRIB='A' AND DEFN.KSEC_RULE_PARAM='TRE' AND DEFN.CHARTFIELD='FUND_CODE' AND OPR.OPRID = 'VALUEOF(NQ_SESSION.USER)'
	UNION
	SELECT DISTINCT 'GL_SEC_BALANCING_FILTEREDACCESSVALUESETS____PSFT', 'Fund Code'||'~'||DEFN.SETID FROM PS_KSEC_RULES RULES, PS_KSEC_RULES_DEFN DEFN,PS_KSEC_RULES_EVEN EVENTS, PS_KSEC_CLSS_RULES CLSS, PSOPRDEFN OP, PSROLEUSER ORL, PSROLECLASS RCL WHERE CLSS.OPRCLASS = RCL.CLASSID AND OP.OPRID = ORL.ROLEUSER AND ORL.ROLENAME = RCL.ROLENAME AND CLSS.KSEC_RULE=EVENTS.KSEC_RULE AND EVENTS.KSEC_RULE=RULES.KSEC_RULE AND RULES.KSEC_RULE=DEFN.KSEC_RULE AND EVENTS.KSEC_EVENT='INQUIRE' AND RULES.KSEC_ATTRIB='A' AND DEFN.KSEC_RULE_PARAM='TRE' AND DEFN.CHARTFIELD='FUND_CODE' AND OP.OPRID = 'VALUEOF(NQ_SESSION.USER)'
		GL_SEC_BALANCING_FILTEREDACCESSVALUESETS____PSFT

Table A–90 (Cont.) Initialization Blocks and Session Variables

Dimension	SQL	Variable Name

Dim – GL Segment<n>	SELECT DISTINCT 'GL_SEC_SEGMENT<n>_FILTEREDACCESSVALUESETS____PSFT', '<ChartfieldString>'||'~'||DEFN.SETID FROM PS_KSEC_RULES RULES, PS_KSEC_RULES_DEFN DEFN, PS_KSEC_RULES_EVEN EVENTS, PS_KSEC_OPR_RULES OPR WHERE OPR.KSEC_RULE=EVENTS.KSEC_RULE AND EVENTS.KSEC_RULE=RULES.KSEC_RULE AND RULES.KSEC_RULE=DEFN.KSEC_RULE AND EVENTS.KSEC_EVENT='INQUIRE' AND RULES.KSEC_ATTRIB='A' AND DEFN.KSEC_RULE_PARAM='TRE' AND DEFN.CHARTFIELD='<ChartfieldCode>' AND OPR.OPRID = 'VALUEOF(NQ_SESSION.USER)'
	UNION
	SELECT DISTINCT 'GL_SEC_SEGMENT<n>_FILTEREDACCESSVALUESETS____PSFT', '<ChartfieldString>'||'~'||DEFN.SETID FROM PS_KSEC_RULES RULES, PS_KSEC_RULES_DEFN DEFN,PS_KSEC_RULES_EVEN EVENTS, PS_KSEC_CLSS_RULES CLSS, PSOPRDEFN OP, PSROLEUSER ORL, PSROLECLASS RCL WHERE CLSS.OPRCLASS = RCL.CLASSID AND OP.OPRID = ORL.ROLEUSER AND ORL.ROLENAME = RCL.ROLENAME AND CLSS.KSEC_RULE=EVENTS.KSEC_RULE AND EVENTS.KSEC_RULE=RULES.KSEC_RULE AND RULES.KSEC_RULE=DEFN.KSEC_RULE AND EVENTS.KSEC_EVENT='INQUIRE' AND RULES.KSEC_ATTRIB='A' AND DEFN.KSEC_RULE_PARAM='TRE' AND DEFN.CHARTFIELD='<ChartfieldCode>' AND OP.OPRID = 'VALUEOF(NQ_SESSION.USER)'
		GL_SEC_SEGMENT<n>_FILTEREDACCESSVALUESETS____PSFT

Connection Pool: "PeopleSoft OLTP"."PeopleSoft OLTP DbAuth Connection Pool"

Notes:

- For the Dim – GL Segment<n> init blocks, use the appropriate chartfield string and the chartfield code based on the chartfield you are securing. You can get the chartfield code from the PeopleSoft source system and the chartfield string should match the names used in file_glacct_segment_config_psft.csv file.

- Use the default value for these variables as 'Default'.

- All the variables created above should end with ____PSFT (4 '_' followed by the string PSFT). This is for multi source implementation where the same variable can be initialized using multiple SQL statements for multiple source systems.

4. Create a 'row wise' session initialization block and a corresponding session variable to get all the SETIDs to which user has full access for a given chartfield. Use the SQL queries and session variable names as given in the table below depending on the dimension that is secured.

Table A–91 Initialization Blocks and Session Variables

Dimension	SQL	Variable Name
Dim – Cost Center	SELECT DISTINCT 'GL_SEC_COSTCENTER_FULLACCESS____PSFT', COST_CENTER_LOV_ID, FROM W_COST_CENTER_D WHERE COST_CENTER_LOV_ID NOT IN VALUELISTOF(NQ_SESSION.GL_SEC_COSTCENTER_FILTEREDACCESSVALUESETS____PSFT)	GL_SEC_COSTCENTER_FULLACCESS____PSFT
Dim – Natural Account	SELECT DISTINCT 'GL_SEC_ACCOUNT_FULLACCESS____PSFT', NATURAL_ACCOUNT_LOV_ID, FROM W_ NATURAL_ACCOUNT _D WHERE NATURAL_ACCOUNT_LOV_ID NOT IN VALUELISTOF(NQ_SESSION.GL_SEC_ACCOUNT_FILTEREDACCESSVALUESETS____PSFT)	GL_SEC_ACCOUNT_FULLACCESS____PSFT
Dim – Balancing Segment	SELECT DISTINCT 'GL_SEC_BALANCING_FULLACCESS____PSFT', BALANCING_SEGMENT_LOV_ID, FROM W_ BALANCING_SEGMENT_D WHERE BALANCING_SEGMENT _LOV_ID NOT IN VALUELISTOF(NQ_SESSION.GL_SEC_BALANCING_FILTEREDACCESSVALUESETS____PSFT)	GL_SEC_BALANCING_FULLACCESS TS____PSFT
Dim – GL Segment<n>	SELECT DISTINCT 'GL_SEC_SEGMENT<n>_FULLACCESS____PSFT', SEGMENT_LOV_I FROM, W_GL_SEGMENT_D WHERE SEGMENT_LOV_ID NOT IN VALUELISTOF(NQ_SESSION.GL_SEC_SEGMENT<n>_FILTEREDACCESSVALUESETS____PSFT) AND SEGMENT_LOV_ID LIKE '<ChartfieldString>%'	GL_SEC_SEGMENT<n>_FULLACCESS____PSFT

Connection Pool: "Oracle Data Warehouse"."Oracle Data Warehouse Repository Initblocks Connection Pool"

Notes:

- For the generic GL Segment dimensions, Dim – GL Segment 1 - 10, you will need to apply an appropriate filter to filter the SETIDs applicable for that chartfield. You can apply a filter on the chartfield string column which should be exactly similar to the one name used in file_glacct_segment_config_psft.csv file.

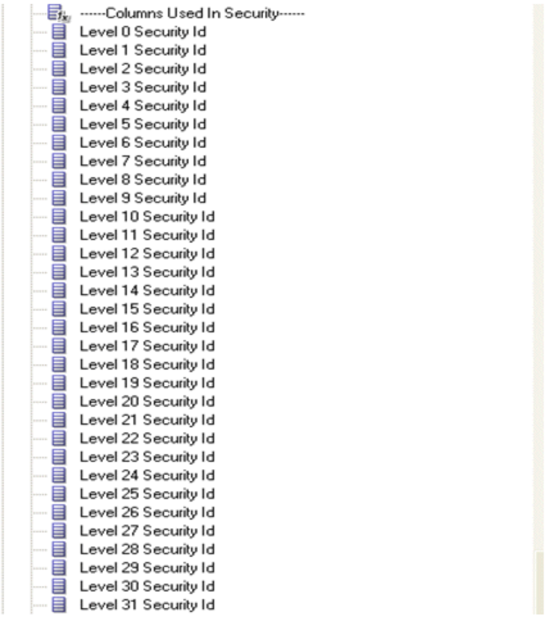
- The 2nd highlighted variable name in the SQL comes from the variable names defined in Step 3. Make sure you use the same names.

- Use the default value for these variables as 'Default'.

- All the variables created above should end with ____PSFT (4 '_' followed by the string PSFT). This is for multi source implementation where the same variable can be initialized using multiple SQL's for multiple source systems.

Security Id Expression in the logical dimensions

1. Each dimension has 32 security columns Level 0 Security Id through Level 31 Security Id as shown below. The expression for each of these logical columns need to be modified using the hierarchy level variable created above.



------Columns Used In Security------
Level 0 Security Id
Level 1 Security Id
Level 2 Security Id
Level 3 Security Id
Level 4 Security Id
Level 5 Security Id
Level 6 Security Id
Level 7 Security Id
Level 8 Security Id
Level 9 Security Id
Level 10 Security Id
Level 11 Security Id
Level 12 Security Id
Level 13 Security Id
Level 14 Security Id
Level 15 Security Id
Level 16 Security Id
Level 17 Security Id
Level 18 Security Id
Level 19 Security Id
Level 20 Security Id
Level 21 Security Id
Level 22 Security Id
Level 23 Security Id
Level 24 Security Id
Level 25 Security Id
Level 26 Security Id
Level 27 Security Id
Level 28 Security Id
Level 29 Security Id
Level 30 Security Id
Level 31 Security Id

2. Open the logical table source of the dimension that maps to the warehouse dimension table and set the expression for each of these columns using the example from 'Dim – Cost Center' dimension. For example, if you are securing by 'Dim – GL Segment3' and the hierarchy level variable for this segment is 'GL_SEC_SEGMENT3_FILTEREDACCESSLEVELS', then you would set the expression for each of the 'Level <n> Security Id' column with the following:

```
INDEXCOL( IFNULL( VALUEOF(<n>, NQ_SESSION."GL_SEC_PROGRAM_
FILTEREDACCESSLEVELS"),  VALUEOF(0, NQ_SESSION."GL_SEC_SEGMENT3_
FILTEREDACCESSLEVELS")),
"Oracle Data Warehouse"."Catalog"."dbo"."Dim_W_GL_SEGMENT_DH_Security_
Segment3"."LEVEL31_SECURITY_ID",
"Oracle Data Warehouse"."Catalog"."dbo"."Dim_W_GL_SEGMENT_DH_Security_
Segment3"."LEVEL30_SECURITY_ID",
"Oracle Data Warehouse"."Catalog"."dbo"."Dim_W_GL_SEGMENT_DH_Security_
Segment3"."LEVEL29_SECURITY_ID",
…and so on for each security id column…
"Oracle Data Warehouse"."Catalog"."dbo"."Dim_W_GL_SEGMENT_DH_Security_
Segment3"."LEVEL1_SECURITY_ID",
"Oracle Data Warehouse"."Catalog"."dbo"."Dim_W_GL_SEGMENT_DH_Security_
Segment3"."LEVEL0_SECURITY_ID")
```

3. Repeat the above steps for each of the segment dimension to be secured.

Security filters in the "Data Security" application roles

Do the following:

1. Navigate to 'Manage –> Identity' from the menu, open the 'General Ledger Data Security' application role and navigate to 'Permissions -> Data Filters'. For each of

the logical facts secured under this role, you will see some existing filters, which are handling ledger security. You will need to append the segment security filters to this with an 'AND' condition. A snippet of the segment security filters to be appended for a given segment dimension is given below, assuming the security is on 'Dim – GL Segment3' and the session variable prefix used in the previous steps was 'GL_SEC_SEGMENT3'.

```
(
"Core"."Dim - GL Segment3"."Segment Value Set Code" IS NULL OR
((
"Core"."Dim - GL Segment3"."Segment Value Set Code" = VALUEOF(NQ_SESSION."GL_
SEC_SEGMENT3_FULLACCESS") OR
"Core"."Dim - GL Segment3"."Level 0 Security Id"    = VALUEOF(NQ_SESSION."GL_
SEC_SEGMENT3_FILTEREDACCESS") OR
"Core"."Dim - GL Segment3"."Level 1 Security Id"    = VALUEOF(NQ_SESSION."GL_
SEC_SEGMENT3_FILTEREDACCESS") OR
"Core"."Dim - GL Segment3"."Level 2 Security Id"    = VALUEOF(NQ_SESSION."GL_
SEC_SEGMENT3_FILTEREDACCESS") OR
...and so on for each security id column...
"Core"."Dim - GL Segment3"."Level 30 Security Id"   = VALUEOF(NQ_SESSION."GL_
SEC_SEGMENT3_FILTEREDACCESS") OR
"Core"."Dim - GL Segment3"."Level 31 Security Id"   = VALUEOF(NQ_SESSION."GL_
SEC_SEGMENT3_FILTEREDACCESS")
)
AND
"Core"."Dim - GL Segment3"."Current Flag Security" = 'Y')
)
```

2. Repeat the above for each segment dimension that is secured using appropriate variable names for each segment and appending each block of filters with an AND. For example, if you are securing by cost center and segment3 dimensions, the filter will look like this, which includes the ledger security:

```
/* Ledger  security filters */
 (
"Core"."Dim - Ledger"."Key Id" = VALUEOF(NQ_SESSION."LEDGER")
)
/* cost center segment security filters */
AND
 (
"Core"."Dim - Cost Center"."Cost Center Value Set Code" IS NULL OR
((
"Core"."Dim - Cost Center"."Cost Center Value Set Code" = VALUEOF(NQ_
SESSION."GL_SEC_COST_CENTER_FULLACCESS") OR
"Core"."Dim - Cost Center"."Cost Center Level 0 Security Id"    = VALUEOF(NQ_
SESSION." GL_SEC_COST_CENTER_FILTEREDACCESS") OR
"Core"."Dim - Cost Center"."Cost Center Level 1 Security Id"    = VALUEOF(NQ_
SESSION." GL_SEC_COST_CENTER_FILTEREDACCESS") OR
"Core"."Dim - Cost Center"."Cost Center Level 2 Security Id"    = VALUEOF(NQ_
SESSION." GL_SEC_COST_CENTER_FILTEREDACCESS") OR
...and so on for each security id column...
"Core"."Dim - Cost Center"."Cost Center Level 30 Security Id"   = VALUEOF(NQ_
SESSION." GL_SEC_COST_CENTER_FILTEREDACCESS") OR
"Core"."Dim - Cost Center"."Cost Center Level 31 Security Id"   = VALUEOF(NQ_
SESSION." GL_SEC_COST_CENTER_FILTEREDACCESS")
)
AND
"Core"."Dim - Cost Center"."Current Flag Security" = 'Y')
)
/* segment3 security filters */
AND
```

```
 (
"Core"."Dim - GL Segment3"."Segment Value Set Code" IS NULL OR
((
"Core"."Dim - GL Segment3"."Segment Value Set Code" = VALUEOF(NQ_SESSION."GL_
SEC_SEGMENT3_FULLACCESS") OR
"Core"."Dim - GL Segment3"."Level 0 Security Id"    = VALUEOF(NQ_SESSION."GL_
SEC_SEGMENT3_FILTEREDACCESS") OR
"Core"."Dim - GL Segment3"."Level 1 Security Id"    = VALUEOF(NQ_SESSION."GL_
SEC_SEGMENT3_FILTERE+CESS") OR
"Core"."Dim - GL Segment3"."Level 2 Security Id"    = VALUEOF(NQ_SESSION."GL_
SEC_SEGMENT3_FILTEREDACCESS") OR
...and so on for each security id column...
"Core"."Dim - GL Segment3"."Level 30 Security Id"   = VALUEOF(NQ_SESSION."GL_
SEC_SEGMENT3_FILTEREDACCESS") OR
"Core"."Dim - GL Segment3"."Level 31 Security Id"   = VALUEOF(NQ_SESSION."GL_
SEC_SEGMENT3_FILTEREDACCESS")
)
AND
"Core"."Dim - GL Segment3"."Current Flag Security" = 'Y')
)
```

Note: When a tree has more than one version, the security filters are always applied on the current version for that tree (CURRENT_FLG='Y'). However you can navigate through any other version of the tree in the reports but security will always be applied on the current version.

