Oracle Product Lifecycle Analytics

Security Guide

Release 3.5

E70278-01

December 2015

ORACLE

Oracle Product Lifecycle Analytics/Security Guide, Release 3.5

E70278-01

Primary Author:

Contributing Author:

Contributor:

Contents

Preface

Oracle Product Lifecycle Analytics (OPLA) is a comprehensive, prebuilt Business Intelligence solution that delivers pervasive intelligence and provides key insights into your Product Lifecycle Management (PLM) data.

Audience

This document is intended for administrators and users of OPLA.

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.

Related Documents

Oracle's Agile PLM documentation set includes Adobe® Acrobat PDF files. The Oracle Technology Network (OTN) Web site http://www.oracle.com/technetwork/documentation/agile-085940.html contains the latest versions of the Agile PLM PDF files. You can view or download these manuals from the Web site, or you can ask your Agile administrator if there is an Agile PLM Documentation folder available on your network from which you can access the Agile PLM documentation (PDF) files.

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.

Convention	Meaning
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

Oracle Product Lifecycle Analytics (OPLA) is a comprehensive, prebuilt Business Intelligence solution that delivers pervasive intelligence and provides key insights into your Product Lifecycle Management (PLM) data. OPLA provides an integrated view enabling greater alignment of information across product organizations. OPLA is built on the Oracle Data Integrator (ODI) ETL and Oracle Business Intelligence Enterprise Edition (OBIEE) platforms.

OPLA addresses business use cases specific to these Agile PLM solutions:

- Product Quality Management (PQM)
- Product Collaboration (PC)
- Product Portfolio Management (PPM)
- Agile PLM for Process: New Product Development (NPD)
- Global Specification Management (GSM)

OPLA allows you to use different source systems. Data is transferred from the source systems to the OPLA target analytical data store. In OPLA, the transactional data sources are either Agile PLM 9.x or Agile PLM for Process.

2

OPLA Architecture Overview

You can deploy OPLA various database and application components with different hardware and machine configurations. Depending on the performance criteria set and based on the source (Agile PLM or Agile PLM for Process) database size, volume of data changes in the source database, IT network, infrastructure constraints, and business requirements.

OPLA Architecture

OPLA is designed and developed using a layered Data Warehouse and OLAP architecture on Oracle enterprise technologies. At the bottom of the stack is the Agile PLM OLTP Agile PLM for Process OLTP database which is optimized for core transactions. The database is the source data system for OPLA, but it can be extended to load data from other data sources.

Layer 2 includes the ODI and PL/SQL ETL tasks for extracting data, including metadata, from the Agile PLM source system and loads it into the Staging Schema (Layer 3). Layer 4 provides ETL tasks using ODI and PL/SQL for extracting data from the operational data store, then transforms, aggregates, and loads data to the pre-defined multi-dimensional schema in Layer 5. MDS as a set of star schemas that were designed based on top-down business analytical requirements. Layer 6 provides the pre-built analytical repository for OBIEE and its metadata repository. Layer 7 has the pre-built roles-based and functional dashboards with a pre-defined set of reports and KPIs along with alerts and guided navigation for providing actionable insights into PLM data.

The following figures show the basic product architecture for OPLA with Agile PLM and for OPLA with Agile PLM for Process, respectively.

