Oracle® Health Sciences Empirica Signal

Secure Configuration Guide

Release 8.0

E50112-01

September 2014

ORACLE®

Oracle Health Sciences Empirica Signal Secure Configuration Guide, Release 8.0

E50112-01

Contents

Preface

This document provides guidance and recommendations on installing, configuring, and managing the Empirica Signal software and its system components securely. This document does not provide step-by-step procedures for performing a secure installation; rather, it is intended as a supplement to the instructions already provided in the *Empirica Signal Installation Guide* and user documentation.

The preface includes the following sections:

Audience

This document is intended for database administrators, Empirica Signal site administrators, IT administrators, and others whose responsibility is to perform the following:

- Install and configure the Empirica Signal software and its system components securely.
- Create security policies and develop best practices to regulate and monitor safety data usage.
- Create and manage user accounts, passwords, roles, and permissions.
- Monitor user activity for inappropriate or unauthorized actions or data misuse.

This document assumes that you have an understanding of operating system and database concepts, and have experience using the software tools described.

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 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.

Related documents

For more information, see the following documents in the Oracle Health Sciences Empirica Signal Release 8.0 documentation set:

- *Oracle Health Sciences Empirica Signal and Topics User Guide*
- *Oracle Health Sciences Empirica Topics Reporting and Oracle Business Intelligence Configuration Guide*
- *Oracle Health Sciences Empirica Signal Installation Guide*
- *Oracle Health Sciences Empirica Signal Release Notes*
- *Oracle Health Sciences Empirica Signal Known Issues*
- *Oracle Health Sciences Empirica Signal Third Party Licenses and Notices*
- *Oracle Health Sciences Empirica Topics API Guide*

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Security overview

The Empirica Signal application is a web application that provides a data mining environment for detecting signals, uncovering patterns, and recognizing trends in adverse event report data. Using the Empirica Signal application, industry and pharmacovigilance professionals can efficiently manage the review, processing, and response to drug and vaccine safety signals.

When your organization implements the Empirica Signal application, it is critical to install the software and its system components using secure installation methods to protect the integrity and confidentiality of your data. It is equally important to manage and monitor your system after installation to ensure that your data is protected from unauthorized access and misuse.

The Secure installation and configuration chapter provides secure installation and configuration guidelines, and the Security features chapter describes the security features provided in the Empirica Signal software to help you manage and monitor your system.

General security principles

- Require strong, complex application and database passwords.

  Create a password policy to establish password requirements. For example, require a minimum password length and at least one of each of the following types of characters:

  - Alphabetic
  - Non-alphabetic
  - Numeric
  - Uppercase character
  - Lowercase character

- Keep passwords secure.

  When you create user accounts in the Empirica Signal application, send users their user names and initial passwords in separate email messages. Instruct your users not to share or write down passwords, or to store passwords in files on their computers. Additionally, require users to change their passwords upon first use.

- Keep software up to date.

  Keep all software versions current by installing the latest patches for all components, including all critical security updates.

- Implement the principle of least privilege.

In implementing the principle of least privilege, you grant users the fewest number of permissions needed to perform their jobs. You should also review user permissions regularly to determine their relevance to users' current job responsibilities.

- Monitor system activity.

  Review user audit records regularly to determine the user activities that constitute normal use and the activities that might indicate unauthorized use or misuse.

- Promote policy awareness.

  Ensure that your employees are aware of Acceptable Use policies, best practices, and standard operating procedures that are relevant to the Empirica Signal application.

2

Secure installation and configuration

This chapter includes the following sections:

Installing and configuring the Empirica Signal software

The *Empirica Signal Installation Guide* includes procedures that install the software and system components in a secure state by default. The accounts that you create during the installation also have restrictive permissions by default. Perform the following steps to secure the Empirica Signal software. Some of the steps are described in further detail in the *Empirica Signal Installation Guide*.

Configure WebLogic to use SSL

Before installing the Empirica Signal software, obtain an SSL certificate, install it on the application server, and configure WebLogic to use the certificate.

