Oracle® Business Intelligence Applications

Securing Business Intelligence Applications

12c (11.1.1.10.3 PS4)
F83297-03
December 2023

Oracle Business Intelligence Applications Securing Business Intelligence Applications, 12c (11.1.1.10.3 PS4)

F83297-03

Copyright © 2014, 2023, Oracle and/or its affiliates.

Primary Author: Hemala Vivek

Contributors: Nick Fry, Christine Jacobs, Padma Rao

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

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

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

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

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

Oracle®, Java, MySQL and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface

Functional Setup Manager - Statement of Direction v
Audience v
Documentation Accessibility v
Diversity and Inclusion v
Related Documentation vi
Conventions vi

1 Overview of Security Integration for Oracle BI Applications

Terminology Used In Security 1-1
What Security Components Are Installed By Default? 1-2
High-Level Steps for Setting Up Security in Oracle BI Applications 1-3
What Tools Configure Security in Oracle BI Applications? 1-3
Duty Roles for Access to Functional Setup Manager or Configuration Manager 1-4
Configuration Manager Permissions Reference 1-5
Functional Setup Manager Permissions Reference 1-6
About Managing Presentation Services Catalog Privileges in Oracle Analytics 1-7
What Security Levels Do Oracle BI Applications Use? 1-7
- About Object-Level Security 1-7
- About Data-Level Security 1-8
- Implement Data-Level Security in the Oracle BI Repository 1-9
- About User-Level Security 1-9

Related Documentation for Oracle BI Applications Security 1-10

2 Managing Duty Roles in Oracle BI Applications

Viewing Duty Roles for Oracle BI Applications 2-2
Provisioning BI Users with Duty Roles 2-4
Creating Duty Roles for Oracle BI Applications 2-5
User Access Using Roles 2-5

3 Setting Up Security with Functional Setup Manager

4 Extending Security in Oracle BI Applications

Preface

Oracle Business Intelligence Applications (Oracle BI 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 Analytics Server, 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.

Functional Setup Manager - Statement of Direction

Functional Setup Manager (FSM) has been desupported in the current release. Ignore the references to FSM that you might see in the online Help.

Audience

This document is intended for BI managers and implementers 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 that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing

technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Related Documentation

See the Oracle BI Applications documentation library for the complete set of Oracle BI 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.

1

Overview of Security Integration for Oracle BI Applications

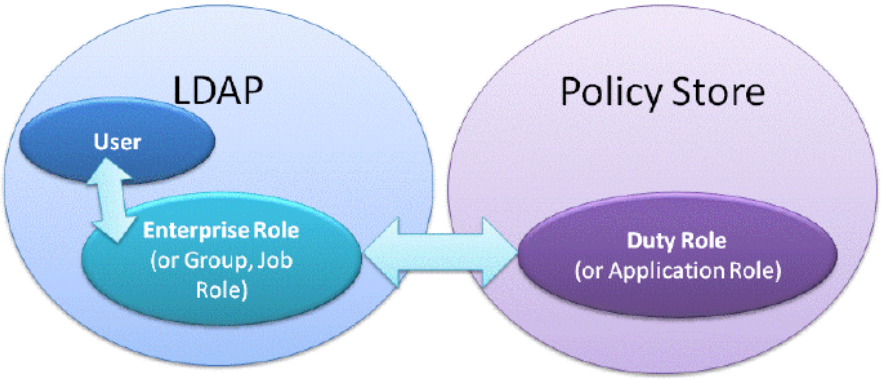
This topic describes key concepts related to security in Oracle Business Intelligence Applications (Oracle BI Applications).

Security administrators can read this topic to understand Oracle BI Applications security and its preconfigured implementation.