Figure 2–1 OPLA with Agile PLM

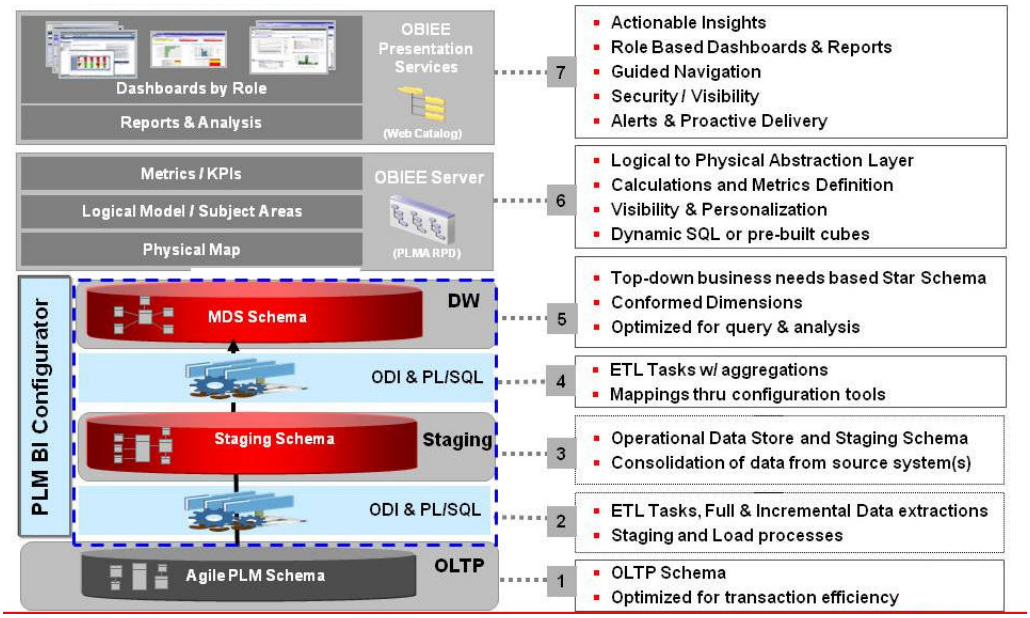
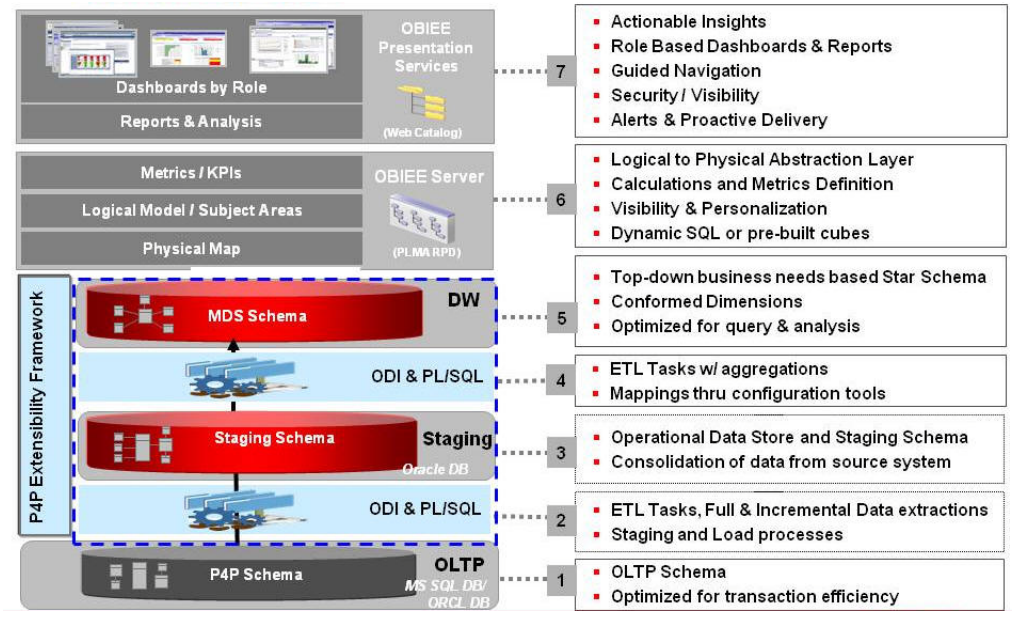


Figure 2–2 OPLA with Agile PLM for Process



3

General Security Principles

The following principles are fundamental to using any application securely.

Keep Software Up-To-Date

One principle for good security practice is to keep all software versions and patches up-to-date. To ensure that you have the most current and updated OPLA software for the latest version, regularly check the Oracle Critical Patch updates page.

Restrict Network Access to Critical Services

Keep both the OPLA application and the database behind a firewall. In addition, place a firewall between the middle-tier and the database. The firewall provides assurance that access to these systems is restricted to a known network route, which can be monitored and restricted, if necessary. As an alternative, a firewall router substitutes for multiple, independent firewalls.

If you cannot use firewalls, then configure the TNS Listener Valid Node Checking feature (it restricts access based upon IP address). Restricting database access by IP address often causes application client/server programs to fail for DHCP clients.

To solve this problem, use any of the following:

- static IP addresses
- software VPN
- hardware VPN
- software VPN and hardware VPN
- Windows Terminal Services or its equivalent.

Follow the Principle of Least Privilege

The principle of least privilege states that users should be given the least amount of privilege to perform their jobs.

Over-ambitious granting of responsibilities, roles, grants, and so on, especially early in an organization's life cycle when people are few and work needs to be done quickly, often leaves a system wide open for abuse.

User privileges should be reviewed periodically to determine relevance to current job responsibilities.

Monitor System Activity

System security stands on three legs:

- good security protocols
- proper system configuration
- system monitoring

Auditing and reviewing audit records address this third requirement. Each component within a system has some degree of monitoring capability. Follow audit advice in this document and regularly monitor audit records.

Keep Up-To-Date on Latest Security Information

Oracle continually improves its software and documentation. Check yearly for revisions.

