Oracle

Primavera
Gateway Security Guide for On-Premises

Version 21
December 2021

Contents

Security Guidance Overview

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

- Review all security documentation for applications and hardware components that interact or integrate with Primavera Gateway. Oracle recommends you harden your environment. See ***Additional Sources for Security Guidance*** (on page 9) for links to information that can help you get started.
- Read through the summary of considerations for Primavera Gateway included in this document. Areas covered include: safe deployment, authentication options, authorization, confidentiality, sensitive data, reliability, and cookies usage.

Safe Deployment of Primavera Gateway

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

Administrative Privileges Needed for Installation and Operation

As the Primavera Gateway Administrator, you should determine the minimum administrative privileges or permissions needed to install, configure, and operate Primavera Gateway. For example, to successfully install the required Java JDK for Primavera Gateway, you must be an administrator on the client machine during installation.

Minimum Client Permissions Needed for Primavera Gateway

Because Primavera Gateway is a web application, 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.

Physical Security Requirements for Primavera Gateway

You should physically secure all hardware hosting Primavera Gateway 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 Primavera Gateway.

- You should install Primavera Gateway components in controlled access facilities to prevent unauthorized access. Only authorized administrators for the systems hosting Primavera Gateway 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 Primavera Gateway.

Application Security Settings in Primavera Gateway

Primavera Gateway contains a number of security settings at the application level. To help you organize your planning, the following are options Oracle recommends enabling or using the following features:

- HTTPS in Gateway WebLogic domain and in the P6 Web Services.
- Single Sign On for authentication

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

- Encryption in the Gateway and in P6 Web Services.
- LDAP for authentication.

Files to Protect after Implementation

While Primavera Gateway 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 or move them to a secure location after installation and configuration:

- Log files

  Windows: The log files are created in the **C:\Program Files\Oracle\Inventory\logs** folder.

  Linux: The log files are created in the **<USER HOME>/oraInventory/logs** folder.
- Any files in the **<installation folder>\cfgtoollogs\oui** folder.

Authentication Options for Primavera Gateway

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

- **Native** is the default mode for Primavera Gateway. In Native mode, the WebLogic server acts as the authority and handles the authentication of the user who is logging into that application.
- **SAML 2.0** authentication to support P6 Web Services in Gateway user interface.
- **SSO** authentication to access multiple connected applications with single sign on credentials.

- **Lightweight Directory Access Protocol (LDAP)** authenticates users through a directory. In LDAP mode, an LDAP directory server database confirms the user's identity when they attempt to login to Primavera Gateway.

  LDAP will help you to create the most secure authentication environment available in Primavera Gateway.
- **Basic Authentication** to support external REST service authentication in Primavera Gateway.

Authorization for Primavera Gateway

Grant authorization carefully to all appropriate Primavera Gateway users.

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

- The Developer role has access to the data dictionary, workflows, and configuration global settings.
- The User role can schedule and run synchronizations and can see monitoring.
- The User with no data access role can run, schedule, and monitor synchronizations. However, they cannot view the log files associated with synchronizations. They can see errors and warning messages regarding synchronizations.
- The superuser, Admin role can access all Gateway features and you should limit who has this role.
- The superuser, Admin with no data access role can access all Gateway features with the following exceptions:
  - They cannot view log files associated with synchronizations.
  - They can only see errors and warning messages regarding synchronizations.

Confidentiality for Primavera Gateway

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

- For data in transit, use SSL to protect network connections among modules.
- If you use LDAP authentication, ensure you use LDAPS to connect to the directory server.
- For inactive data or data at rest, refer to the documentation included with the database server for instructions on securing the database.

Sensitive Data for Primavera Gateway

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

- Determine which flows display or transmit data that your organization considers sensitive. For example, Primavera Gateway sync sensitive data, such as syncing a project with budgeted costs in the ERP.
- Implement security measures in Primavera Gateway to carefully grant users access to sensitive data.
- Implement security measures for applications that interact with Primavera Gateway, as detailed in the documentation included with those applications. For example, follow the security guidance provided with Oracle WebLogic.
- Implement consent notices in Primavera Gateway 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 Primavera Gateway

Ensure that you protect Primavera Gateway against attacks that could deny a service by:

- installing the latest security patches.
- 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 Primavera Gateway

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.

Primavera Gateway API

Primavera Gateway API are REST services which can be used for retrieving data from Gateway, and for creating and running Gateway synchronizations. Primavera Gateway API platform employs Web-based technology to handle requests from external programs. External client programs can use the Primavera Gateway API by creating a request based on the available REST services and send it to the application server for a response. REST services are available when Gateway is installed on a managed server and secured using basic authentication.

For a list of REST services available in Primavera Gateway, see the *Primavera Gateway API Programming Guide*.

For secure development, see ***Authorization for Primavera Gateway*** (on page 7) and ***Confidentiality for Primavera Gateway*** (on page 7) sections in this guide.

Additional Sources for Security Guidance

You should properly secure the databases, platforms, and servers you use for your Primavera Gateway. 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 19c Security Guide

https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/index.html

Microsoft Windows Server 2016 and 2019 Security Documentation

https://docs.microsoft.com/en-us/windows-server/security/security-and-assurance

Oracle WebLogic

http://www.oracle.com/technetwork/middleware/weblogic/overview/index.html

Copyright

Oracle Primavera Gateway Security Guide for On-Premises

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.