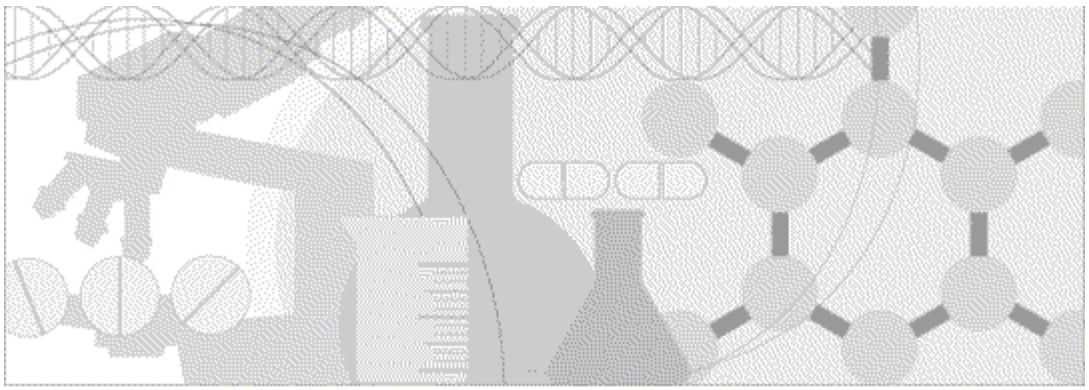
Secure Configuration Guide

Oracle® Health Sciences Empirica Signal 8.1



ORACLE

Part number: E60408-01

Contents

CHAPTER 1

Security overview

In this chapter

Overview

Empirica Signal 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 manage the review, processing, and response to drug and vaccine safety signals.

To protect the integrity and confidentiality of your data, install the Empirica Signal software and system components using secure installation methods. After installation, manage and monitor your system to ensure that your data is protected from unauthorized access and misuse.

The following sections provide secure installation and configuration guidelines, and describe the security features provided in Empirica Signal 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
  - Upper-case character
  - Lower-case character

- Keep passwords secure.

  When you initially create user accounts in the Empirica Signal software, send users their user name and initial password 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 which user activities constitute normal use, and which may 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 software.

CHAPTER 2

Secure installation and configuration

In this chapter

Installing and configuring the Empirica Signal software

The Empirica Signal *Installation Guide* includes procedures that install the application and system components into a secure state by default. The accounts that you create during the installation also have restrictive permissions by default. In addition to performing the standard installation procedures, you can perform the following steps to secure the Empirica Signal software:

Configure Oracle WebLogic Server to use TLS

Before you install the Empirica Signal software, obtain a TLS certificate, install the certificate on the application server, and configure Oracle WebLogic Server to use the certificate.

Use a separate port for the Empirica Signal application

Install the Empirica Signal application so that the application listens on a different port than the Oracle WebLogic Server administration console and Oracle Enterprise Manager console. The *Installation Guide* describes how to configure the Empirica Signal application to use a unique port.

Enable only what is required

When you have completed the installation, disable features that you might not use, such as LDAP, 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 appropriate script execution examples.

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 reset the file permissions to read only unless explicitly instructed otherwise in the *Installation Guide*.

Use secure Empirica Signal database and Topics credentials

The Empirica Signal *Installation Guide* includes directions for configuring database and Topics credentials. To ensure secure installation, use passwords that observe complexity standards.

Turn on the HttpOnly flag for session cookies within Oracle WebLogic Server for the Empirica Signal software

Using the HttpOnly flag when generating a cookie helps mitigate the risk of a client-side script accessing the protected cookie.

Perform these steps on the application server.

To turn on the HttpOnly flag for session cookies:

1 Navigate to the **<INSTALL_DIR>/Signal/WEB-INF** directory.

2 Open the **weblogic.xml** file, and locate the <session-descriptor> section.

3 If the section does not contain the following element, add the element:

```
<wls:cookie-http-only>true</wls:cookie-http-only>
```

Note: When the element is set to true, users must use Microsoft Internet Explorer 10 or 11 and Java 8 or later to run DataMontage patient profiles as applets. Users running older releases should deselect the Run DataMontage as applet user preference.

