# Security Guidance for P6 Analytics and P6 Reporting Database
## Release 3.2

October 2013

# Contents

# Analytics Suite Security Guidance Overview

During the installation and configuration process for P6 Analytics and P6 Reporting Database, several options are available that impact security. Depending on your organization's needs, you might need to create a highly secure environment for P6 Analytics and P6 Reporting Database. Use the following guidelines to plan your security strategy for P6 Analytics and P6 Reporting Database:

- Review all security documentation for applications and hardware components that interact or integrate with P6 Analytics and P6 Reporting Database. Oracle recommends you harden your environment.
- Read through the summary of considerations for P6 Analytics and P6 Reporting Database included in this document. Areas covered include: safe deployment, authentication options, authorization, confidentiality, sensitive data, and reliability.
- Throughout this documentation, the Security Guidance icon 🔒 helps you to quickly identify security-related content to consider during the installation and configuration process. Once you begin the installation and configuration of your P6 Analytics and P6 Reporting Database environment, use the Security Guidance icon as a reminder to carefully consider all security options.

### Tips

As with any software product, be aware that security changes made for third party applications might affect P6 Analytics and P6 Reporting Database applications.

# Safe Deployment of P6 Analytics and P6 Reporting Database

To ensure overall safe deployment, you should carefully plan security for all components, such as database servers and client computers that are required for and interact with P6 Analytics and P6 Reporting Database. In addition to the documentation included with other applications and hardware components, follow the P6 Analytics and P6 Reporting Database-specific guidance below.

## Administrative Privileges Needed for Installation and Operation of P6 Analytics and P6 Reporting Database

As the administrator, you should determine the minimum administrative privileges or permissions needed to install, configure, and operate P6 EPPM.

## Physical Security Requirements for P6 Analytics and P6 Reporting Database

You should physically secure all hardware hosting P6 Analytics and P6 Reporting Database to maintain a safe implementation environment. See the *P6 Analytics and P6 Reporting Database Planning and Sizing Guide*.

## Files to Protect after Implementing P6 Analytics and P6 Reporting Database

While P6 Analytics and P6 Reporting Database require specific files for installation and configuration, you do not need some for daily operations. The following is not a comprehensive list, but you should protect these files after installation and configuration:

- **staretl.properties** (if you installed the Star database)
    - Must have read and write privileges to access this file.
    - Contains given paths, DB user names, installation options, and encrypted passwords.
    - Protect and back up this file.

  Default Location = <installation path>\star\res\
- **odsetl.properties** (if you installed the ODS database)
    - Must have read and write privileges to access this file.
    - Contains given paths, DB user names, installation options, and encrypted passwords.
    - Protect and back up this file.

  Default Location = <installation path>\ods\res\

# Authentication Options

When you set up P6 EPPM, it offers the following authentication modes:

- **Native** is the default mode for P6 EPPM. In Native mode, the P6 EPPM database acts as the authority and the application handles the authentication of the user who is logging into that application.

- **Single Sign-On (SSO)** controls access to Web applications, specifically P6 Progress Reporter and P6. In SSO mode, P6 EPPM applications are protected resources. When a user tries to login to one, a Web agent intercepts the login and prompts the user for login credentials. The Web agent passes the user's credentials to a policy server, which authenticates them against a user data store. With SSO, once the users login, they are logged into all Web applications during their browser session (as long as all Web applications authenticate against the same policy server).
- **Lightweight Directory Access Protocol (LDAP)** authenticates users through a directory and is available for all P6 EPPM applications. P6 EPPM supports LDAP referrals with Oracle Internet Directory and Microsoft Windows Active Directory. LDAP referrals allow authentication to extend to another domain. You can also configure multiple LDAP servers, which supports failover and enables you to search for users in multiple LDAP stores. In LDAP mode, an LDAP directory server database confirms the user's identity when they attempt to log in to a P6 EPPM application.

When connecting P6 Reporting Database to BI Publisher, you should use LDAP.

# Authorization for P6 EPPM and P6 Reporting Database

Grant authorization carefully to all appropriate P6 EPPM and P6 Reporting Database users. The *P6 EPPM Post Installation Administrator's Guide* and installation and configuration guides for P6 Analytics and P6 Reporting Database details the most secure application security options.