The OPLA application's foundation is Oracle Business Intelligence Enterprise Edition (OBIEE). OBIEE is a comprehensive suite of enterprise business intelligence products containing the programs, servers, and tools to support broad self-service access across the organization.

OPLA uses ODI (a comprehensive data integration platform) to build its out-of-the-box Multi-Dimensional Schema (MDS).

For more information, go to the Oracle Technology Network website (http://www.oracle.com/technetwork/middleware/data-integrator/downloads/index.htmlhttp://www.oracle.com/technetwork/middleware/data-integrator/downloads/index.html).

4

Secure Installation and Configuration

This chapter describes recommended deployment topologies and also provides recommendations for installing and configuring a secure setup for your Oracle Product Lifecycle Analytics (OPLA) application.

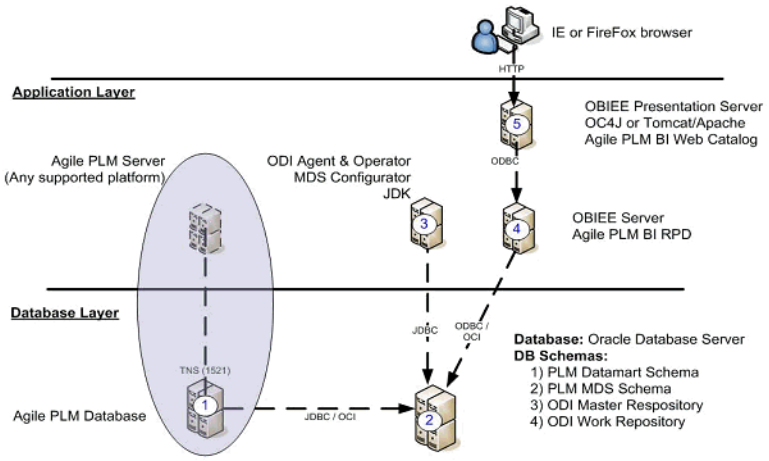
Installation Overview

Various database and application components for Oracle Product Lifecycle Analytics (OPLA) can be deployed in different hardware and machine configurations.

The complexity of your deployment configuration depends on the performance criteria set, which in turn, is based on the following:

- Business requirements
- Source - that is the Agile PLM database size or the Agile PLM for Process database size
- Volume of data changes in the source database
- IT network constraints
- Infrastructure constraints

Figure 4–1 OPLA Agile PLM Deployment Configuration for a Large Customer Base



To successfully install or upgrade to OPLA, you must be familiar with, or have working knowledge of the following:

- ODI

- OBIEE
- Agile PLM
- Agile PLM for Process
- Oracle Database Server

For more information on the privileges needed for different deployment methods, see the Appendix on Oracle PLA Database Schema Privileges on page 37.

Installation - Prerequisites

The Oracle Product Lifecycle Analytics (OPLA) application comes bundled with a number of third party software. OPLA is tested and certified with latest security patches for the following third party software:

- Bouncy Castlehttp://www.bouncycastle.org
- Apache Xerces Projecthttp://xerces.apache.org
- InstallAnywherehttp://www.flexerasoftware.com/products/installanywhere.htm
- Apache Anthttp://ant.apache.org
- LOG4PLSQLhttp://log4plsql.sourceforge.net

Before installing OPLA you must install and configure the following Oracle products:

- Oracle Enterprise Database
- Oracle Data Integrator
- Oracle Business Intelligence Enterprise Edition

Important: You should also consult the following Security Guides: *Oracle Business Intelligence Suite Enterprise Edition Documentation Library Oracle Database Security Guides*

5

Security Features

Oracle Product Lifecycle Analytics (OPLA) includes security features to provide data protection.

These features include:

- **Authentication** allows only permitted individuals to get access to the system and data.
- **Access Control (Authorization)** provides authorized individuals access control to system privileges and data.
- **Audit** allows Administrators to detect attempted breaches of authorization and attempted (or successful) breaches of access control.

Table 5-1 provides a high level overview of the various OPLA security features.