Establish best practices for downloading data

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

Route email to a secure address

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

Use of TLS

Oracle strongly recommends configuring WebLogic to use TLS and accessing the Empirica Signal software using only TLS connections. For more information, see the *Installation Guide*.

To ensure that your use of TLS is secure, perform the following steps:

- Disable the use of vulnerable TLS protocols by adding the following JVM option to the JAVA_OPTIONS settings in the **setDomainEnv.sh** file, for example:

  ```
  -Dweblogic.security.SSL.protocolVersion=TLS1
  ```

  You can find the setDomainEnv.sh file in a location such as:

  ```
  /u01/app/oracle/Middleware/user_projects/domains/empirica/bin/setDomainEnv
  .sh
  ```

- Enable only strong ciphers in the WebLogic **config.xml** file by listing only strong ciphers in the SSL section of the file.

  For more information, see the Open Web Application Security Project website:

  http://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet#Rule_-_Only_Support_Strong_Cryptographic_Ciphers

Encrypt the database connection

If you install the Empirica Signal software and Oracle Database software on different servers, secure configuration requires encryption of the communication channel between the servers. For more information, see the section about configuring the thin JDBC client network in the *Oracle Database Security Guide*:

https://docs.oracle.com/database/121/DBSEG/asojbdc.htm#DBSEG030

Install the Empirica Signal application on a separate managed server

Do not install the Empirica Signal application on the Oracle WebLogic Server administration server.

Install the application on a separate managed server in the WebLogic domain. When you use a separate managed server for the application, you access the application on a different port than the port for the administration server.

Installing the Oracle Database software

The following steps allow you to install the Oracle Database software securely.

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

- For Oracle Database 12c Release 1:

  http://docs.oracle.com/database/121/DBSEG/toc.htm

- For Oracle Database 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 security alerts about 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 is installed 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.

Configure components to use FIPS 140-2 compliant cryptographic implementations

You can configure the Oracle Database and WebLogic Server used with the Empirica Signal application to use FIPS 140-2 approved and validated encryption modules. For more information, see the following link:

http://www.oracle.com/technetwork/topics/security/oracle-fips140-validations-100923.html

Installing Oracle Business Intelligence Enterprise Edition (Oracle BI EE)

For information on installing and configuring Oracle BI EE and its components securely, see the Oracle BI EE security guide at:

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

CHAPTER 3

Security features

In this chapter

Overview of security features

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

- Authentication

  You can choose from three authentication methods to ensure only authorized users have access. You can also select from flexible password options to establish a user account password policy.

- 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 software also provides publishing capabilities to restrict user access to objects.

- Auditing

  Empirica Signal automatically tracks user activity, including successful and failed logins, for local users. The tracked activities provide a comprehensive audit trail of actions performed.

- User Session Timeout

  Empirica Signal automatically ends user sessions that have been inactive for a specified period of time. The Empirica Signal *Installation Guide* describes how to change the default timeout period.

Authentication

Authentication methods

The Empirica Signal software 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 Empirica Signal is used for authentication.
- **Single Sign-On (SSO)**—User information stored in a single sign-on application is used for authentication. For example, you might use Oracle Health Sciences Identity and Access Management Services or Oracle Access Manager for single sign-on.
- **LDAP**—User information stored in a Lightweight Directory Access Protocol (LDAP) directory is used for authentication.

With local and LDAP authentication, Empirica Signal captures successful and failed login attempts in the User Activity Audit Trail. For more information, see *Auditing* (on page 15).

In addition, when a locally authenticated user exceeds the allowable number of login attempts that you set in your password requirements, Empirica Signal sends an account lockout email notification to the site administrator.

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

Password requirements

The Empirica Signal software 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 software provides the following password options and default values. You can edit the default values to suit the requirements of your organization.