- Terminology Used in Security
- What Security Components Are Installed By Default?
- High-Level Steps for Setting Up Security in Oracle BI Applications
- What Tools Configure Security in Oracle BI Applications?
- Duty Roles for Access to Functional Setup Manager or Configuration Manager
- Configuration Manager Permissions Reference
- Functional Setup Manager Permissions Reference
- About Managing Presentation Services Catalog Privileges in Oracle BI
- What Security Levels Does Oracle BI Applications Use?
- Related Documentation for Oracle BI Applications Security

Terminology Used In Security

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



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

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

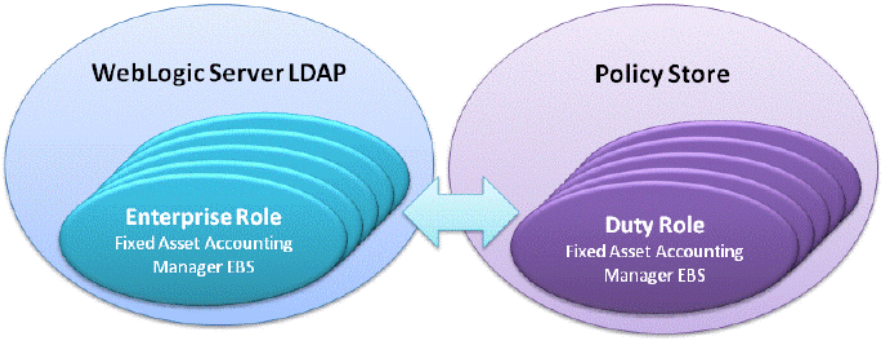
What Security Components Are Installed By Default?

After installing Oracle BI Applications on the Oracle Analytics platform, you get the following ready-to-use security components.

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

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

- Oracle BI Applications



For illustrative purposes, it is assumed that you are using the default Oracle 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. If you to deploy a different LDAP, such as Oracle Internet Directory, then you can migrate Users and Enterprise Roles from Oracle WebLogic Server LDAP to that LDAP.

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

Here are the high-level steps for setting up security in Oracle BI Applications.

This content in this guide supplements *Managing Security for Oracle Analytics Server*, and contains additional security information that is specific to Oracle BI Applications running on Oracle Analytics Server. In addition to the content in this guide, *Oracle Business Intelligence Applications Functional Configuration Reference* contains the security-related help topics that are included in the product UI.

1. Familiarize yourself with the overview of security concepts, tools, and terminology, in particular, Duty Roles and how they control user privileges.
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 (Configuration Manager), FSM, and ODI User, and assign an appropriate Duty Role to each User.
   - 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 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 FSM tasks to set up security for your Offerings and Functional Areas. See Setting Up Security with Functional Setup Manager.
   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).

See How to Define New Groups and Mappings for Users and BI Roles in *Oracle Business Intelligence Applications Functional Configuration Reference*.

What Tools Configure Security in Oracle BI Applications?

Use these tools to manage security settings in Oracle BI Applications.

- Oracle BI Applications Functional Setup Manager (FSM)

  Use FSM informational tasks to set up security for Oracle BI Applications offerings and modules. See Setting Up Security with Functional Setup Manager.

- 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. See Work with Logical Tables, Joins, and Columns in *Managing Metadata Repositories for Oracle Analytics Server*.

- 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. See *Managing Security for Oracle Analytics Server*.

- Oracle Enterprise Manager Fusion Middleware Control

  Use Oracle Enterprise Manager Fusion Middleware Control to manage the policy store, Duty Roles, and permissions for determining functional access. See *Securing Resources Using Roles and Policies for Oracle WebLogic Server*.

- 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. See *Managing Security for Oracle Analytics Server*.

Duty Roles for Access to Functional Setup Manager or Configuration Manager

Duty Roles define a set of permissions granted typically to an Enterprise Role.

To access Configuration Manager or FSM (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 FSM User Interfaces.

- 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 FSM, 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 FSM, 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.

To grant users access to Oracle BI Applications components, see User Access to Configuration Manager, FSM, and Oracle Data Integrator in *Oracle Business Intelligence Applications Installation Guide*.