Table 5–1 Overview of Security Features

Security Features/Technology Stack		Authentication	Access Control (Authorization)	Audit
Web Browser (Desktop Tier)		**Default Security Feature**	**Default Security Feature**	**Default Security Feature**
Application Layer	OBIEE	Default OBIEE authentication	No out of box access control provided. Object level security Model. Refer to security model Object level security Data level security is provided. Refer to security model: Data Level security	Default OBIEE audit feature Refer to section "Configuring and Using Security Audit"
	ODI	Default ODI authentication	Default ODI access control	Default ODI feature
	Configurator	Default DB authentication based on DataMartConfig.properties	Default access control provided at DB level	Audit details are captured at OPLA Install Home/logs/Configurator.log Detailed logging is enabled in ETL level for ODI and PL/SQL code.
Data Layer		Default Oracle DB authentication. Default file based authentication for external csv files	Access to source is based on DB link. Access to Staging Objects is based on Synonyms. Specific privileges are provided to Staging and Target users Access to external csv files are controlled by access privileges to folder at which OPLA is deployed.	Default Oracle DB audit feature Default OS audit feature at file level for external csv files

Password Policy

A password policy is a set of rules dictating how to use passwords. Some of the rules a password policy sets are:

- The maximum length of time a password is valid
- The minimum number of characters in a password
- The mandatory number of numeric characters in a password

Password policies play an important role when attempting to access a directory. The directory server ensures that the password entered adheres to the password policy.

Oracle Product Lifecycle Analytics (OPLA) is dependent on Oracle Business Intelligence Enterprise Edition (OBIEE) password policy.

If you are using the OBIEE 11.**x**.**x**.**x** version, you automatically adhere to the Oracle password policy. Use the Oracle Internet Directory to set passwords. For more information, see the *OracleÂ® Fusion Middleware Administrator's Guide for Oracle Internet Directory 11g Release 1*.

Note: You must secure Oracle Fusion Middleware components using SSL version 3 or TLS version 1. For more information, see *Oracle® Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition 11g*

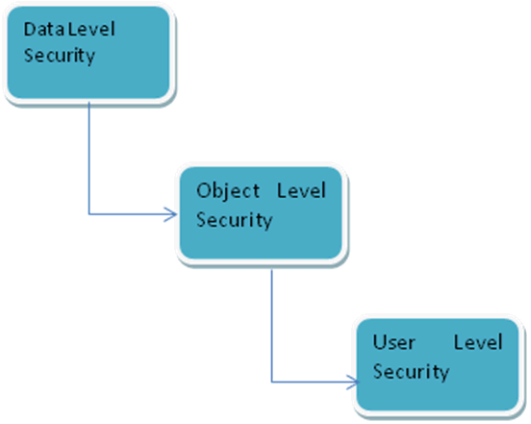
Security Model

In today's environment it is critical to have a properly secured computing infrastructure. A secured infrastructure strikes a balance between:

- Exposure risk
- Security costs
- Value of the information to protect (monetary or other)

Oracle Product Lifecycle Analytics (OPLA) achieves this balance and protects information by using a three-level hierarchy model. See the OPLA Security Hierarchy figure for a better understanding.

Figure 5–1 OPLA Security Hierarchy



Data-Level Security

Data level security is a restricted security status. Restriction, or access, is based on access control permissions given by an Administrator. The security level determines (through the Administrator) who gets to see particular data, *and* if they can access it.For example, you can restrict a user's access to project analysis to only their product lines.

Object Level Security

Object level security controls and restricts the visibility to business logic objects by user role. For example, object level security for dashboards can be set up based on subject areas and roles.

User-Level Security (User Authentication)

User level security is the authentication and confirmation of a user's identity based on the credentials provided. This is your basic login and password at the lowest level. At higher levels, it can consist of a number of authentications and confirmations (at various degrees of encryption).

Configuring and Using Authentication in OPLA

Oracle Product Lifecycle Analytics (OPLA) supports both of the following high-level authentication configurations:

1. OPLA authentication at ETL layer
2. OPLA authentication at OBIEE layer

Authentication at ETL Layer

You can change or modify your password *after* installing Oracle Product Lifecycle Analytics (OPLA). At the ETL layer different methods are used for changing different passwords.You change the password for the Staging Schema connection details in the Physical Repository of ODI Topology Manager. For more information, see the *Oracle Data Integrator Installation and Configuration Guide*.You can change the OPLA Configurator password using OPLA encryption methods.You can change the password for the ODI repositories using the ODI Agent.

Authentication at the ETL Layer using OPLA Encryption Methods

You can change the passwords for the OPLA Configurator using OPLA encryption methods.

