PRIMAVERA

Security Guidance for P6 Reporting Database
Release 3.0

January 2013

Copyright

Oracle Primavera Security Guidance for P6 Reporting Database

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 failsafe, 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.

This software or hardware and documentation may provide access to or information on 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. 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.

To view the list of third party technology disclosures related to this product, please see the *Commercial Notices and Disclosures* document for the release.

Contents

Preface

With P6 Reporting Database, you can generate databases that can be used to extract and transform data from the P6 EPPM database. You can use this data to create reports using Oracle Business Intelligence Suite or other third-party reporting tools

The two types of databases are the Operational Data Store (ODS) and the Star Schema Database (Star).

In This Section

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. See Additional Sources for Security Guidance for links to information that can help you get started.
- 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 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**
  - Must have read and write privileges to access this file.
  - Contains given paths, DB usernames, installation options, and encrypted passwords.
  - Protect and back up this file.

  Default Location = <installation path>\star\res\
- **odsetl.properties**
  - Must have read and write privileges to access this file.
  - Contains given paths, DB usernames, 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, Microsoft Windows Active Directory, and Microsoft Windows Active Directory Lightweight Directory Services (AD LDS). 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 login to a P6 EPPM application.

When connecting P6 Reporting Database to BI Publisher, you will 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 *P6 Reporting DatabaseInstallation and Configuration Guide* 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.

About ODS Security

The ODS security model emulates the P6 EPPM security model. The Resource and Project Access control policies are maintained in ODS. See "ODS Security Configuration" in the *P6 Reporting Database Installation and Configuration Guide* for more information.

ODS Database User Security Guidance

ODS user security has changed between the following releases:

ODS User Security in P6 Reporting Database 2.0 and 2.1

In P6 Reporting Database 2.0 and 2.1, P6 EPPM application users need the report_user_flag set to **'Y'** in the USERS table in the P6 EPPM database. When runetl.bat (or runetl.sh) runs, it checks the USERS table. It creates an ODS database user for the flagged users, with the same username and password as the P6 EPPM users. The new ODS database users are able to view only the data they have permissions to view in the P6 EPPM database.

ODS User Security in P6 Reporting Database 2.2

For P6 Reporting Database 2.2, the administrator must give P6 EPPM users the Enterprise Reports module access so they can be reporting users in the ODS database. If a P6 EPPM user is a reporting user in a previous version, the administrator must still give them module access through P6 EPPM application. Users with the reporting_flag set to **'Y'** will not become reporting users unless they receive Enterprise Reports module access. When granted module access, a database user is created in the ODS instance for the username.

The ODS database users can view only 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 other user's passwords) can reset the database user password to connect directly as the ODS database user.

ODS User Security in P6 Reporting Database 3.0

In P6 Reporting Database 3.0, you have two security options: the Database Security Model and the Security Package (SECPAC). For the database model, database users are created for you, and their views are based on what they have security access to view. For the SECPAC model, session variables are set for security. See the *P6 Reporting Database Installation and Configuration Guide* for more information.

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 Installation and Configuration Guide* (or the *P6 Analytics 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. See "Star Security Configuration" in the *P6 Reporting Database Installation and Configuration Guide* for more information.

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 database. See the *P6 Reporting Database Installation and Configuration Guide* for more information.

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 usernames are the same in the P6 EPPM database, P6 EPPM Extended Schema, STAR (W_USER_S), and in the OBI\Weblogic server.