Oracle

Primavera
Unifier Security Guide for On-Premises

Version 20

December 2020

Contents

Security Guidance Overview

The Unifier Security Guide provides guidelines on how to plan your security strategy for Oracle Primavera Unifier.

During the installation and configuration process for Oracle Primavera Unifier, 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 Unifier environments. Use the following guidelines to plan your security strategy for Primavera Unifier:

- Review all security documentation for applications and hardware components that interact or integrate with Primavera Unifier. 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 Unifier 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 Unifier applications. For example, if you configure WebLogic to use only SSL v3.0, you must disable TLS v1.0 for the client JRE for Primavera Unifier to launch properly. If using Internet Explorer browser, you must also disable TLS v1.0 in Internet Options.

Safe Deployment of Primavera Unifier

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

Administrative Privileges Needed for Installation and Operation

As the Primavera Unifier Administrator, you should determine the minimum administrative privileges or permissions needed to install, configure, and operate Primavera Unifier. For example, to successfully install the required JRE for Primavera Unifier, you must be an administrator on the server machine during this installation or update.

Minimum Client Permissions Needed for Primavera Unifier

You do not have to be an Administrator to run Unifier.

Physical Security Requirements for Primavera Unifier

You should physically secure all hardware hosting Primavera Unifier 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 Unifier.
- You should install Primavera Unifier components in controlled access facilities to prevent unauthorized access. Only authorized administrators for the systems hosting Primavera Unifier 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 server machines only when you install and configure Primavera Unifier modules.

Application Security Settings in Primavera Unifier

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

- Turn on Password Policy. An enabled Password Policy will increase the required length and quality of the password.
- Use Security Accounts if using Oracle WebCenter Content for the Content Repository.
- Enable OAM, SSO, and OHS/Webgate for authentication.
- Enable the HTTPS authentication.

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

For details about configuring the OHTTP Server (OHS), refer to the Configuring the OHTTP Server (OHS) section of the *Unifier Installation Guide (WebLogic)*.

Files to Protect after Implementation

While Primavera Unifier 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.

- EM Connector (.opar file)
- OIMConnector.zip

Note: For the full list of system requirements, applications, and application version levels refer to the *Primavera Unifier Tested Configurations* in the Primavera Unifier Documentation Library.

Authentication Options for Primavera Unifier

Authentication is a process that Primavera Unifier uses to verify the identity of a user.

Unifier offers the following authentication modes:

- Native
- OAM/OIM
- WebLogic Authentication
- LDAP Single Bind
- LDAP Double Bind
- Generic SSO

Refer to the *Unifier Installation Guide (WebLogic)* details.

The Single Sign-On (SSO) authentication method helps you to create the most secure authentication environment available in Primavera Unifier.

> **Note**: The P6 EPPM Web Services offers its own authentication options. If you use Security Assertion Markup Language (SAML) for P6 EPPM Web Services, you must use Single Sign-on authentication for Primavera Unifier.

Authorization for Primavera Unifier

Authorization to use the Unifier application is based on permissions. You also have super-user, the Administrator. Grant authorization carefully to all appropriate Primavera Unifier users.

> **Note**: Oracle recommends that you limit users who have admin permissions.

Confidentiality for Primavera Unifier

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 Unifier-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 data at rest, refer to the documentation included with the database server for instructions on securing the database.

Unifier Mobile App for iOS: User Identity

If Unifier has been configured to sign in users using single sign-on (SSO), then the Sign In window will not appear on your device screen. In addition:

- Unifier does not capture the user’s username and password.
- The user’s first name, last name, and email address are all stored in Unifier database, but they are not shared with any other applications, including third-party applications.

If Unifier has been configured to sign in users using basic authentication, then the Sign In window will appear on your device screen. In addition:

- Unifier captures the user’s username, password, first name, last name, and email address.
- The user’s username, password, first name, last name, and email address are stored in a shared object that uses encrypted format, and they are not shared with any other applications, including third-party applications.

Security Basics

The term "administrator" or "application administrator" is used to refer to the individual who is responsible for managing the company data and can access that data. This term can also be used for the IT professionals who define roles in the Primavera Unifier application, or the IT professionals who manage company servers. An administrator must be able to:

- Set up Single Sign-On (SSO) and enable multi-factor authentication to minimize the number of passwords that users have to remember and to consolidate risk.
- Educate users on how they can avoid unwittingly helping hackers. One of the best ways an administrator (and security advocates) can help users is by helping them to prevent security breaches.
- Use a VPN to encrypt data being sent over the internet.
- Stay up-to-date about security trends and best practices.

The term "user" or "end-user" is used to refer to the individual who uses the Primavera Unifier application to complete tasks. This term also refers to an individual who signs in to the Primavera Unifier application from an office or job-site to complete tasks. A user must be able to:

- Follow security guidelines created by their companies and the administrators of any network applications they use.
- Use strong passwords. The more random-looking the better. Avoid reusing passwords.
- Learn to recognize phishing. Phishing is when someone disguises an email or some other transmission as a legitimate message in an attempt to get a user to reveal sensitive information. For example, a hacker may send you an email disguised to look like an email from your employer requesting login information. These attacks are becoming more sophisticated, but you can still protect yourself by making sure any emails you receive or websites you visit are legitimate before using them to share sensitive information.

Sensitive Data for Primavera Unifier

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

- Identify which Primavera Unifier modules you will use.

- Determine which modules and interacting applications display or transmit data that your organization considers sensitive. For example, Primavera Unifier displays sensitive data, such as costs and secure codes.
- Ensure you assign security-sensitive permissions sparingly to your users.
- Implement security measures for applications that interact with Primavera Unifier, as detailed in the documentation included with those applications. For example, follow the security guidance provided with Oracle WebLogic.

Reliability for Primavera Unifier

Protect against attacks that could deny a service by:

- Installing the latest security patches.
- 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 an expiry date (Expires) for when a cookie gets deleted.
- Protecting access to configuration files with physical and file system security.

Cookies Usage

As stated in ***Reliability for Primavera Unifier*** (on page 9), set a maximum age for the session cookie on the application server.

When using Unifier, the server may generate 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.

Each user that signs in to Unifier web will see a notification banner (Cookies in Unifier) that notifies the user that Unifier uses cookies. This banner has a link to the Unifier cookie policy which explains what information is being tracked by way of cookies. The user must click **Got It** in order to access the rest of the Unifier application.

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 must secure the databases, platforms, and servers you use for your Primavera Unifier. Refer to the material listed below (not a comprehensive list), when you are planning your security strategy.

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

Oracle Database

Go to https://docs.oracle.com/en/database/ and select the supported version. See Tested Configuration for details.

Oracle WebLogic

Go to https://docs.oracle.com/en/middleware/ and select Oracle WebLogic Server.

Oracle Fusion Middleware Security Guides

Go to https://docs.oracle.com/en/middleware/ and select Oracle Fusion Middleware.

Note: For the full list of system requirements, applications, and application version levels refer to the Unifier Tested Configurations in the Unifier Documentation Library.

Copyright

Oracle Primavera Unifier 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.