To change passwords:

1. From the command prompt navigate to <OPLA_Home>\bin\.
2. For Windows: Type, DMEncoder.bat <new password> For Linux: Type, DMEncoder.sh <new password>
3. The system generates an encoded password. Copy the encoded password, and exit the command prompt.
4. Navigate to <OPLA_Home>\bin\DataMartConfig.properties and open the DataMartConfig.properties file.
5. In the DataMartConfig.properties file navigate to the parameter whose password you want changed, and manually replace the old password with the new encoded password. Refer to the table below to locate the parameter you need to change.
6. Save and close the DataMartConfig.properties file

To Change the Password for:	Parameter to Navigate to in the DataMartConfig.properties file
Agile PLM Source schema password	PLM_DB_PWD

To Change the Password for:	Parameter to Navigate to in the DataMartConfig.properties file
Agile PLM for Process Source schema password	PLM4P_DB_USER_PWD
Data Mart Database sys schema password	SYS_USER_PASSWORD
Data Mart Database system schema password	DB_SYSTEM_PWD
Data Mart schema password	MDS_USER_PASSWORD
Source schema Password, if installed as a separate schema	ODM_USER_PASSWORD
Master Repository schema password	MASTER_PWD
Work Repository schema password	WORK_PWD
Work Repository password	WORK_REP_PWD

Authentication at the ETL Layer using the ODI Agent

You can also change passwords at the ETL layer employing the ODI Agent or the ODI Studio for the following:

- Master Repository Database password
- Work Repository Database password
- ODI Work Repository password

To change passwords in ODI:

1. From the command prompt navigate to <ODI_HOME>\Oracle_ODI_1\oracledi\agent\bin.
2. For Windows: Type, encode.bat <new password> For Linux: Type, encode.sh <new password>

Authentication at the Oracle Business Intelligence Enterprise Edition Layer

The Oracle Product Lifecycle Analytics (OPLA) application utilizes the Oracle Business Intelligence Enterprise Edition Layer (OBIEE) layer's platform authentication features. You change the password for the PLMAXX_11G.rpd repository file (where XX represents either Agile PLM or Agile PLM for Process) using the OBIEE Admin Tool. For more information, see the *OBIEE Installation and Configuration Guide*.

OPLA uses OBIEE authentication features. We recommend you use the authentication features in the order shown below:

- LDAP authentication - We recommend that you configure the OPLA application to use LDAP authentication, only if your Agile PLM application is configured to LDAP authentication.
- External table authentication - We recommend that you configure the OPLA application to use external table authentication, only if your Agile PLM application is configured to external table authentication.
- Database authentication - We recommend that you configure the OPLA application to use database authentication, only if your Agile PLM application is configured to database authentication.

- Oracle BI Server user authentication maintenance - We do not recommend using the Oracle BI Server authentication mechanism.

LDAP Authentication

LDAP authentication is used as an alternative to storing user IDs and passwords in an Oracle BI repository.You can set up the Oracle BI Server to take the user ID and password, and have it then pass the user ID and password to an LDAP server for authentication. For LDAP authentication the server uses clear text passwords.

You can configure OBIEE to secure communications between different points in the network. OBIEE 11g supports SSL version 3, and TLS version 1. For more information on how to configure SSL,

Important You must configure your LDAP servers to allow this.

External Table Authentication

You can maintain lists of users and their passwords in an external database table, instead of storing user IDs and passwords in an Oracle BI repository. You can then use this table for authentication purposes. The external database table contains the following information:

- User IDs
- Passwords
- Group membership
- Display names (used for Oracle BI Presentation Services users)
- Specific database catalog names
- Schemas to use for individual users(when querying data)

You can also configure user level security with the user authentication information (stored in the external source system). For example, in Agile PLM the **AgileUser** table (stores encrypted user IDs and passwords).

Database Authentication

The Oracle BI Server authenticates users through database logons. If a user has Read permission on a specified database, the Oracle BI Server trusts that user. This authentication method can also be applied for Oracle BI Presentation Services users.

Maintaining Oracle BI Server User Authentication

Using the Administration Tool, you can maintain lists of users and their passwords in the Oracle BI repository. The Oracle BI Server authenticates users against this list when a user logs on (unless another authentication method has already been used, or a database authentication is specified in the NQSConfig.INI file).The Oracle BI Server user IDs are case insensitive and stored in a non-encrypted form in the Oracle BI repository. Whereas, Oracle BI Server passwords are case sensitive and stored in an encrypted form. If the user has the required access privileges, the Oracle BI Server user IDs can access any business model in a repository.

Important: User IDs are valid only for the repository in which they are set up. They do not span multiple repositories.

For more information on password policy settings in OBIEE, see the OracleÂ® Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition 11g Release 1 (11.1.1)http://download.oracle.com/docs/cd/e14571_01/bi.1111/e10541/toc.htm.

Configuring and Using Access Control

Authorization primarily includes two processes:

1. Permitting only certain users to access, process, or alter data
2. Applying varying limitations on user access or actions.

