ORACLE®

PRIMAVERA

P6 Professional Security Guide

May 2011

Copyright

Oracle Primavera P6 Professional Security Guide

Copyright © 1999, 2011, Oracle and/or its affiliates. All rights reserved.

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

The platform-specific hardware and software requirements included in this document were current when this document was published. However, because new platforms and operating system software versions might be certified after this document is published, review the certification matrix on the My Oracle Support (formerly OracleMetaLink) Web site for the most up-to-date list of certified hardware platforms and operating system versions. The My Oracle Support (formerly OracleMetaLink) Web site is available at the following URL:

http://metalink.oracle.com/

or

http://support.oracle.com/

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable: U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software -- Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

Oracle and Primavera are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners. The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

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

Oracle provides comprehensive, multiproject planning and control software, built on Oracle and Microsoft® SQL Server databases for organization-wide project management scalability. The P6 Professional solution includes P6, which provides comprehensive project and resource management, project analysis across the organization, and allows users to access project management data via the Internet; P6 Progress Reporter, which enables Web-based team communication and time keeping; and P6 Professional, which provides a client/server connection for P6 Professional planning- and scheduling-focused users.P6 Professional provides a client/server connection for planning- and scheduling-focused users.

In This Chapter

P6 Professional Documentation

You can access reference manuals and administrator's guides from the P6 Professional Documentation Center, located in the \Documentation\<language> folder of the P6 Professional physical media or download. Most documentation assumes a standard setup of the product, with full access rights to all features and functions.

Media packs include all files necessary to install P6 Professional applications, all manuals and technical documents related to the installation, administration, and use of P6 Professional components, and the Quick Install Guide. For information on the contents of the P6 Professional Media Pack, see the *P6 Professional Quick Install Guide*.

The following table describes documentation publications and lists the recommended readers by role. P6 Professional roles are described in the *P6 Professional Administrator's Guide*.

Title	Description
P6 Professional Administrator's Guide	Explains how to set up the P6 Professional database, servers, and components; it also provides an overview of all the components in the P6 Professional solution. The guide describes the procedures required to administer P6 Professional, including setting up security and configuring global preferences. 🛡 The P6 Professional network administrator/database administrator should read this guide.
Tested Configurations	Lists the configurations that have been tested and verified to work with P6 Professional. The network administrator/database administrator and P6 Professional administrator should read this document.
P6 Professional Standalone Installation and Configuration Guide	Explains how to install and configure P6 Professional as a standalone application.
P6 Professional Help	Explains how to use P6 Professional to plan, set up, and manage projects in a multiuser environment. If you are new to P6 Professional, use this Help to learn how to use the software effectively to plan and manage projects. The P6 Professional administrator, program manager, project manager, resource/cost manager, and team leader should read this Help.
P6 Professional User's Guide	This guide explains how to plan, set up, and manage projects in a multiuser environment. If you are new to P6 Professional, start with this guide to learn how to use the software effectively to plan and manage projects. When you need more detail, refer to the P6 Professional Help. The program manager, project manager, resource/cost manager, and team leader should read this guide.
Primavera Timescaled Logic Diagram Help	Describes how to create, modify, and manage Timescaled Logic Diagrams. Timescaled Logic Diagrams condense the project schedule displayed in the Gantt Chart into a more readable, easier to understand format that provides a snapshot of the entire project plan and the chains of activities that drive the project schedule.

Title	Description
P6 SDK *Web-based documentation*	Describes how to use the P6 SDK to connect to the P6 Professional database. The tables, fields, and stored procedures that you can access through the P6 SDK are described. Examples are also provided to show how you can use the P6 SDK to perform several basic tasks, such as creating a new project or assigning a resource to a project activity. The P6 Professional network administrator/database administrator should read this documentation, which is available in *local drive*\Program Files\Oracle\Primavera P6 Professional\PMSDK\Doc\ by default. Double-click the INDEX.HTML file to open the Table of Contents.
P3 to P6 Professional Migration Guide	This guide provides best practices for migrating your P3 data to P6 Professional, and details how P3 functionality maps to P6 Professional functionality.

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 Documentation Updates

For the latest updates to the P6 Professional Documentation library, go to **http://download.oracle.com/docs/cd/E23006_01/index.htm**.

Where To Get Training

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

http://education.oracle.com

Where to Get Support

If you have a question about using Oracle products that you or your network administrator cannot resolve with information in the documentation or help, go to:

http://www.oracle.com/us/support/index.html

This page provides the latest information on contacting Oracle Global Customer Support and the support renewals process.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit ***http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info*** or visit ***http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs*** if you are hearing impaired.

P6 Professional Security Guide

The *P6 Professional Security Guide* provides guidelines on creating an overall secure environment for P6 Professional. It summarizes security options to consider for each installation and configuration process and details additional security steps that you can perform before and after P6 Professional implementation.

