PRIMAVERA

P6 EPPM Security Guide
Release 8.0

Copyright

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.

Contents

Section 1

P6 EPPM Security Guide

The *P6 EPPM Security Guide* provides guidelines on creating an overall secure environment for P6 EPPM. 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 EPPM implementation.

Security Guidance Overview

During the installation and configuration process for P6 EPPM, 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 EPPM applications. Use the following guidelines to plan your security strategy for P6 EPPM:

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

Tip

As with any software product, be aware that security changes made for third party applications might affect P6 EPPM applications. For example, if you configure WebLogic to only use SSL v3.0, you must disable TLS v1.0 for the client JRE in order 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 EPPM

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

Administrative Privileges Needed for Installation and Operation

As the P6 EPPM Administrator, you should determine the minimum administrative privileges or permissions needed for installation, configuration, and daily operation of P6 EPPM. For example, to successfully install the required JRE for P6 EPPM 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 and P6 Progress Reporter

Because P6 and P6 Progress Reporter are Web applications, users do not have to be administrators on their machines to run them. Instead, you can successfully run these applications with security at the highest level to create a more secure environment.

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:

Files within Window Folders:

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

  dbexpsda40.dll

  dbexpsda30.dll

  dbexpint.dll

  dbexpoda40.dll

  dbexpoda30.dll

  DbExpPrC.dll

  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 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\Primavera P6 Professional\Java\

  dbconfig.cmd

admin.cmd

Read&Execute/Read permissions to run the Database Configuration setup, the P6 Administrator application, and API tools (Update Baseline and Schedule Comparison/Claim Digger).

Write permission may be required for the Database Configuration Setup utility (dbconfig.cmd) for the API tools if you need to create a new configuration and update the BREBootStrap.xml file with the new database configuration information.

For your reference, the following are the default installation locations for the PrmBootStrap.xml and BREbootstrap.xml files:

- Windows XP:

  \%USERPROFILE%\Local Settings\Application Data\Primavera P6 Professional
- Windows Vista and 7:

  \%LOCALAPPDATA%\Primavera P6 Professional

During installation, the PrmBootStrap.xml and BREbootstrap.xml files are 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\Primavera P6 Professional
- Windows Vista and 7:

  \%PROGRAMDATA%\Primavera 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 EPPM

All hardware hosting P6 EPPM 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 EPPM.
- Components of P6 EPPM should be installed in controlled access facilities to prevent unauthorized physical access. Only authorized administrators for the systems hosting P6 EPPM 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 EPPM components.

Application Security Settings in P6 EPPM

P6 EPPM contains a number of security settings at the application level. All of these settings are detailed in the *P6 EPPM Administrator's Guide*. Use the Security Guidance icon  to quickly identify them.

To help you organize your planning, the following is a sampling of recommended options to consider:

- In your production environment, opt for empty data instead of sample data during the P6 EPPM database setup.
- Turn on Password Policy in Application Settings. An enabled Password Policy will increase the required length and quality of the password.
- In the P6 Administrator application:
  - evaluate the Login Lockout Count; the default is 5.
  - keep Multiple User for the Content Repository authentication mode.
  - use Security Accounts if using Oracle Universal Content Management for the Content Repository.
  - use STRONG for the Directory Services security level.
  - keep the Enable Cross Site Scripting Filter setting set to true.
  - enable LDAP or WebSSO for authentication.
  - keep the HTTPS authentication setting enabled.

Files to Protect after Implementation

While P6 EPPM 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 EPPM 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 EPPM database and P6.

  Default location = P6 home directory, as specified during installation
- **p6-emplugin.jar**

  A P6 EPPM-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 EPPM

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

- **Native** authentication is the default mode for P6 EPPM. In this mode, when a user attempts to log into a P6 EPPM application, authentication is handled directly through the module with the P6 EPPM 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 EPPM 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 EPPM applications. In this mode, when a user attempts to log into a P6 EPPM application, the user's identity is confirmed in an LDAP-compliant directory server database. Additionally, P6 EPPM supports the use of LDAP referrals with Oracle Internet Directory, Microsoft Windows Active Directory, and Microsoft Windows Active Directory Lightweight Directory Services (AD LDS). Referrals chasing allows authentication to extend to another domain.

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

P6 EPPM Web Services offers its own authentication options. If you use SAML for P6 EPPM Web Services, you must use Single Sign-on or LDAP authentication for P6 EPPM. See P6 EPPM Web Services Settings and the *P6 Web Services Programmer's Guide* for more information on P6 EPPM Web Services authentication options.