Use a separate port for the Empirica Signal application

Install the Empirica Signal application so that it listens on a separate port from WebLogic Console and Enterprise Manager. The installation instructions guide you through configuring the Empirica Signal application to run in its own WebLogic managed server with its own port.

Install only what is required

Install only the Empirica Signal components that you plan to use. If you do not plan to use Topics or Signal Management in your Empirica Signal deployment, you can skip the optional installation instructions. After you complete the installation, you can disable other features that you might not use, such as interactive reports, in the site options.

Execute scripts without passwords on the command line

When you are required to authenticate to your Oracle database during the Empirica Signal installation, do not provide database account passwords as arguments from the

command prompt. The standard installation instructions provide examples of appropriate scripts.

Reset the Read Only attribute

The standard Empirica Signal installation requires you to make several files editable. After the installation completes, make sure that you set the files to read-only again unless explicitly instructed otherwise in the *Empirica Signal Installation Guide*.

Establish best practices for downloading data

The Empirica Signal application provides the option to download table data to a Microsoft Excel spreadsheet or to other file types, such as PDF, text, or SAS files. Establish best practices for downloading data to ensure the data remains secure outside the Empirica Signal application.

Route email to a secure address

In the Empirica Signal application, provide secure email addresses for the Feedback Email and Error Email site options. Consider providing email addresses that are not routed over the Internet.

Install the Empirica Signal application on a separate Managed Server

Do not install the Empirica Signal application on the WebLogic Administration Server.

Install the Empirica Signal application on its own Managed Server in the WebLogic domain. When you use a separate Managed Server for the Empirica Signal application, you access the Empirica Signal using a different port than that of the Administration Server.

Installing the Oracle database

The following steps allow you to install the Oracle database securely.

For more information and additional guidelines for securely installing and managing the Oracle database, see the *Oracle® Database Security Guide, 11g Release 2*:

http://docs.oracle.com/cd/E11882_01/network.112/e16543/toc.htm

Patch the database regularly and apply security updates

Periodically check the security site on Oracle Technology Network for details about security alerts for Oracle products.

http://www.oracle.com/technetwork/topics/security/alerts-086861.html

Patch the Oracle Java SE regularly and apply security updates

Periodically check the security site on Oracle Technology Network for details about security alerts on Oracle Java SE:

http://www.oracle.com/technetwork/topics/security/alerts-086861.html

Allow database passwords to expire, and change default passwords

Oracle Database is installed with several default database user accounts, such as SYS and SYSTEM. After the database installs successfully, the Database Configuration

Assistant automatically locks most built-in database user accounts and marks them as expired. After the accounts expire, you should configure strong and secure passwords for them.

Installing Oracle Access Manager

For information on securely installing and configuring Oracle Access Manager, see the Oracle Identity and Access Management Security guides:

http://docs.oracle.com/cd/E21764_01/security.htm

Installing Oracle Business Intelligence Enterprise Edition (OBIEE)

For information on installing and configuring Oracle BI EE and its components securely, see the *Oracle® Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition, 11g Release 1*:

http://docs.oracle.com/cd/E23943_01/bi.1111/e10543/toc.htm

3

Security features

The Empirica Signal application provides the following security features to help you secure your system:

- **Authentication**—You can choose from three different authentication methods to ensure only authorized users have access. You can also select from flexible password options to establish a password policy for user accounts. For more information, see Authentication.
- **Auditing**—The Empirica Signal application automatically tracks user activity, including successful and failed logins, for local users. The tracked activities provide a comprehensive audit trail of actions performed. For more information, see Auditing.
- **User Access Control**—You can assign users to several built-in or custom roles. You can also assign permissions to restrict user access to only the features that are appropriate for their job responsibilities. The Empirica Signal application also provides publishing capabilities to restrict user access to objects. For more information, see User access control.
- **User Session Timeout**—The Empirica Signal application automatically cancels user sessions that have been inactive for a specified period of time. To update the default session timeout period, see the *Empirica Signal Installation Guide*.
- **Topics**—You can place an additional layer of security on topics. You can create work teams to support visibility of topics among separate groups of users. For more information, see Topics.