A.1.29.4 Configuring BI Duty Roles

The following BI Duty Roles are applicable to the General Ledger subject area.

- Budget Director PSFT
- Budget Analyst PSFT
- Financial Analyst PSFT
- CFO Group PSFT
- Controller Group PSFT

These Duty Roles control the subject areas and dashboard content to which the user has access. These Duty Roles also ensure the data security filters are applied to all the queries. For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

Note: These roles will have access to Account Payables, Account Receivables and Fixed Assets data in BI to facilitate the drill down from GL to those modules. However, access to data in the respective modules must be provisioned in the E-Business Suite system for these users in order to use the drill down capabilities.

A.1.30 How to Set Up Project GL Reconcilliation Security for PeopleSoft

Overview

Project Analytics supports security using Ledger dimension in Project GL Recon.

Table A–92 Project Costing and Control Facts

Security Entity	GL Recon Cost Fact	GL Recon Revenue Fact
Project Business Unit	N	N

Table A–92 (Cont.) Project Costing and Control Facts

Security Entity	GL Recon Cost Fact	GL Recon Revenue Fact
Project Organization	N	N
Expenditure Business Unit	N	N
Contract Business Unit	N	N
Project	N	N
Resource Organization	N	N
Ledger	Y	Y

Configuring PROJECT GL RECON FOR PeopleSoft

In order for data security filters to be applied, appropriate initialization blocks need to be enabled depending on the deployed source system.

> **Note:** On installation, initialization blocks are enabled for E-Business Suite R12. If you are deploying on a source system other than E-Business Suite R12, then you must enable the appropriate initialization blocks.

Enable data security for Project GL Reconciliation for PeopleSoft by enabling PeopleSoft data security initialization block listed below. If only one source system is deployed, then you must make sure that all Project Security initialization blocks for other adapters are disabled. If more than one source system is deployed, then you must also enable the initialization blocks of those source systems.

Init Blocks

PeopleSoft: Project GL Recon Ledger List PSFT

To Set Up Project GL Reconcilliation Security for PeopleSoft

1. In Oracle BI Administration Tool, edit the BI metadata repository (for example, OracleBIAnalyticsApps.rpd) in online mode, and select Manage, then Identity, then Application Roles.
2. Double click on OBIA_PROJECT_LEDGER_DATA_SECURITY, navigate to Permissions, then Data Filters, and enable all data security filters.
3. Save the metadata repository.

A.1.30.1 Configuring BI Duty Roles

The following BI Duty Roles are applicable to the Project GL Recon subject area.

- OBIA_PSFT_PROJECT_EXECUTIVE_ANALYSIS_DUTY
- OBIA_PSFT_PROJECT_MANAGEMENT_ANALYSIS_DUTY
- OBIA_PSFT_PROJECT_DATA_SECURITY

These Duty Roles control the subject areas and dashboard content to which the user has access. These Duty Roles also ensure the data security filters are applied to all the queries. For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

A.1.31 How to Set Up General Ledger Security for E-Business Suite

Overview

Financial Analytics supports a combination of the following security mechanisms for GL subject areas:

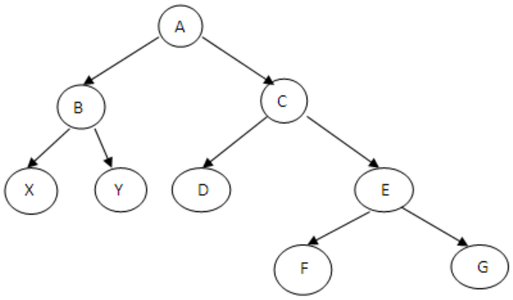
- Security using Ledgers
- Security using GL Accounting Segments

This section gives an overview of the segment security using GL Accounting Segments and supported scenarios in BI Applications.

One or more value sets are used to define the accounting segments in your OLTP. A user can have two different types of access for each value set:

- Partial Access - The user has access to specific nodes within a value set. If the value set has hierarchical relationships defined between nodes, access to the user can be granted using the 'include' access type to a given node. This allows the user to access that node and all its child nodes.

  For example, if a user is granted access to node C, then the user has access to nodes C, D, E, F and G.

  Note: Oracle BI Applications does not support security rules that are set up using the 'exclude' access type in Oracle E-Business Suite.

- Full Access – The user has complete access to all the value set.

A.1.31.1 Configuring Ledger Security

In order for data security filters to be applied, appropriate initialization blocks need to be enabled depending on the deployed source system. To enable Ledger Security for PeopleSoft, enable PeopleSoft initialization block and make sure the initialization blocks of all other source systems are disabled. The initialization block names relevant to various source systems are given below. If more than one source system is deployed, then you must also enable the initialization blocks of those source systems.

- E-Business Suite 11i: Ledgers EBS11
- E-Business Suite R12: Ledgers EBS12
- Oracle PeopleSoft: Ledgers PeopleSoft

To enable initialization blocks, follow the steps below:

1. In Oracle BI Administration Tool, edit the BI metadata repository (for example, OracleBIAnalyticsApps.rpd).
2. Choose Manage, then Variables.

3. Under Session – Initialization Blocks, open the initialization block that you need to enable.
4. Clear the **Disabled** check box.
5. Save the metadata repository (RPD file).

A.1.31.2 Configuring GL Segment Security

GL Segment Security can be applied on the qualified GL Segment Dimensions: 'Dim – Cost Center', 'Dim – Natural Account' & 'Dim – Balancing Segment', as well as the 10 generic dimensions 'Dim – GL Segment1 to 'Dim – GL Segment 10' which are configurable to be any of the accounting segments.

Before setting up the security, you need to first identify which of these segment dimensions you need to apply security on depending on your security requirements and the security setup in the E-Business Suite system. Once that is determined the following steps to configure the RPD metadata need to be repeated for each of the securing segment dimension.

Initialization Blocks and Session Variables

1. Create a 'row wise' session initialization block and a corresponding session variable to get all the parent nodes the user has access to in a tree. Use the SQL queries and session variable names as given in the table below depending on the dimension that is secured.

Table A–93 Initialization Blocks and Session Variables

Dimension	SQL	Variable Name
Dim – Cost Center	SELECT DISTINCT 'GL_SEC_COSTCENTER_VALUESETS____EBS', COST_CENTER_LOV_ID FROM W_COST_CENTER_D WHERE ROW_WID > 0	GL_SEC_COSTCENTER_VALUESETS____EBS
Dim – Natural Account	SELECT DISTINCT 'GL_SEC_ACCOUNT_VALUESETS____EBS', NATURAL_ACCOUNT_LOV_ID FROM W_NATURAL_ACCOUNT_D WHERE ROW_WID > 0	GL_SEC_ACCOUNT_VALUESETS____EBS
Dim – Balancing Segment	SELECT DISTINCT 'GL_SEC_BALANCING_VALUESETS____EBS', BALANCING_SEGMENT_LOV_ID FROM W_BALANCING_SEGMENT_D WHERE ROW_WID > 0	GL_SEC_BALANCING_VALUESETS____EBS
Dim – GL Segment<n>	SELECT DISTINCT 'GL_SEC_SEGMENT<n>_VALUESETS____EBS', SEGMENT<n>_ATTRIB FROM W_GLACCT_SEG_CONFIG_TMP	GL_SEC_SEGMENT<n>_VALUESETS____EBS

Connection Pool: "Oracle Data Warehouse"."Oracle Data Warehouse Repository Initblocks Connection Pool"

Notes:

- For the generic GL Segment dimensions, Dim – GL Segment 1 - 10, you will need to select the corresponding segment column from W_GLACCT_SEG_CONFIG_TMP which will have all the value sets corresponding to that segment.

- Use the default value for these variables as 'Default'.

- All the variables created above should end with ____EBS (4 '_' followed by the string EBS). This is for multi source implementation where the same variable can be initialized using multiple SQL's for multiple source systems.

2. Create a 'row wise' session initialization block and a corresponding session variable to get all the parent nodes the user has access to in a value set. Use the SQL queries and session variable names as given in the table below depending on the dimension that is secured.

Table A–94 Initialization Blocks and Session Variables

Dimension	SQL	Variable Name
Dim – Cost Center	select DISTINCT 'GL_SEC_COSTCENTER_FILTEREDACCESS____EBS', TO_CHAR(C.FLEX_VALUE_SET_ID) ||'~'||C.FLEX_VALUE from FND_FLEX_VALUE_RULE_USAGES a, FND_FLEX_VALUE_RULE_LINES B, FND_FLEX_VALUES C where a.FLEX_VALUE_RULE_ID = B.FLEX_VALUE_RULE_ID and a.FLEX_VALUE_SET_ID = B.FLEX_VALUE_SET_ID and B.FLEX_VALUE_SET_ID = C.FLEX_VALUE_SET_ID and C.FLEX_VALUE between B.FLEX_VALUE_LOW and B.FLEX_VALUE_HIGH and B.INCLUDE_EXCLUDE_INDICATOR = 'I' and C.SUMMARY_FLAG = 'Y' and TO_CHAR(a.FLEX_VALUE_SET_ID) = VALUELISTOF(NQ_SESSION.GL_SEC_COSTCENTER_VALUESETS____EBS) and TO_CHAR(a.RESPONSIBILITY_ID) = VALUELISTOF(NQ_SESSION.GL_SEC_EBS_RESP_ID) and a.APPLICATION_ID = 101	GL_SEC_COSTCENTER_FILTEREDACCESS____EBS
Dim – Natural Account	select DISTINCT 'GL_SEC_ACCOUNT_FILTEREDACCESS____EBS', TO_CHAR(C.FLEX_VALUE_SET_ID) ||'~'||C.FLEX_VALUE from FND_FLEX_VALUE_RULE_USAGES a, FND_FLEX_VALUE_RULE_LINES B, FND_FLEX_VALUES C where a.FLEX_VALUE_RULE_ID = B.FLEX_VALUE_RULE_ID and a.FLEX_VALUE_SET_ID = B.FLEX_VALUE_SET_ID and B.FLEX_VALUE_SET_ID = C.FLEX_VALUE_SET_ID and C.FLEX_VALUE between B.FLEX_VALUE_LOW and B.FLEX_VALUE_HIGH and B.INCLUDE_EXCLUDE_INDICATOR = 'I' and C.SUMMARY_FLAG = 'Y' and TO_CHAR(a.FLEX_VALUE_SET_ID) = VALUELISTOF(NQ_SESSION.GL_SEC_ACCOUNT_VALUESETS____EBS) and TO_CHAR(a.RESPONSIBILITY_ID) = VALUELISTOF(NQ_SESSION.GL_SEC_EBS_RESP_ID) and a.APPLICATION_ID = 101	GL_SEC_ACCOUNT_FILTEREDACCESS____EBS

Table A–94 (Cont.) Initialization Blocks and Session Variables

Dimension	SQL	Variable Name
Dim – Balancing Segment	select DISTINCT 'GL_SEC_BALANCING_FILTEREDACCESS____EBS', TO_CHAR(C.FLEX_VALUE_SET_ID) ||'~'||C.FLEX_VALUE from FND_FLEX_VALUE_RULE_USAGES a, FND_FLEX_VALUE_RULE_LINES B, FND_FLEX_VALUES C where a.FLEX_VALUE_RULE_ID = B.FLEX_VALUE_RULE_ID and a.FLEX_VALUE_SET_ID = B.FLEX_VALUE_SET_ID and B.FLEX_VALUE_SET_ID = C.FLEX_VALUE_SET_ID and C.FLEX_VALUE between B.FLEX_VALUE_LOW and B.FLEX_VALUE_HIGH and B.INCLUDE_EXCLUDE_INDICATOR = 'I' and C.SUMMARY_FLAG = 'Y' and TO_CHAR(a.FLEX_VALUE_SET_ID) = VALUELISTOF(NQ_SESSION.GL_SEC_BALANCING_VALUESETS____EBS) and TO_CHAR(a.RESPONSIBILITY_ID) = VALUELISTOF(NQ_SESSION.GL_SEC_EBS_RESP_ID) and a.APPLICATION_ID = 101	GL_SEC_BALANCING_FILTEREDACCESS____EBS
Dim – GL Segment<n>	select DISTINCT 'GL_SEC_SEGMENT<n>_FILTEREDACCESS____EBS', TO_CHAR(C.FLEX_VALUE_SET_ID) ||'~'||C.FLEX_VALUE from FND_FLEX_VALUE_RULE_USAGES a, FND_FLEX_VALUE_RULE_LINES B, FND_FLEX_VALUES C where a.FLEX_VALUE_RULE_ID = B.FLEX_VALUE_RULE_ID and a.FLEX_VALUE_SET_ID = B.FLEX_VALUE_SET_ID and B.FLEX_VALUE_SET_ID = C.FLEX_VALUE_SET_ID and C.FLEX_VALUE between B.FLEX_VALUE_LOW and B.FLEX_VALUE_HIGH and B.INCLUDE_EXCLUDE_INDICATOR = 'I' and C.SUMMARY_FLAG = 'Y' and TO_CHAR(a.FLEX_VALUE_SET_ID) = VALUELISTOF(NQ_SESSION.GL_SEC_SEGMENT<n>_VALUESETS____EBS) and TO_CHAR(a.RESPONSIBILITY_ID) = VALUELISTOF(NQ_SESSION.GL_SEC_EBS_RESP_ID) and a.APPLICATION_ID = 101	GL_SEC_SEGMENT<n>_FILTEREDACCESS____EBS

Connection Pool: "Oracle EBS OLTP"."Oracle EBS OLTP DbAuth Connection Pool"

Notes:

- The 2nd highlighted variable name in the SQL comes from the variable names defined in Step 1. Make sure you use the same names.

- Use the default value for these variables as 'Default'

- All the variables created above should end with ____EBS (4 '_' followed by the string EBS). This is for multi source implementation where the same variable can be initialized using multiple SQL's for multiple source systems.

3. Create a 'row wise' session initialization block and a corresponding session variable to get the level in the hierarchy the above nodes fall in a hierarchical value set. Use the SQL queries and session variable names as given in the table below depending on the dimension that is secured.