Configuration Manager Permissions Reference

The screens you can view in Configuration Manager depend on the duty roles to which you are assigned.

This table shows the list of Configuration Manager screens visible to each of the Oracle BI Applications roles.

Oracle BI Applications Duty Role	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 FSM	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
BI Applications Functional Developer	Functional Configurations - 'Perform Functional Configurations' link to launch FSM	BIA_FUNCTIONAL_SETUPS_PRIV

Oracle BI Applications Duty Role	Configuration Manager screen	Associated Privilege
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

Functional Setup Manager Permissions Reference

FSM roles are associated with Oracle BI Applications roles.

- The BI Applications Administrator role (BIA_ADMINISTRATOR_DUTY) is associated to the following FSM 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

About Managing Presentation Services Catalog Privileges in Oracle Analytics

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 Analytics environment.

To register the catalog privilege, both the administrator and the user must perform the following tasks:

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

  To manage Presentation Services catalog privileges, see *Managing Security for Oracle Analytics Server*.
- Users belonging to that Duty Role must log out from the Oracle BI Applications (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.

What Security Levels Do Oracle BI Applications Use?

Security in Oracle BI Applications can be classified broadly into 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.
- 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.
- 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.

About Object-Level Security

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-Level Security in the Oracle BI Repository

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. 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 Analytics 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.

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. To manage object-level security in Presentation Services, see *Managing Security for Oracle Analytics Server*.

About Data-Level Security

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.

During installation and configuration, you must make sure the correct Duty Roles and initialization blocks are set up for your environment.

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

Initialization blocks are deployed as part of your configuration using guidance provided in FSM tasks. See Setting Up Security with Functional Setup Manager.

To use FSM tasks, see Roadmap for Functional Configuration in *Oracle Business Intelligence Applications Configuration Guide*.

To use initialization blocks in Oracle Analytics, see Work with Initialization Blocks.

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.

Implement Data-Level Security in the Oracle BI Repository

Data-level security in Oracle BI Applications is implemented in three major steps.

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 Dimension Ids for each user session in order to restrict row-level access to factual or dimensional data. See About Data-Level Security for a description of the preconfigured initialization blocks.
2. Set up the joins to the appropriate security tables in the metadata physical and logical layers.
3. Set up the data filters for each Duty Role on each logical table that needs to be secured.

   See Apply Data Access Security to Repository Objects in *Managing Metadata Repositories for Oracle Analytics Server*.

About User-Level Security

User security concerns the authentication and confirmation of the identity of the user based on the credentials provided, such as user name and password. By default, user-level security is set up in the embedded Oracle WebLogic Server LDAP and Policy Store in Oracle Analytics Server.

See *Managing Security for Oracle Analytics Server*.

Related Documentation for Oracle BI Applications Security

Oracle offers additional documentation to help you configure security for Oracle BI Applications.

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

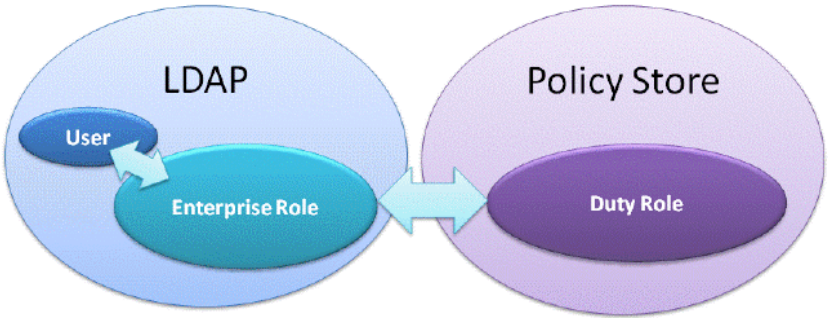
- Oracle Fusion Applications security; see the Fusion Applications Security documentation.
- Oracle Analytics Server security implementation; see Oracle Analytics Server documentation Oracle Analytics Server documentation:
  - *Managing Security for Oracle Analytics Server*
  - *Managing Metadata Repositories for Oracle Analytics Server*

2

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.