   Oracle Product Lifecycle Analytics (OPLA) supports access control at the folder and file level, as well as at the following configurations:

3. Access control at the data-level
4. Access control at the object-level security
5. Access control at the user-level security

Access Control at the Folder and File Level

Oracle Product Lifecycle Analytics (OPLA) uses host Operating System file permission features to control authentication of directories, executables, server software, data files, logs, external csv files. When OPLA is deployed appropriate access privileges are provided to the directories and folders. Files often contain sensitive and critical information, and must be protected from prying eyes, modification, or deletion.

Caution You must secure all Oracle PLA log files, external files, configurator files, product line security files (rpd) listed below. Not doing so can result in files being corrupted, destroyed, or rewritten.

1. Only Administrators should have Read, Write and Execute privileges for the DataMartConfig.properties file, located at <Oracle_PLA_Home>\bin\DataMartConfig.properties.

   For *both* OPLA with Agile PLM and OPLA with Agile PLM for Process.

2. Make sure that the external (csv) files listed in the table below are secured. The files location is <OPLA_Home>\install\et\srcfiles.

Administrator	**User**
Post-Installation File **Value**	**Value**
PPM_PRD_DEMAND.CSV Read	Read & Write
PPM_PRD_INV_QTY.CSV Read	Read & Write
PPM_PRD_INV_VALUE.CSV Read	Read & Write
PPM_PRD_INV_VALUE.CSV Read	Read & Write

PPM_PRD_UNIT_REC.CSV Read	Read & Write
PPM_PRD_UNIT_SHIP.CSV Read	Read & Write
PRJ_COST.CSV Read	Read & Write
PRJ_FORECAST.CSV Read	Read & Write

3. Make sure that the log files listed in the table below are secured. Log files are located at <OPLA_Home>\logs.

Administrator	**User**
Post-Installation File **Value**	**Value**
BI_DATA_DICT_PC_SD.log Read	Read, Write, Execute
BI_DATA_DICT_PPM_SD.log Read	Read, Write, Execute
BRIDGE_SD.log Read	Read, Write, Execute
ControlTables.log Read	Read, Write, Execute
install_logger4odm.log Read	Read, Write, Execute
LIST_DM_SD.log Read	Read, Write, Execute
MDS_COMMENT.log Read	Read, Write, Execute
MDS_DDL.log Read	Read, Write, Execute
MDS_IND.log Read	Read, Write, Execute
MDS_PROCS.log Read	Read, Write, Execute
MDS_SD.log Read	Read, Write, Execute
MDS_TEMP_DDL.log Read	Read, Write, Execute
MDS_VIEWS.log Read	Read, Write, Execute

ODM_DDL.log Read	Read, Write, Execute
ODM_PROC.log Read	Read, Write, Execute
PC_DDL.log Read	Read, Write, Execute
PPM_DDL.log Read	Read, Write, Execute
SEED_DATA_GLOBAL.log Read	Read, Write, Execute
SingleSchemaCreation.log Read	Read, Write, Execute
USERDEF_OBJ.log Read	Read, Write, Execute

4. Make sure that the following rpd file is secure. Location for RPD file: <OPLA_ Home>\olap\rpd. The RPD File name isPLMA_11G.rpd

Access Control at the Data-Level

Data-level security controls the visibility of data (content in subject areas, dashboards, Oracle BI Answers, and so on) based on the user's association to data in the transactional system.For example, restricting authorized users access to Project Analysis for their assigned Product Lines is provided in OPLA.

To extend data level security for repository objects:

1. Extend the physical table by adding the attribute by which the dimension, or fact, needs to be secured.

   This step *may* result in a change to the data model.

   a. For enabling existing out-of-the-box defined dimensions and measures *without* changing ETL Mapping you can map attributes in the OPLA Configurator.

   b. For enabling new user-defined dimensions and measures by changing ETL mapping and BI repository, new user defined attributes can be added using Schema Enhancer that comes with OPLA Configurator

      This step results in a change to the data model.

      Populate the relevant attribute value for each row in the fact or dimension table.

      This step results in a change to the ETL mapping.

2. Use the Oracle BI Administration Tool to create an initialization block. When a user logs into OPLA, the initialization block fetches the attribute values and populates them into a session variable. You can then create a target session variable for the initialization block. For detailed instructions, see Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition.

You can only create a target session variable if the initialization block is *not* a row-wise initialization block. This step results in a change to the Oracle BI repository.

3. 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.

4. Use Presentation Services administration to set up the Presentation Services catalog privileges - based on the application role you created in step 4. For detailed instructions, see Oracle Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition 11g.

   Note You can also leverage the existing OPLA security objects (when extending data-level security). To do this, copy existing security objects for secured dimensions, such as initialization blocks, and then modify them to apply to the additional dimensions.

