# Oracle® Fusion Middleware

Security Guide for Oracle Business Intelligence Applications

11g Release 1 (11.1.1.7)

**E37986-01**

April 2013

Explains security considerations for Oracle BI Applications.

ORACLE

Oracle Fusion Middleware Security Guide for Oracle Business Intelligence Applications, 11g Release 1 (11.1.1.7)

E37986-01



Primary Author: Dan Hilldale

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

# Contents

## Index

# 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 for a list of related Oracle Business Intelligence Applications documents: http://docs.oracle.com/cd/E38317_01/index.htm

# 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. |

# What's New in This Guide

Oracle BI Applications 11.1.1.7 is a new release. This chapter describes features in Oracle Business Intelligence Applications 11g Release 1 (11.1.1.7) documented in this guide, *Oracle Fusion Middleware Security Guide for Oracle Business Intelligence Applications*, that may be of note.

## Notable Features in Oracle BI Applications Documented in This Guide

New features in Oracle BI Applications 11g Release 1 (11.1.1.7) that are documented in this guide include the following:

#### Functional Setup Manager Security Tasks

Security for different offerings in Oracle BI Applications is configured using guidance in informational Functional Setup Manager tasks.

# 1 Integrating Security for Oracle BI Applications

This chapter is for security administrators. It describes the security features in Oracle Business Intelligence Applications.

This chapter contains the following topics:

- Section 1.1, "Introduction"
- Section 1.2, "Extending Security in Oracle BI Applications"
- Section 1.3, "Using Oracle BI Applications Functional Setup Manager Informational Tasks to Set Up Security"

## 1.1 Introduction

This section contains the following topics:

Section 1.1.1, "High Level Steps for Setting Up Security in Oracle BI Applications"

Section 1.1.2, "What Tools Configure Security in Oracle Business Intelligence Applications?"

Section 1.1.3, "What Security Levels Does Oracle BI Applications Use?"

Section 1.1.4, "About Duty Roles in Oracle BI Applications"

Section 1.1.6, "Checking Oracle BI Applications User Responsibilities"

Section 1.1.7, "About Managing Presentation Services Catalog Privileges in Oracle Business Intelligence"

Section 1.1.8, "About Object-Level Security"

Section 1.1.9, "About Data-Level Security"

Section 1.1.10, "About User-Level Security"

### 1.1.1 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 2.1, "Introduction" to get an overview of security concepts, tools, and terminology.

   For background information about security in the Oracle Business Intelligence Enterprise Edition platform, see *Oracle Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition*.

2. Learn about duty roles and how they control user privileges. For more information, see Section 1.1.4, "About Duty Roles in Oracle BI Applications".
3. The Oracle BI Applications provisioning process creates default BI duty roles and groups.
4. Define users, groups, and security mappings. For more information, see Section 1.1.5, "How to Define New Groups and Mappings for Users and BI Roles"
5. Use Functional Setup Manager tasks for your module to properly set up security. For more information, see Section 1.3, "Using Oracle BI Applications Functional Setup Manager Informational Tasks to Set Up Security"

### 1.1.2 What Tools Configure Security in Oracle Business Intelligence Applications?

Security settings for Oracle Business Intelligence Enterprise Edition are made in the following Oracle Business Intelligence components:

- Oracle BI Applications Functional Setup Manager

  Use Oracle BI Applications Functional Setup Manager informational tasks to set up security for Oracle BI Applications offerings and modules. For detailed information, see *Oracle Fusion Middleware Configuration Guide for Oracle Business Intelligence Applications*.

- Oracle BI Administration Tool

  Use the 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 groups in the embedded 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*.

### 1.1.3 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 1.1.8, "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 1.1.9, "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 1.1.10, "About User-Level Security."

## 1.1.4 About Duty Roles in Oracle BI Applications

Object-level and data-level security are implemented in Oracle BI Applications using duty roles. Duty roles define a set of permissions granted to a user or group. 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.

To view pre-configured duty roles in the RPD, select **Manage**, then select **Identity** in the Oracle BI Administration Tool. 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 the Administration Tool in online mode.

For detailed information about setting up and managing duty roles, see *Oracle Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition*. For information about using the Oracle BI Administration Tool Identity Manager to apply data access security in the Oracle BI repository, see *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition*.

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 group (also called enterprise role), then user. It is a best practice to use this structure when setting up security.

The remainder of this topic describes how Oracle BI Applications controls user access using roles, and contains the following section:

### 1.1.4.1 Viewing, Creating, and Editing Duty Roles

An administrator can view, modify, and create duty roles in the Oracle Enterprise Manager Fusion Middleware Control. To view roles:

1. Log in to Oracle Enterprise Manager Fusion Middleware Control as an administrator.
2. Expand Business Intelligence, right-click coreapplication, and select Security and then Duty Roles.

   A list of the configured duty roles is displayed. By default, Oracle BI includes four duty roles: BISystem, BIAdministrator, BIAuthor, and BIConsumer. When BI Applications are installed, additional pre-defined duty roles are created that map

to operational application responsibilities, so the list of pre-configured duty roles depends on your installation. These duty roles have pre-defined permissions for the repository objects, and pre-defined data filters. Permissions for the roles are defined in the BI Administration Tool.