This figure illustrates how users are assigned to Enterprise Roles in the LDAP, which are associated with Duty Roles in the Policy Store.



Duty Roles are typically related to either data or object security. For example, the Oracle BI Applications repository (OracleBIApps.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.

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.

Matching Pre-Configured Duty Roles with 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 Applications, select **Signed In As**, ***username***, then **My Account**. Then, click the Application Roles 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.

Tools to View Pre-configured Duty Roles

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

- Oracle BI Administration Tool

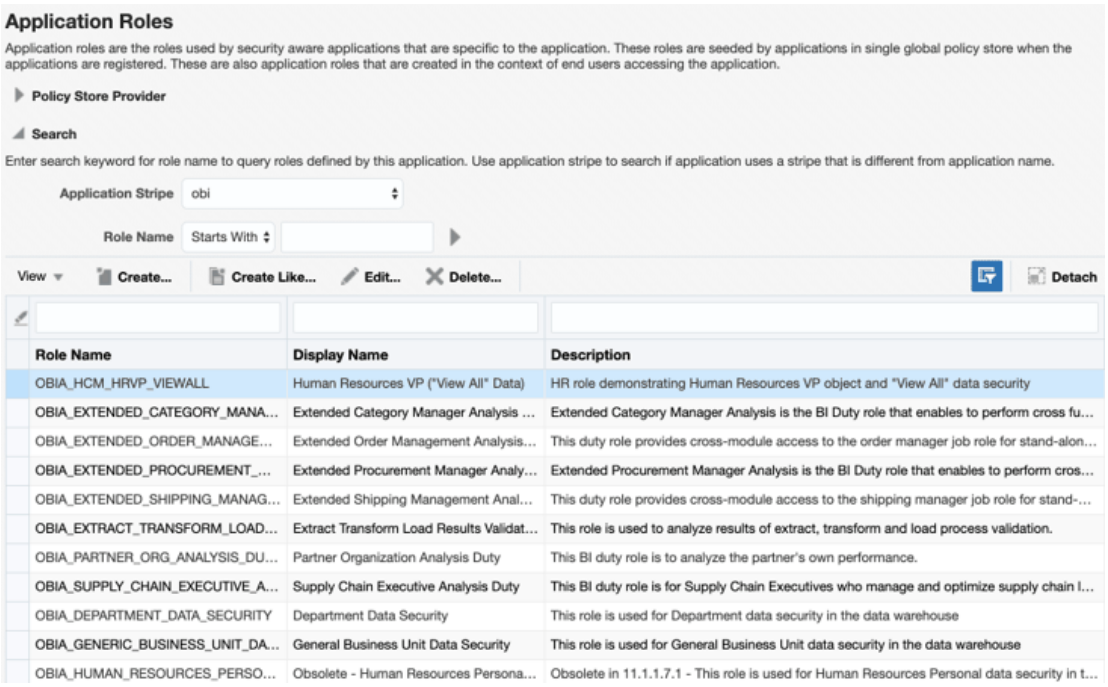
  To view pre-configured Duty Roles using Oracle BI Administration Tool, open the repository, select **Manage**, then **Identity**. Duty Roles are visible in the Identity Manager dialog in online mode. In offline mode, only Duty Roles that have had permissions, filters, or query limits set for them appear. 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 , see Viewing Duty Roles for Oracle BI Applications.
- Oracle Authorization Policy Manager (APM) - 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.

Viewing Duty Roles for Oracle BI Applications

You can view the Duty Roles for Oracle BI Applications using Oracle Enterprise Manager Fusion Middleware Control.