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

If you use single sign-on (SSO) for authentication, you should set similar password requirements in your SSO application.

Disabling user accounts

When an employee leaves your organization, the Empirica Study software 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 better 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 Study software.

The Empirica Study software auditing feature is a standard feature that cannot be disabled.

Oracle Database Client Identifier

For each connection to the Oracle Database, Empirica Signal sets the **CLIENT_IDENTIFIER** attribute to the **ID** value for the currently connected user. Oracle activities which include **CLIENT_IDENTIFIER**, such as the SQL trace files, performance tuning tools, and enabled audit policies, reflect the Empirica Signal user **ID**.

User access control

The Empirica Study software allows you to implement user access control. Using roles and permissions, you can restrict user access to only the activities that are 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 software 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.

You can also assign permissions to users.

Publishing objects

You can control user access to objects, such as analysis runs and 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 *User Guide*.

Topics

You can add a layer of security on Empirica Topics by creating work teams. Work teams enable different groups of users to view a topic. Within a work team, you can give users different work team permissions, which determine the level of access users have to topics that are 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 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.

A 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.

User session timeout

The Empirica Signal application cancels user sessions that have been inactive for a specified period of time. To change the default user session timeout value, see the *Installation Guide*.

About the documentation

Where to find the product documentation

The product documentation is available from the following locations:

- **My Oracle Support** (https://support.oracle.com)—*Release Notes* and *Known Issues*.
- **Oracle Technology Network** (http://www.oracle.com/technetwork/documentation/hsgbu-154445.html)—The most current documentation set, excluding the *Release Notes* and *Known Issues*.

If the software is available for download, the complete documentation set is available from the Oracle Software Delivery Cloud (https://edelivery.oracle.com).

All documents may not be updated for every Empirica Signal release. Therefore, the version numbers for the documents in a release may differ.

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.

Documentation

Item	Description	Part number	Last updated
Release Notes	The *Release Notes* document provides descriptions of new features, enhancements, and bug fixes as well as system requirements.	E60410-01	8.1
Known Issues	The *Known Issues* document provides detailed information about the known issues in the release, along with workarounds, if available.	E70268-01	8.1
User Guide and Online Help	The *User Guide and Online Help* provides step-by-step instructions on how to use the Empirica Signal and Empirica Topics applications to perform statistical analyses of safety data.	E70269-01	8.1
Installation and Upgrade Guide	The *Installation and Upgrade Guide* document provides instructions on how to install and configure the environment for the Empirica Signal software.	E60411-01	8.1
Secure Configuration Guide	The *Secure Configuration Guide* provides guidance and recommendations on securely installing, configuring, and managing the Empirica Signal software and its system components.	E60408-01	8.1
Topics API Guide	The *Topics API Guide* describes how to integrate a proprietary application with Empirica Topics.	E77813-01	8.1
Topics Reporting and Oracle Business Intelligence Configuration Guide	The *Topics Reporting and Oracle Business Intelligence Configuration Guide* provides system requirements and configuration instructions for integrating OBIEE with the Empirica Signal application.	E60409-01	8.1
Argus Mart Data and Argus Signal Management Installation Instructions	The *Argus Mart Data and Argus Signal Management Installation Instructions* describe how to import proprietary data maintained in Argus Mart to Empirica Signal and how to install and configure Argus signal management.	E70267-01	8.1
Argus Mart Data and Argus Signal Management Release Notes	The *Argus Mart Data and Argus Signal Management Release Notes* describe new features, enhancements, and bug fixes to the Argus Mart data configurations for Empirica Signal. They also document the Argus Mart data tables available to Empirica Signal and the default signal management configuration.	E76553-01	8.1

Item	Description	Part number	Last updated
Third Party Licenses and Notices	The *Third Party Licenses and Notices* document includes licenses and notices for third party technology that may be included or distributed with the Empirica Signal software.	E78170-01	8.1