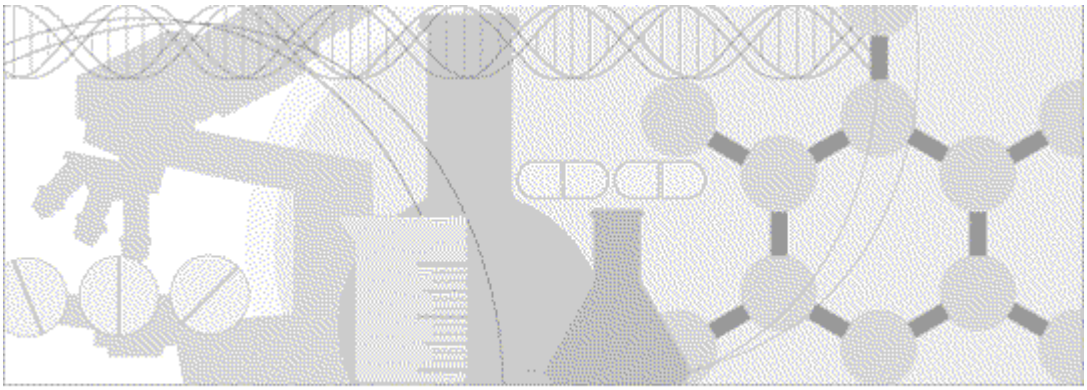
Secure Configuration Guide

Oracle® Health Sciences Empirica Healthcare 1.0



ORACLE

Part number: E49242-01

Contents

About this guide

In this preface

Overview of this guide

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

Audience

This guide is for database administrators, Empirica Healthcare site administrators, IT administrators, and others whose responsibility is to perform the following:

- Install and configure the Empirica Healthcare 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 guide assumes that you have an understanding of operating system and database concepts, and have experience using the software tools described.

Related information

Empirica Healthcare 1.0 documentation

All documentation is available from the Oracle Software Delivery Cloud (https://edelivery.oracle.com) and the Oracle Technology Network.

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

Document	Description	Last updated
Release Notes	The *Release Notes* document provides high-level descriptions of the main features in this release of the Empirica Healthcare application, as well as system requirements.	1.0
Known Issues	The *Known Issues* document provides detailed information about the known issues in this release, along with workarounds, if available.	1.0
User Guide	The *User Guide* describes how to use the Empirica Healthcare application to perform epidemiologic and statistical analyses of commercially available healthcare and administrative claims data.	1.0
Installation Instructions	The *Installation Instructions* document describes how to install the Empirica Healthcare software.	1.0
Secure Configuration Guide	The *Secure Configuration Guide* provides guidance and recommendations on securely installing, configuring, and managing the Empirica Healthcare software and its system components.	1.0

If you need assistance

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

CHAPTER 1

Security overview

In this chapter

Overview

The Empirica Healthcare software is a web application that provides a high-performance epidemiologic data analysis environment for exploring multiple sources of population-based data, such as:

- Clinical data from electronic healthcare records.
- Administrative data from insurance claims.

The software allows industry and pharmacovigilance professionals at pharmaceutical sponsors, regulatory agencies, and health care organizations to explore and review the following types of activities:

- Pharmacovigilance activities
- Pharmacoepidemiological activities
- Risk management activities

When your organization implements the Empirica Healthcare software, Oracle recommends that you install the software and its system components using secure installation methods to protect the integrity and confidentiality of your data. Additionally, Oracle recommends managing and monitoring your system after installation to make sure that your data is protected from unauthorized access and misuse.

This document provides guidelines for secure installation and configuration and describes the security features provided 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 Healthcare 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 Healthcare software.

CHAPTER 2

Secure installation and configuration

In this chapter

Installing and configuring the Empirica Healthcare software

The Empirica Healthcare *Installation Instructions* include 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 Healthcare software:

Execute scripts without passwords on the command line

When you are required to authenticate to your Oracle database during the Empirica Healthcare 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 Healthcare 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 *Installation Instructions*.

Encrypt the Empirica Healthcare database account password

The Empirica Healthcare *Installation Instructions* include directions for encrypting the Empirica Healthcare database account password. To ensure a secure installation, Oracle recommends following the instructions.

Turn on the HttpOnly flag for session cookies within WebLogic for the Empirica Healthcare 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 following directory:

$INSTALL_DIR/Healthcare/WEB-INF

2 Open the **weblogic.xml** file, and scroll to 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 flag is turned on, users must use Microsoft Internet Explorer 8 or later and Java 7 or later to view single-patient and multi-patient timelines as applets. Users running older releases should deselect the Display Patient Timelines as applets user preference. Alternatively, you can deselect the Enable User Preference to display Patient Timelines as applet site option, which turns off the applet viewing mode for all users.

Establish best practices for downloading data

The Empirica Healthcare software 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 Healthcare software.

Route email to a secure address

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

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

Allow database passwords to expire, and change default passwords

Oracle Database is installed with several default database user accounts, such as SYS and SYSTEM. Upon successful installation of the database, the Database Configuration Assistant automatically locks and expires most built-in database user accounts. Upon account expiration, configure strong and secure passwords for the accounts.

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

Regenerating the license.config file

The license.config file holds a site-specific key used to encrypt and decrypt the database passwords. The installation kit contains a utility that generates the license.config file. You might need to regenerate the key if it becomes corrupted or compromised.

To create and install a new site-specific key:

1 Navigate to the following directory, and delete the license.config file.

$INSTALL_DIR/Healthcare/WEB_INF/classes

Information about $INSTALL_DIR is in the Empirica Healthcare *Installation Instructions*.

2 Create the site-specific key by using bin/generate_keys.sh.

Instructions are in the Empirica Healthcare *Installation Instructions*.

3 After generate_keys.sh completes, update and redeploy the Empirica Healthcare application in WebLogic.

Instructions are in the Empirica Healthcare *Installation Instructions*.

4 Log in to the Empirica Healthcare application as a super user or a user with the Manage Configurations permission.

5 Edit a configuration. For more information, see the Empirica Healthcare *User Guide*.

You are prompted to specify the password of the database account on which the configuration is based. The new key is used to generate an encrypted version of the password, which is retained for future use.

6 Edit every configuration so that encrypted passwords can be regenerated for all of them.

CHAPTER 3

Security features

In this chapter

Overview of security features

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

- Authentication

  You can 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 Healthcare software also provides publishing capabilities to restrict user access to objects.

- Auditing

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

Authentication

Authentication methods

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

With local authentication, the Empirica Healthcare software captures successful and failed login attempts in the User Activity Audit Trail, described in *Auditing* (on page 13).

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

Password requirements

The Empirica Healthcare 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 Healthcare 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

Disabling user accounts

When an employee leaves your organization, the Empirica Healthcare 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 Healthcare software.

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

User access control

The Empirica Healthcare software 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 Healthcare 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 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 Healthcare *User Guide*.