



**Security Guide
Release 9.0**

December 2014

Contents

Security Guidance Overview	5
Safe Deployment	5
Administrative Privileges Needed for Installation and Operation	5
Minimum Client Permissions Needed.....	6
Security Requirements.....	6
Application Security Settings	6
Files to Protect.....	6
Authentication Options	7
Authorization.....	7
Confidentiality	7
Sensitive Data.....	8
Reliability	8
Cookies Usage	8
Additional Sources for Security Guidance	9
For More Information.....	10
Where to Get Documentation.....	10
Where to Get Training	12
Where to Get Support	13
Legal Notices	14

Security Guidance Overview

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

- ▶ Review all security documentation for applications and hardware components that interact or integrate with EnterpriseTrack. Oracle recommends you harden your environment after the installation. 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 EnterpriseTrack included in this document. Areas covered include: safe deployment, authentication options, authorization, confidentiality, sensitive data, reliability, and cookies usage.
- ▶ Throughout this documentation, the Security Guidance icon  helps you to quickly identify security-related content to consider during the installation and configuration process. Once you begin the installation and configuration of your EnterpriseTrack environment, use the Security Guidance icon as a reminder to carefully consider all security options.

Tips

As with any software product, be aware that security changes made for third party applications might affect EnterpriseTrack applications.

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 are required for and interact with EnterpriseTrack. In addition to the documentation included with other applications and hardware components, follow the EnterpriseTrack-specific guidance below.

Administrative Privileges Needed for Installation and Operation

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

Minimum Client Permissions Needed

Because EnterpriseTrack 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.

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 for EnterpriseTrack.
- ▶ 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. To help you organize your planning, EnterpriseTrack security settings are configured by the Engagement Managers as part of customer onboarding.

Files to Protect

Ensure 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 them 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 Basic (User ID and password) forms-based authentication, LDAP/ActiveDirectory-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. This server needs to be accessible to the EnterpriseTrack application via a LDAP-provider URL and the associated domain name.
- ▶ **Single Sign-On (SSO)** When hosted by Oracle, 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 them. EnterpriseTrack can also support SSO when the application is hosted on the user's premise.

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 Engagement Managers as part of customer onboarding. There are detailed in the user and administration guides.

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 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 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 e-mail 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.

Cookies Usage

When using EnterpriseTrack, the server generates the following cookies and sends 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
sessionSecurityCookie	Secondary session identifier for enhanced security	default	None (expires at end of session)	No
OpenData	Helps with dashboards	default	None (expires at end of session)	No
_ga	Used to distinguish users on OTN.		2 years	

Additional Sources for Security Guidance

You should properly secure the databases, platforms, and servers you use for your EnterpriseTrack. 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>

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

For More Information

In This Section

Where to Get Documentation	10
Where to Get Training	12
Where to Get Support	13

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.

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.

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

The following table describes the core documents available for EnterpriseTrack and lists the recommended readers by role.

Title	Description
<i>EnterpriseTrack User Help</i>	Describes how to work with EnterpriseTrack and provides information to assist users with using EnterpriseTrack features. All users should read this Help.

Title	Description
<i>EnterpriseTrack Administrator's Help</i>	Describes how to work with EnterpriseTrack Administrator's console to manage your deployment and change various aspects of the application. EnterpriseTrack administrator should read this Help.
<i>EnterpriseTrack User Guide</i>	Guides users on how to use the EnterpriseTrack application. All users should read this guide.
<i>EnterpriseTrack Administrator's Guide</i>	Provides detailed information on using the EnterpriseTrack Administrator's console. EnterpriseTrack administrator should read this guide.
<i>EnterpriseTrack Dashboards User's Guide</i>	Provides detailed instruction on using the EnterpriseTrack Dashboards modules to view and generate dashboards. All users should read this guide.
<i>EnterpriseTrack Reports User's Guide</i>	Provides detailed instruction on using the EnterpriseTrack Reports modules to generate standard reports, ad-hoc reports and user-defined reports. All users should read this guide.
<i>EnterpriseTrack Quick Reference Guide</i>	Provides a quick introduction to common EnterpriseTrack tasks. All users should read this guide.
<i>EnterpriseTrack Installation Guide</i>	Provides information on how to install and configure EnterpriseTrack. EnterpriseTrack administrator, network administrator and database administrator should read this guide.
<i>EnterpriseTrack MSP Integration Guide</i>	Provides an overview of MS Project integration for EnterpriseTrack. EnterpriseTrack users who will perform MS Project integration should read this guide.
<i>EnterpriseTrack API Integration Guide</i>	Provides information that allows customers to customize existing third-party integration. Developers interested in customization and existing third-party providers that integrate with EnterpriseTrack should read this book.
<i>EnterpriseTrack Upgrade Guide</i>	Provides a sequence of procedures that must be completed to upgrade to a new version of EnterpriseTrack. EnterpriseTrack administrator and database administrator should read this guide.
<i>EnterpriseTrack Architecture Data Sheet</i>	Provides the server system requirements and the deployment configuration options for EnterpriseTrack.

Title	Description
<i>EnterpriseTrack Tested Configurations</i>	Lists the configurations that have been tested and verified to work with EnterpriseTrack. EnterpriseTrack administrator, network administrator, and database administrator should read this guide.
<i>EnterpriseTrack Cumulative Features Overview Tool</i>	Provides an overview of features and enhancements included in the Oracle EnterpriseTrack product. It is intended solely to help you assess the business benefits of upgrading. All users should read this guide.
<i>EnterpriseTrack Security Guide</i>	Provides guidelines on how to plan your security strategy for EnterpriseTrack. All users, EnterpriseTrack administrators, network administrators and database administrators should read this guide.

Distributing Information to the Team

You can copy the online documentation to a network drive for access by project participants. Each team member can then view or print those portions that specifically relate to his or her role in the organization.

Throughout this documentation, the Security Guidance icon  helps you to quickly identify security-related content to consider during the installation and configuration process.

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

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/us/support/contact-068555.html> or visit <http://www.oracle.com/us/corporate/accessibility/support/index.html> if you are hearing impaired.

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.

For more information about working with Support, visit <https://support.oracle.com/epmos/faces/DocumentDisplay?id=888813.2>.

Legal Notices

Oracle Instantis EnterpriseTrack Security Guide

Copyright © 2000, 2014, 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.