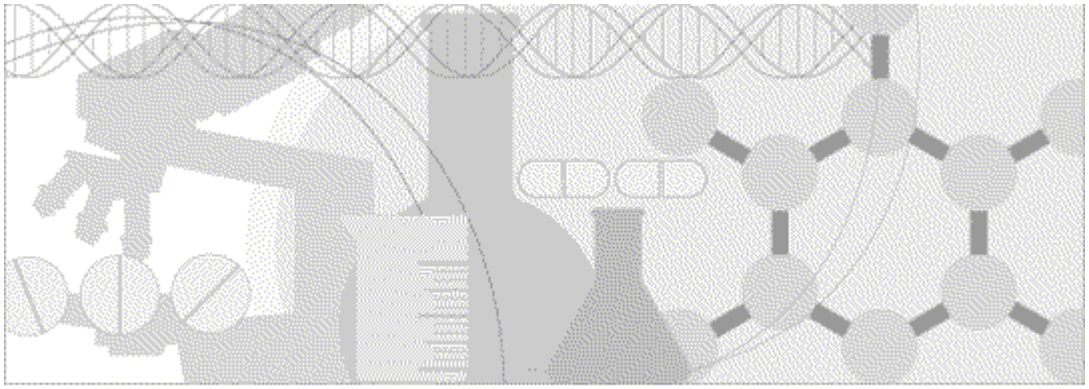
Secure Configuration Guide

Oracle® Health Sciences Empirica Healthcare Analysis Release 1.0.2



ORACLE

Part number: E66637-01

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 Analysis 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 Analysis *Installation Guide* and user documentation.

Audience

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

- Install and configure the Empirica Healthcare Analysis 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.

Documentation

The product documentation is available from the following locations:

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

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

Document	Description	Last updated
Release Notes	The *Release Notes* document provides descriptions of enhancements and bug fixes as well as system requirements.	1.0.2
Known Issues	The *Known Issues* document provides detailed information about the known issues in this release, along with workarounds, if available.	1.0.2
User Guide	The *User Guide* describes how to use the Empirica Healthcare Analysis application to perform epidemiologic and statistical analyses of healthcare and administrative claims data.	1.0.1
Installation Guide	The *Installation Guide* document describes how to install the Empirica Healthcare Analysis software.	1.0.1
Secure Configuration Guide	The *Secure Configuration Guide* provides guidance and recommendations on securely installing, configuring, and managing the Empirica Healthcare Analysis software and its system components.	1.0.2
Transferring Data from the Common Data Model	The *Transferring Data from the Common Data Model* document describes how to use the Empirica Healthcare Analysis ETL utility to transfer data in the OMOP Common Data Model (CDM) Version 4 from a source system to the Empirica Healthcare Analysis database.	1.0.2
Third Party Licenses and Notices	The *Third Party Licenses and Notices* document includes licenses and notices for third party technology that may be included with the Empirica Healthcare Analysis software.	1.0.2

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.

If you need assistance

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.

Finding Empirica Healthcare Analysis information and patches on My Oracle Support

The latest information about the Empirica Healthcare Analysis application is on the Oracle Support self-service website, My Oracle Support. Before you install and use the Empirica Healthcare Analysis application, check My Oracle Support for the latest information, including *Release Notes* and *Known Issues*, alerts, white papers, bulletins, and patches.

Creating a My Oracle Support account

You must register at My Oracle Support to obtain a user name and password before you can enter the site.

1 Open a browser to https://support.oracle.com.

2 Click the **Register** link.

3 Follow the instructions on the registration page.

Finding information and articles

1 Sign in to My Oracle Support at https://support.oracle.com.

2 If you know the ID number of the article you need, enter the number in the text box at the top right of any page, and then click the magnifying glass icon or press **Enter**.

3 To search the knowledge base, click the **Knowledge** tab, and then use the options on the page to search by:

- Product name or family.
- Keywords or exact terms.