Security Guidance Overview

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

▸ Review all security documentation for applications and hardware components that interact or integrate with P6 Professional. Hardening your environment is recommended. See *Additional Sources for Security Guidance* (on page 17) for links that can help you to get started.

▸ Read through the summary of considerations for P6 Professional included in this document. Areas covered include: safe deployment, authentication options, authorization, confidentiality, sensitive data, reliability, and cookies usage.

▸ 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 Professional 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 Professional applications. For example, if you configure WebLogic to use only SSL v3.0, you must disable TLS v1.0 for the client JRE for P6 to launch properly. If using an Internet Explorer browser, you must also disable TLS v1.0 in Internet Options.

Safe Deployment of P6 Professional

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

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

Administrative Privileges Needed for Installation and Operation

As the P6 Professional Administrator, you should determine the minimum administrative privileges or permissions needed for installation, configuration, and daily operation of P6 Professional. For example, to successfully install the required JRE for P6 Professional Web applications (for example, P6 and P6 Progress Reporter), you must be an administrator on the client machine during this installation or update.

Minimum Client Permissions Needed for P6 Professional

Users do not have to be administrators on their machines to run P6 Professional. Instead, you can grant minimum permissions to create a more secure environment.

The following is a summary of the minimum system requirements needed to access and run components of P6 Professional R8.1:

Files within Window Folders:

▸ *local drive*\Program Files\Oracle\Primavera P6\P6 Professional

dbexpsda40.dll

dbexpsda30.dll

dbexpint.dll

dbexpoda40.dll

dbexpoda30.dll

DbExpPrC.dll (only needed when using Compression Server)

dbexpsda.dll

dbxadapter30.dll (only needed when using Compression Server)

Read&Execute/Read permission to access files needed to run P6 Professional applications and to create and modify database alias connections.

▸ *local drive*\Program Files\Oracle\Primavera P6\P6 Professional\pm.ini

Read&Execute/Read/Write permission to access the ini file, which is required to log into P6 Professional applications.

▸ *local drive*\Program Files\Oracle\Primavera P6\P6 Professional\Java\

dbconfig.cmd

admin.cmd

Read&Execute/Read permissions to run the Database Configuration setup, the P6 Administrator application.

For your reference, the following are the default installation locations for the PrmBootStrap.xml file:

Windows XP:

\%USERPROFILE%\Local Settings\Application Data\Oracle\Primavera P6\P6 Professional

Windows Vista and 7:

\%LOCALAPPDATA%\Oracle\Primavera P6\P6 Professional

During installation, the PrmBootStrap.xml file is also copied to one of the locations below, depending on your operating system. The files will never be modified during use of P6 Professional, so they can be copied to the current user location (USERPROFILE or LOCALAPPDATA) if you need to revert P6 Professional back to its original state (for example, if files become corrupted).

Windows XP:

\%ALLUSERSPROFILE%\Application Data\Oracle\Primavera P6\P6 Professional

Windows Vista and 7:

\%PROGRAMDATA%\Oracle\Primavera P6\P6 Professional

▸ Output directory for File > Export, Log output files

Read&Execute/Read/Write to create and write output files.

Registry Keys:

▸ HKEY_LOCAL_MACHINE\Software\Primavera

READ

> **Note:** For the Update Baseline and Schedule Comparison/Claim Digger tools, the key is opened in Read/Write/Delete mode.

Physical Security Requirements for P6 Professional

All hardware hosting P6 Professional should be physically secured to maintain a safe implementation environment. Consider the following when planning your physical security strategy:

▶ Components of the intended environment should be properly installed, configured, managed, and maintained according to guidance in all applicable Administrator's Guides for P6 Professional.

▶ Components of P6 Professional should be installed in controlled access facilities to prevent unauthorized physical access. Only authorized administrators for the systems hosting P6 Professional should have physical access to those systems. Such administrators include the Operating System Administrators, Application Server Administrators, and Database Administrators.

▶ Administrator access to client machines should only be used for installation and configuration of P6 Professional modules.

Files to Protect after Implementation

While P6 Professional requires specific files for installation and configuration, some are not needed for daily operations. Although not intended as a comprehensive list, the following are files that should be protected or moved to a secure location after installation and configuration:

▶ **DatabaseSetup.log**

Captures processes performed during P6 Professional database installation.

Default Location = user home directory (for example, C:\Documents and Settings\Administrator)

▶ **adminpv.cmd** (or **adminpv.sh** for Linux)

Launches the P6 Administrator application.

Default location = P6 home directory, as specified during installation

▶ **dbconfigpv.cmd** (or **dbconfig.sh** for Linux)

Tool used to create the connection between the P6 Professional database and P6.

Default location = P6 home directory, as specified during installation

▶ **p6-emplugin.jar**

A P6 Professional-specific plug-in used to enable the display of P6 metrics in Oracle Enterprise Manager.

