Oracle
Primavera
P6 Professional Security Guide for On-Premises

Version 20
December 2020

Contents

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.

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.

Administrative Privileges Needed for Installation and Operation

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

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:

Files

The following files in <local drive>\Program Files\Oracle\Primavera P6\P6 Professional require **Read&Execute/Read** permission to run P6 Professional applications and to create and modify database alias connections:

- dbconfig.cmd
- dbexpsda30.dll
- dbexpsda40.dll
- dbexpoda40.dll
- dbexpoda30.dll
- dbexpoda40.dll
- dbexpsda.dll

The following file in <local drive>\Program Files\Oracle\Primavera P6\P6 Professional\P6Tools requires **Read&Execute/Read** permission to log in to P6 Professional applications:

- PrimaveraAdminConfig.exe

The default location for **pm.ini** and **PrmBootStrapV2.xml** is \%LOCALAPPDATA%\Oracle\Primavera P6\P6 Professional.

During installation, this file is also copied to \%PROGRAMDATA%\Oracle\Primavera P6\P6 Professional. This file is not modified during use of P6 Professional, so you can copy it 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).

The Output directory for File, Export, Log output files requires **Read&Execute/Read/Write** to create and write output files.

Physical Security Requirements for P6 Professional

You should physically secure all hardware hosting P6 Professional 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 Professional.
- You should install P6 Professional components in controlled access facilities to prevent unauthorized 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.
- You should use Administrator access to client machines only when you install and configure P6 Professional modules.

Authentication Options for P6 Professional

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

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

Lightweight Directory Access Protocol (LDAP) authenticates users through a directory and is available for P6 Professional applications. P6 Professional 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 login to a P6 Professional application.

LDAP helps you create the most secure authentication environment available in P6 Professional.

Authorization for P6 Professional

Grant authorization carefully to all appropriate P6 Professional users.

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

- 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 only authorized users see stored and transmitted information. 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 you use LDAP 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.

Sensitive Data for P6 Professional

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

- 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 on each user's hard drive to protect data cached by P6 Professional. For example, use endpoint encryption.
- Implement security measures for applications that interact with P6 Professional, as detailed in the documentation included with those applications.
- Implement consent notices in P6 Professional to gather the consent of users to store, use, process and transmit personal information (PI) and to alert users when there is a risk of PI being exposed.

Reliability for P6 Professional

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.

Cookies Usage in P6 Professional

Oracle might use cookies for authentication, session management, remembering application behavior preferences and performance characteristics, and to provide documentation support.

Also, Oracle might use cookies to remember your log-in details, collect statistics to optimize site functionality, and deliver marketing based on your interests.

Additional Sources for Security Guidance

You should properly secure the databases, platforms, and servers you use for your P6 Professional. You might find the links below helpful when planning your security strategy.

Oracle Database 12c

https://docs.oracle.com/database/121/nav/portal_25.htm

Oracle Linux Security Guide

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

Microsoft Windows Server 2012

https://technet.microsoft.com/en-us/library/jj898542.aspx

Microsoft SQL Server 2012 Database

https://msdn.microsoft.com/en-us/library/bb283235(v=sql.110).aspx

Microsoft SQL Server 2014 Database

https://msdn.microsoft.com/en-us/library/bb283235(v=sql.120).aspx

Note: This is not a comprehensive list.

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 need to create a highly secure environment for all P6 Professional environments. 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. Oracle recommends you harden your environment. See ***Additional Sources for Security Guidance*** (on page 8) for links to information that can help you 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.

Tips

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

Encryption for P6 Professional

P6 Professional uses external AES encryption to store various database and integration passwords. During the installation or upgrade of your P6 Professional database, the Installation Wizard can create an AES encryption key which is stored in a Java Keystore file (p6keystore.jks).

You do not need to use a keystore for your P6 Professional database, but Oracle recommends that you do.

The preferred method for enabling external encryption on your database is to run the Installation or Upgrade Wizard, as they generate and copy the required files to the correct locations.

Using the P6 Professional Keystore Installer

Certain administrative actions require you to use the P6 Keystore Installer. For example, if you need to change the P6 Professional keystore password or want to see a list of all keys stored in the keystore file.

This section describes common uses of the Keystore Installer.

Creating a New Keystore for P6 Professional

To create a new keystore using the Keystore Installer:

1) Using your command-line interface, navigate to the P6 database folder. For example, P6EPPM_1/Database.
2) Do the following, depending on your OS:

For Windows, run: installp6keystore.bat -createnew

For Linux, run: installp6keystore.sh -createnew

3) Enter and confirm the password for the new keystore.

This will create a new keystore using the password you entered and a passwordfile for the location where you created the keystore.

Copying a Key for P6 Professional

P6 Professional encryption requires you to have a keystore and password file in each of the module folders associated with the installation.

To transfer a keystore file located in your database folder:

1) Copy your existing p6keystore.jsk file to the <EPPM_Home>/P6 folder.
2) Depending on your OS do the following:

   For Windows, run: <EPPM_Home>\database\installp6keystore.bat -genpassfile

   For Linux, run: ../database/installp6keystore -genpassfile
3) The Keystore Installer will create a p6kspass.pwf in the P6 folder.
4) Repeat steps 1 and 2 for the following P6 folders:

   <EPPM_HOME>/ws

   <EPPM_HOME>/tmws

   <EPPM_HOME>/api

   <EPPM_HOME>/p6procloudconnect

   Note: You must generate a new password file for each location, as the password file is bound to the folder it was created in.
5) Run the database configuration wizard (dbconfigpv.cmd or sh) to regenerate the BREBootStrap.xml file.

   Note: For more information on running the database configuration wizard, see the database administrators guide.

Uninstalling the Keystore for P6 Professional

If you decide you no longer want to use a keystore with your P6 Professional database, you can uninstall the keystore.

To uninstall the keystore:

1) Remove the p6keystore.jks file from your <EPPM_HOME>/database folder.
2) Run databaselogins.cmd (on Windows) or databaselogin.sh (on Linux).
3) Reset the Privileged User password.

Changing your Encryption Key for P6 Professional

Changing your encryption key can be a lengthy process. You must generate a new keystore, distribute it to all modules, and re-save stored passwords.

To change your encryption key:

1) Remove the p6keystore.jks file from the /database folder.
2) Do the following, depending on your operating system:
3) For Windows, run: installp6keystore.bat -createnew
4) For Linux, run: installp6keystore.sh -createnew
5) You must then copy the p6keystore.jks file to of the module folders, and generate a new password file. See Copying a Key for more information.
6) Run dbconfigpv.sh or .cmd.
7) Open the Primavera P6 Administrator.
8) Re-save the following fields to encrypt them using the new key:
   - Database/Instance[n]/Password
   - Database/Instance[n]/Content Repository/SharePoint/Password
   - Database/Instance[n]/Content Repository/CMIS/Password
   - Database/Instance[n]/Content Repository/OracleDatabase/Password
   - Database/Instance[n]/BI Publisher/Password
   - Database/Instance[n]/BPM Settings/PCS (SaaS only)/Password
   - Services/Mail Service/Authorized User Password
   - Integration API/RMI/Keystore Password
   - Web Services/Security/Authentication/Signed SAML Tokens/Keystore Password
   - Web Services/Security/Authentication/Signed SAML Tokens/Private Key Password
   - Web Services/Security/Message Protection/Keystore Password
   - Web Services/Security/Message Protection/Private Key Password
   - Authentication/LDAP/SSL Store Password
   - Database Instance/LDAP Connection Settings[n]/Password

> **Note**: You do not need to re-save fields without stored passwords.

Copyright