Access Control at the Object-Level

You can enable object level security using the Oracle Business Intelligence Enterprise Edition Layer (OBIEE) platform features.Oracle Product Lifecycle Analytics (OPLA) tightly integrates with OBIEE, as well as the security model of the operational source system, to allow the right content to be shown to the right user.

Important: You should be thoroughly familiar with the security features of OBIEE before you begin working with OPLA.

Security settings for OBIEE are made in the following Oracle Business Intelligence (Oracle BI) components:

1. **Oracle BI Administration Tool**

   You can 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
   - Setting authentication options

   For more detailed information, *see Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition 11g.*

2. **Oracle BI Presentation Services Administration**

   You can use Oracle BI Presentation Services Administration to perform tasks such as setting permissions to Presentation Catalog objects (including dashboards and dashboard pages).

   For more detailed information, see *Oracle Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition 11g.*

3. **Oracle Enterprise Manager Fusion Middleware Control**

   You can use Fusion Middleware Control to manage the policy store, application roles, and permissions for determining functional access.

   For detailed information, see *Oracle Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition 11g*.

4. **Oracle WebLogic Server Administration Console**

   You can 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 11g*.

Access Control at the User-Level

User level security involves the authentication and confirmation of the user's identity - based on the credentials provided, such as username and password.By default, user level security is set up in the embedded Oracle WebLogic Server, the LDAP server, and the policy store.

See also *Oracle Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition 11g*.

Configuring and Using Security Audit

This section explains how to enable the security audit feature in OPLA.

Oracle Business Intelligence Enterprise Edition (OBIEE) supports extensive audit features including, but not limited to, error events, informational events, and warning events. Some examples are, server starting and server shutdown, failed login attempts, and failed access control authorizations. In OBIEE 11g, security auditing is integrated into the Oracle Fusion Middleware Audit Framework in Oracle Fusion Middleware Application Security, and it provides a range of out-of-the-box reports that are accessible through Oracle Business Intelligence Publisher.

The reports are grouped according to the type of audit data they contain:

- Common Audit Reports
  - Account Management
  - User Activities
  - Errors and Exceptions
- Component-Specific Audit Reports
  - Oracle Fusion Middleware Audit Framework
  - Oracle HTTP Server
  - Oracle Internet Directory
  - Oracle Virtual Directory
  - Reports Server
  - Oracle Directory Integration Platform
  - Oracle Identity Federation
  - Oracle Platform Security Services
  - Oracle Web Services Manager
  - Oracle Web Cache

For more information, see the OracleÂ® Fusion Middleware Application Security Guide http://docs.oracle.com/cd/E21764_01/core.1111/e10043/toc.htm

Configuring and Using OPLA Configurator

Oracle Product Lifecycle Analytics (OPLA) comes with the OPLA Configurator tool. The OPLA Configurator provides the ability to map source columns to target columns (based on customer choice) in the data layer.

It is a standalone feature and uses independent encryption algorithms to connect with source and target Data Schema for Agile PLM 9 Schema

The following security features are implemented with OPLA:

Uses 3rd party software components XML Parser. This component is upgraded to latest patch. (From Xerces 2.9.0 to Xerces2 2.11.0).

Note: OPLA also provides the ability to map extended attributes with the MDS Layer for Agile PL M for Process source. Manual SQL scripts are supplied for updating the MDS schema.

Uses default DB level authentication.

6

Security Considerations for Developers

Oracle Product Lifecycle Analytics (OPLA) supports the extension of the standard product functionality *only* in the following two scenarios:

1. You can enable existing defined dimensions and measures without changing ETL Mapping. This requires changes *only* to the BI repository.
2. You can enable new user-defined dimensions and measures. This requires changes to *both* the ETL Mapping and the BI repository.

In both scenarios you must ensure that the preconfigured OPLA security model is updated to match your operational source system.

When you extend OPLA, you must ensure that your customizations and any new objects are valid and functional.

A

OPLA Secure Deployment Checklist

Secure Deployment Checklist

The following security checklist includes guidelines that help secure your database:

1. Install only what is required.
2. Lock and expire default user accounts.
3. Enforce password management.
4. Enable data dictionary protection.
5. Practice the principle of least privilege.
   a. Grant necessary privileges only.
   b. Revoke unnecessary privileges from the PUBLIC user group.
   c. Restrict permissions on run-time facilities.
6. Enforce access controls effectively and authenticate clients stringently.
7. Restrict network access.
   a. Use a firewall.
   b. Never poke a hole through a firewall.
   c. Protect the Oracle listener.
   d. Monitor listener activity.
   e. Monitor who accesses your systems.
   f. Check network IP addresses.
   g. Encrypt network traffic.
   h. Harden the operating system.
8. Apply all security patches and workarounds.
9. Contact Oracle Security Products if you come across any vulnerability in the Oracle Database.

