



**Security Guide
16 R1**

June 2016

Contents

Security Guidance Overview	5
Safe Deployment	5
Administrative Privileges Needed for Installation and Operation	5
Minimum Client Permissions Needed.....	5
Physical Security Requirements.....	6
Application Security Settings	6
Files to Protect.....	6
Authentication Options	6
Authorization.....	7
Confidentiality.....	7
Sensitive Data.....	7
Reliability	8
Cookie Usage	8
For More Information.....	10
Where to Get Documentation.....	10
Documentation Accessibility.....	10
Where to Get Training	10
Where to Get Support	11
Legal Notices	13

Security Guidance Overview

During the installation and configuration process, you will have several options for how to handle security. Depending on your organization's needs, you might need to create a highly secure environment. Use the following guidelines to plan your security strategy:

- ▶ Review all security documentation for applications and hardware components that interact or integrate with EnterpriseTrack. Oracle recommends you harden your environment after the installation.
- ▶ Read through the summary of considerations for EnterpriseTrack 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 EnterpriseTrack.

Safe Deployment

To ensure overall safe deployment of EnterpriseTrack, you should carefully plan security for all components, such as database servers and client computers that interact with EnterpriseTrack. In addition to the documentation included with other applications and hardware components, follow the guidance provided in the following sections.

Administrative Privileges Needed for Installation and Operation

The system administrator should determine the minimum administrative privileges or permissions needed to install, configure, and operate EnterpriseTrack. For example, to successfully install the required JDK for EnterpriseTrack, you may be required to be an administrator on the middle-tier machine during installation or update.

Minimum Client Permissions Needed

Users do not have to be OS-level administrators on their machines to run EnterpriseTrack. You can successfully run these applications with the browser/OS security settings set at a high level to create a more secure environment.

Physical Security Requirements

You should physically secure all hardware hosting EnterpriseTrack to maintain a safe implementation environment. Consider the following when planning your security strategy:

- ▶ You should install, configure, manage, and maintain your environment according to guidance in all applicable installation and configuration documentation.
- ▶ You should install EnterpriseTrack components in controlled access facilities to prevent unauthorized access. Only authorized administrators for the systems hosting EnterpriseTrack 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 EnterpriseTrack modules. EnterpriseTrack has plugins that help interface with Microsoft Office products such as Excel, PowerPoint, and Project. The plugins are downloaded from EnterpriseTrack and can be installed in client machines. Such installation may require administrator access, depending on how the client machine is configured.

Application Security Settings

EnterpriseTrack contains a number of security settings at the application level. Using requirements collected from the customer, EnterpriseTrack security settings are configured by the Solution Architect as part of customer onboarding.

Files to Protect

Ensure that you protect the files you install for EnterpriseTrack. You can protect files by ensuring they are readable/writable only by the account that runs the server and the account associated with the system:

- ▶ For Windows, install the files in a directory with the appropriate minimal inheritable permissions.
- ▶ For Linux, set the appropriate minimal permissions on the installation directory using the unmask of 022.
- ▶ Protect the `IETRACK_ROOT` directory.

Authentication Options

To validate user identities, EnterpriseTrack supports (User ID and password) forms-based authentication, LDAP/Active Directory-based authentication, and various Single Sign-On (SSO)-based authentication mechanisms, including those based on SAML.

- ▶ **User Password** is the default mode for EnterpriseTrack. In User Password mode, the EnterpriseTrack database acts as the authority and the application handles the authentication of the user who is logging into that application.

- ▶ **Active Directory (AD)/LDAP** EnterpriseTrack can use an AD/LDAP server for user authentication. The server's details, such as its LDAP Provider URL, must be specified in EnterpriseTrack.
- ▶ **Single Sign-On (SSO)** EnterpriseTrack can support SAML-based SSO where the EnterpriseTrack application acts as the service provider and can use the user's Identity Provider to authenticate users.

Authorization

Grant authorization carefully to all appropriate EnterpriseTrack users. To protect against unauthorized access to your critical information, EnterpriseTrack supports fine-grained Roles-Based Authorization to control access to various objects and operations within the application.

To help you with security planning, EnterpriseTrack roles/permissions settings are configured by the Solution Architect using the requirements collected from the customer. These are detailed in the *EnterpriseTrack User's Guide* and the *EnterpriseTrack Application Administrator's Guide*.

Confidentiality

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

- ▶ For data in transit, use TLS with recommended and strong cipher suites 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 at rest, refer to the documentation included with the database server for instructions on securing the database.

Sensitive Data

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

- ▶ Identify which EnterpriseTrack modules you will use.
- ▶ Determine which modules and interacting applications display or transmit data that your organization considers sensitive. For example, EnterpriseTrack displays sensitive data, such as costs and team information.

- ▶ Ensure you assign security-sensitive permissions sparingly to your users.
- ▶ Implement security measures for applications that interact with EnterpriseTrack, as detailed in the documentation included with those applications. For example, follow the security guidance provided with Oracle WebLogic.