Default location = P6 home directory, as specified during installation

Authentication Options for P6 Professional

Authentication determines the identity of users prior to granting access to P6 Professional modules. P6 Professional offers the following authentication modes:

▸ **Native** authentication is the default mode for P6 Professional. In this mode, when a user attempts to log into a P6 Professional application, authentication is handled directly through the module with the P6 Professional database acting as the authority.

▸ **Single Sign-On** authentication, which provides access control for Web applications, is available for P6 Progress Reporter and P6. In this mode, when a user attempts to log into a P6 Professional application (protected resource), a Web agent intercepts the request and prompts the user for login credentials. The user's credentials are passed to a policy server and authenticated against a user data store. With Single Sign-On, a user logs on only once and is authenticated for all Web applications for the duration of the browser session (provided that all Web applications authenticate against the same policy server).

▸ **LDAP** (Lightweight Directory Access Protocol) is directory-based authentication and is available for all P6 Professional applications. In this mode, when a user attempts to log into a P6 Professional application, the user's identity is confirmed in an LDAP-compliant directory server database. Additionally, P6 Professional supports the use of LDAP referrals with Oracle Internet Directory and Microsoft Windows Active Directory. Referrals chasing allows authentication to extend to another domain.

You can also configure multiple LDAP servers to use for authentication. This allows failover support and enables you to search for users in multiple LDAP stores.

The use of Single Sign-On or LDAP will help you to create the most secure authentication environment available in P6 Professional.

The use of LDAP will help you to create the most secure authentication environment available in P6 Professional.

Authorization for P6 Professional

Appropriate authorization should be granted carefully to all users of P6 Professional. The most secure application security options are detailed in the *P6 Professional Administrator's Guide*.

To help you with security planning, the following are authorization-related options to consider:

▸ Use Module Access rights to limit access to P6 Professional modules.

- Use Global profiles to limit privileges to global data. Assign the Admin Superuser account sparingly.
- Use Project profiles to limit privileges to project data. Assign the Project Superuser account sparingly.
- Assign OBS elements to EPS and WBS nodes to limit access to projects.
- Assign resource access limitations to each user.

Confidentiality for P6 Professional

Confidentiality ensures that stored and transmitted information is disclosed only to authorized users. In addition to the documentation included with other applications and hardware components, follow the P6 Professional-specific guidance below.

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

Sensitive Data for P6 Professional

Measures should be taken to protect sensitive data in P6 Professional, such as user names, passwords, and e-mail addresses. Use the process below as an aid during your security planning:

- Identify which P6 Professional modules will be used.
- Determine which modules and interacting applications display or transmit data that your organization considers sensitive. For example, P6 allows the display of sensitive data, such as costs and secure codes.
- Implement security measures in P6 Professional 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 Professional, as detailed in the documentation included with those applications. For example, be sure to follow the security guidance provided with Oracle WebLogic.

Reliability for P6 Professional

The following measures can be taken to protect against attacks that could cause a denial of service:

▶ Ensure that the latest security patches are installed.
▶ Replace the default Admin Superuser (admin) immediately after a manual database installation or an upgrade from P6 version 7.0 and earlier.
▶ Ensure that log settings meet the operational needs of the server environment. Refrain from using "Debug" log level in production environments.
▶ Document the configuration settings used for servers and create a process for changing them.
▶ Consider setting a maximum age for the session cookie on the application server.
▶ Protect access to configuration files with physical and file system security.

Additional Sources for Security Guidance

The databases, platforms, and servers that you use for your P6 Professional implementation should be properly secured. Although not intended as a comprehensive list, you might find the links below helpful when planning your security strategy.

> **Note:** Due to the dynamic nature of the Web, the URLs below might have changed since publication of this guide.

Oracle Database

http://download.oracle.com/docs/cd/B19306_01/network.102/b14266/toc.htm

Microsoft SQL Server 2005 Database

http://www.microsoft.com/sqlserver/2005/en/us/security.aspx

Microsoft SQL Server 2008 Database

http://www.microsoft.com/sqlserver/2008/en/us/Security.aspx

Microsoft Windows 2008 Server

http://technet.microsoft.com/en-us/library/dd548350(WS.10).aspx

Microsoft Windows 2003 Server

http://www.microsoft.com/downloads/details.aspx?familyid=8A2643C1-0685-4D89-B655 -521EA6C7B4DB&displaylang=en

Oracle WebLogic

http://download.oracle.com/docs/cd/E12839_01/web.1111/e13710/intro.htm#sthref8

http://download.oracle.com/docs/cd/E15523_01/web.1111/e13707/toc.htm

http://download.oracle.com/docs/cd/E15523_01/web.1111/e13705/intro.htm

http://download.oracle.com/docs/cd/E12840_01/wls/docs103/secmanage/ssl.html

Oracle Fusion Middleware Security Guides

http://download.oracle.com/docs/cd/E12839_01/security.htm