Table A–95 Initialization Blocks and Session Variables

Dimension	SQL	Variable Name
Dim – Cost Center	SELECT DISTINCT 'GL_SEC_COSTCENTER_FILTEREDACCESSLEVELS____EBS', FIXED_HIER_LEVEL FROM W_COST_CENTER_DH WHERE LEVEL0_SECURITY_ID IN (VALUELISTOF(NQ_SESSION.GL_SEC_COSTCENTER_FILTEREDACCESS____EBS)) AND CURRENT_FLG='Y'	GL_SEC_COSTCENTER_FILTEREDACCESSLEVELS____EBS
Dim – Natural Account	SELECT DISTINCT 'GL_SEC_ACCOUNT_FILTEREDACCESSLEVELS____EBS', FIXED_HIER_LEVEL FROM W_NATURAL_ACCOUNT_DH WHERE LEVEL0_SECURITY_ID IN (VALUELISTOF(NQ_SESSION.GL_SEC_ ACCOUNT_FILTEREDACCESS____EBS)) AND CURRENT_FLG='Y'	GL_SEC_ACCOUNT_FILTEREDACCESSLEVELS____EBS
Dim – Balancing Segment	SELECT DISTINCT 'GL_SEC_BALANCING_FILTEREDACCESSLEVELS____EBS', FIXED_HIER_LEVEL FROM W_BALANCING_SEGMENT_DH WHERE LEVEL0_SECURITY_ID IN (VALUELISTOF(NQ_SESSION.GL_SEC_ BALANCING_FILTEREDACCESS____EBS)) AND CURRENT_FLG='Y'	GL_SEC_BALANCING_FILTEREDACCESSLEVELS____EBS
Dim – GL Segment<n>	SELECT DISTINCT 'GL_SEC_SEGMENT<n>_FILTEREDACCESSLEVELS____EBS', FIXED_HIER_LEVEL FROM W_GL_SEGMENT_DH WHERE LEVEL0_SECURITY_ID IN (VALUELISTOF(NQ_SESSION.GL_SEC_SEGMENT<n>_FILTEREDACCESS____EBS)) AND CURRENT_FLG='Y'	GL_SEC_SEGMENT<n>_FILTEREDACCESSLEVELS____EBS

Connection Pool: "Oracle Data Warehouse"."Oracle Data Warehouse Repository Initblocks Connection Pool"

Notes:

- The 2nd highlighted variable name in the SQL comes from the variable names defined in Step 2. Make sure you use the same names.

- Use the default value for these variables as 0.

- All the variables created above should end with ____EBS (4 '_' followed by the string EBS). This is for multi source implementation where the same variable can be initialized using multiple SQL's for multiple source systems.

4. Create a 'row wise' session initialization block and a corresponding session variable to get all the value sets to which user has partial access for a given

segment. Use the SQL queries and session variable names as given in the table below depending on the dimension that is secured.

Table A–96 Initialization Blocks and Session Variables

Dimension	SQL	Variable Name
Dim – Cost Center	select DISTINCT 'GL_SEC_COSTCENTER_FILTEREDACCESSVALUESETS____EBS', TO_CHAR(A.FLEX_VALUE_SET_ID) FROM FND_FLEX_VALUE_RULE_USAGES A WHERE TO_CHAR(A.FLEX_VALUE_SET_ID) = VALUELISTOF(NQ_SESSION.GL_SEC_COSTCENTER_VALUESETS____EBS) AND TO_CHAR(A.RESPONSIBILITY_ID) = VALUELISTOF(GL_SEC_EBS_RESP_ID)AND A.APPLICATION_ID = 101	GL_SEC_COSTCENTER_FILTEREDACCESSVALUESETS____EBS
Dim – Natural Account	select DISTINCT 'GL_SEC_ACCOUNT_FILTEREDACCESSVALUESETS____EBS', TO_CHAR(A.FLEX_VALUE_SET_ID) FROM FND_FLEX_VALUE_RULE_USAGES A WHERE TO_CHAR(A.FLEX_VALUE_SET_ID) = VALUELISTOF(NQ_SESSION.GL_SEC_ACCOUNT_VALUESETS____EBS) AND TO_CHAR(A.RESPONSIBILITY_ID) = VALUELISTOF(GL_SEC_EBS_RESP_ID)AND A.APPLICATION_ID = 101	GL_SEC_ACCOUNT_FILTEREDACCESSVALUESETS____EBS
Dim – Balancing Segment	select DISTINCT 'GL_SEC_BALANCING_FILTEREDACCESSVALUESETS____EBS', TO_CHAR(A.FLEX_VALUE_SET_ID) FROM FND_FLEX_VALUE_RULE_USAGES A WHERE TO_CHAR(A.FLEX_VALUE_SET_ID) = VALUELISTOF(NQ_SESSION.GL_SEC_BALANCING_VALUESETS____EBS) AND TO_CHAR(A.RESPONSIBILITY_ID) = VALUELISTOF(GL_SEC_EBS_RESP_ID)AND A.APPLICATION_ID = 101	GL_SEC_BALANCING_FILTEREDACCESSVALUESETS____EBS
Dim – GL Segment<n>	select DISTINCT 'GL_SEC_SEGMENT<n>_FILTEREDACCESSVALUESETS____EBS', TO_CHAR(A.FLEX_VALUE_SET_ID) FROM FND_FLEX_VALUE_RULE_USAGES A WHERE TO_CHAR(A.FLEX_VALUE_SET_ID) = VALUELISTOF(NQ_SESSION.GL_SEC_SEGMENT<n>_VALUESETS____EBS) AND TO_CHAR(A.RESPONSIBILITY_ID) = VALUELISTOF(GL_SEC_EBS_RESP_ID)AND A.APPLICATION_ID = 101	GL_SEC_SEGMENT<n>_FILTEREDACCESSVALUESETS____EBS

Connection Pool: "Oracle EBS OLTP"."Oracle EBS OLTP DbAuth Connection Pool"

Notes:

- The 2nd highlighted variable name in the SQL comes from the variable names defined in Step 1. Make sure you use the same names.

- Use the default value for these variables as 'Default'.

- All the variables created above should end with ____EBS (4 '_' followed by the string EBS). This is for multi source implementation where the same variable can be initialized using multiple SQL's for multiple source systems.

Table A–97 Initialization Blocks and Session Variables

Dimension	SQL	Variable Name
Dim – Cost Center	SELECT DISTINCT 'GL_SEC_ COSTCENTER_FULLACCESS____EBS', COST_CENTER_LOV_ID, FROM W_ COST_CENTER_D WHERE COST_ CENTER_LOV_ID NOT IN VALUELISTOF(NQ_SESSION.GL_SEC_ COSTCENTER_ FILTEREDACCESSVALUESETS____ EBS)	GL_SEC_COSTCENTER_ FULLACCESS____EBS
Dim – Natural Account	SELECT DISTINCT 'GL_SEC_ ACCOUNT_FULLACCESS____EBS', NATURAL_ACCOUNT_LOV_ID, FROM W_ NATURAL_ACCOUNT _D WHERE NATURAL_ACCOUNT_LOV_ ID NOT IN VALUELISTOF(NQ_ SESSION.GL_SEC_ACCOUNT_ FILTEREDACCESSVALUESETS____ EBS)	GL_SEC_ACCOUNT_ FULLACCESS____EBS
Dim – Balancing Segment	SELECT DISTINCT 'GL_SEC_ BALANCING_FULLACCESS____EBS', BALANCING_SEGMENT_LOV_ID, FROM W_ BALANCING_SEGMENT_D WHERE BALANCING_SEGMENT _ LOV_ID NOT IN VALUELISTOF(NQ_ SESSION.GL_SEC_BALANCING_ FILTEREDACCESSVALUESETS____ EBS)	GL_SEC_BALANCING_ FULLACCESS TS____EBS
Dim – GL Segment<n>	SELECT DISTINCT 'GL_SEC_ SEGMENT<n>_FULLACCESS____EBS', SEGMENT<n>_ATTRIB, FROM W_ GLACCT_SEG_CONFIG_TMP WHERE SEGMENT<n>_ATTRIB NOT IN VALUELISTOF(NQ_SESSION.GL_SEC_ SEGMENT<n>_ FILTEREDACCESSVALUESETS____ EBS)	GL_SEC_SEGMENT<n>_ FULLACCESS____EBS

Connection Pool: "Oracle Data Warehouse"."Oracle Data Warehouse Repository Initblocks Connection Pool"

- For the generic GL Segment dimensions, Dim – GL Segment 1 - 10, you will need to select the corresponding segment column from W_GLACCT_SEG_CONFIG_ TMP which will have all the value sets corresponding to that segment.

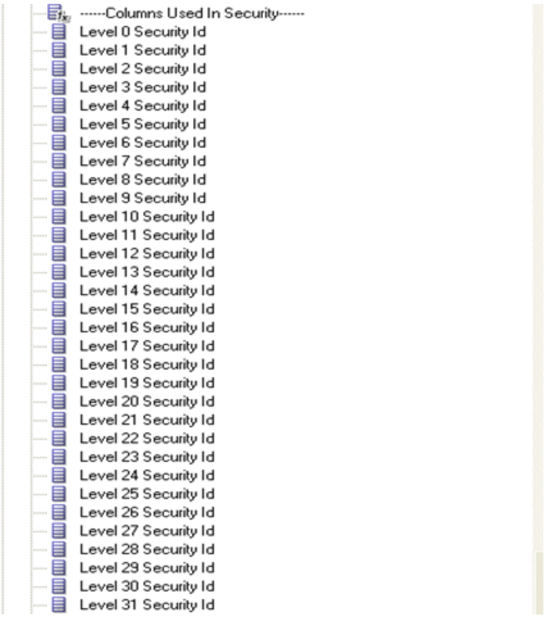
- The 2nd highlighted variable name in the SQL comes from the variable names defined in Step 4. Make sure you use the same names.

- Use the default value for these variables as 'Default'.

- All the variables created above should end with ____EBS (4 '_' followed by the string EBS). This is for multi source implementation where the same variable can be initialized using multiple SQL's for multiple source systems.

Logical Column Expression in the BMM layer

1. Each dimension has 32 security columns Level 0 Security Id through Level 31 Security Id as shown below. The expression for each of these logical columns need to be modified using the hierarchy level variable created above.



------Columns Used In Security------
Level 0 Security Id
Level 1 Security Id
Level 2 Security Id
Level 3 Security Id
Level 4 Security Id
Level 5 Security Id
Level 6 Security Id
Level 7 Security Id
Level 8 Security Id
Level 9 Security Id
Level 10 Security Id
Level 11 Security Id
Level 12 Security Id
Level 13 Security Id
Level 14 Security Id
Level 15 Security Id
Level 16 Security Id
Level 17 Security Id
Level 18 Security Id
Level 19 Security Id
Level 20 Security Id
Level 21 Security Id
Level 22 Security Id
Level 23 Security Id
Level 24 Security Id
Level 25 Security Id
Level 26 Security Id
Level 27 Security Id
Level 28 Security Id
Level 29 Security Id
Level 30 Security Id
Level 31 Security Id

2. Open the logical table source of the dimension that maps to the warehouse dimension table and set the expression for each of these columns using the example from "Dim – Cost Center" dimension.

   For example, if you are securing by "Dim – GL Segment3" and the hierarchy level variable for this segment is "GL_SEC_SEGMENT3_FILTEREDACCESSLEVELS", you would set the expression for each of the "Level <n> Security Id" column with the following:

```
INDEXCOL( IFNULL( VALUEOF(<n>, NQ_SESSION."GL_SEC_SEGMENT3_
FILTEREDACCESSLEVELS"),  VALUEOF(0, NQ_SESSION."GL_SEC_SEGMENT3_
FILTEREDACCESSLEVELS")),
"Oracle Data Warehouse"."Catalog"."dbo"."Dim_W_GL_SEGMENT_DH_Security_
Segment3"."LEVEL31_SECURITY_ID",
"Oracle Data Warehouse"."Catalog"."dbo"."Dim_W_GL_SEGMENT_DH_Security_
Segment3"."LEVEL30_SECURITY_ID",
"Oracle Data Warehouse"."Catalog"."dbo"."Dim_W_GL_SEGMENT_DH_Security_
Segment3"."LEVEL29_SECURITY_ID",
…and so on for each security id column…
"Oracle Data Warehouse"."Catalog"."dbo"."Dim_W_GL_SEGMENT_DH_Security_
Segment3"."LEVEL1_SECURITY_ID",
"Oracle Data Warehouse"."Catalog"."dbo"."Dim_W_GL_SEGMENT_DH_Security_
Segment3"."LEVEL0_SECURITY_ID")
```

Security filters in the "Data Security" application roles

Do the following:

1. Navigate to 'Manage –> Identity' from the menu, open the 'General Ledger Data Security' application role and navigate to 'Permissions -> Data Filters'. For each of the logical facts secured under this role, you will see some existing filters, which are handling ledger security. You will need to append the segment security filters to this with an 'AND' condition. A snippet of the segment security filters to be appended for a given segment dimension is given below, assuming the security is on 'Dim – GL Segment3' and the session variable prefix used in the previous steps was 'GL_SEC_SEGMENT3'.

```
(
"Core"."Dim - GL Segment3"."Segment Value Set Code" IS NULL OR
((
"Core"."Dim - GL Segment3"."Segment Value Set Code" = VALUEOF(NQ_SESSION."GL_
SEC_SEGMENT3_FULLACCESS") OR
"Core"."Dim - GL Segment3"."Level 0 Security Id"    = VALUEOF(NQ_SESSION."GL_
SEC_SEGMENT3_FILTEREDACCESS") OR
"Core"."Dim - GL Segment3"."Level 1 Security Id"    = VALUEOF(NQ_SESSION."GL_
SEC_SEGMENT3_FILTEREDACCESS") OR
"Core"."Dim - GL Segment3"."Level 2 Security Id"    = VALUEOF(NQ_SESSION."GL_
SEC_SEGMENT3_FILTEREDACCESS") OR
...and so on for each security id column...
"Core"."Dim - GL Segment3"."Level 30 Security Id"   = VALUEOF(NQ_SESSION."GL_
SEC_SEGMENT3_FILTEREDACCESS") OR
"Core"."Dim - GL Segment3"."Level 31 Security Id"   = VALUEOF(NQ_SESSION."GL_
SEC_SEGMENT3_FILTEREDACCESS")
)
AND
"Core"."Dim - GL Segment3"."Current Flag Security" = 'Y')
)
```

2. Repeat the above for each segment dimension that is secured using appropriate variable names for each segment and appending each block of filters with an AND. For example, if you are securing by cost center and segment3 dimensions, the filter will look like this, which includes the ledger security:

```
/* Ledger security filters */
(
"Core"."Dim - Ledger"."Key Id" = VALUEOF(NQ_SESSION."LEDGER")
)
/* cost center segment security filters */
AND
 (
"Core"."Dim - Cost Center"."Cost Center Value Set Code" IS NULL OR
((
"Core"."Dim - Cost Center"."Cost Center Value Set Code" = VALUEOF(NQ_
SESSION."GL_SEC_COST_CENTER_FULLACCESS") OR
"Core"."Dim - Cost Center"."Cost Center Level 0 Security Id"    = VALUEOF(NQ_
SESSION."GL_SEC_COST_CENTER _FILTEREDACCESS") OR
"Core"."Dim - Cost Center"."Cost Center Level 1 Security Id"    = VALUEOF(NQ_
SESSION."GL_SEC_COST_CENTER _FILTEREDACCESS") OR
"Core"."Dim - Cost Center"."Cost Center Level 2 Security Id"    = VALUEOF(NQ_
SESSION."GL_SEC_COST_CENTER _FILTEREDACCESS") OR
...and so on for each security id column...
"Core"."Dim - Cost Center"."Cost Center Level 30 Security Id"   = VALUEOF(NQ_
SESSION."GL_SEC_COST_CENTER _FILTEREDACCESS") OR
"Core"."Dim - Cost Center"."Cost Center Level 31 Security Id"   = VALUEOF(NQ_
SESSION."GL_SEC_COST_CENTER _FILTEREDACCESS")
)
AND
"Core"."Dim - Cost Center"."Current Flag Security" = 'Y')
)
/* segment3 security filters */
AND
 (
"Core"."Dim - GL Segment3"."Segment Value Set Code" IS NULL OR
((
"Core"."Dim - GL Segment3"."Segment Value Set Code" = VALUEOF(NQ_SESSION."GL_
SEC_SEGMENT3_FULLACCESS") OR
"Core"."Dim - GL Segment3"."Level 0 Security Id"    = VALUEOF(NQ_SESSION."GL_
SEC_SEGMENT3 _FILTEREDACCESS") OR
"Core"."Dim - GL Segment3"."Level 1 Security Id"    = VALUEOF(NQ_SESSION."GL_
SEC_SEGMENT3_FILTEREDACCESS") OR
"Core"."Dim - GL Segment3"."Level 2 Security Id"    = VALUEOF(NQ_SESSION."GL_
SEC_SEGMENT3_FILTEREDACCESS") OR
...and so on for each security id column...
"Core"."Dim - GL Segment3"."Level 30 Security Id"   = VALUEOF(NQ_SESSION."GL_
SEC_SEGMENT3_FILTEREDACCESS") OR
"Core"."Dim - GL Segment3"."Level 31 Security Id"   = VALUEOF(NQ_SESSION."GL_
SEC_SEGMENT3 _FILTEREDACCESS")
)
AND
"Core"."Dim - GL Segment3"."Current Flag Security" = 'Y')
)
```

Note: When a tree has more than one version, the security filters are always applied on the current version for that tree (CURRENT_FLG='Y'). However you can navigate through any other version of the tree in the reports but security will always be applied on the current version.