Authorization for P6 EPPM

Appropriate authorization should be granted carefully to all users of P6 EPPM. The most secure application security options are detailed in the *P6 EPPM 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 EPPM 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 EPPM

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 EPPM-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 at rest, refer to the documentation included with the database server for instructions on securing the database.

Sensitive Data for P6 EPPM

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

- Identify which P6 EPPM 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 EPPM 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 EPPM, 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 EPPM

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.

Cookies Usage in P6 EPPM

View the details below for information on when cookies are created and stored when using P6 and P6 Progress Reporter. As stated in ***Reliability for P6 EPPM*** (on page 12), consider setting a maximum age for the session cookie on the application server.

Cookies Usage in P6

When using P6, the following cookies are generated by the server and sent to the user's browser. They are stored on the user's machine, either temporarily by the browser, or permanently until they expire or are removed manually.

Cookie Name	Description	Scope	Retention	Encrypted?
ORA_PWEB_CLIENTLOCALE_1111	Browser client locale	/p6/	One year	No
ORA_PWEB_SELECTED_DBID_1111	The last database identifier selected by the user	/p6/	One year	No
ORA_PWEB_IA_HD_CODE_1111	IP and identifier of client machine	/p6/	One year	No
ORA_PWEB_LANGUAGE_1111	The translation selected by the user	/p6/	One year	No
ORA_PWEB_Composite_Cookie_1111	Login and user customizations accumulated throughout the session	/p6/	One year	No
ORA_PWEB_COMPOSITE_SESSION_COOKIE_1111	Statistics portlet customizations	/p6/	None (expires at end of session)	No

JSESSIONID	Session identifier	default	None (expires at end of session)	No
sw	Applies only for P6 Help systems. The last search term used in the search tab located on the table of contents frame.	Current working directory only on the current host (for example, if located at http://*host*/p6help, only valid for the http://*host*/p6help directory).	None (expires at end of session)	No
sm	Applies only for P6 Help systems. The type of search used in the search tab located on the table of contents frame. Value corresponds as: 0: All words, 1: Any words, 2: Exact phrase. Any other value is invalid.	Current working directory only on the current host (for example, if located at http://*host*/p6help, only valid for the http://*host*/p6help directory).	None (expires at end of session)	No
style	Applies only for P6 Help systems. The current style for the help reference manual. Only valid values are "contrast" or "default".	Any location on the current domain.	One year	No

Cookies Usage in P6 Progress Reporter

When using P6 Progress Reporter, the following cookies are generated by the server and sent to the user's browser. They are stored on the user's machine, either temporarily by the browser, or permanently until they expire or are removed manually.

Cookie Name	Description	Scope	Retention	Encrypted?
ORA_PR_OPENMETHOD_1111	Saves the method to load activities into Timesheet in Progress Reporter based on user's selected options	/pr/	One year	No
ORA_PR_AUTOINC_1111	Selects the option for adding completed assignments in the dialog	/pr/	One year	No
ORA_PR_COPYADD_1111	Determines whether to select the add current option in the open dialog	/pr/	One year	No
ORA_PR_ COPYINC_1111	Determines whether to select the copy completed option in the open dialog	/pr/	One year	No
ORA_PR_HIGHBANDWIDTH_1111	Has the user specified that the network connection is fast?	/pr/	One year	No

Cookie Name	Description	Scope	Retention	Encrypted?
sw	Applies only for P6 Help systems. The last search term used in the search tab located on the table of contents frame.	Current working directory only on the current host (for example, if located at http://*host*/p6help, only valid for the http://*host*/p6help directory).	None (expires at end of session)	No
sm	Applies only for P6 Progress Reporter Help systems. The type of search used in the search tab located on the table of contents frame. Value corresponds as: 0: All words, 1: Any words, 2: Exact phrase. Any other value is invalid.	Current working directory only on the current host (for example, if located at http://*host*/p6help, only valid for the http://*host*/p6help directory).	None (expires at end of session)	No
ORA_PHELP_1111	Applies only for P6 Progress Reporter Help systems. The current style for the help reference manual. Only valid values are "contrast" or "default".	Any location on the current domain.	One year	No

Additional Sources for Security Guidance

The databases, platforms, and servers that you use for your P6 EPPM 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