Oracle
Primavera P6 EPPM
Security Guide for On-Premises

Version 23
December 2023

Oracle Primavera P6 EPPM Security Guide for On-Premises

Primary Author: Oracle Corporation

Contents

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 11) 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.

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 the P6 application server components, you must have administrative access on that server during the 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 default installation folder for P6 Professional is:

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

However, because the install location can be modified, we will refer instead to \\<Install directory>\ in these instructions.

The following list summarizes the minimum system requirements needed to access and run components of P6 Professional Version 23:

Files within Folders:

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

- \\<Install directory>\
  dbexpsda40.dll
  dbexpsqlite40.dll
  dbexpoda40.dll
  dbxadapter.dll

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

- \\<Install directory>\Data\pm.ini

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

- \\<Install directory>\
  dbconfig.exe
  primavera.adminconfig.exe

During installation, the PrmBootStrapV2.xml file is copied from the install location to the user location. It will also be copied to this location if it is not present when P6 Professional starts or during database configuration. The version of the file stored in the install location will never be modified while using P6 Professional, so it can be copied to the current user location if you need to revert P6 Professional back to its original state (for example, if files become corrupted).

- To run P6 Professional, users require Read permission to the following file:
  \\<Install directory>\Data\ PrmBootStrapV2.xml
- To run P6 Professional, users require Read&Execute/Read/Write permissions to the following file:

%APPDATA%\Oracle\Primavera P6\P6 Professional\<VERSION>\PrmBootStrapV2.xml

- To export data and for log files to be created, users require Read&Execute/Read/Write permissions to any location that will be used as an output directory. Depending on your configuration, this might include the %APPDATA% and %LOCALAPPDATA% directories.

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 log in, a Web agent intercepts the request 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 log in, they are logged in to 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, 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.
- Implement consent notices in P6 EPPM 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 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 cookies in P6 and P6 Team Member Web.

Cookies Usage in P6

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.

Cookies Usage in P6 Team Member Web

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.

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 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

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

Encryption for P6 Professional (P6 EPPM only)

P6 EPPM applications, including P6 Professional, use AES encryption to store various database and integration passwords. By default, encryption and decryption keys are stored as part of the P6 EPPM application. However, you can configure P6 EPPM to use an external key for your environment using a java keystore. See: *P6 EPPM Installation and Configuration Guide for On-Premises*.

For more information, see: ***External Storage Of Encryption Keys For P6 EPPM (Doc ID 2268703.1) https://mosemp.us.oracle.com/epmos/faces/DocumentDisplay?id=2268703.1***

Configuring P6 Professional to Use an External Keystore

If you use a Cloud Connect alias to connect P6 Professional to the EPPM database, the encryption key is accessed server side when the application caches the keystore during initialization. Therefore, when you connect to an EPPM database using Cloud Connect no additional configuration is required to allow P6 Professional to use the external key.

If you use a database direct connection alias to connect P6 Professional to the EPPM database, the alias must be configured to use the new encryption key.

To configure a P6 Professional alias to use an external encryption key you must:

1) Export the key for your P6 EPPM environment from the server-side keystore.
   See: ***Exporting the Key from P6 EPPM*** (on page 12)
2) Configure an alias to use the encryption key.
   See: ***Configuring a P6 Professional Alias to Use an Encryption Key*** (on page 13)

Exporting the Key from P6 EPPM

To export the encryption key from the P6 EPPM keystore:

1) Open a command prompt or terminal.
2) Change current directory to the location of the keystore for your P6 EPPM environment.
3) Use the P6 Keystore Installer with the -exportkeys command to export the key to a p6.key file

   For example:

   - If you are browsing to the database directory where a keystore is present:

     On Windows, type `installp6keystore.bat -exportkeys`

     On Linux, type `./installp6keystore.sh -exportkeys`
   - If you are browsing to a component home directory where a keystore is present but using the database installp6keystore:

     On Windows, type `$path_to_database/installp6keystore.bat -exportkeys`

     On Linux, type `sh $path_to_database/installp6keystore.sh -exportkeys`
   - If you are browsing to a component home directory where a keystore is present but calling the class file directly:

On Windows, type `"%JAVA_HOME%/bin/java" -classpath "lib/prm-common.jar"` com.primavera.common.KeyStoreInstaller -exportkeys

On Linux, type `"$JAVA_HOME/bin/java" -classpath "lib/prm-common.jar"` com.primavera.common.KeyStoreInstaller -exportkeys

Configuring a P6 Professional Alias to Use an Encryption Key

To configure an alias to use an encryption key:

1) Save the p6.key file locally on the workstation running P6 Professional.
2) Run Primavera.Launcher.DBconfig.exe.

   Primavera.Launcher.DBconfig.exe is in the install location of P6 Professional. For example, <local drive>\Program Files\Oracle\Primavera P6\P6 Professional.
3) In the Database Configuration window:
   a. Click **Add**.
   b. On the **Driver Type** list, select your database type.
   c. In the **Database Alias** field, type a name for the alias you will create.
   d. In the **Connection String** field, type the connection string to access your database.
   e. Clear the **Use default database keystore** option.
   f. In the **Keystore file** field, click **Browse...** and browse to the p6.key file.

      The Key Name field will populate with your key.
   g. Click **Next**.
   h. In the **Username** field, type the public login user name for the database.
   i. In the **Password** field, type the public login password for the database.
   j. Click **Test**.
   k. When the connection test completes successfully, click **Save**.

Uninstalling the Keystore

If you decide you no longer want to use a keystore with your P6 EPPM 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

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:
   - For Windows, run: `installp6keystore.bat -createnew`
   - For Linux, run: `installp6keystore.sh -createnew`
3) Copy the p6keystore.jks file to the module folders, and generate a new password file.
4) Run dbconfigpv.sh or .cmd.
5) Open the Primavera P6 Administrator.
6) 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.