A.1.31.3 Configuring BI Duty Roles

The following BI Duty Roles are applicable to the General Ledger subject area.

- Budget Director
- Budget Analyst
- Financial Analyst
- CFO Group
- Controller Group

These Duty Roles control the subject areas and dashboard content to which the user has access. These Duty Roles also ensure the data security filters are applied to all the queries. For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

Note: These roles will have access to Account Payables, Account Receivables and Fixed Assets data in BI to facilitate the drill down from GL to those modules. However, access to data in the respective modules must be provisioned in the E-Business Suite system for these users in order to use the drill down capabilities.

A.1.32 How to Set Up General Ledger Security for Fusion Applications

This topic describes how to implement GL segment security in Oracle BI Applications with a Fusion Applications source system, and contains the following sections:

- Section A.1.32.1, "Introduction"
- Section A.1.32.2, "Configuring GL Segment Security"

A.1.32.1 Introduction

Oracle Financial Analytics supports a combination of the following security mechanisms for GL subject areas:

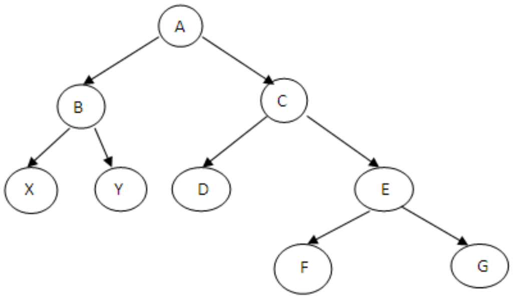
- Security using GL Data Access Sets
- Security using GL Accounting Segments

Data Access Set security is configured during installation and does not require additional configuration. This section gives an overview of the segment security, and describes how to configure security using GL Accounting Segments.

One or more value sets define the accounting segments in your OLTP. You can set up these value sets as a tree value set or non-tree value set. Users can have different types of access for each value set:

- NOACCESS - User has access to none of the values in that value set.
- FULLACCESS - User has access to all the values in that value set.
- FILTEREDACCESS - User has access to specific values in that value set, defined as follows:
  - Tree valueset: If the valueset has a tree, then access to the user can be granted using 'is-descendant of' hierarchical operator. This means that the user has access to that node and all the descendants of that node within that value set.

    For example in the following illustration, if the user is granted 'is-descendant of' node C, then the user has access to nodes C, D, E, F and G.



  - Non-tree valueset: If the valueset does not have a tree, then the user can be granted access to specific node/s or a range of nodes

A.1.32.2 Configuring GL Segment Security

Prior to configuring the segment security in the Oracle BI Repository, you should have completed configuring the segment dimensions in the Oracle BI Repository by mapping the segment VOs to the appropriate logical dimensions using BI Extender. Then perform the following tasks for each of the segment that you are securing. Based on the value sets used for those segments, the segment can be a tree enabled segment or a non-tree segment. The security implementation is different for these cases.

- Section A.1.32.2.1, "Tree Segment Security Implementation"
- Section A.1.32.2.2, "Non-Tree Segment Security Implementation"

A.1.32.2.1 Tree Segment Security Implementation Perform the following steps when the segment on which security to be applied is a tree-based segment.

Task 1 Define Initialization Blocks and Session Variables

1. For tree-based value sets, the data security VO 'FscmTopModelAM.DataSecurityAM.KFFHierFilter1' will give the different access types for the user as mentioned in the previous section. You will need to create a row wise session initialization block which reads from this VO. A sample SQL for this initialization block is as follows.

   ```
   SET variable DISABLE_SQL_BYPASS=1, ApplicationIdBind='101',
   KeyFlexfieldCodeBind='GL#', SegmentLabelCodeBind='FA_COST_CTR': SELECT DISTINCT
   'COST_CENTER_'||AccessType, CASE WHEN AccessType = 'FULLACCESS' THEN
   ValueSetCode ELSE ValueSetCode||'~'||TreeCode||'~'||TreeNodePk1Value END FROM
   "oracle.apps.fscm.model.analytics.applicationModule.FscmTopModelAM_
   FscmTopModelAMLocal"..."FscmTopModelAM.DataSecurityAM.KFFHierFilter1"
   ```

   Turn ON the 'Allow deferred execution' option for this initialization block.

   Use the appropriate segment label code for the particular segment and any suitable prefix for the variable name, which are highlighted in bold text. In the above example, the segment label code used is 'FA_COST_CTR' and the variable prefix used is 'COST_CENTER_'. This SQL will give (a) the value set codes the user has been granted full access to and/or (b) specific parent nodes within a tree the user has been granted access to using 'is-descendant of' operator.

2. Create two session variables for the initialization block with names <*prefix*>_FULLACCESS and <*prefix*>_FILTEREDACCESS, where <*prefix*> is the variable prefix used in the initialization block SQL. For example, in the above case you will define two session variables with the name COST_CENTER_FULLACCESS and COST_CENTER_FILTEREDACCESS. Default them with a value '-1' (Varchar).

3. When the user has filtered access, we need to determine the hierarchy level in the hierarchy/tree where the node falls. For this you will need to create another row wise session initialization block. A sample SQL for this would be as follows. You will need to use the FILTEREDACCESS variable created in the previous step.

   ```
   SELECT DISTINCT 'COST_CENTER_LEVELS', FIXED_HIER_LEVEL FROM "Oracle Data
   Warehouse"."Catalog"."dbo"."W_COST_CENTER_DH" WHERE LEVEL0_SECURITY_ID IN
   (VALUELISTOF(NQ_SESSION.COST_CENTER_FILTEREDACCESS)) AND CURRENT_FLG='Y'
   ```

   Turn ON the 'Allow deferred execution' option for this initialization block.

   Use '<*prefix*>_LEVELS' for the variable name in the select clause, where <*prefix*> is the same variable prefix that is used in Steps 2 and 3. **Note**: The variable name used (in the where clause), should be the same as defined in the previous initialization block.

4. Create a session variable for the initialization block with the same name as used in the initialization block (COST_CENTER_LEVELS in this example) and default it with a value 0 (number). Set the execution precedence to make the initialization block mentioned in the previous step to run first.

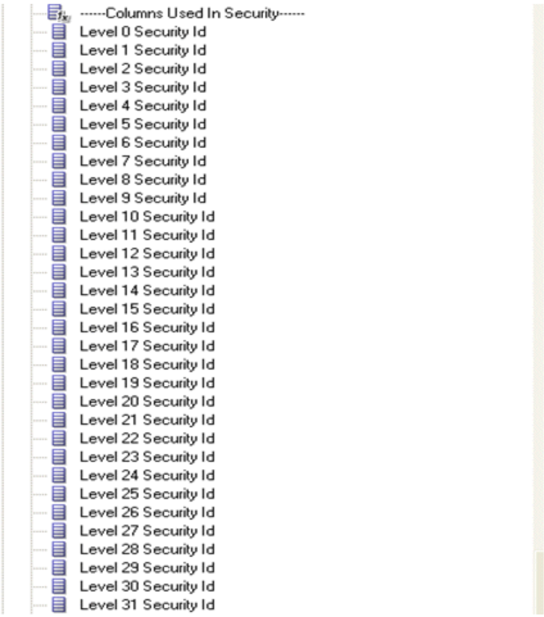
5. You can refer to the initialization blocks 'Cost Center Security' and 'Cost Center Security Top Node Levels' in the repository installed by default, as a reference to create the above two initialization blocks.

6. Repeat the previous steps for each of the segment to be secured, giving a different name for the two initialization blocks and the three session variables for each segment.

Task 2 Security id Expression in the logical dimensions

Each segment dimension in the Oracle BI Repository (Dim - Cost Center, Dim - Balancing Segment, Dim - Natural Account Segment and Dim - GL Segment 1-10) can be either a tree or non-tree segment based on your requirements. In case you have configured them to be tree segments, perform the steps below after creating the initialization blocks and variables mentioned in Task 1.

1. Each dimension has 32 security columns, Level 0 Security Id through Level 31 Security Id, as shown below. The expression for each of these logical columns must be modified using the hierarchy level variable created above.



------Columns Used In Security------
Level 0 Security Id
Level 1 Security Id
Level 2 Security Id
Level 3 Security Id
Level 4 Security Id
Level 5 Security Id
Level 6 Security Id
Level 7 Security Id
Level 8 Security Id
Level 9 Security Id
Level 10 Security Id
Level 11 Security Id
Level 12 Security Id
Level 13 Security Id
Level 14 Security Id
Level 15 Security Id
Level 16 Security Id
Level 17 Security Id
Level 18 Security Id
Level 19 Security Id
Level 20 Security Id
Level 21 Security Id
Level 22 Security Id
Level 23 Security Id
Level 24 Security Id
Level 25 Security Id
Level 26 Security Id
Level 27 Security Id
Level 28 Security Id
Level 29 Security Id
Level 30 Security Id
Level 31 Security Id

2. Open the logical table source of the dimension that maps to the warehouse dimension table and set the expression for each of these columns using the example from 'Dim - Cost Center' dimension. For example, if you are securing by 'Dim - GL Segment3' and the hierarchy level variable for this segment is 'SEGMENT3_LEVELS', you would set the expression for each of the 'Level <*n*> Security Id' column with the following:

```
INDEXCOL( IFNULL( VALUEOF(<n>, NQ_SESSION."SEGMENT3_LEVELS"),  VALUEOF(0, NQ_
SESSION."SEGMENT3_LEVELS")),
"Oracle Data Warehouse"."Catalog"."dbo"."Dim_W_GL_SEGMENT_DH_Security_
Segment3"."LEVEL31_SECURITY_ID",
"Oracle Data Warehouse"."Catalog"."dbo"."Dim_W_GL_SEGMENT_DH_Security_
Segment3"."LEVEL30_SECURITY_ID",
"Oracle Data Warehouse"."Catalog"."dbo"."Dim_W_GL_SEGMENT_DH_Security_
Segment3"."LEVEL29_SECURITY_ID",
…and so on for each security id column…
"Oracle Data Warehouse"."Catalog"."dbo"."Dim_W_GL_SEGMENT_DH_Security_
Segment3"."LEVEL1_SECURITY_ID",
"Oracle Data Warehouse"."Catalog"."dbo"."Dim_W_GL_SEGMENT_DH_Security_
Segment3"."LEVEL0_SECURITY_ID")
```

3. Repeat the above steps for each of the segment dimension to be secured.

Task 3 Security Filters in the Data Security Duty Roles

After completing Task 2, filters need to be added to the appropriate Data Role for data security predicates to be applied to queries.

1. Navigate to 'Manage -> Identity' from the menu.
2. Open the 'OBIA_GENERAL_LEDGER_DATA_SECURITY' Duty Role.
3. Navigate to 'Permissions -> Data Filters'.

   For each of the logical facts secured under this role, you will see some existing filters, which are handling data access security. You will need to append the segment security filters to this with an 'AND' condition. A snippet of the segment security filters to be appended for a given segment dimension is given below, assuming the security is on 'Dim - GL Segment3' and the session variable prefix used in the previous steps was 'SEGMENT3'.

```
(
"Core"."Dim - GL Segment3"."Segment Value Set Code" IS NULL OR
((
"Core"."Dim - GL Segment3"."Segment Value Set Code" = VALUEOF(NQ_
SESSION."SEGMENT3_FULLACCESS") OR
"Core"."Dim - GL Segment3"."Level 0 Security Id"    = VALUEOF(NQ_
SESSION."SEGMENT3_FILTEREDACCESS") OR
"Core"."Dim - GL Segment3"."Level 1 Security Id"    = VALUEOF(NQ_
SESSION."SEGMENT3_FILTEREDACCESS") OR
"Core"."Dim - GL Segment3"."Level 2 Security Id"    = VALUEOF(NQ_
SESSION."SEGMENT3_FILTEREDACCESS") OR
...and so on for each security id column...
"Core"."Dim - GL Segment3"."Level 30 Security Id"   = VALUEOF(NQ_
SESSION."SEGMENT3_FILTEREDACCESS") OR
"Core"."Dim - GL Segment3"."Level 31 Security Id"   = VALUEOF(NQ_
SESSION."SEGMENT3_FILTEREDACCESS")
)
AND
"Core"."Dim - GL Segment3"."Current Flag Security" = 'Y')
)
```

4. Repeat the above for each tree based segment dimension that is secured using appropriate variable names for each segment and appending each block of filters with an AND. For example, if you are securing by cost center and segment3 dimensions, the filter including the data access set security, will be as follows:

```
/* data access security filters */
 (
"Core"."Dim - GL Data Access Set Security"."Ledger List" = VALUEOF(NQ_
SESSION."LEDGER_LIST")
OR
"Core"."Dim - GL Data Access Set Security"."Ledger BSV List" = VALUEOF(NQ_
SESSION."LEDGER_BSV_LIST")
OR
"Core"."Dim - GL Data Access Set Security"."Ledger MSV List" = VALUEOF(NQ_
SESSION."LEDGER_MSV_LIST")
)
/* cost center segment security filters */
AND
 (
"Core"."Dim - Cost Center"."Cost Center Value Set Code" IS NULL OR
((
"Core"."Dim - Cost Center"."Cost Center Value Set Code" = VALUEOF(NQ_
SESSION."COST_CENTER_FULLACCESS") OR
"Core"."Dim - Cost Center"."Cost Center Level 0 Security Id"    = VALUEOF(NQ_
SESSION." COST_CENTER _FILTEREDACCESS") OR
"Core"."Dim - Cost Center"."Cost Center Level 1 Security Id"    = VALUEOF(NQ_
SESSION." COST_CENTER _FILTEREDACCESS") OR
"Core"."Dim - Cost Center"."Cost Center Level 2 Security Id"    = VALUEOF(NQ_
SESSION." COST_CENTER _FILTEREDACCESS") OR
...and so on for each security id column...
"Core"."Dim - Cost Center"."Cost Center Level 30 Security Id"   = VALUEOF(NQ_
SESSION." COST_CENTER _FILTEREDACCESS") OR
"Core"."Dim - Cost Center"."Cost Center Level 31 Security Id"   = VALUEOF(NQ_
SESSION." COST_CENTER _FILTEREDACCESS")
)
AND
"Core"."Dim - Cost Center"."Current Flag Security" = 'Y')
)
/* segment3 security filters */
AND
 (
"Core"."Dim - GL Segment3"."Segment Value Set Code" IS NULL OR
((
"Core"."Dim - GL Segment3"."Segment Value Set Code" = VALUEOF(NQ_
SESSION."SEGMENT3_FULLACCESS") OR
"Core"."Dim - GL Segment3"."Level 0 Security Id"    = VALUEOF(NQ_
SESSION."SEGMENT3_FILTEREDACCESS") OR
"Core"."Dim - GL Segment3"."Level 1 Security Id"    = VALUEOF(NQ_
SESSION."SEGMENT3_FILTEREDACCESS") OR
"Core"."Dim - GL Segment3"."Level 2 Security Id"    = VALUEOF(NQ_
SESSION."SEGMENT3_FILTEREDACCESS") OR
...and so on for each security id column...
"Core"."Dim - GL Segment3"."Level 30 Security Id"   = VALUEOF(NQ_
SESSION."SEGMENT3_FILTEREDACCESS") OR
"Core"."Dim - GL Segment3"."Level 31 Security Id"   = VALUEOF(NQ_
SESSION."SEGMENT3_FILTEREDACCESS")
)
AND
"Core"."Dim - GL Segment3"."Current Flag Security" = 'Y')
)
```

Note: When a tree has more than one version, the security filters are always applied on the current version for that tree (CURRENT_FLG='Y'). However, you can navigate through any other version of the tree in the reports but security will always be applied on the current version.

