



PRIMAVERA

P6 EPPM Security Guide 16 R2

March 2018

Contents

P6 EPPM Security Guide.....	5
Security Guidance Overview	5
Safe Deployment of P6 EPPM	5
Administrative Privileges Needed for Installation and Operation	5
Minimum Client Permissions Needed for P6 and P6 Team Member Web.....	6
Minimum Client Permissions Needed for P6 Professional.....	6
Physical Security Requirements for P6 EPPM	7
Application Security Settings in P6 EPPM.....	7
Files to Protect after Implementation	8
Authentication Options for P6 EPPM	8
Authorization for P6 EPPM	9
Confidentiality for P6 EPPM.....	9
Sensitive Data for P6 EPPM	10
Reliability for P6 EPPM	10
Cookies Usage in P6 EPPM.....	10
Cookies Usage in P6.....	11
Cookies Usage in P6 Team Member Web.....	12
Additional Sources for Security Guidance	14
Legal Notices	15

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 need to create a highly secure environment for all P6 EPPM environments. 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. Oracle recommends you harden your environment. See ***Additional Sources for Security Guidance*** (on page 14) for links to information that can help you 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.

Tips

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 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 EPPM

To ensure overall safe deployment of P6 EPPM, you should carefully plan security for all components, such as database servers and client computers 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 consider the minimum administrative privileges or permissions needed to install, configure, and operate P6 EPPM. For example, to successfully install the required JRE for P6 EPPM Web applications (for example, P6), you must be an administrator on the client machine during this installation or update.

Minimum Client Permissions Needed for P6 and P6 Team Member Web

Because P6 and P6 Team Member Web 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 list summarizes the minimum system requirements needed to access and run components of P6 Professional 16 R2:

Files within Folders:

To run P6 Professional, users require Read & Execute permissions for the following files:

- ▶ *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)

To log into P6 Professional applications, users require Read&Execute/Read/Write permissions to access the ini file.

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

To run the Database Configuration setup and the Primavera P6 Administrator users require Read&Execute/Read permissions for the following files:

- ▶ *local drive*\Program Files\Oracle\Primavera P6\P6 Professional\Java\
 - dbconfig.cmd
 - admin.cmd

Note: 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 PrmBootstrapV2.xml and BREbootstrap.xml files:

- %LOCALAPPDATA%\Oracle\Primavera P6\P6 Optional Client
- %LOCALAPPDATA%\Oracle\Primavera P6\P6 Professional

During installation, the PrmBootStrapV2.xml and BREbootstrap.xml files are also copied to the location below. The files will never be modified while using 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).

\\%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 tool, the key opens in Read/Write/Delete mode.

Physical Security Requirements for P6 EPPM

You should physically secure all hardware hosting P6 EPPM to maintain a safe implementation environment. Consider the following when planning your physical security strategy:

- ▶ You should install, configure, manage, and maintain your environment according to guidance in all applicable installation and configuration documentation for P6 EPPM.
- ▶ You should install P6 EPPM components in controlled access facilities to prevent unauthorized 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.
- ▶ You should use Administrator access to client machines only when you install and configure P6 EPPM modules.

Application Security Settings in P6 EPPM

P6 EPPM contains a number of security settings at the application level. The *P6 EPPM Application Administrator's Guide* details these settings.

To help you organize your planning, the following are options Oracle recommends:

- ▶ In your production environment, opt for empty data instead of sample data during the P6 EPPM database setup.
- ▶ If using P6 EPPM native authentication, enable Password Policy in Application Settings
- ▶ If using LDAP and SSO authentication, configure the LDAP and SSO components to enforce high quality passwords within their password policy settings.
- ▶ Enable firewall software on the application server and database server. Based on your installation, add exceptions for appropriate ports.
For instance, P6 EPPM SQL Server Database runs on 1433 port and Oracle Database runs on 1521 port by default. P6 EPPM and P6 Team Member Web run on 8203 and 8207 ports respectively in the default installation.
- ▶ In the Primavera P6 Administrator:

- ▶ evaluate the Login Lockout Count; the default is 5.
- ▶ set the Enable Cross Site Request Forgery Checking Filter setting to true.
- ▶ set the Enable Session Hijack Checking setting to true.

Caution: If this setting is set to true, the server will bind the user's IP Address with session id for authentication and authorization. If a user's IP address changes, this setting may cause authentication issues. Oracle recommends testing this setting thoroughly before implementation.

- ▶ 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.
- ▶ if using WebSSO, set "Application\Logout URL" in the Primavera P6 Administrator to your SSO logout URL to ensure that the SSO sessions end.

Note: The HTTPS authentication setting requires that web server and application server settings support SSL.

Files to Protect after Implementation

While P6 EPPM requires 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 and their corresponding folders from unauthorized access after installation is complete:

- ▶ **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 Primavera P6 Administrator.
Default location = P6 EPPM home directory, as specified during installation
- ▶ **dbconfigpv.cmd** (or **dbconfig.sh** for Linux)
Used to create the connection between the P6 EPPM database and P6.
Default location = P6 EPPM home directory, as specified during installation

Authentication Options for P6 EPPM

Authentication determines the identity of users before granting access to P6 EPPM modules. P6 EPPM 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. In SSO mode, the 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 applications. You can use 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. An LDAP directory server database confirms the user's identity when they attempt to login to the application.

