ORACLE®
Primavera

Portfolio Management Security Guide
19

December 2019

Contents

Oracle Primavera Portfolio Management Security Guide

The Oracle Primavera Portfolio Management (PPM) Security Guide provides guidelines on creating an overall secure environment for PPM. It summarizes security options to consider for each installation and configuration process and details additional security steps that you can perform before and after PPM implementation.

Security Guidance Overview

During the installation and configuration process for PPM, several options are available that impact security. Depending on your organization's security requirements/policy, you might need to create a highly secure environment. Use the following guidelines to plan your security strategy for PPM:

- Review all security documentation for applications and hardware components that interact or integrate with PPM. Oracle recommends you harden your environment, but be aware of the following: PPM is based on the Microsoft .NET Framework and needs to install assemblies in the Global Assembly Cache, so the PPM installation uses the Microsoft Windows Installer.

  That means the environment should not be hardened before PPM is installed because doing so would cause an installation of PPM to fail. For more information, refer to *Primavera Portfolio Management Enabling Single Sign-On* in the *Oracle Primavera Portfolio Management System Administration Guide*. The environment can be hardened after the installation. However, the hardening needs to be undone whenever a patch, upgrade or new version is installed. This is usually achieved by running “undo” scripts that reverse the hardening. After the patch, upgrade or new version is installed, the hardening needs to be done again. Specific steps for hardening and undoing the hardening depend on the exact operating system version used to host PPM, on the needs of other applications hosted on the same server, as well as on a number of other factors. It is not possible to simply provide steps; and Microsoft no longer provides a simple guide but instead provides numerous tools to achieve hardening.
- Read through the summary of considerations for PPM included in this document. Areas covered include: secure deployment, authentication options, authorization, confidentiality, sensitive data, and reliability.

> **Note:** As with any software product, be aware that security changes made for third party applications might affect the PPM application.

Secure Deployment of PPM

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

Administrative Privileges Needed for Installation and Operation

As the PPM Administrator, you should determine the minimum administrative privileges or permissions needed to install, configure, and operate PPM. For example, when you use the PPM installer you must have full administrative privileges on the server. The minimum privileges required by PPM are documented in this KM article located in the Oracle Support Knowledge Base: https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=1138963.1.

The PPM install grants exactly these privileges and nothing more.

Note: The term "server" in this guide can have one of three meanings, depending on your PPM configuration. It can mean one of the following:

- The PPM Front-End server, which is where IIS resides. Be aware there may be many PPM Front-End servers in one PPM installation.
- The PPM Primary Back-End server, which is where the PPM function engine resides.
- The database server.

Additionally, starting with PPM release 8.0 you have the option to add more back-end servers to enhance performance and scalability. Each additional back-end server is referred to as a PPM Secondary Back-End server.

As a minimum, every installation of PPM must consist of one and only one instance of the Primavera Portfolio Management Primary Back-End, one or more instances of the Primavera Portfolio Management Front-End, and one database server.

A typical configuration has both the PPM Front-End server and the PPM Primary Back-End server on one machine and the database server on another machine.

Minimum Client Permissions Needed for PPM

Because PPM is a Web application, users do not have to be administrators on their machines to run it. Instead, you can successfully run the application with security at the highest level to create a more secure environment.

Physical Security Requirements for PPM

You should physically secure all hardware hosting PPM 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 PPM.
- You should install PPM components in controlled access facilities to prevent unauthorized access. Only authorized administrators for the systems hosting PPM 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 PPM.

MSDTC Security Settings

PPM is a .NET-based application, so there are Microsoft Distributed Transaction Coordinator (MSDTC) security settings that are critical to the security of the application.

You need to ensure that particular settings are selected. If you are using Windows 2008, these settings are located on the Local DTC dialog box Security tab:

- The Network DTC Access option
- The Allow Inbound and Allow Outbound options
- The No Authentication Required option

Ensure that these settings are set correctly on all servers, including the database server.

Refer to the *Installation and Upgrade Guide for Primavera Portfolio Management* for more information about MSDTC settings for PPM and for details about how to set them.

IIS Settings for a Secure PPM Deployment

Refer to the *Installation and Upgrade Guide for Primavera Portfolio Management* for more information about IIS settings for PPM and for details about how to set them.