A.1.32.2.2 Non-Tree Segment Security Implementation

Perform the following steps when the segment on which security to be applied is not a tree based segment.

Task 1 Define Initialization Blocks and Session Variables

1. Determine the name of the VO that was generated for the segment. It will follow a naming pattern such as FLEX_VS_<*label*>_VI, where <*label*> is the segment label defined in the OLTP.
2. Create a session row wise initialization block reading from this VO.

   A sample SQL statement might be:

   ```
   SELECT 'GL_MANAGEMENT_FILTEREDACCESS', ValueSetCode||'~'||Value FROM
   "oracle.apps.fscm.model.analytics.applicationModule.FscmTopModelAM_
   FscmTopModelAMLocal"..."FscmTopModelAM.AccountBIAM.FLEX_VS_GL_MANAGEMENT2_VI"
   ```

   Use an appropriate prefix for the variable name, highlighted above. This initialization block gives a concatenation of value set code and values the user has access to.

3. Create appropriate session variable with the same name as used above and default it with a value '-1' (Varchar). In the above example, the variable name is 'GL_MANAGEMENT_FILTEREDACCESS'.
4. Repeat the above steps for each non-tree segment that needs to be secured.

Task 2 Security Filters in the "Data Security" Data Roles

After you have completed Task 1, filters need to be added to the appropriate Data Role for data security predicates to be applied to queries.

1. Navigate to 'Manage -> Identity' from the menu, and open the 'OBIA_GENERAL_LEDGER_DATA_SECURITY' Data Role.
2. Navigate to 'Permissions -> Data Filters', and for each of the logical facts secured under this role, append the following filter to any existing filters with an 'AND' condition. The sample filter will look like:

```
(
"Core"."Dim - GL Segment2"."Segment Value Set Code" IS NULL OR
"Core"."Dim - GL Segment2"."Segment Code Id"  = VALUEOF(NQ_SESSION."GL_
MANAGEMENT_FILTEREDACCESS")
)
```

3. Repeat the previous steps for each non-tree segment dimension that is secured using appropriate variable names for each segment and appending each block (one block per segment) with an 'AND' condition. If you have a combination of non-tree and tree segments, then apply the data filters accordingly (as explained for each case) appending each filter with an 'AND' condition.

A.1.33 How to Set Up CRM Territory Hierarchy Based Security for Oracle Fusion

Overview

Territory hierarchy based security is widely used in many CRM subject areas, such as Sales, Marketing and Partner Management. Territory based security control starts with the list of territories that the login user works for and the levels these territories belong to in the territory hierarchy. The list of territories and the levels in the territory hierarchy are then used as part of the data filter condition in queries.

There are variations of territory hierarchy based security when it's actually applied in different areas, although they are all territory based by nature.

- For Opportunity and Revenue, visibility is granted to the login user via the following:
  - As member of the territory team that the opportunity is assigned to.
  - As owner or administrator of a parent territory in the hierarchy.
- For Territory Quota and Resource Quota, visibility is granted to the login user via the following:
  - As team member of the territory that the Quota is created on.
  - As an owner or administrator of a parent territory in the hierarchy.
- For Forecasting, visibility is granted to the login user via the following:
  - As team member of the territory that the Forecast is created on.
  - As owner or administrator of a parent territory in the hierarchy.
- For Leads, visibility is granted to the login user via the following:

  - As team member of the territory that is assigned to lead.
  - As owner or administrator of a parent territory in the hierarchy of the territory assigned to lead.

Configuring Resource Hierarchy Based Security

There are 3 session variables used in territory hierarchy based data security roles.

- TERR_LIST contains the list of Ids of the territory, in which the login user is a team member. This variable is initialized via the session Init Block 'Territory List'.
- SUPER_TERR_LIST contains the list of Ids of the territory, in which the login user is an owner or administrator. This variable is initialized via the session Init Block 'Super Territory List'.
- TERR_HIER_LEVEL_LIST contains the list of the levels in territory hierarchy that the login user is an owner or administrator of the territory. This variable is initialized via the session Init Block 'Territory Hierarchy Level List'.

A.1.33.1 Configuring BI Duty Roles

All the Territory Hierarchy Based security roles should be defined as member of the internal role OBIA_TERRITORY _HIERARCHY_DATA_SECURITY, under which, all the necessary data filters are defined. In the default configuration, OBIA_TERRITORY_HIERARCHY_DATA_SECURITY has the following members:

- OBIA_LEAD_ANALYSIS_DUTY
- OBIA_PARTNER_ANALYSIS_DUTY
- OBIA_PARTNER_ADMINISTRATIVE_ANALYSIS_DUTY
- OBIA_PARTNER_CHANNEL_ACCOUNT_MANAGER_ANALYSIS_DUTY
- OBIA_PARTNER_CHANNEL_ADMINISTRATIVE_ANALYSIS_DUTY
- OBIA_PARTNER_CHANNEL_ANALYSIS_DUTY
- OBIA_OPPORTUNITY_LANDSCAPE_ANALYSIS_DUTY
- OBIA_SALES_EXECUTIVE_ANALYSIS_DUTY
- OBIA_SALES_MANAGERIAL_ANALYSIS_DUTY
- OBIA_SALES_TRANSACTIONAL_ANALYSIS_DUTY

These Duty Roles control the subject areas and dashboard content to which the user has access. These Duty Roles also ensure the data security filters are applied to all the queries. For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

A.1.34 How to Set Up Project Billing and Revenue Security for E-Business Suite

Overview

Project Analytics supports security over following dimensions in Project Billing and Revenue subject areas. In Oracle Business Intelligence Applications, the 'Business Unit' entity refers to 'Operating Unit Organizations' in E-Business Suite. The list of Business Units that a user has access to, is determined by E-Business Suite grants.

Table A–98 Supported Project Billing and Revenue subject areas

Project Billing & Revenue Facts Dimension Used For Securing	Billing	Revenue	Contract	Funding	Cross Charge- Receiver	Cross Charge - Provider	Cross Charge - Invoice
Project Business Unit	Y	Y	N	Y	Y	N	Y
Project Organization	Y	Y	N	Y	Y	N	Y
Expenditure Business Unit	N	N	N	N	N	Y	N
Contract Business Unit	Y	Y	Y	Y	N	N	N
Project	Y	Y	N	Y	Y	Y	Y
Resource Organization	N	N	N	N	N	N	N
Ledger	N	N	N	N	N	N	N

Configuring Project Billing and Revenue Security for E-Business Suite

In order for data security filters to be applied, appropriate initialization blocks need to be enabled depending on the deployed source system.

> **Note:** On installation, initialization blocks are enabled for E-Business Suite R12. If you are deploying on a source system other than E-Business Suite R12, then you must enable the appropriate initialization blocks.

Enable data security for Project Billing and Revenue in E-Business Suite by enabling the initialization blocks listed below based on the E-Business Suite adaptor. If only one source system is deployed, then you must make sure that all Project Security initialization blocks for other adapters are disabled. If more than one source system is deployed, then you must also enable the initialization blocks of those source systems.

Initialization Blocks for Project Billing and Revenue

- For R11x
  - Expenditure Business Unit List EBS11x
  - Project Business Unit List Funding EBS11x
  - Project Business Unit List Invoice EBS11x
  - Project Business Unit List Revenue EBS11x
  - Project Contract Business Unit List EBS11x
  - Project Contract Business Unit List Invoice EBS11x
  - Project Contract Business Unit List Revenue EBS11x
- For R12
  - Expenditure Business Unit List EBSR12
  - Project Business Unit List Funding EBSR12
  - Project Business Unit List Invoice EBSR12
  - Project Business Unit List Revenue EBSR12
  - Project Contract Business Unit List EBSR12

  - Project Contract Business Unit List Invoice EBSR12
  - Project Contract Business Unit List Revenue EBSR12
- For both R11x and R12
  - Project List Funding EBS
  - Project List Invoice EBS
  - Project List Revenue EBS
  - Project Organization List Funding EBS
  - Project Organization List Invoice EBS
  - Project Organization List Revenue EBS

A.1.34.1 Configuring BI Duty Roles

The following BI Duty Roles are applicable to the Project Billing and Revenue subject area.

- OBIA_EBS_PROJECT_EXECUTIVE_ANALYSIS_DUTY
- OBIA_EBS_PROJECT_MANAGEMENT_ANALYSIS_DUTY
- OBIA_EBS_PROJECT_DATA_SECURITY

These Duty Roles control the subject areas and dashboard content to which the user has access. These Duty Roles also ensure the data security filters are applied to all the queries.

For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

A.1.35 How to Set Up CRM Resource Organization Based Security for Oracle Fusion

Overview

Oracle Fusion CRM resource organization based security is applied when the Fusion marketing managers or marketing operational managers access marketing campaigns. It provides BI Users with access to all marketing campaigns primarily owned by their organizations or child organizations.

Configuring Resource Organization Based Security

There are two session variables used in resource organization based data security role.

- RESOURCE_ORG_LIST contains the list of resource organization id that the login user belongs to. It is initialized via Init Block 'Resource Org List'.
- RESOURCE_ORG_HIER_LEVEL_LIST contains the list of levels of resource organization hierarchy. It is initialized via Init Block 'RESOURCE_ORG_HIER_LEVEL_LIST'.

A.1.35.1 Configuring BI Duty Roles

OBIA_RESOURCE_ORGANIZATION_HIERARCHY_DATA_SECURITY is the internal BI Duty Role to define data filter for resource organization hierarchy based data security. By default, it has the following members:

- OBIA_MARKETING_OPERATIONAL_ANALYSIS_DUTY

- OBIA_MARKETING_MANAGERIAL_ANALYSIS_DUTY

These Duty Roles control the subject areas and dashboard content to which the user has access. And as members of OBIA_RESOURCE_ORGANIZATION_HIERARCHY_DATA_SECURITY, they also ensure the primary resource organization hierarchy based data security filters are applied to all the queries involving marketing campaign.

For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

A.1.36 How to Set Up Price Analytics Security for Siebel Applications

Overview

There is Primary Employee/Position Hierarchy based data security applied to Price Analytics reports and metrics. Users who can access Price Analytics Subject areas can view all Order and Quote data in the related reports with/without data security filters based on the BI Duty Role assigned as specified in the following section.

A.1.36.1 Configuring BI Duty Roles

This table lists BI Duty Roles (and applicable data security) that can be assigned to users in order to give them access to Price Subject Areas.

Table A–99 BI Duty Roles and applicable data security

BI Duty Role	Data Security	Subject Areas
Pricing Administrator	None	Sales – CRM - Price Sales – CRM Price Waterfall Sales – CRM Price Waterfall – Orders Sales – CRM Price Waterfall – Quotes
Pricing Manager	Primary Employee/Position Hierarchy based data security	Sales – CRM - Price Sales – CRM Price Waterfall Sales – CRM Price Waterfall – Orders Sales – CRM Price Waterfall – Quotes

For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

A.1.37 How to Set Up Project Cost and Control Security for E-Business Suite

Overview

Oracle Project Analytics supports security over following dimensions in Project Costing and Project Control subject areas. In Oracle Business Intelligence Applications, the 'Business Unit' entity refers to 'Operating Unit Organizations' in E-Business Suite. The list of Business Units that a user has access to is determined by E-Business Suite grants.

Table A–100 Supported Project Costing and Project Control subject areas

Project Costing and Control Facts Security Entity	Cost	Commitment	Budget	Forecast
Project Business Unit	Y	Y	Y	Y
Project Organization	Y	Y	Y	Y
Expenditure Business Unit	Y	N	N	N
Contract Business Unit	N	N	N	N
Project	Y	Y	Y	Y
Resource Organization	N	N	N	N
Ledger	N	N	N	N

Configuring Project Cost and Control Security For E-Business Suite

In order for data security filters to be applied, appropriate initialization blocks need to be enabled depending on the deployed source system.

> **Note:** On installation, initialization blocks are enabled for E-Business Suite R12. If you are deploying on a source system other than E-Business Suite R12, then you must enable the appropriate initialization blocks.

You must enable data security for Project Cost and Control in E-Business Suite by enabling the initialization blocks listed below based on your E-Business Suite adaptor. You must disable Project Security initialization blocks for other adapters. If more than one source system is deployed, then you must also enable the initialization blocks of those source systems.

Init Blocks: EBS R11x

- Expenditure Business Unit List EBS11x
- Project Business Unit List Budget EBS11x
- Project Business Unit List Costing EBS11x
- Project Business Unit List Forecast EBS11x

Init Blocks: EBS R12

- Expenditure Business Unit List EBSR12
- Project Business Unit List Budget EBSR12
- Project Business Unit List Costing EBSR12
- Project Business Unit List Forecast EBSR12

Init Blocks: EBS R11x and EBS R12

- Project List Budget EBS
- Project List Costing EBS
- Project List Forecast EBS
- Project Organization List Budget EBS

- Project Organization List Costing EBS
- Project Organization List Forecast EBS

A.1.37.1 Configuring BI Duty Roles

The following BI Duty Roles are applicable to the Project Costing and Control subject area.

- OBIA_EBS_PROJECT_EXECUTIVE_ANALYSIS_DUTY
- OBIA_EBS_PROJECT_MANAGEMENT_ANALYSIS_DUTY
- OBIA_EBS_PROJECT_DATA_SECURITY

These Duty Roles control the subject areas and dashboard content to which the user has access. These Duty Roles also ensure the data security filters are applied to all the queries. For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

A.1.38 How to implement Security for Supply Chain Analytics

Overview

Supply Chain Analytics supports role-based and organization-based security in Inventory and Costing subject areas. Assign users to the appropriate roles to control which subject areas they can access. The list of Inventory Organizations that a user has access to is determined by the grants in the source application system.

