Security Guide
Release 8.6

September 2013

Contents

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 of EnterpriseTrack

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 for Instantis EnterpriseTrack

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 for EnterpriseTrack

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.

Application Security Settings in EnterpriseTrack

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 for EnterpriseTrack

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.

- **Native** is the default mode for Instantis EnterpriseTrack. In Native mode, the Instantis 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** Instantis EnterpriseTrack can use an AD/LDAP server for user authentication. This server needs to be accessible to the Instantis EnterpriseTrack application via a LDAP-provider URL and the associated domain name.
- **Single Sign-On (SSO)** When hosting with Oracle, Instantis 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 for EnterpriseTrack

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 for EnterpriseTrack

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 for EnterpriseTrack

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 for EnterpriseTrack

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 in EnterpriseTrack

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

BIGipServerProd-80 or BIGipServerProd-443	Load-balancer related cookie	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

Microsoft SQL Server 2008 Database

http://www.microsoft.com/sqlserver/2008/en/us/Security.aspx

Microsoft Windows 2008 Server

http://technet.microsoft.com/en-us/library/dd548350(WS.10).aspx

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

Legal Notices

Oracle Primavera Oracle Instantis EnterpriseTrack Security Guide