Authentication

The Empirica Signal application allows you to authenticate and set password options using several ways. You can disable accounts to prevent unauthorized access of the application.

Authentication methods

The Empirica Signal application requires users to authenticate by logging in with a unique user name and password. You can use the following authentication methods:

- **Local**—User information stored in the Empirica Signal application is used for authentication.
- **LDAP**—User information stored in a Lightweight Directory Access Protocol directory is used for authentication.

- **Single Sign-On (SSO)**—User information stored in Oracle® Access Manager (OAM) is used for authentication.

With local and LDAP authentication, the Empirica Signal application captures successful and failed login attempts in the User Activity Audit Trail. For more information, see Auditing.

With local authentication, when a user exceeds the allowable number of login attempts that you set in your password requirements, the Empirica Signal application sends an account lockout email notification to the site administrator.

For more information on configuring and implementing authentication methods, see the *Empirica Signal and Topics User Guide*.

Password requirements

The Empirica Signal application provides password options that you can select to establish a password policy for the user accounts for your local users. Using the options, you can require specific password content, complexity, and expiration. The Empirica Signal application provides the following password options and default values. You can edit the default values to suit the requirements of your organization.

Option	Default value
Expiration	90 days
Expiration warning	15 days
Minimum Length	8 characters
Number of Attempts Allowed	3
Number of Passwords Retained	8
Minimum Alphabetic	1
Minimum Numeric	1
Minimum Non-alphanumeric	1
Minimum Lowercase	1
Minimum Uppercase	1

If you are using SSO with OAM, you should set similar password requirement options in the OAM Access Manager Console.

Disabling user accounts

When an employee leaves your organization, the Empirica Signal application allows you to disable the employee's user account to prevent unauthorized system access.

Auditing

The User Activity Audit Trail tracks user activity that occurs in the application, capturing detailed information for user actions and providing you with an easily accessible, historical account of user activity. Using the User Activity Audit Trail, you can enforce your company's security policy and monitor your system for attempts at unauthorized actions or misuse.

Audited user activity is retained indefinitely. You cannot modify or delete audit records through the Empirica Signal application.

The Empirica Signal application auditing feature is a standard feature that cannot be disabled.

User access control

The Empirica Signal application allows you to implement user access control. Using roles and permissions, you can restrict user access to only what is necessary for users to perform their job responsibilities.

Before implementing user access control, establish an access control policy based on business and security requirements for each user. Review your access control policy periodically to determine if changes to roles and permissions are necessary.

Assigning roles

During installation, several built-in roles are created. The roles are designed for least privilege and separation of duties. You can modify the permissions assigned to the roles and create new roles, if needed.

Granting permissions

The Empirica Signal application defines permissions that grant or restrict user access to different application features. When you assign a role to a user, the user receives all the permissions assigned to the role. Review the permissions assigned to roles to make sure users can perform only the tasks relevant to their job responsibilities.

If necessary, you can also assign permissions to individual users.

Publishing objects

You can control user access to objects, such as analysis runs or report outputs, by publishing the objects to specific login groups. By default, the publication level of every newly created object is Private.

Users without the Administer Users permission can publish only objects they have created. Users with the Administer Users permission can publish objects that they or any users in their login group created. Superusers can publish any object.

For more information on user access control, see the *Empirica Signal and Topics User Guide*.

Topics

You can place an additional layer of security on topics. You can create work teams to support visibility of topics among separate groups of users. Within each work team, users can have different work team permissions that determine the level of access to the topics visible to them.

Additionally, you can configure Topic Email Notifications to alert individual users or work teams of significant changes to topics. Topic email notifications optionally can include topic or action fields from the topic workflow configuration. Before including fields in email notifications, you should ensure that the resulting email messages do not contain sensitive or confidential information.

The user can view changes to topics in the history of a topic or action, or both, and can track the deleted attachments and actions in the audit trail.