Configuring Inventory Org Based Security for E-Business Suite

In order for data security filters to be applied, appropriate initialization blocks need to be enabled depending on the deployed source system. To enable Inventory Org Based security for E-Business Suite, enable the Oracle EBS initialization block. If more than one source system is deployed, then you must also enable the initialization blocks of those source systems.

To enable initialization blocks, follow the steps below:

1. In Oracle BI Administration Tool, edit the BI metadata repository (for example, OracleBIAnalyticsApps.rpd).
2. Open the variable by navigating to: Manage, then Variables.
3. Open the initialization block that needs to be enabled under Session – Initialization Blocks (Inventory Organizations EBS).
4. Clear the **Disabled** check box.
5. Repeat the above steps for the following initialization blocks:
   - SCOM_AN:SECURITY:Inv Org CycleCount List
   - SCOM_AN:SECURITY:Inv Org InvTxns List
   - SCOM_AN:SECURITY:Inv Org Onhand List
   - SCOM_AN:SECURITY:Inv Org Shipments List
6. Save the RPD.

A.1.38.1 Configuring BI Duty Roles

The following BI Duty Roles are applicable to the Order Management subject area.

- Inventory Analyst

  This role provides secured access to Inventory Analysts with detailed insight into transactions, balances, aging, bill of materials, cycle counts and returns, and covers the following Subject Areas:

  - Inventory – Cycle Count
  - Inventory – Transactions
  - Inventory – Customer and Supplier Returns
  - Inventory – Bill of Materials
  - Inventory – Balances
  - Inventory - Aging

- Inventory Manager

  This role provides secured access to Inventory Managers with insight into inventory details and costing data, and covers the following Subject Areas:

  - Inventory – Cycle Count
  - Inventory – Transactions
  - Inventory – Customer and Supplier Returns
  - Inventory – Bill of Materials
  - Inventory – Balances
  - Inventory - Aging
  - Costing – Margin Analysis
  - Costing – Item Cost
  - Costing – Inventory Valuation

These Duty Roles control the subject areas and dashboard content to which the user has access. These Duty Roles also ensure the data security filters are applied to all the queries.

For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

A.1.39 How to Set Up CRM Partner Organization Based Security for Oracle Fusion

Oracle Fusion CRM partner organization based security is applied when fusion partner administrator access partner organization, partner owned leads and opportunity/revenue. Partner administrator should be able to access the above entities owned by his partner organization.

Configuring Partner Organization Based Security

The session variable PARTNER_ORG_HIER_LIST stores a list of partner organizations the login user belongs to. It is initialized via Init Block Partner Org Hierarchy List and then used in partner organization based data security role.

A.1.39.1 Configuring BI Duty Roles

OBIA_PARTNER_ORGANIZATION_DATA_SECURITY is the internal BI Duty Role to define data filter for partner organization based data security. By default, it has one member BI Duty Role:

- OBIA_PARTNER_ADMINISTRATIVE_ANALYSIS_DUTY

These Duty Roles control the subject areas and dashboard content to which the user has access. And as members of OBIA_RESOURCE_ORGANIZATION_HIERARCHY_DATA_SECURITY, they also ensure the primary resource organization hierarchy based data security filters are applied to all the queries involving marketing campaign.

For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

A.1.40 How to Set Up Service Analytics Security for Siebel

Overview

There is no row-level security applied to Service Analytics reports and metrics. Users who can access Service Analytics Subject areas can view all data in the related reports without any data-security filter.

Configuring BI Duty Roles

This table lists BI Duty Roles that can be assigned to users in order to give them access to Service Subject Areas.

Table A–101 BI Duty Roles and Associated Subject Areas

BI Duty Roles	Subject Areas
Service Agent	Service - CRM Activities Service - CRM Service Requests Service - CRM Agreements Service - CRM Assets Service - CRM Customer Satisfaction Service - CRM Orders
Service Manager	Service - CRM Activities Service - CRM Service Requests Service - CRM Agreements Service - CRM Assets Service - CRM Email Response Service - CRM Customer Satisfaction Service - CRM Orders
Service Executive	Service - CRM Activities Service - CRM Service Requests Service - CRM Agreements Service - CRM Assets Service - CRM Customer Satisfaction Service - CRM Orders

Table A–101 (Cont.) BI Duty Roles and Associated Subject Areas

BI Duty Roles	Subject Areas
Service Delivery and Costs Analyst	Service - CRM Agreements

For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

A.1.41 How to implement Inventory Org Based Security for EBS Manufacturing Analytics

Overview

Manufacturing Analytics supports security over Inventory Organizations in manufacturing subject areas. The list of Inventory Organizations to which a user has access is determined by the grants in E-Business Suite.

Configuring Inventory Org Based Security

In order for data security filters to be applied, appropriate initialization blocks need to be enabled depending on the deployed source system. To enable Inventory Org Based security for EBS, enable E-Business Suite initialization block and make sure the initialization blocks of all other source systems are disabled.

Oracle EBS: Inventory Org-based Security

To enable initialization blocks, follow the steps below:

1. In Oracle BI Administration Tool, edit the BI metadata repository (for example, OracleBIAnalyticsApps.rpd).
2. Navigate to Manage and open variables from menu ('INV_ORG').
3. Open the initialization block that you need to enable under Session – Initialization Blocks (Inventory Organizations EBS).
4. Clear the **Disabled** check box.
5. Save the metadata repository.

Configuring BI Duty Roles

The following BI Duty Roles are applicable to the Manufacturing Analytics subject area.

- OBIA_MANUFACTURING_EXECUTION_ANALYSIS_DUTY
- OBIA_MANUFACTURING_EXECUTIVE_ANALYSIS_DUTY
- OBIA_MANUFACTURING_COST_ANALYSIS_DUTY

Table A–102 BI Duty Roles and Associated Subject Areas

BI Duty Roles	Subject Areas
OBIA_ MANUFACTURING_ EXECUTION_ANALYSIS_ DUTY Manufacturing Execution Analyst for E-Business Suite.This role provides secured access to Operations Manager, Production Supervisor with Manufacturing execution.	Manufacturing – Material Usage Manufacturing –Work Order Performance Manufacturing –Work OrderSnapshot Manufacturing –Resource Usage Manufacturing –Resource Utilization Manufacturing –Work Order Cycle Time Manufacturing –Kanban Manufacturing –WorkOrderAging
OBIA_ MANUFACTURING_ EXECUTIVE_ANALYSIS_ DUTY Manufacturing Executive for E-Business Suite.This role provides secured access to VP Manufacturing, Plant Manager, Plant General Manager with insight into Planning Manufacturing execution and costing.	Manufacturing –Production Plan Manufacturing –Actual Production Manufacturing – Material Usage Manufacturing –Work Order Performance Manufacturing –Work OrderSnapshot Manufacturing –Resource Usage Manufacturing –Resource Utilization Manufacturing –Work Order Cycle Time Manufacturing –Kanban Manufacturing –WorkOrderAging Manufacturing-Production Cost Manufacturing-Plan to Produce Manufacturing-Discrete Quality
OBIA_ MANUFACTURING_ COST_ANALYSIS_DUTY Manufacturing Cost Analyst for E-Business Suite.This role provides secured access to Production Controller, Cost Accountant with insight over Production costing.	Manufacturing-Production Cost

These Duty Roles control the subject areas and dashboard content to which the user has access. These Duty Roles also ensure the data security filters are applied to all the queries. For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

A.1.42 How To Customize Extended Cross Functional Security for Employee Expenses

To facilitate procurement users (such as Procurement VP or Spend Analyst) to perform deeper and cross functional analysis apart from their regular duty, Oracle Procurement and Spend Analytics has data and functional security to access the employee expenses transactions (such as expense report, credit card transaction and expense violation) through extended Duty Roles. If you would like to provision this duty to the procurement and spend users, then follow the steps below.

Understanding Extended Duty Roles: BI seeded Duty Roles for Fusion Applications includes a 'Procurement Executive Analysis Duty' role (Role name: OBIA_ PROCUREMENT_EXECUTIVE_ANALYSIS_DUTY) to act like a Spend Analyst/ Executive duty. This extended role is not mapped to any enterprise job roles by default, but it is pre-configured within Oracle BI Applications to enforce object and data level security for Employee Expenses. Internally, data security is implemented using 'Extended Procurement and Spend Business Unit Data Security' (Role name: OBIA_EXTENDED_PROCUREMENT_AND_SPEND_BUSINESS_UNIT_DATA_ SECURITY). This data security role enables cross functional analysis by manage spend Business Unit Data Security.

Follow the steps below to implement 'Procurement Executive Analysis Duty' role:

1. Create 'VP of Procurement' or similar executive job role in your Fusion Applications deployment and assign BI duty 'Procurement Executive Analysis Duty' to 'VP of Procurement'.
2. Assign appropriate Fusion Applications Duty Roles to the job role - 'VP of Procurement' and assign BU privileges. Data security of 'Procurement Executive Analysis Duty' (OBIA Duty Role) is controlled by the BUs assigned to the user in the agent access 'manage spend' action.
3. Customize Presentation catalog permissions (for Employee Expense dashboard and related analyses) and Subject Area permissions as desired for 'Procurement Executive Analysis Duty' role.

For more information on how to create and manage job roles in Fusion Applications, refer to section 'Understanding How to Secure Oracle Fusion Applications' in *Oracle Fusion Applications Administrator's Guide*.

A.1.43 How To Customize Extended Cross Functional Security for Accounts Payables

To facilitate procurement users (such as Category Managers and Procurement Managers) to perform deeper and cross functional analysis apart from their regular duty, Oracle Procurement and Spend Analytics includes configured data and functional security to access the accounts payable transactions (such as invoices, payments, payment schedules) through extended Duty Roles. To implement these duties, follow steps below.

Understanding Extended Duty Roles: Seeded security roles for Oracle BI Applications for Fusion Applications include the following additional Duty Roles. These extended roles are not mapped to any enterprise job roles by default, but they are pre-configured within Oracle BI Applications to enforce object and data level security for Accounts Payables.

- 'Procurement Managerial Extended Analysis Duty' role (Role name: OBIA_ PROCUREMENT_MANAGERIAL_ANALYSIS_DUTY) – This BI Duty Role enables users to perform cross functional analysis outside of Category Management. Internally, data security on Oracle BI Applications is implemented using 'Extended Procurement and Payable Business Unit Data Security' (Role name: OBIA_EXTENDED_PROCUREMENT_AND_PAYABLE_BUSINESS_UNIT_ DATA_SECURITY).
- 'Category Manager Extended Analysis Duty' role (Role name: OBIA_CATEGORY_ MANAGER_ANALYSIS_DUTY) – This BI Duty Role enables to perform cross functional analysis outside of Procurement Management. Internally, data security on Oracle BI Applications is implemented using 'Extended Procurement and Payable Business Unit Data Security' (Role name: OBIA_EXTENDED_ PROCUREMENT_AND_PAYABLE_BUSINESS_UNIT_DATA_SECURITY).

- 'Procurement Executive Analysis Duty' role (Role name: OBIA_PROCUREMENT_EXECUTIVE_ANALYSIS_DUTY) to act also like a Spend Analyst/ Executive duty. Internally, data security on Oracle BI Applications is implemented using 'Extended Procurement and Spend Business Unit Data Security' (Role name: OBIA_EXTENDED_PROCUREMENT_AND_SPEND_BUSINESS_UNIT_DATA_SECURITY). This data security role enables cross functional analysis by manage spend Business Unit Data Security.

Follow the steps below to implement 'Procurement Executive Analysis Duty' role:

1. Assign BI duty 'Procurement Managerial Extended Analysis Duty' to Fusion Applications job role, 'Procurement Manager' or similar.
2. Assign BI duty 'Category Manager Extended Analysis Duty' to Fusion Applications job role, 'Category Manager' or similar.
3. Create 'VP of Procurement' or similar executive job role in your Fusion Applications deployment and assign BI duty 'Procurement Executive Analysis Duty' to 'VP of Procurement'.
4. Assign appropriate Fusion Applications Duty Roles to the job role - 'VP of Procurement' and assign BU privileges. Data security of 'Procurement Executive Analysis Duty' (OBIA Duty Role) is controlled by the BUs assigned to the user in the agent access 'manage spend' action.
5. Customize Presentation catalog permissions (for Supplier Performance – AP Transactions related content) and Subject Area permissions as desired for above mentioned roles.

For more information on how to create and manage job roles in Fusion Applications, refer to section 'Understanding How to Secure Oracle Fusion Applications' in *Oracle Fusion Applications Administrator's Guide*.

A.1.44 How to Grant GL Security Data Role to HR VP Users

In Oracle Business Intelligence Applications, in order for a BI User with VP of HR job role to see GL data, he/she needs to be provisioned with GL data role pertaining to a Financial Analyst job role. The GL data role provisioned will control the data security that will be enforced upon the GL data the user is trying to view. To understand more details on how GL data are provisioned in Fusion Applications, refer to *Oracle General Ledger User's Guide* for more information.

A.1.45 How To Customize Security for Procurement Executive / Spend Analyst

To enable procurement users (such as Procurement VP or Spend Analyst) to perform deeper and cross functional analysis apart from their regular duties, Oracle Procurement and Spend Analytics includes data and functional security to access the employee expenses transactions (such as expense report, credit card transaction and expense violation) through extended Duty Roles. If you would like to provision such duty to the procurement and spend users, then follow the steps below.

Understanding Extended Duty Roles: BI seeded Duty Roles for Fusion Applications includes 'Procurement Executive Analysis Duty' role (Role name: OBIA_PROCUREMENT_EXECUTIVE_ANALYSIS_DUTY) to act also like a Spend Analyst/ Executive duty. This extended role is not mapped to any enterprise job roles by default, but it is pre-configured within Oracle BI Applications to enforce object and data level security for Spend Analysis. Internally, data security on Oracle BI Applications is implemented using 'Extended Procurement and Spend Business Unit Data Security' (Role name: OBIA_EXTENDED_PROCUREMENT_AND_SPEND_

BUSINESS_UNIT_DATA_SECURITY). This data security role enables cross functional analysis by manage spend Business Unit Data Security.

Follow the steps below to implement 'Procurement Executive Analysis Duty' role:

1. Create 'VP of Procurement' or similar executive job role in your Fusion Applications deployment and assign BI duty 'Procurement Executive Analysis Duty' to 'VP of Procurement'.
2. Assign appropriate Fusion Applications Duty Roles to the job role - 'VP of Procurement' and assign BU privileges. Data security of 'Procurement Executive Analysis Duty' (OBIA Duty Role) is controlled by the BUs assigned to the user in the agent access 'manage spend' action.
3. Customize Presentation catalog permissions (for Spend Analyzer dashboard and related analyses) and Subject Area permissions as desired for 'Procurement Executive Analysis Duty' role.

For more information on how to create and manage job roles in Fusion Applications, refer to section 'Understanding How to Secure Oracle Fusion Applications' in *Oracle Fusion Applications Administrator's Guidee*. For more information on how to define and customize security in Oracle BI Applications, refer to *Oracle Fusion Middleware Security Guide for Oracle Business Intelligence Applications*.