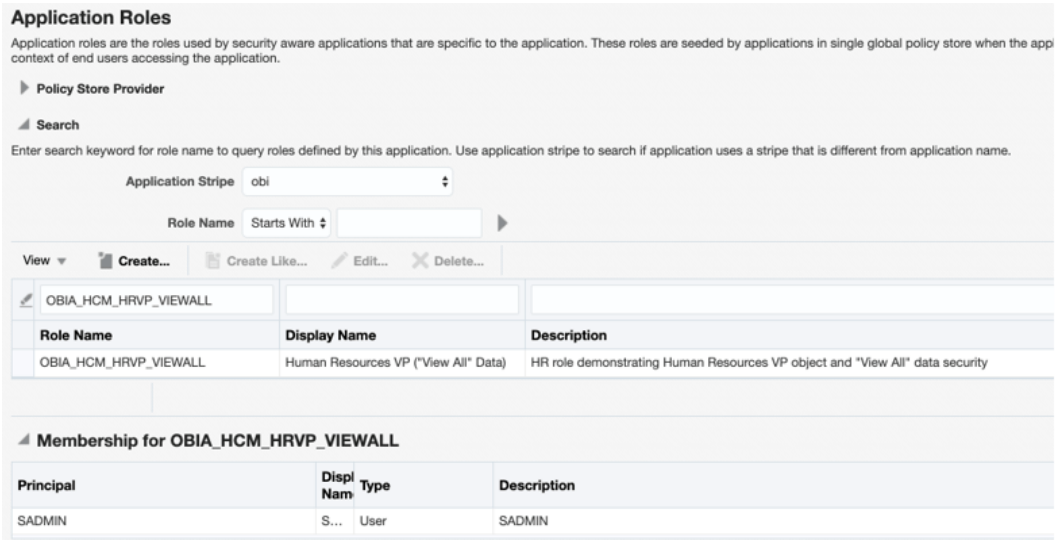
The following figure shows an example of additional predefined Duty Roles that are created when Oracle BI Applications is installed. The list of Duty Roles depends on

your installation.



1. Log in to Oracle Enterprise Manager Fusion Middleware Control as an administrator.
2. Click **Target Navigation**, expand **Business Intelligence**, select **biinstance**, select **Security**, and then **Application Roles**.

   You see the list of available Duty roles. The Membership for <Duty Role name> area displays Enterprise Roles or other Duty Roles that are associated with the selected Duty Role.



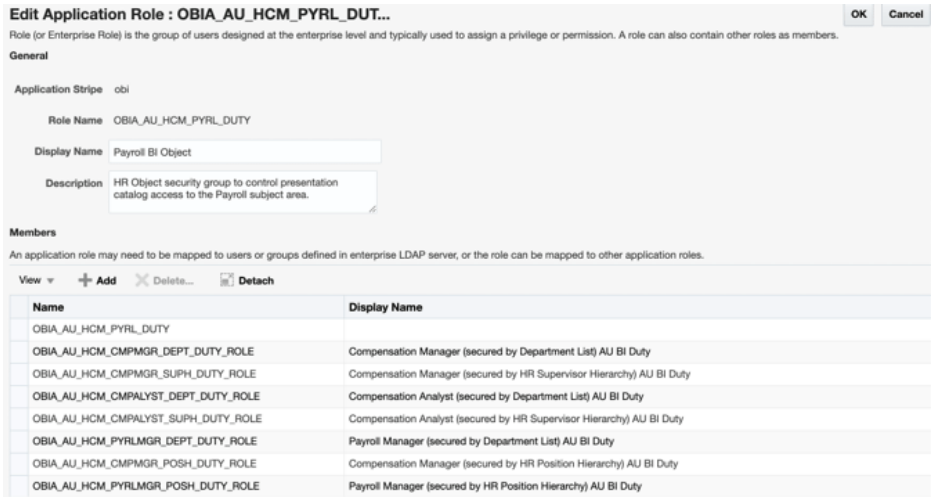
Provisioning BI Users with Duty Roles

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.

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 the Oracle BI Repository initialization blocks. 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.