The information below provides only a brief highlight of a few details.

Ensure the following when configuring for IIS for PPM:

- If you are using Windows 2016 or 2019:

Verify that Role Services for the Web Server are installed as shown below:

Role Service	Windows 2016	Windows 2019
File and Storage Services	Installed	Installed
Web Server (IIS)	Installed	Installed
Expand **Windows Process Activation Service Support** and ensure the following roles are selected		
HTTP Activation	Not available	Not available

Role Service	Windows 2016	Windows 2019
Message Queuing Activation		
Named Pipes Activation		
TCP Activation		
Expand **File and Storage Services** and ensure the following roles are selected:		
File and iSCSI Services	Installed	Installed
Storage Services	Installed	Installed
Expand **File and iSCSI Services** and ensure the following roles are selected:		
File Server	Installed	Installed
Expand **Web Server (IIS)** and ensure the following roles are selected for the Web Server:		
Web Server	Installed	Installed
FTP Server	Installed	Installed
Management Tools	Installed	Installed
Expand **Web Server** and select the following roles:		
Common HTTP Features	Installed	Installed
Health and Diagnostics	Installed	Installed
Performance	Installed	Installed
Security	Installed	Installed
Application Development	Installed	Installed
Expand **Common HTPP Features** and select the following roles:		
Default Document	Installed	Installed
Directory Browsing	Installed	Installed
HTTP Errors	Installed	Installed
Static Content	Installed	Installed
HTTP Redirection	Installed	Installed
WebDav Publishing	Installed	Installed
Expand **Health and Diagnostics** and select the following roles:		
HTTP Logging	Installed	Installed
Custom Logging	Not Installed	Not Installed
Logging Tools	Installed	Installed

Role Service	Windows 2016	Windows 2019
ODBC Logging	Not Installed	Not Installed
Request Monitor	Installed	Installed
Tracing	Installed	Installed
Expand **Performance** and select the following roles:		
Static Content Compression	Installed	
Dynamic Content Compression	Installed	
Expand **Security** and select the following roles:		
Request Filtering	Installed	Installed
Basic Authentication	Installed	Installed
Centralized SSL Certificate Support	Installed	Installed
Client Certificate Mapping Authentication	Installed	Installed
Digest Authentication	Installed	Installed
IIS Client Certificate Mapping Authentication	Installed	Installed
IP and Domain Restrictions	Installed	Installed
URL Authentication	Installed	Installed
Windows Authentication	Installed	Installed
Expand **Application Development** and select the following roles:		
.NET Extendibility 3.5	Installed	Installed
.NET Extendibility 4.6	Installed	Install (.NET Extensibility 4.7)
Application Initialization	Installed	Installed
ASP	Installed	Installed
ASP.NET 3.5	Installed	Installed
ASP.NET 4.6	Installed	Install (ASP .NET 4.7)
CGI	Installed	Installed
ISAPI Extensions	Installed	Installed
ISAPI Filters	Installed	Installed
Server Side Includes	Installed	Installed
WebSocket Protocol	Installed	Installed

Role Service	Windows 2016	Windows 2019
Expand **FTP Server** and select the following roles:		
FTP Service	Installed	Installed
FTP Extensibility	Installed	Installed
Expand **Management Tools** and select the following roles:		
IIS Management Console	Installed	Installed
IIS 6 Management Compatibility	Installed	Installed
[]S Management Scripts and Tools	Installed	Installed
Management Service	Installed	Installed
Expand **IIS 6 Management Compatibility** and select the following roles:		
IIS 6 Metabase Compatibility	Installed	Installed
IIS 6 Management Console	Installed	Installed
IIS 6 Scripting Tools	Installed	Installed
IIS 6 WMI Compatibility	Installed	Installed

For more information, see the *Installation and Upgrade Guide for Primavera Portfolio Management*.

Application Security Settings in PPM

PPM contains a number of security settings at the application level. The *Installation and Upgrade Guide for Primavera Portfolio Management* provides procedures for setting security within the application. Also refer to the *Primavera Portfolio Management User Guide* for information about security settings within the application.