A.1.46 How to Set Up CRM Partner Channel Based Security for Oracle Fusion

Overview

Oracle Fusion CRM partner channel based security is applied when fusion channel administrator or channel operation manager access partner owned leads and opportunity/revenue. For leads, this means user can see all the leads that have sales channel stamped as indirect or partner. For opportunity/revenue, this means that user can access all opportunities (and associated revenue) that have a partner assigned to them.

Configuring Partner Channel Based Security

There is no session variable involved in the setting up for this data security.

A.1.46.1 Configuring BI Duty Roles

OBIA_PARTNER_ALL_INDIRECT_TRANSACTIONAL_DATA_SECURITY is the internal BI Duty Role used to define data filter for partner channel based data security. And by default, it only has one member Duty Role:

- OBIA_PARTNER_CHANNEL_ADMINISTRATIVE_ANALYSIS_DUTY

This Duty Role controls which subject areas and dashboard content the user gets access to. And as a member of OBIA_PARTNER_ALL_INDIRECT_TRANSACTIONAL_DATA_SECURITY, it ensures the partner channel based data security filter is applied in all queries involving lead or opportunity/revenue.

For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

A.1.47 How to Set Up CRM Partner Account Team Based Security for Oracle Fusion

Overview

Oracle Fusion CRM partner account team based security is applied when fusion channel account manager access partner owned opportunity/revenue. Partner channel account managers should be able to access all opportunities/revenue owned by the partner organization on whose partner account team they are a member of.

Configuring Partner Account Team Based Security

The session variable USER_PARTY_ID is the resource party Id that uniquely defines the login user. It is initialized via session Init Block GET_PARTY_ID and then used in partner account team based data security role.

A.1.47.1 Configuring BI Duty Roles

OBIA_PARTNER_TEAM_DATA_SECURITY is the internal BI Duty Role to define data filter for partner account team based data security. By default, it has one member BI Duty Role:

- OBIA_PARTNER_CHANNEL_ACCOUNT_MANAGER_ANALYSIS_DUTY

This Duty Role controls which subject areas and dashboard content the user gets access to. And as a member of OBIA_PARTNER_TEAM_DATA_SECURITY, it ensures that the partner account team based data security filter is applied to all queries involving opportunity or revenue.

For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

A.1.48 How to Set Up Project Resource Management Security for E-Business Suite

Overview

Project Analytics supports security over following dimensions in Project Resource Management subject areas. In the Business Intelligence Applications solution, the 'Business Unit' entity refers to 'Operating Unit Organizations' in E-Business Suite. The list of Business Units that a user has access to, is determined by E-Business Suite grants.

Table A–103 Supported Project Resource Management Security subject areas

Project Resource Management Facts						
Securing Entity	**Resource Availability**	**Resource Requirement**	**Resource Utilization Assignment**	**Resource Utilization Capacity**	**Resource Utilization Expected**	**Employee Job/Competency**
Project Business Unit	N	Y	Y	N	Y	N
Project Organization	N	Y	Y	N	Y	N
Expenditure Business Unit	N	N	N	N	N	N
Contract Business Unit	N	N	N	N	N	N

Table A–103 (Cont.) Supported Project Resource Management Security subject areas

Project Resource Management Facts Securing Entity	Resource Availability	Resource Requirement	Resource Utilization Assignment	Resource Utilization Capacity	Resource Utilization Expected	Employee Job/Competency
Project	N	Y	Y	N	Y	N
Resource Organization	N	N	N	Y	Y	Y
Ledger	N	N	N	N	N	N

Configuring Project Resource Management For E-Business Suite

In order for data security filters to be applied, appropriate initialization blocks need to be enabled depending on the deployed source system.

> **Note:** On installation, initialization blocks are enabled for E-Business Suite R12. If you are deploying on a source system other than E-Business Suite R12, then you must enable the appropriate initialization blocks.

You must enable data security for Project Resource Management in E-Business Suite by enabling the initialization blocks listed below based on your E-Business Suite adaptor. Make sure that all Project Security initialization blocks for other adapters are disabled. If more than one source system is deployed then, you must also enable the initialization blocks of those source system.

Init Blocks

Init Blocks for E-Business Suite R11x only:

- Project Business Unit List RM EBS11x

Init Blocks for E-Business Suite R11x only:

- Project Business Unit List RM EBSR12

Init Blocks for both E-Business Suite R11x and R12:

- Project List RM EBS
- Project Organization List RM
- Project Resource Organization List

Configuration

1. In Oracle BI Administration Tool, edit the BI metadata repository (for example, OracleBIAnalyticsApps.rpd) in online mode, and select Manage, then Identity.
2. Double click on OBIA_PROJECT_DATA_SECURITY, navigate to Permissions, then Data Filters, and enable data security filters related to Resource Management Fact Tables.

   This activates Project based Security which is needed for Resource Management Module in E-Business Suite.

3. Double click on OBIA_PROJECT_RESOURCE_ORGANIZATION_DATA_SECURITY, navigate to Permissions, then Data Filters, and enable all data security filters related to Resource Management Fact Tables.

   This activates Resource Organization based Security which is needed for Resource Management Module in E-Business Suite.

4. Double click on OBIA_PROJECT_ORGANIZATION_DATA_SECURITY, navigate to Permissions, then Data Filters, and enable data security filters related to Resource Management Fact Tables.

   This activates Project Organization based Security which is needed for Resource Management Module in E-Business Suite.

5. Double click on OBIA_PROJECT_BUSINESS_UNIT_DATA_SECURITY, navigate to Permissions, then Data Filters, and enable data security filters related to Resource Management Fact Tables.

   This activates Project Business Unit based Security which is needed for Resource Management Module in E-Business Suite.

A.1.48.1 Configuring BI Duty Roles

The following BI Duty Roles are applicable to the Project Resource Management subject area.

- OBIA_EBS_PROJECT_EXECUTIVE_ANALYSIS_DUTY
- OBIA_EBS_PROJECT_MANAGEMENT_ANALYSIS_DUTY
- OBIA_EBS_PROJECT_DATA_SECURITY

These Duty Roles control the subject areas and dashboard content to which the user has access. These Duty Roles also ensure the data security filters are applied to all the queries. For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

A.1.49 How to Implement Procurement and Spend Analytics Security

This topic contains the following sections:

- Section A.1.49.1, "How to implement Hierarchy Based Security for Employee Expense Subject Areas"
- Section A.1.49.2, "How to implement Org Based Security for Employee Expense Subject Areas"
- Section A.1.49.3, "How to implement Procurement and Spend Subject Areas Security for Suppliers"
- Section A.1.49.4, "How to implement Procurement and Spend Security for Procurement users"
- Section A.1.49.5, "Other Security in Procurement and Spend"

About Duty Roles

The following sections explain which Duty Roles you need to deploy for each functional area. Duty Roles control which subject areas and dashboard content a user can access. Duty Roles also ensure that appropriate data security filters are applied to the SQL queries that power the dashboards and reports.

For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles", or in FSM refer to the FSM Task 'How to Define New Groups and Mappings for Users and BI Roles'.

A.1.49.1 How to implement Hierarchy Based Security for Employee Expense Subject Areas

This section covers Hierarchy-based security for Employee Expense Subject Areas.

A.1.49.1.1 Overview The employee expense subject areas support security by employee hierarchy for line managers. The list of values a user has access to is determined by the grants in the source application system.

A.1.49.1.2 Enabling Initialization Blocks In order for data security filters to be applied, appropriate initialization blocks need to be enabled depending on the deployed source system. For example, to enable security for EBS, enable Oracle EBS initialization block and make sure the initialization blocks of all other source systems are disabled.

To enable initialization blocks, follow the steps below:

1. In Oracle BI Administration Tool, edit the BI metadata repository (for example, OracleBIAnalyticsApps.rpd).
2. Choose Manage, then Variables.
3. Under Session – Initialization Blocks, open the initialization block that you need to enable.

   Use the table below for guidance on which Initialization Blocks to enable for your Source System.
4. Clear the **Disabled** check box.
5. Save the metadata repository (RPD file).

The table below shows which Initialization Blocks need to be enabled for each Source System.

Table A–104 List of Source Systems and related Initialization Blocks

Source System	Initialization Block
Oracle Fusion Applications	HR Security Person ID List (Fusion)
Oracle EBS	HR Security Person ID List (EBS)
Oracle PeopleSoft	HR Security Person ID List (PeopleSoft)

A.1.49.1.3 Configuring BI Duty Roles

For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles", or in FSM refer to the FSM Task 'How to Define New Groups and Mappings for Users and BI Roles'.

The following BI Duty Roles are applicable to the Employee Expense Subject Areas:

Table A–105 List of BI Duty Roles and Related Subject Areas

Role	Employee Expenses - Credit Card	Employee Expenses - Overview	Employee Expenses - Violations
OBIA_LINE_MANAGER_ EXPENSE_ANALYSIS_DUTY	X	X	X
OBIA_AU_LINE_MANAGER_ EXPENSE_ANALYSIS_DUTY	X	X	X

A.1.49.2 How to implement Org Based Security for Employee Expense Subject Areas

This section covers Org-based security for Employee Expense Subject Areas.

A.1.49.2.1 Overview The employee expense subject areas support security by Business Unit for corporate card administrators, expense managers, and spend executives. The list of values a user has access to is determined by the grants in the source application system.

A.1.49.2.2 Enabling Initialization Blocks In order for data security filters to be applied, appropriate initialization blocks need to be enabled depending on the deployed source system. For example, to enable security for EBS, enable Oracle EBS initialization block and make sure the initialization blocks of all other source systems are disabled.

To enable initialization blocks, follow the steps below:

1. In Oracle BI Administration Tool, edit the BI metadata repository (for example, OracleBIAnalyticsApps.rpd).
2. Choose Manage, then Variables.
3. Under Session – Initialization Blocks, open the initialization block that you need to enable.

   Use the table below for guidance on which Initialization Blocks to enable for your Source System.
4. Clear the **Disabled** check box.
5. Save the metadata repository (RPD file).

The table below shows which Initialization Blocks need to be enabled for each Source System.

Table A–106 List of Source Systems and related Initialization Blocks

Source System	Initialization Block
Oracle Fusion Applications	PROC_SPEND_AN:SECURITY:Employee Expense Corporate Card BU List PROC_SPEND_AN:SECURITY:Employee Expense Violation BU List
Oracle EBS	Operating Unit Org-based Security
Oracle PeopleSoft	Operating Unit Org-based Security

A.1.49.2.3 Configuring BI Duty Roles

For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles", or in FSM refer to the FSM Task 'How to Define New Groups and Mappings for

Users and BI Roles'.

The following BI Duty Roles are applicable to the Employee Expense Subject Areas:

Table A–107 List of BI Duty Roles and Related Subject Areas

Role	Employee Expenses - Credit Card	Employee Expenses - Overview	Employee Expenses - Violations
OBIA_CORPORATE_CARD_ ADMINISTRATION_ANALYSIS_ DUTY	X		
OBIA_EXPENSE_ MANAGEMENT_ANALYSIS_ DUTY			X
OBIA_PROCUREMENT_ EXECUTIVE_ANALYSIS_DUTY	X	X	X
Procurement and Spend Executive	X	X	X
Procurement and Spend Executive PSFT	X	X	X

A.1.49.3 How to implement Procurement and Spend Subject Areas Security for Suppliers

This section covers security for Suppliers.

A.1.49.3.1 Overview The procurement and spend subject areas support security for suppliers in the Fusion Applications. The list of values a user has access to is determined by the grants in the source application system.

A.1.49.3.2 Enabling Initialization Blocks In order for data security filters to be applied, appropriate initialization blocks need to be enabled depending on the deployed source system. For example, to enable security for EBS, enable Oracle EBS initialization block and make sure the initialization blocks of all other source systems are disabled.

To enable initialization blocks, follow the steps below:

1. In Oracle BI Administration Tool, edit the BI metadata repository (for example, OracleBIAnalyticsApps.rpd).
2. Choose Manage, then Variables.
3. Under Session – Initialization Blocks, open the initialization block that you need to enable.

   Use the table below for guidance on which Initialization Blocks to enable for your Source System.
4. Clear the **Disabled** check box.
5. Save the metadata repository (RPD file).

The table below shows which Initialization Blocks need to be enabled for each Source System.

Table A–108 List of Source Systems and related Initialization Blocks

Source System	Initialization Block
Oracle Fusion Applications	PROC_SPEND_AN:SECURITY:Procurement Supplier Access Level PROC_SPEND_AN:SECURITY:Procurement Supplier Access List

A.1.49.3.3 Configuring BI Duty Roles

For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles", or in FSM refer to the FSM Task 'How to Define New Groups and Mappings for Users and BI Roles'.

The BI Duty Role 'OBIA_SUPPLIER_ANALYSIS_DUTY' is applicable to these Subject Areas:

- Fact - Purchasing - Agreement
- Fact - Purchasing - Order
- Fact - Purchasing - Receipt
- Fact - Spend and AP Invoice Distribution
- Dim - Supplier
- Dim - Supplier Site

A.1.49.4 How to implement Procurement and Spend Security for Procurement users

This section covers security for Procurement users.

A.1.49.4.1 Overview The procurement and spend subject areas support security by agent security for procurement users. The list of values a user has access to is determined by the grants in the source application system.

A.1.49.4.2 Enabling Initialization Blocks In order for data security filters to be applied, appropriate initialization blocks need to be enabled depending on the deployed source system. For example, to enable security for EBS, enable Oracle EBS initialization block and make sure the initialization blocks of all other source systems are disabled.

To enable initialization blocks, follow the steps below:

1. In Oracle BI Administration Tool, edit the BI metadata repository (for example, OracleBIAnalyticsApps.rpd).
2. Choose Manage, then Variables.
3. Under Session – Initialization Blocks, open the initialization block that you need to enable.

   Use the table below for guidance on which Initialization Blocks to enable for your Source System.
4. Clear the **Disabled** check box.
5. Save the metadata repository (RPD file).

The table below shows which Initialization Blocks need to be enabled for each Source System.