Authentication for P6 Analytics depends on your authorization method for the Oracle Business Intelligence application; however, the user name must match in all the following: P6, Star, and OBI authentication.

# Confidentiality for P6 Analytics and P6 Reporting Database

Confidentiality ensures only authorized users see stored and transmitted information. In addition to the documentation included with other applications and hardware components, follow the guidance below.

- For data in transit, use SSL/TLS to protect network connections among modules. If you use LDAP or SSO authentication, ensure you use LDAPS to connect to the directory server.
- For data at rest, refer to the documentation included with the database server for instructions on securing the database.

# Reliability for P6 Analytics and P6 Reporting Database

Protect against attacks that could deny a service by:

- Installing the latest security patches.
- Replacing the default Admin Superuser (admin) immediately after a manual database installation or an upgrade from P6 version 7.0 and earlier.
- Ensuring log settings meet the operational needs of the server environment. Do not use "Debug" log level in production environments.
- Documenting the configuration settings used for servers and create a process for changing them.
- Protecting access to configuration files with physical and file system security.

# Sensitive Data for P6 Reporting Database and P6 Analytics

Protect sensitive data in P6 Reporting Database and P6 Analytics, such as user names, passwords, and e-mail addresses. Use the process below to help during your security planning:

- Determine which products and interacting applications display or transmit data that your organization considers sensitive. For example, costs and secure codes.
- Implement security measures in P6 Reporting Database and P6 Analytics to carefully grant users access to sensitive data. For example, use a combination of Global Profiles, Project Profiles, and OBS access to limit access to data.
- Implement security measures for applications that interact with P6 Reporting Database and P6 Analytics, as detailed in the documentation included with those applications.

# About Security in P6 Reporting Database

This section provides an overview of security in P6 Reporting Database.

## ODS Database User Security Guidance

### ODS User Security in P6 Reporting Database 3.2

For P6 Reporting Database 3.2, P6 EPPM users had to be given Enterprise Reports module access to become reporting users in the ODS database. When granted module access, a database user is created in the ODS instance for the user name.

The ODS database users can only view the data they have permissions to view in the P6 EPPM database. P6 EPPM user passwords are not used as the ODS database users passwords. The ODS database users that are created for these P6 EPPM users have randomly generated passwords. An administrator (or a user with privileges to change the password of other users) can reset the database user password in order to connect directly as the ODS database user.

### User Database Access

The database access that the user has is based on a new role called **P6Reports**. This role gives the database user permissions to create a session. The user can only access public synonyms. These synonyms enable the user to view their P6 Reporting Database data. Because the user does not know the password, the recommended method for configuring P6 EPPM with the ODS reporting database is an SSO\LDAP configuration.

### Configuration Information

See the *P6 Reporting Database for ODS Installation and Configuration Guide* (or the *P6 Analytics and Star Database Installation and Configuration Guide* if you purchased P6 Analytics) for specific configuration information. See Pre-defined BI Publisher Reports in the P6 online help for information about pre-defined reports.

# About Star Security

The Star maintains security similar to P6 EPPM. The security being maintained consists of Project/Cost security, Resource security, and OBS security.

## Star Security Guidance

The Star maintains security similar to P6 EPPM. The security being maintained consists of Project/Cost security, Resource security, and OBS security. The Star database has row-level security that is built into the Enterprise Edition database. See the *P6 Analytics and Star Database Installation and Configuration Guide* for more information.

For customers using Oracle Standard Edition, Oracle has supplied an RPD that has security enforced at the RPD level.

# P6 Analytics Security Guidance

Star row-level security is enforced when queries are executed from the OBI server. To apply the proper security and ensure users have access to their data, ensure user names are the same in the P6 EPPM database, P6 EPPM Extended Schema, STAR (W_USER_S), and in the OBI\WebLogic server.

# For More Information

## In This Section

## Where to Get Documentation

For the most up-to-date versions of all manuals and technical documents related to installing, administering, and using P6 Analytics, go to:

http://download.oracle.com/docs/cd/E49048_01/index.htm

Most documentation assumes a standard setup of the product, with full access rights to all features and functions.