3. Click Create to create a new duty role and map it to LDAP users and groups; note that each duty role has a corresponding LDAP group to which it is assigned. To edit an duty role's mappings, select it in the list and click Edit.

#### 1.1.4.2 Authorizing User Access Using Roles

Authorization for Oracle BI Applications is controlled by security policies (Oracle BI Applications privileges) defined for users using a role-based model.

Every Oracle Applications user is hired by their company to perform a role in the organization, for example, Payroll Manager or Accounts Payable Manager. An Oracle Applications user is granted a role and thus inherits one or more associated privileges that were granted to the role.

It is possible to grant multiple duty roles to a user; however Oracle recommends that job roles, also known as enterprise roles and groups, are defined in such a way that need to grant multiple duty roles to user should be minimized.

Note that in cases where Oracle Business Intelligence Enterprise Edition test servers are 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, a refresh of the LDAP GUIDs is needed for the system to function correctly. 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 environments, it is optional for other source applications.

### 1.1.5 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. A separate set of roles are used to implement BI object security and BI data security.

To simplify BI duty role provisioning to application users, Oracle BI Applications also provides a BI duty role hierarchy of the roles used in BI object security and BI data security. The BI duty role hierarchy is structured in such a way that for each application area, typically a single BI duty role encapsulates the BI object and data security role hierarchy that is built using multiple other BI duty roles. This single BI duty role can then be provisioned to the end user to enable access to a specific BI application.

For example, the BI duty role 'Fixed Asset Accounting Manager EBS' provides the encapsulation for EBS Fixed Asset Accounting security. The end user just needs to be provisioned with this single BI duty role – there is no need to separately provision underlying data/object security BI duty roles for this application to the user.

There are two ways to provision a BI duty role to a BI end user:

- Use Fusion Middleware (FMW) to provision a BI duty role to an end user, as described in Section 1.1.5.1, "How to Use Fusion Middleware to Provision an End User".

  **Note**: You use this provisioning method if you are using Fusion Middleware to authenticate the user.

- Use an RPD initilalization block to associate a BI duty role to an end user, as described in Section 1.1.5.2, "How to Use a Repository Initialization Block to Provision an End User".

  **Note**: You can only use this provisioning method if you are not using Fusion Middleware to authenticate the user.

#### 1.1.5.1 How to Use Fusion Middleware to Provision an End User

To use the FMW provisioning for BI duty role, the users and enterprise roles must be present in a LDAP and that LDAP should have been configured as the source for authentication for BI.

In this approach, you can use your existing enterprise roles to associate a BI duty role to an end user. If your installation has existing enterprise roles that you wish to use for BI security; you may want to consider using this approach.

For example, assume that an installation LDAP has enterprise role "ABC Corp Americas Account Manager", the users and enterprise roles are present in this LDAP, and this LDAP is used as source for authentication for the BI installation. Use Enterprise Manager (EM) of the BI instance and make the enterprise role "ABC Corp Americas Account Manager" a member of the BI duty role "Fixed Asset Accounting Manager EBS". After this association, all users that are members of enterprise role "ABC Corp Americas Account Manager" will inherit BI duty role "Fixed Asset Accounting Manager EBS".

Note that in this example, enterprise role "ABC Corp Americas Account Manager" is a custom enterprise role. Enterprise roles do not have to be provided by Oracle.

Oracle BI Applications also provides a sample set of default enterprise roles (also called groups) that inherit the BI duty role hierarchy. For example, BI Applications provide enterprise role "Fixed Asset Accounting Manager EBS", which is member of BI duty role "Fixed Asset Accounting Manager EBS". You can associate this enterprise role to your BI users. Any users made members of enterprise role "Fixed Asset Accounting Manager EBS" will automatically inherit BI duty role "Fixed Asset Accounting Manager EBS" and will have the correct security for Fixed Assets Accounting reporting for EBS. This association can be done in following ways:

- When you install BI Applications, the installation provides a default LDAP using Weblogic Embedded LDAP. If you plan to use this LDAP as the LDAP for users and enterprise roles, then you can upload all default enterprise roles provided by BI Applications. These enterprise roles are provided as a .ldif file and once the LDIF file is uploaded to Weblogic Embedded LDAP, then enterprise roles like "Fixed Asset Accounting Manager EBS" are available in the embedded LDAP. You can define your BI users in this LDAP and associate the users to one or more enterprise roles. Creation of users and association of users to enterprise roles in Weblogic Embedded LDAP is done using Weblogic Administration Console.

- If your installation has a existing LDAP for authentication, and you do not wish to use the Weblogic Embedded LDAP that comes with the installation, then you can add the enterprise role "Fixed Asset Accounting Manager EBS" to your LDAP and associate this enterprise role with existing users. Any users made members of

enterprise role "Fixed Asset Accounting Manager EBS" in your LDAP inherit BI duty role "Fixed Asset Accounting Manager EBS" and will have the correct security for this application. Addition of enterprise roles to your LDAP and association of enterprise roles to user should be done using native LDAP tools.