Table A–109 List of Source Systems and related Initialization Blocks

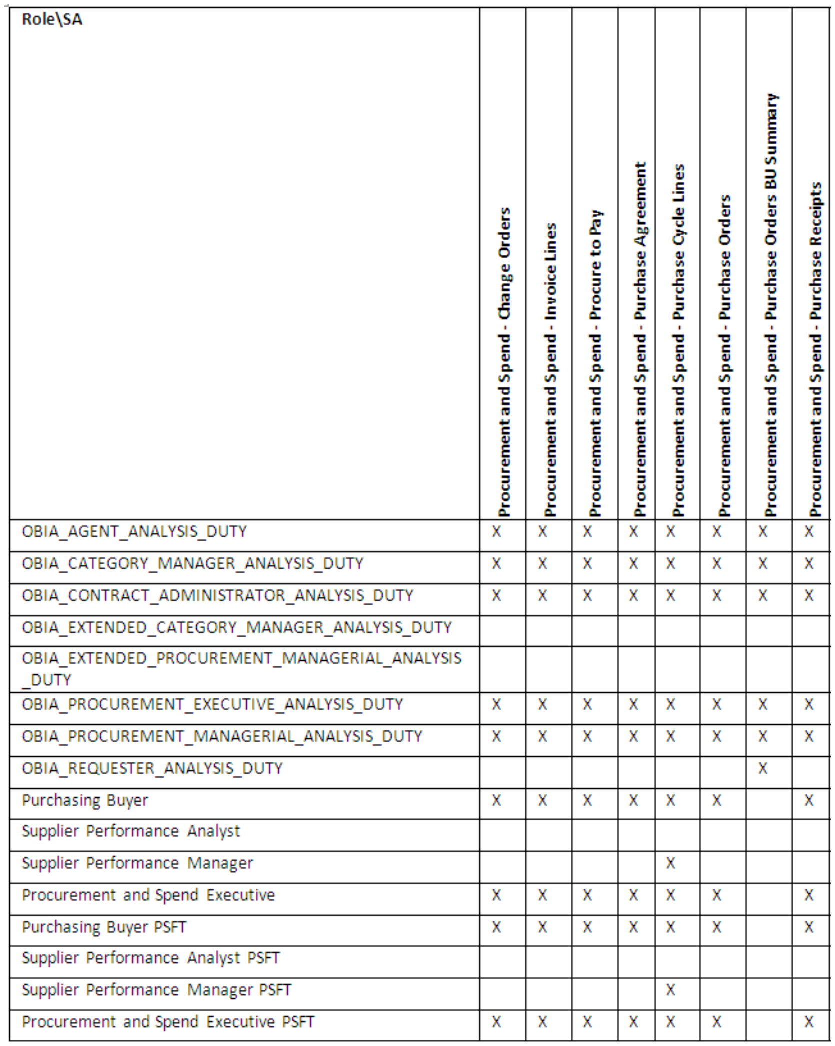
Source System	Initialization Block
Oracle Fusion Applications	PROC_SPEND_AN:SECURITY:Procurement Agreement BU List PROC_SPEND_AN:SECURITY:Procurement Agreement View Others BU List PROC_SPEND_AN:SECURITY:Procurement PurchaseOrder BU List PROC_SPEND_AN:SECURITY:Procurement PurchaseOrder View Others BU List PROC_SPEND_AN:SECURITY:Procurement Requisition BU List PROC_SPEND_AN:SECURITY:Procurement Requisition View Others BU List PROC_SPEND_AN:SECURITY:Procurement Sourcing BU List PROC_SPEND_AN:SECURITY:Procurement Sourcing View Others BU List PROC_SPEND_AN:SECURITY:Procurement Spend View BU List PROC_SPEND_AN:SECURITY:Procurement Supplier Site Access List Operating Unit Organizations
Oracle EBS	Operating Unit Org-based Security
Oracle PeopleSoft	Operating Unit Org-based Security

A.1.49.4.3 Configuring BI Duty Roles

For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles", or in FSM refer to the FSM Task 'How to Define New Groups and Mappings for Users and BI Roles'.

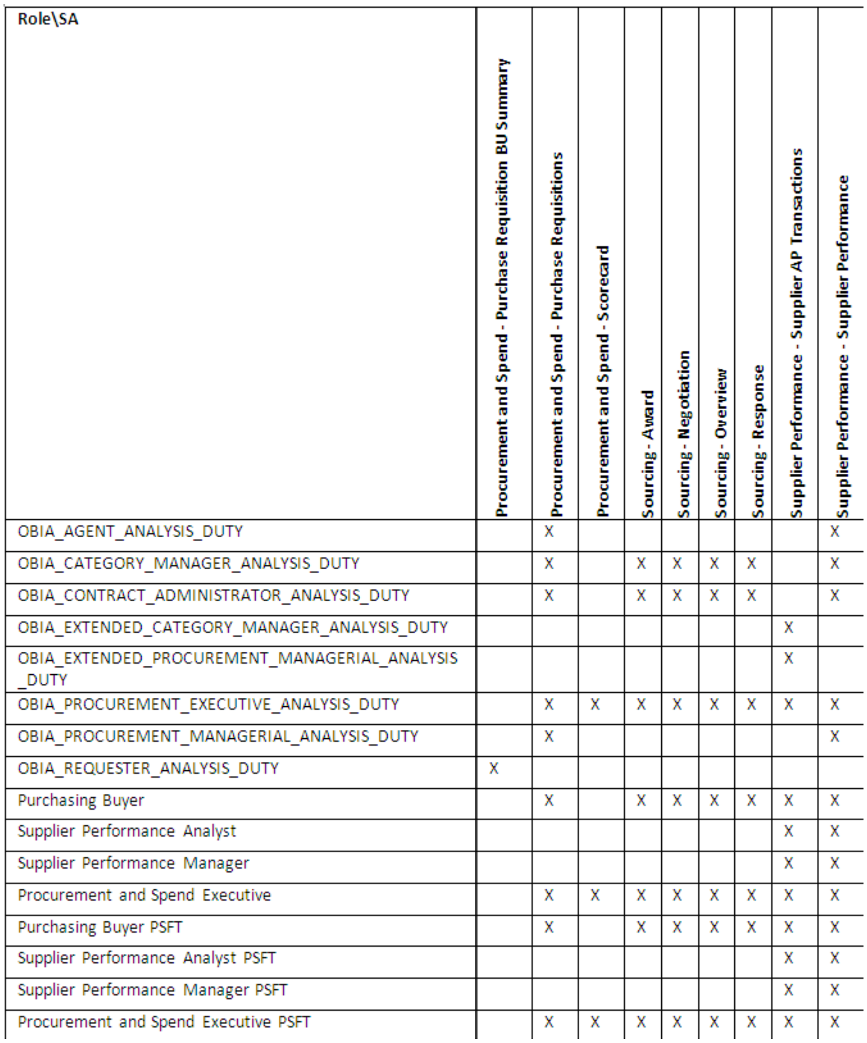
The two graphics below show which BI Duty Roles are applicable to the Procurement and Spend Subject Areas.

Graphic one:



Role\SA	Procurement and Spend - Change Orders	Procurement and Spend - Invoice Lines	Procurement and Spend - Procure to Pay	Procurement and Spend - Purchase Agreement	Procurement and Spend - Purchase Cycle Lines	Procurement and Spend - Purchase Orders	Procurement and Spend - Purchase Orders BU Summary	Procurement and Spend - Purchase Receipts
OBIA_AGENT_ANALYSIS_DUTY	X	X	X	X	X	X	X	X
OBIA_CATEGORY_MANAGER_ANALYSIS_DUTY	X	X	X	X	X	X	X	X
OBIA_CONTRACT_ADMINISTRATOR_ANALYSIS_DUTY	X	X	X	X	X	X	X	X
OBIA_EXTENDED_CATEGORY_MANAGER_ANALYSIS_DUTY								
OBIA_EXTENDED_PROCUREMENT_MANAGERIAL_ANALYSIS_DUTY								
OBIA_PROCUREMENT_EXECUTIVE_ANALYSIS_DUTY	X	X	X	X	X	X	X	X
OBIA_PROCUREMENT_MANAGERIAL_ANALYSIS_DUTY	X	X	X	X	X	X	X	X
OBIA_REQUESTER_ANALYSIS_DUTY							X	
Purchasing Buyer	X	X	X	X	X	X		X
Supplier Performance Analyst								
Supplier Performance Manager					X			
Procurement and Spend Executive	X	X	X	X	X	X		X
Purchasing Buyer PSFT	X	X	X	X	X	X		X
Supplier Performance Analyst PSFT								
Supplier Performance Manager PSFT					X			
Procurement and Spend Executive PSFT	X	X	X	X	X	X		X

Graphic two:



Role\SA	Procurement and Spend - Purchase Requisition BU Summary	Procurement and Spend - Purchase Requisitions	Procurement and Spend - Scorecard	Sourcing - Award	Sourcing - Negotiation	Sourcing - Overview	Sourcing - Response	Supplier Performance - Supplier AP Transactions	Supplier Performance - Supplier Performance
OBIA_AGENT_ANALYSIS_DUTY		X							X
OBIA_CATEGORY_MANAGER_ANALYSIS_DUTY		X		X	X	X	X		X
OBIA_CONTRACT_ADMINISTRATOR_ANALYSIS_DUTY		X		X	X	X	X		X
OBIA_EXTENDED_CATEGORY_MANAGER_ANALYSIS_DUTY								X	
OBIA_EXTENDED_PROCUREMENT_MANAGERIAL_ANALYSIS_DUTY								X	
OBIA_PROCUREMENT_EXECUTIVE_ANALYSIS_DUTY		X	X	X	X	X	X	X	X
OBIA_PROCUREMENT_MANAGERIAL_ANALYSIS_DUTY		X							X
OBIA_REQUESTER_ANALYSIS_DUTY	X								
Purchasing Buyer		X		X	X	X	X	X	X
Supplier Performance Analyst								X	X
Supplier Performance Manager								X	X
Procurement and Spend Executive		X	X	X	X	X	X	X	X
Purchasing Buyer PSFT		X		X	X	X	X	X	X
Supplier Performance Analyst PSFT								X	X
Supplier Performance Manager PSFT								X	X
Procurement and Spend Executive PSFT		X	X	X	X	X	X	X	X

A.1.49.5 Other Security in Procurement and Spend

To implement security for executive roles or to extend cross functional security, refer to the following topics:

- Section A.1.42, "How To Customize Extended Cross Functional Security for Employee Expenses"
- Section A.1.43, "How To Customize Extended Cross Functional Security for Accounts Payables"
- Section A.1.45, "How To Customize Security for Procurement Executive / Spend Analyst".

A.1.50 How to Set Up CRM Resource Hierarchy Based Security for Oracle Fusion

Overview

Resource hierarchy based security is widely used in many CRM subject areas, such as Sales, Marketing and Partner Management. Resource based security control starts with the current login user. The login user's party Id and the levels that the login user belongs to in resource hierarchy are then used as part of the data filter condition in queries.

There are variations of the resource hierarchy based security rule when it is applied in different areas, although they are all resource-based by nature.

For Opportunity and Revenue, visibility is granted to the login user as:

- A member of the opportunity team.

- Direct manager or above in the managerial hierarchy of the team member.

For Resource Quota, visibility is granted to the login user as:

- The resource that the resource quota is created for.

- Direct manager or above in the managerial hierarchy of the owner.

For Leads, visibility is granted to the login user as:

- A member of the lead team.

- Direct manager or above in the managerial hierarchy of the team member.

For Sales Campaigns, visibility is granted to the login user as:

- Direct owner of the campaign.

- Direct manager or above in the managerial hierarchy of the owner.

Configuring Resource Hierarchy Based Security

There are 2 session variables used in resource hierarchy based data security roles.

- RESOURCE_HIER_LEVEL_LIST contains the list of all the possible levels that the login user belongs to. This variable is initialized by session Init Block 'Resource Hierarchy Level List'.

- USER_PARTY_ID is the resource party Id that uniquely defines the login user. This variable is initialized by session Init Block GET_PARTY_ID.

A.1.50.1 Configuring BI Duty Roles

All the Resource Hierarchy Based security roles should be defined as member of the internal role OBIA_RESOURCE_HIERARCHY_DATA_SECURITY, under which, all the necessary data filters are defined. In the default (that is, installed) configuration, OBIA_RESOURCE_HIERARCHY_DATA_SECURITY has the following members.

- OBIA_LEAD_ANALYSIS_DUTY
- OBIA_PARTNER_ANALYSIS_DUTY
- OBIA_PARTNER_ADMINISTRATIVE_ANALYSIS_DUTY
- OBIA_PARTNER_CHANNEL_ACCOUNT_MANAGER_ANALYSIS_DUTY
- OBIA_PARTNER_CHANNEL_ADMINISTRATIVE_ANALYSIS_DUTY
- OBIA_PARTNER_CHANNEL_ANALYSIS_DUTY
- OBIA_OPPORTUNITY_LANDSCAPE_ANALYSIS_DUTY
- OBIA_SALES_CAMPAIGN_ANALYSIS_DUTY
- OBIA_SALES_EXECUTIVE_ANALYSIS_DUTY
- OBIA_SALES_MANAGERIAL_ANALYSIS_DUTY
- OBIA_SALES_TRANSACTIONAL_ANALYSIS_DUTY

These Duty Roles control the subject areas and dashboard content to which the user has access.

For more information about how to define new groups and mappings for Users and BI Roles, see Section A.1.13, "How to Define New Groups and Mappings for Users and BI Roles".

A.1.51 How to Set Up Security for PIM in Oracle EBS

Overview

In order for data security filters to be applied, appropriate initialization blocks need to be enabled depending on the deployed source system. For example, to enable security for EBS, enable Oracle EBS initialization block and make sure the initialization blocks of all other source systems are disabled. The PIM repository has two initialization blocks which are applicable only to Fusion. These must be manually disabled for an EBS source.

Initialization blocks which have to be disabled are ItemClass and PIM_EGO_ENABLED.

To disable initialization blocks, follow the steps below:

1. In Oracle BI Administration Tool, edit the BI metadata repository (for example, OracleBIAnalyticsApps.rpd).
2. Choose Manage, then Variables.
3. Right-click the ItemClass and PIM_EGO_ENABLED initialization blocks and select Disable.

A.1.52 How to Set Up Security for Enterprise Asset Management Analytics

Overview

Enterprise Asset Management supports security over Maintenance Organizations in Enterprise Asset Management subject areas. The list of Maintenance Organizations that a user has access to, is determined by the grants in EBS.

Configuring Maintenance Organization Data Security

In order for data security filters to be applied, appropriate initialization blocks need to be enabled depending on the deployed source system. To enable Maintenance Organization Data Security for EBS, enable Oracle EBS initialization block and make sure the initialization blocks of all other source systems are disabled.

To enable initialization blocks, follow the steps below:

1. In Oracle BI Administration Tool, edit the BI metadata repository (for example, OracleBIAnalyticsApps.rpd).
2. Navigate to Manage and open variables from menu ('MAINT_ORG_LIST').
3. Under Session – Initialization Blocks, open the initialization block that you need to enable (Maintenance Organizations EBS).
4. Clear the **Disabled** check box.
5. Save the metadata repository (RPD file).

Configuring BI Duty Roles

The BI Duty Roles below are applicable to the Enterprise Asset Management subject area. These Duty Roles control which subject areas and dashboard content users have access to. These Duty Roles also ensure the data security filters are applied to all the queries.

- Operations Manager

  EAM Operation Analyst for EBS. This Role provides secured access to VP Operation, Plant Manager, and EAM Analyst about organization level visibility to utilize Asset optimally.

- Maintenance Super User

  EAM Super User for EBS. This role provides secured access to Maintenance Planner and Super User for planning and managing asset maintenance activities.

- Maintenance User

  EAM Maintenance Use for EBS. This role provides secured access to Maintenance User for completing tasks assigned to maintenance work orders.

Duty Roles Subject Areas

Duty Roles control which subject areas and dashboard content the user has access to, as well as ensure data security filters are applied to all queries. The Duty Roles provide access to the following subject areas.

- Operations Manager
  - EAM - Asset Failure Analysis
  - EAM - Asset History
  - EAM - Asset Maintenance Cost
  - EAM - Asset Maintenance Work Orders
  - EAM - Asset Meter Reading
  - EAM - Asset Quality
  - EAM - MRO Inventory
  - EAM - Maintenance Material Usage
  - EAM - Maintenance Resource Usage
  - EAM - Maintenance Resource Availability
- Maintenance Super User
  - EAM - Asset Failure Analysis
  - EAM - Asset Maintenance Work Orders
  - EAM - Asset Meter Reading
  - EAM - Asset Quality
  - EAM - Maintenance Material Usage
  - EAM - Maintenance Resource Usage
  - EAM - Maintenance Resource Availability
- Maintenance User
  - EAM - Asset Failure Analysis
  - EAM - Asset Failure Analysis
  - EAM - Asset Failure Analysis

- EAM - Asset Failure Analysis

Index