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

- Turn on and configure Password Policy using the Access tab of the Admin dialog box. An enabled Password Policy will increase the required length and quality of the password.
- Using the Access tab of the Admin dialog box, evaluate the User Lockout policy.
- Providing rigorous security for the various PPM components and operations, as discussed in the Security Section of the Primavera Portfolio Management User Guide.
- Enable the HTTPS authentication setting.

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

Authentication Options for PPM

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

- **Forms based (Native)**, which is the default mode for PPM. In this mode, the PPM 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, specifically PPM. In SSO mode, the PPM application is a protected resource. When a user tries to login to it, 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).

  Two types of Single Sign-On apply to PPM:

  - **Integrated Windows Authentication** - The PPM application can be integrated with Microsoft Windows domain authentication, such that a user, who has been authenticated by a Microsoft Windows domain controller, will automatically be authenticated with PPM as well. By enabling this functionality users will not be prompted for their usernames and passwords by PPM, but will be automatically logged into the PPM application without the need to use the login dialog screen.
  - **Integration with Third-Party Single Sign-On Products** - The PPM application can be integrated with third-party Single Sign-On (SSO) products, such that a user, who has been authenticated by a third-party SSO product, will automatically be authenticated with PPM as well. By enabling this functionality users will not be prompted for their usernames and passwords by PPM, but will be automatically logged into the PPM application without the need to use the login dialog screen.

  For more information, refer to *Primavera Portfolio Management Enabling Single Sign-On* in the *Oracle Primavera Portfolio Management System Administration Guide*.

Single Sign-On will help you to create the most secure authentication environment available in PPM.

P6 EPPM Web Services offers its own authentication options. If you use SAML for P6 EPPM Web Services, you must use Single Sign-on authentication for PPM.

Authorization for PPM

Grant authorization carefully to all appropriate PPM users.

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

- Use Module Access rights to limit access to PPM modules.
- Organize all your entities and your security hierarchy according to your organization charts. Then try to define your security at the organization unit level. Try to set up security at role and group level before setting it up at the user level.

- By default security is defined by project. Assign the "Category defines the data security" property when you want to define security vertically, rather than by portfolio or item.
- Be careful when defining functions, workflows, and query-based portfolios so as not to compromise data.

Confidentiality for PPM

Confidentiality ensures only authorized users see stored and transmitted information. In addition to the documentation included with other applications and hardware components, follow the PPM-specific guidance below.

- For data in transit, use SSL/TLS to protect network connections among modules. If you use SSO authentication, ensure you use LDAPS to connect to the directory server. For more information, refer to *Primavera Portfolio Management Enabling SSL* in the *Oracle Primavera Portfolio Management System Administration Guide*.
- For data at rest, refer to the documentation included with the database server for instructions on securing the database. With PPM you can use all options that are transparent to the application.

Sensitive Data for PPM

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

- Identify which PPM modules you will use.
- Determine which modules and interacting applications display or transmit data that your organization considers sensitive.
- Implement security measures in PPM to carefully grant users access to sensitive data. For example, secure data, objects, and components in such a way as to limit access to those users who need that access.
- Implement security measures for applications that interact with PPM, as detailed in the documentation included with those applications. For example, follow the security guidance provided with IIS. Also refer, as applicable, to the document For more information, refer to *Primavera Portfolio Management Enabling SSL* in the *Oracle Primavera Portfolio Management System Administration Guide*.
- Implement consent notices in Primavera Portfolio Management to gather the consent of users to store, use, process, and transmit personally identifiable information (PII) and to alert users when there is a risk of PII being exposed.

Reliability for PPM

Protect against attacks that could deny a service by:

- Installing the latest security patches.

- Entering account/password information during creation of a new database, at which time the product prompts for the creation of the first (administrative) account. PPM does not ship with a default Administrator sign-on.
- 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.
- Limit the maximum age for the session cookie on the application server.
- Protecting access to configuration files with physical and file system security. (The product installs and configures all files with limited file permissions for all files it installs. However, there are system folders and files belonging to the operating system which, by default, may have wider permissions. PPM does not modify these file permissions, so you as administrator need to consider enhancing the associated physical and file system security.)

Cookies Usage

When using PPM, 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.

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.

Copyright

Oracle Primavera Portfolio Management Security Guide

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.