1. Log in to Oracle Enterprise Manager Fusion Middleware Control as an administrator.
2. Click **Target Navigation**, expand **Business Intelligence**, select **biinstance**, select **Security**, and then **Application Roles**.

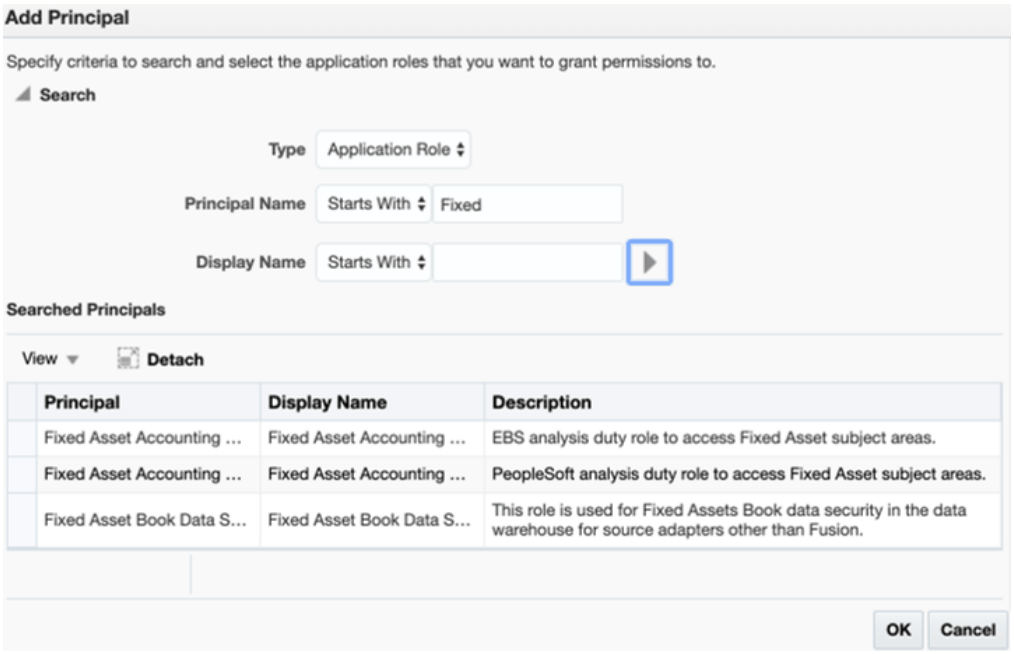
   You see the list of available Duty Roles.
3. Provision a BI User with a Duty Role.
   a. Select the Duty Role that a BI User requires access to.
   b. Click **Edit** to display the Edit Application Role dialog.



   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 the "Fixed Assets Accounting" reporting for E-Business Suite, you edit the BI Duty Role "Fixed Asset Accounting Manager EBS" and add Enterprise Role "Fixed Asset

Accounting Manager EBS" as a Member.



e. Click **OK**.

Creating Duty Roles for Oracle BI Applications

You can edit or create Duty roles.

1. Log in to Oracle Enterprise Manager Fusion Middleware Control as an administrator.
2. Click **Target Navigation**, expand **Business Intelligence**, select **biinstance**, select **Security**, and then **Application Roles**.

   You see the list of available Duty roles.
3. 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).
4. Use the General area to specify the details.
5. 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.
6. Click **OK**.

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 Enterprise Roles are defined so that a User is provisioned with a single Duty Role.

Note that while LDAP is required for Oracle Fusion Applications environments, it is optional for other source applications.