Reliability

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 a maximum duration for the session on the application server.
- ▶ Protecting access to configuration files with physical and file system security.

Cookie Usage

When using EnterpriseTrack, 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.

Cookie Name	Description	Scope	Retention	Encrypted ?
JSESSIONID	Session identifier	default	None (expires at end of session)	No
ialog	Session performance analytics info	default	None (expires at end of session)	No
OpenData	Used to keep track of open nodes in a tree.	default	None (expires at end of session)	No

sw	Applies only for the Help system. Stores the last search term used in the help system.	Current working directory only on the current host (for example, if located at <code>http://host/help</code> , only valid for the <code>http://host/help</code> directory).	None (expires at end of session)	No
sm	Applies only for the Help system. Stores the type of search used in the help system. Value corresponds as: 0: All words, 1: Any words, 2: Exact phrase. Any other value is invalid.	Current working directory only on the current host (for example, if located at <code>http://host/help</code> , only valid for the <code>http://host/help</code> directory).	None (expires at end of session)	No
ORA_PHELP_1111	Applies only for the Help system. Stores the current style for the help system. Only valid values are "contrast" or "default".	Any location on the current domain.	One year	No

For More Information

In This Section

Where to Get Documentation	10
Documentation Accessibility	10
Where to Get Training	10
Where to Get Support	11

Where to Get Documentation

Complete documentation libraries for EnterpriseTrack releases are available on the Oracle Technology Network (OTN) at:

<http://www.oracle.com/technetwork/documentation/default-1956119.html>

From this location you can either view libraries online or download them to have local copies. We recommend viewing them from OTN to ensure you always access the latest versions, including critical corrections and enhancements.

The documentation assumes a standard setup of the product, with full access rights to all features and functions.

Help System Access

EnterpriseTrack is configured to access its help system directly on OTN. However, a downloadable version of the help system is also available on OTN if you need to download, deploy, and access a local copy.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Where to Get Training

To access comprehensive training for all Primavera products, go to:

<http://education.oracle.com>

Oracle Learning Library

The Oracle Learning Library (OLL) provides online learning content covering Primavera products. Content includes videos, tutorials, articles, demos, step-by-step instructions to accomplish specific tasks, and self-paced interactive learning modules.

To access the learning library's Primavera content, go to:

<http://www.oracle.com/oll/primavera>

Where to Get Support

If you have a question about using Oracle products that you or your network administrator cannot resolve with information in the documentation or help, click <http://support.oracle.com>. This page provides the latest information on contacting Oracle Global Customer Support, knowledge articles, and the support renewals process. For more information about working with Support, visit <https://support.oracle.com/epmos/faces/DocumentDisplay?id=888813.2> to view **Support Tools & Tips**.

Using Primavera's Support Resource Centers

Primavera's Support Resource Center provides links to important support and product information. Primavera's Product Information Centers (PICs) organize documents found on My Oracle Support (MOS), providing quick access to product and version specific information such as important knowledge documents, Release Value Propositions, and Oracle University training. PICs also offer documentation on Lifetime Management, from planning to installs, upgrades, and maintenance.

Visit <https://support.oracle.com/epmos/faces/DocumentDisplay?id=1486951.1> to access links to all of the current PICs.

PICs also provide access to:

- ▶ **Communities** are moderated by Oracle providing a place for collaboration among industry peers to share best practices.
- ▶ **News** from our development and strategy groups.
- ▶ **Education** contains a list of available Primavera product trainings through Oracle University. The Oracle Advisor Webcast program brings interactive expertise straight to the desktop using Oracle Web Conferencing technology. This capability brings you and Oracle experts together to access information about support services, products, technologies, best practices, and more.

Creating a Service Request

EnterpriseTrack integrates with different Oracle applications; when you create a Service Request, be sure to open the request with the proper Support team. To ensure you reach the proper Support team, enter the correct product information when you create the Service Request. Each product has its own support line.

- ▶ Use the **Instantis EnterpriseTrack** support line when you are having installation, configuration, or connection issues related to EnterpriseTrack.

- ▶ Use one of the following support lines when you are having installation or configuration issues that do not relate to EnterpriseTrack:
 - ▶ Oracle WebLogic Server
 - ▶ Oracle Database Server
 - ▶ BI Publisher
 - ▶ Oracle Access Manager

Keeping Your Software Up to Date

To ensure you have the latest versions of your products, be sure to download and install all available patch sets from <http://support.oracle.com>.

Finding Security-related Patches

To get the latest information about Critical Patch Updates, visit <http://www.oracle.com/technetwork/topics/security/alerts-086861.html>.

Legal Notices

Oracle Instantis EnterpriseTrack Security Guide

Copyright © 2000, 2016, Oracle and/or its affiliates. All rights reserved.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

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.