The FMW approach to BI duty role user association can be used only if Fusion Middleware is also used for the user authentication. If the user is being authenticated by a method other than Fusion Middleware Authentication, then Fusion Middleware cannot be used to associate a BI duty role to a user. For example, if a user is being authenticated using initialization block authentication, then the user association with a BI duty role cannot be done using Fusion Middleware.

#### 1.1.5.2 How to Use a Repository Initialization Block to Provision an End User

Oracle BI Applications provides an initialization block named "Authorization" that queries the roles/responsibilities associated to the user in the source system and populates an Oracle BI Enterprise Edition variable called GROUP. Oracle BI EE associates BI duty roles to the users that are populated in the GROUP variable.

The initialization block approach to BI duty role association can be used only if user is not being authenticated using Fusion Middleware.

For example, to associate BI duty role "Fixed Asset Accounting Manager EBS" to a user using the initialization block approach, perform the following steps:

1. In the Administration Tool, enable the "Authorization" initialization block if disabled.
2. Update the initialization 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 initialization block.
3. Create a responsibility named "Fixed Asset Accounting Manager EBS" in the E-Business Suite source system and assign it to the user.
4. When the initialization block is run for the user, the GROUP variable is populated with the value "Fixed Asset Accounting Manager EBS". The BI Server will then assign BI duty role "Fixed Asset Accounting Manager EBS" to the user, in effect assigning the BI duty role of same name. If the user has multiple responsibilities in source system, the GROUP variable will contain name of all the responsibilities.

Oracle BI EE assign BI duty roles that match any names contained in the GROUP variable. If one of the names within GROUP variable does not match any BI duty role 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, the user will be assigned BI duty roles (A, B, C). The value D will be ignored.

### 1.1.6 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.

## 1.1.7 About Managing Presentation Services Catalog Privileges in Oracle Business Intelligence

When you add a new catalog privilege to an 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.

## 1.1.8 About Object-Level Security

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

- Section 1.1.8.1, "Metadata Object-Level Security in the RPD"
- Section 1.1.8.2, "Metadata Object-Level Security in Presentation Services"

### 1.1.8.1 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 let permissions 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'.

#### 1.1.8.2 Metadata Object-Level Security in Presentation Services

Access to Oracle BI Presentation Services objects, such as dashboards, pages, reports, and Web folders, are 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*.

### 1.1.9 About Data-Level Security

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

- Section 1.1.9.1, "Overview of Data-Level Security in Oracle BI Applications"
- Section 1.1.9.2, "Implementing Data-Level Security in the Oracle BI Repository"
- Section 1.1.9.3, "Initialization Blocks Used for Data-Level Security in Oracle BI Applications"
- Section 1.1.9.4, "Data-Level Security Duty Roles in Oracle BI Applications"
- Section 1.1.9.5, "About Data-Level Security Design in Oracle BI Applications"

#### 1.1.9.1 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*.

#### 1.1.9.2 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 1.1.9.3, "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*.

#### 1.1.9.3 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 tasks. For more information about using these FSM tasks, see *Oracle Fusion Middleware Configuration Guide for Oracle Business Intelligence Applications*. 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'.

#### 1.1.9.4 Data-Level Security Duty Roles in Oracle BI Applications

There are many pre-built duty roles used in Oracle BI Applications. Some duty roles share the same name as responsibilities for Siebel CRM and Oracle EBS applications and roles for PeopleSoft applications. A user who has any of these responsibilities or roles in the source application will be a member of the corresponding duty role automatically upon logging in to the Oracle BI application. Other duty roles based on similar objects in the source application can be added to the policy store, and then added to these data-level duty roles, if you need the corresponding data filters to apply to any additional group of users. For details about the duty roles that are supported in Oracle BI Applications, 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'.

#### 1.1.9.5 About Data-Level Security Design in Oracle BI Applications

As discussed in the preceding sections, 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 each user is allowed to see. A user is assigned an 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.

### 1.1.10 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 server and policy store in Oracle Business Intelligence Enterprise Edition. For more information, see *Oracle Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition*.

### 1.1.11 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 granted one of the following roles:

- BI Applications Administrator Duty (BIA_ADMINISTRATOR_DUTY)

  Users with the BI Applications Administrator duty role have access to all Configuration Manager User Interfaces and all Functional Setup Manager User Interfaces. For 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 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 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.

## 1.1.12 About Permissions in Configuration Manager and Functional Setup Manager

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

- Section 1.1.12.1, "About Permissions in Configuration Manager"
- Section 1.1.12.2, "About Permissions in Functional Setup Manager"

### 1.1.12.1 About Permissions in Configuration Manager

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

***Table 1–1 List of 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 |

***Table 1–1 (Cont.) List of 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 | 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 |
| 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 |

#### 1.1.12.2 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

### 1.1.13 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*

## 1.2 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*

---

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

Security for different offerings in Oracle BI Applications is configured using guidance in informational Functional Setup Manager tasks. For details about the informational tasks related to your offering, see *Oracle Fusion Middleware Configuration Guide for Oracle Business Intelligence Applications*.

# Index

## T



## U