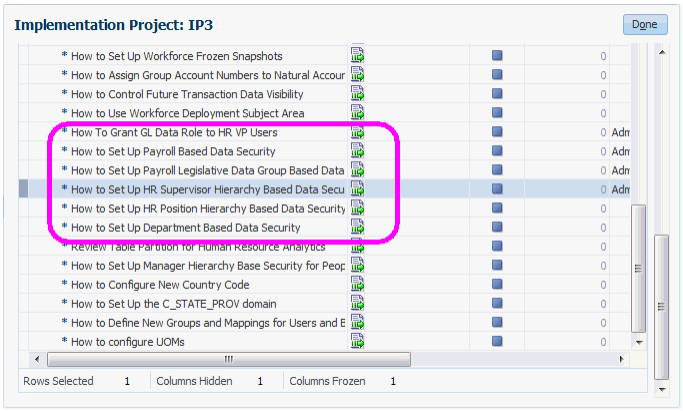
3

Setting Up Security with Functional Setup Manager

To set up security for Offerings in Oracle Business Intelligence Applications (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.

To use the FSM tasks, see About Task Lists and Tasks for Oracle BI Applications Offerings and Additional Steps for Managing Projects in FSM in *Oracle Business Intelligence Applications Configuration Guide*.

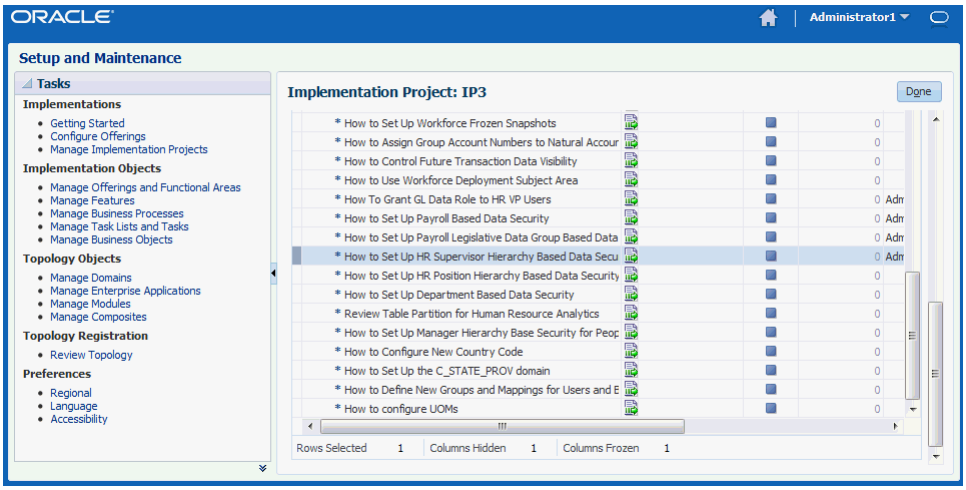
For example, the screenshot below shows a list of FSM Tasks for a Functional Area in Human Resources. A number of security-related tasks are highlighted, for example, 'How to Set Up Payroll Based Data Security'.



1. Log into FSM.
2. Navigate to the Implementation Project that has been created to configure a Functional Area.

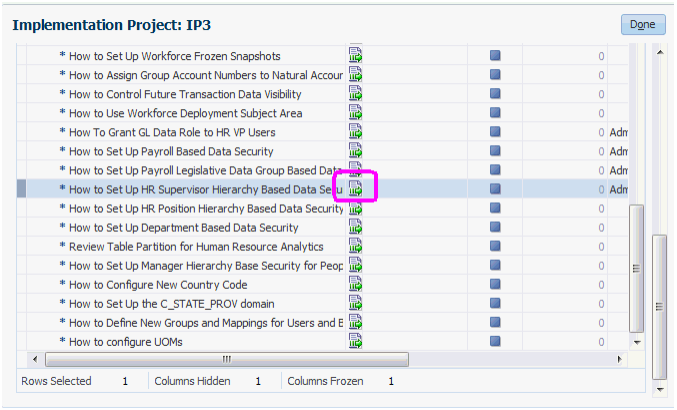
   If you log in as an Administrator, then you have access to all FSM Tasks. If you log in as a Functional Developer, then the Assigned Implementation Tasks tab provides a list of FSM Tasks that have been assigned to you by the Administrator.

   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.