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 the *P6 EPPM System Administrator's Guide* for more information on P6 EPPM Web Services authentication options.

Authorization for P6 EPPM

Grant authorization carefully to all appropriate P6 EPPM users. The *P6 EPPM Application Administration Guide* details the most secure application security options.

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

- ▶ 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 nodes to limit access to projects.
- ▶ Assign resource access limitations to each user.

Confidentiality for P6 EPPM

Confidentiality ensures only authorized users see stored and transmitted information. 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 you use LDAP or SSO authentication, ensure you use LDAPS to connect to the directory server.

- ▶ For data in transit, use SSL/TLS to protect network connections among modules. If you use LDAP authentication, ensure you use LDAPS to connect to the directory server.
- ▶ For data in transit, disable http listener on your application server or fronting web server, only allow https connections from browsers.
- ▶ For data at rest, refer to the documentation included with the database server for instructions on securing the database.

Sensitive Data for P6 EPPM

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

- ▶ Identify which P6 EPPM modules you will use.
- ▶ Determine which modules and interacting applications display or transmit data that your organization considers sensitive. For example, P6 displays 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, follow the security guidance provided with Oracle WebLogic.

Reliability for P6 EPPM

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.
- ▶ Setting a maximum age for the session cookie on the application server.
- ▶ Protecting 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 Team Member Web. As stated in **Reliability for P6 EPPM** (on page 10), set a maximum age for the session cookie on the application server.

Cookies Usage in P6

When using P6, the server may generate the following cookies and send them to the user's browser. The user's machine stores the cookies, either temporarily by the browser, or permanently until they expire or are removed manually.

Cookie Name	Description	Scope	Retention	Encrypted ?
ORA_PWEB_CLIENTLOCAL_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 the Help system. Stores the last search term used in the help system.	Current working directory only on the current host (for example, if located at <code>http://host/help</code> , only valid for the <code>http://host/help</code> directory).	None (expires at end of session)	No
sm	Applies only for the Help system. Stores the type of search used in the help system. 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 <code>http://host/help</code> , only valid for the <code>http://host/help</code> directory).	None (expires at end of session)	No
ORA_PHELP_1111	Applies only for the Help system. Stores the current style for the help system. Only valid values are "contrast" or "default".	Any location on the current domain.	One year	No

Cookies Usage in P6 Team Member Web

When using P6 Team Member Web, the server may generate the following cookies and send them to the user's browser. The user's machine stores the cookies, either temporarily by the browser, or permanently until they expire or are removed manually.

Cookie Name	Description	Scope	Retention	Encrypted ?
JSESSIONID	Session Identifier	/p6tmweb	None	No
ORA_OPEN_TS_CHOICE	Saves the method that loads activities into a timesheet in P6 TimeSheet based on a user's selected options	/p6tmweb	One year	No
ORA_ADD_COMP	Determines whether to select the Add Completed Tasks option in the Open Timesheet Settings dialog box	/p6tmweb	One year	No
ORA_COPY_COMP	Determines whether to select the Copy Completed Tasks option in the Open Timesheet Settings dialog box	/p6tmweb	One year	No
ORA_ADD_CURR	Determines whether to select the Add Current Tasks option in the Open Timesheet Settings dialog box	/p6tmweb	One Year	No
sw	Applies only for the Help system. Stores the last search term used in the help system.	Current working directory only on the current host (for example, if located at <code>http://host/help</code> , only valid for the <code>http://host/help</code> directory).	None (expires at end of session)	No

sm	Applies only for the Help system. Stores the type of search used in the help system. 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 <code>http://host/help</code> , only valid for the <code>http://host/help</code> directory).	None (expires at end of session)	No
ORA_PHELP_1111	Applies only for the Help system. Stores the current style for the help system. Only valid values are "contrast" or "default".	Any location on the current domain.	One year	No

Additional Sources for Security Guidance

You should properly secure the databases, platforms, and servers that you use for P6 EPPM. You might find the links below helpful when planning your security strategy (not a comprehensive list).

Note: The URLs below might have changed after Oracle published this guide.

Oracle Database

<https://docs.oracle.com/database/121/DBSEG/toc.htm>

Oracle Linux Security Guide

<http://www.oracle.com/technetwork/articles/servers-storage-admin/secure-linux-env-1841089.html>

Microsoft SQL Server 2014 SP1 Database

<https://www.microsoft.com/en-us/server-cloud/products/sql-server/Resources.aspx>

Microsoft Windows 2012 R2 Server

<https://www.microsoft.com/en-us/server-cloud/products/sql-server-editions/overview.aspx>

Oracle WebLogic

<http://www.oracle.com/technetwork/middleware/weblogic/documentation/index.html>

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

Legal Notices

Oracle Primavera P6 EPPM Security Guide

Copyright © 1999, 2017, Oracle and/or its affiliates. All rights reserved.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are “commercial computer software” pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

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.