Finding patches

You can search for patches by patch ID or number, product, or family.

1 Sign in to My Oracle Support at https://support.oracle.com.

2 Click the **Patches & Updates** tab.

3 Enter your search criteria and click **Search**.

4 Click the patch ID number.

The system displays details about the patch. You can view the Read Me file before downloading the patch.

5 Click **Download**, and then follow the instructions on the screen to download, save, and install the

patch files.

Finding Oracle documentation

The Oracle website contains links to Oracle user and reference documentation. You can view or download a single document or an entire product library.

Finding Oracle Health Sciences documentation

For Oracle Health Sciences applications, go to the Oracle Health Sciences Documentation page at http://www.oracle.com/technetwork/documentation/hsgbu-clinical-407519.html.

Note: Always check the Oracle Health Sciences Documentation page to ensure you have the most up-to-date documentation.

Finding other Oracle documentation

1 Do one of the following:

- Go to http://www.oracle.com/technology/documentation/index.html.
- Go to http://www.oracle.com, point to the **Support** tab, and then click **Product Documentation**.

2 Scroll to the product you need, and click the link.

CHAPTER 1

Security overview

In this chapter

Overview

The Empirica Healthcare Analysis 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 Analysis 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
  - Uppercase character
  - Lowercase character

- Keep passwords secure.

  When you create user accounts in the Empirica Healthcare Analysis software, send users their user names and initial passwords in separate email messages. Instruct 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 Healthcare Analysis software.

CHAPTER 2

Secure installation and configuration

In this chapter

Installing and configuring the Empirica Healthcare Analysis software

The Empirica Healthcare Analysis *Installation Instructions* include 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. In addition to performing the standard installation procedures, you can perform the following steps to secure the Empirica Healthcare Analysis software:

Execute scripts without passwords on the command line

When you are required to authenticate to your Oracle database during the Empirica Healthcare Analysis installation, do not provide database account passwords as arguments from the command prompt. The standard installation instructions provide examples of execution scripts.

Reset the Read Only attribute

The standard Empirica Healthcare Analysis 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 Analysis database account password

The Empirica Healthcare Analysis *Installation Instructions* include directions for encrypting the Empirica Healthcare Analysis 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 Analysis 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 Analysis 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 Analysis software.

Route email to a secure address

In the Empirica Healthcare Analysis 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.

Use of SSL

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

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

- Disable the use of vulnerable SSL protocols by adding the following JVM option to the JAVA_OPTIONS settings in the setDomainEnv.sh file:

  -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 WebLogic config.xml file.

  Do not include the following weak ciphers:

  - DES 56/56
  - NULL
  - RC2 40/12k
  - RC2 56/128
  - RC4 40/128
  - RC4 56/128
  - RC4 64/128
  - PCT1.0\Server
  - SSL 2.0/Server
  - SSL 3.0/Server

Encrypt the database connection

If you install the Empirica Healthcare Analysis software and Oracle Database 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 one of the following documents:

- For Oracle Database 11g, see the *Oracle Database Advanced Security Administrator's Guide*:

  http://docs.oracle.com/cd/B28359_01/network.111/b28530/asojbdc.htm#g1007990

- For Oracle Database 12c, see the *Oracle Database Security Guide*:

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

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. 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.

Configure components to use FIPS 140-2 compliant cryptographic implementations

You can configure the Oracle Database and WebLogic Server used with the Empirica Healthcare Analysis 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

CHAPTER 3

Security features

In this chapter

Overview of security features

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

- Authentication

  You can select from flexible password options to establish a password policy for user accounts.

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

- Auditing

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

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

Password requirements

The Empirica Healthcare Analysis 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 Analysis 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
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 Lower case	1
Minimum Upper case	1

Disabling user accounts

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

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

User access control

The Empirica Healthcare Analysis 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 Analysis 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.

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 Healthcare Analysis *User Guide*.