You can also access the versions of the product manuals and technical documents that were available at the time of the release from the P6 Analytics Documentation Center, located in the \Documentation\Documentation_library\*language* folder of the P6 Analytics physical media or download.

The following table describes the core documents available for P6 Analytics and lists the recommended readers by role.

| **Title** | **Description** |
|---|---|
| *What's New in P6 Analytics* | This guide highlights the new and enhanced features included in this release.<br>You can also use the *Cumulative Feature Overview Tool* to identify the features that have been added since a specific release level.<br>All users should read this guide. |
| *P6 Analytics and P6 Reporting Database Planning and Sizing Guide* | This guide details how to plan your installation and ensures you have the necessary technical specifications to successfully install P6 Analytics and P6 Reporting Database. It also includes checklists for P6 Analytics and P6 Reporting Database to help guide you through the installation.<br>All administrators should read this guide. |
| *P6 Analytics and Star Database Installation and Configuration Guide* | This guide gives step-by-step instructions for installing and configuring P6 Analytics and the Star database portion of P6 Reporting Database.<br>All administrators should read this guide. |

| Title | Description |
|---|---|
| *P6 Reporting Database for ODS Installation and Configuration Guide* | This guide explains how to install and configure the ODS portion of P6 Reporting Database. It describes how to install and configure the Oracle Gateway if the P6 Reporting Database is installed on a Microsoft SQL Server. It also provides information about how to run the Configuration Utility and configure P6 Reporting Database with BI Publisher.<br>All administrators should read this guide. |
| *P6 Analytics Post Installation Administrator's Guide* | This guide provides information about P6 Analytics administrative tasks. It also includes information for Star security configuration, OBI installation and configuration, Financial Periods installation and configuration, and for configuring the Secure Sockets layer.<br>All administrators should read this guide. |
| *P6 Analytics Reference Manual* | This manual has examples of sample dashboards and Burn Down activity use cases. It also tells users how to get started with P6 Analytics.<br>All non-administrator users should read this guide. |
| *P6 EPPM and P6 Analytics 3.2 System Architecture Data Sheet* | The data sheet provides information on P6 EPPM, P6 Analytics, and P6 Reporting Database. It also provides a diagram to show how all products work together.<br>All administrators should read this guide. |
| *Security Guidance for P6 Analytics and P6 Reporting Database* | This guide enables you to plan your security strategy for P6 Analytics and P6 Reporting Database. It includes information on safe deployments, authentication options, and specific security settings for the Star and ODS database.<br>All administrators should read this guide. |
| *Tested Configurations* | Lists the configurations that have been tested and verified to work with P6 Analytics.<br>The network administrator/database administrator and P6 Analytics administrator should read this document. |

### Distributing Information to the Team

You can copy the online documentation to a network drive for access by project participants. Each team member can then view or print those portions that specifically relate to his or her role in the organization.

Throughout this documentation, the Security Guidance icon 🔒 helps you to quickly identify security-related content to consider during the installation and configuration process.

## Where to Get Training

To access comprehensive training for all Primavera products, go to:

http://education.oracle.com

## Where to Get Support

### Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/us/support/contact-068555.html or visit http://www.oracle.com/us/corporate/accessibility/support/index.html if you are hearing impaired.

### Using Primavera's Support Resource Centers

Primavera’s Support Resource Center provides links to important support and product information. Primavera's Product Information Centers (PICs) organize documents found on My Oracle Support (MOS), providing quick access to product and version specific information such as important knowledge documents, Release Value Propositions, and Oracle University training. PICs also offer documentation on Lifetime Management, from planning to installs, upgrades, and maintenance.

Visit https://support.oracle.com/epmos/faces/DocumentDisplay?id=1486951.1 to access links to all of the current PICs.

PICs also provide access to:

- **Communities** which are moderated by Oracle providing a place for collaboration among industry peers to share best practices.
- **News** from our development and strategy groups.
- **Education** via a list of available Primavera product trainings through Oracle University. The Oracle Advisor Webcast program brings interactive expertise straight to the desktop using Oracle Web Conferencing technology. This capability brings you and Oracle experts together to access information about support services, products, technologies, best practices, and more.

# Legal Notices

Oracle Primavera Security Guidance for P6 Analytics and P6 Reporting Database