B

Database Schema Privileges

In Oracle Product Lifecycle Analytics (OPLA), database privileges vary for single schema and multiple schema installations.

Single Database Schema Privileges

This table lists and explains the privileges required to use a single schema to host the DataMart, ODI Master, and the ODI Work Repository objects in Oracle Product Lifecycle Analytics (OPLA).

Privilege	Purpose
CONNECT,RESOURCE	Basic privilege for the Schema User
CREATE DATABASE LINK	Create DBLink to Agile PLM source system for every ETL run
CREATE JOB	Create a job in the schema
CREATE TABLE	Create table privilege for the schema
CREATE SYNONYM*	Create a synonym for the source table
CREATE MATERIALIZED VIEW*	Create materialized view on the schema
SELECT ON V_$DATABASE	Read Platform information
ALL ON SYS.DBMS_PIPE	PL/SQL logger privileges
EXECUTE ON, SYS.DBMS_ SYSTEM	
CREATEVIEW	Create a View on the Schema
* Agile PLM databases only	

OPLA Multiple Schema Privileges

This table lists and explains the privileges required when you install the ODM and MDS on one schema, and the ODI Master and ODI Work repositories on a separate schema.

Privilege	Purpose
CONNECT, RESOURCE	Required for MDS and ODI Repository schemas
CREATE DATABASE LINK	Create DBLink to Agile PLM source database for every ETL run.

Privilege	Purpose
CREATE SYNONYM	Create a synonym for the source table in the ODI Work Repository schema
CREATE TABLE	Create i$, e$, c$ tables in the ODI Work Repository schema.
CREATE VIEW	Create a view privilege for the schema.
CREATE MATERIALIZED VIEW	Create a materialized view on the schema.
CREATE JOB	Create a job in the schema
SELECT ON V_$DATABASE	Reads Platform information.
ALL ON SYS.DBMS_PIPE	
EXECUTE ON SYS.DMBS_ SYSTEM	

This table lists and explains the privileges required when you install ODM and MDS in different schemas.

Privilege	Purpose
CONNECT, RESOURCE	Basic privilege for schema user
CREATE SYNONYM	Create a synonym for the source table in the ODI Work Repository schema
CREATE DATABASE LINK	Create DBLink to Agile PLM source database for every ETL run.
CREATE MATERIALIZED VIEW	Create a materialized view on the schema.
CREATE VIEW	Create a view privilege for the schema.
CREATE TABLE	Create i$, e$, c$ tables in the ODI Work Repository schema
CREATE JOB	Create a job in the schema
SELECT ON V_$DATABASE	Reads Platform information.
ALL ON SYS.DBMS_PIPE	
EXECUTE ON SYS.DMBS_SYSTEM	

C

SSL Configuration in Oracle Business Intelligence

Secure Socket Layer (SSL) is a cryptographic protocol that enables secure communication between applications across a network. Enabling SSL communication provides several benefits, including message encryption, data integrity, and authentication. An encrypted message ensures confidentiality in that only authorized users have access to it. Data integrity ensures that a message is received intact without any tampering. Authentication guarantees that the person sending the message is who they claim to be.

The SSL Everywhere feature of Oracle Business Intelligence enables secure communications between the components.You can configure SSL communication between the Oracle Business Intelligence components and between Oracle WebLogic Server for secure HTTP communication across your deployment.

The table below contains common SSL configuration tasks. For more information on these tasks, see the "SSL Configuration in Oracle Business Intelligence" chapter in *Security Guide for Oracle Business Intelligence Enterprise Edition 11g Release 1 (11.1.1).*

Task Map: Configuring SSL Communication for Oracle Business Intelligence

Task	Description
Understand SSL communication in Oracle Business Intelligence.	Understand how SSL communication between components and the application server works.
Configure SSL communication between the Oracle WebLogic Server Managed servers.	The Web server must be configured to use HTTPS before enabling SSL communication for Oracle Business Intelligence. **Note** Also see the "SSL Configuration in Oracle Fusion Middleware" chapter in the Oracle Fusion Middleware Administrator's Guide.
Configure SSL communication between components.	Configure SSL communication between Oracle Business Intelligence components.

Additional references:

For more information about SSL concepts and public key cryptography, see "How SSL Works" in Oracle Fusion Middleware Administrator's Guide.

For information about how to configure SSL for Oracle WebLogic Server, see "SSL Configuration in Oracle Fusion Middleware" in *Oracle Fusion Middleware Administrator's Guide.*