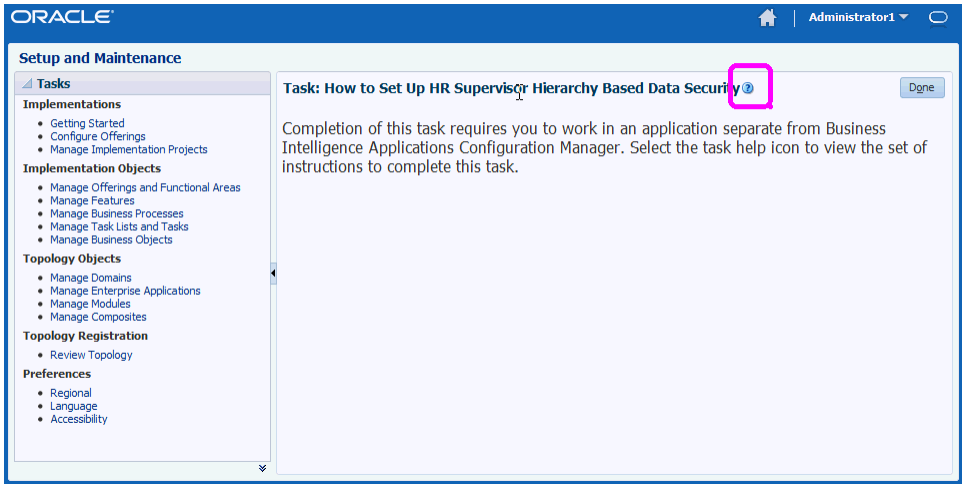


3. For each security task, do the following:

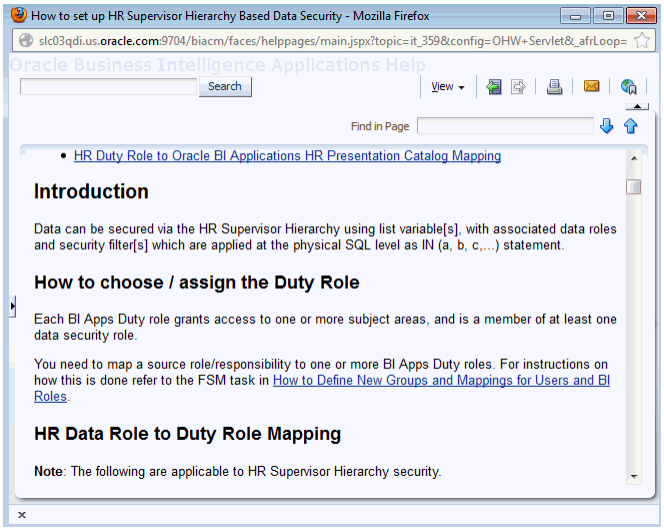
   a. Click the **Go to Task** icon next to the security task.



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



The instructions are displayed in a Help topic.



c. Follow the instructions in the Help topic.

   To complete the task, you typically use one of the security tools such as Oracle Enterprise Manager 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**.

4
Extending Security in Oracle BI Applications

You can extend the preconfigured Oracle Business Intelligence Applications (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.

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.

To work with security objects like Duty Roles and initialization blocks, see:

- *Securing Resources Using Roles and Policies for Oracle WebLogic Server*
- *Managing Metadata Repositories for Oracle Analytics Server*

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.) See *Managing Metadata Repositories for Oracle Analytics Server*.
4. Use Oracle Enterprise Manager Fusion Middleware Control to create a Duty Role in the policy store. Then, restart the Oracle BI Server. See *Administering Oracle Fusion Middleware with Fusion Middleware Control*.
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.) See *Managing Metadata Repositories for Oracle Analytics Server*.
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.) See *Managing Metadata Repositories for Oracle Analytics Server*.
7. Use Presentation Services administration to set up Presentation Services catalog privileges based on the Duty Role you created in step 4. See *Managing Security for Oracle Analytics Server*.