Empirica™ Signal Secure Configuration Guide

Release 7.3.3.0.354

April 2012

Oracle Health Sciences Empirica Signal 7.3.3.0.354 English Documentation

Updated 4-Apr-2012

Contents

About this guide

This guide provides guidance and recommendations on installing, configuring, and managing Empirica Signal and its system components securely. 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 Signal installation guide and user documentation.

Audience

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

- Install and configure Empirica Signal 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.

Security 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 Empirica Signal, industry and pharmacovigilance professionals can efficiently manage the review, processing, and response to drug and vaccine safety signals. When your organization implements Empirica Signal, 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 once installed 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 one aspect of complexity, such as non-alphabetical characters.

- Keep passwords secure.

  When you initially create user accounts in Empirica Signal, send users their username and initial password in separate email messages. Instruct your users not to share or write down passwords, or store passwords in files on their computers. In addition, require users to change their default 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 least amount 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 Empirica Signal.

Installing and configuring your system securely

Installing and configuring Empirica Signal

The Empirica Signal 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 do the following to secure Empirica Signal:

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. When you have completed the installation, you can disable other features that you may not use, such as interactive reports, in the site options.

Execute scripts without passwords on the command line

Where it is 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.

Disable weak IIS encryption ciphers

The standard Empirica Signal installation requires you to run the `iis_cipher_configuration.reg` script, which disables all weak TLS/SSL ciphers automatically. This ensures that only strong encryption algorithms are used.

Reset the Read Only attribute

The standard Empirica Signal installation requires you to deselect the read-only attribute for several files to edit them. When the installation completes, ensure that you re-select the read-only attribute.

Encrypt the database password

The Empirica Signal installation instructions include optional instructions for encrypting the database password. To ensure a secure installation, follow the procedures in *Empirica Signal Windows 2003/2008 Server Installation and Upgrade Instructions* to encrypt the database password.

Establish best practices for downloading data

Empirica Signal provides the option to download table data to a Microsoft Excel spreadsheet or to an RTF file. Establish best practices for downloading data to ensure the data remains secure outside of Empirica Signal.

Route email to a secure address

In Empirica Signal, 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 your Oracle database

You can do the following to install your Oracle database securely:

Patch your database regularly and apply security updates

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

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

Allow database passwords to expire and change default passwords

Oracle Database installs 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 default database user accounts. Upon account expiration, configure strong, secure passwords for the default accounts.

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

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

Installing Oracle Access Manager

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

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

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`

Installing Internet Information Services (IIS)

The standard Empirica Signal installation provides instructions for configuring IIS for Windows 2003 Server and Windows 2008 Server. Additionally, you should configure IIS for SSL. For more information and specific instructions, see the Microsoft Support knowledgebase article 299875 at:

`http://support.microsoft.com/kb/299875`

Regenerating the license.config file

The `license.config` file holds a site-specific key to encrypt and decrypt the database passwords. The installation kit contains a utility that generates this file. You may need to regenerate the key if it becomes corrupted or compromised. In this instance, do the following to create the site-specific key:

1. Navigate to `C:\Lincoln\apps\webvdme\lib`.
2. Delete the license.config file, if it exists.
3. For Windows 2008, right-click on the `C:\Lincoln\apps\webvdme\bin\generate_keys.bat` file, and then select **Run as administrator**.

   Or

   For Windows 2003, double-click on the `C:\Lincoln\apps\webvdme\bin\generate_keys.bat` file.
4. After `generate_keys.bat` has completed, when prompted, type any key.
5. After `set_permissions.bat` has completed, when prompted, type any key.
6. If you are using LDAP authentication with a search dn password, regenerate the password.

   For Windows 2008, right-click on the `C:\Lincoln\apps\webvdme\bin\ldap_search_password.bat` file, and then select **Run as Administrator**.

   Or

   For Windows 2003, double-click the `C:\Lincoln\apps\webvdme\bin\ldap_search_password.bat` file.
7. After `ldap_search_password.bat` has completed, when prompted, press any key.
8. For Windows 2008, right-click on the `set_permissions.bat` file, and then select **Run as administrator**.

   Or

   For Windows 2003, double-click on the `set_permissions.bat` file.
9. Restart the Empirica Signal service.
   a. Right-click on the server's desktop **My Computer** icon and select **Manage**.
   b. Expand the Services and Applications directory, and then click **Services**.
   c. Right-click on the **webvdme** service and select **Start**.

      Alternatively, type `net start webvdme` in a command prompt.
   d. Right-click the **World Wide Web Publishing** service, and click **Start**.
10. Log in to Empirica Signal.
11. Edit each of your data configurations specifically to re-enter the data configuration password.
12. If you are using Topics, delete and then re-import each topic workflow configuration. Ensure that you select **Remove reference only (You may re-import the configuration later)** when you delete each topic workflow configuration.

For more information on editing data configurations or deleting or importing topic workflow configurations, see the Empirica Signal Help.

Empirica Signal security features

Empirica Signal provides three main 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 user account password policy.

- User Access Control

  Empirica Signal provides several default roles to which you can assign users. You can also assign permissions to restrict user access to only the features that are appropriate for their job responsibilities. Empirica Signal also provides publishing capabilities to restrict user access to objects.

- Auditing

  Empirica Signal tracks user activity automatically, including successful and failed logins, to provide a comprehensive audit trail of actions performed.

Authentication

Authentication methods

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

- **Local**—User information stored in Empirica Signal is used for authentication.
- **LDAP**—User information stored in a Lightweight Directory Access Protocol directory is used for authentication.
- **Single Sign-On**—User information stored in Oracle® Access Manager is used for authentication.

With local and LDAP authentication, Empirica Signal captures successful and failed login attempts in the User Activity Audit Trail, described in **Auditing** below. In addition, when a user exceeds the allowable number of login attempts that you set in your password requirements, Empirica Signal sends an account lockout email notification to your site administrator.

For more information on configuring and implementing authentication methods, see the Empirica Signal Help.

Password requirements

Empirica Signal provides password options that you can select to establish a user account password policy for your local and LDAP users. Using the options, you can require specific password content, complexity, and expiration. Empirica Signal provides the following password options and default values:

- 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 — 0
- Minimum Lowercase — 1
- Minimum Uppercase — 0

You can edit the default values to suit your organization's requirements. For more information on password requirements, see the Empirica Signal Help.

Disabling user accounts

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

Auditing

The Empirica Signal auditing feature is a standard feature that cannot be disabled. The User Activity Audit Trail tracks user activity that occurs in the Signal 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 unauthorized actions or misuse.

Empirica Signal maintains audited user activity indefinitely. You cannot modify or delete audit records through Empirica Signal.

For more information on auditing, see the Empirica Signal Help.

User access control

Empirica Signal allows you to implement user access control using roles and permissions to 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 roles are created by default. The roles are designed for least privilege and separation of duties. You can modify the permissions assigned to the roles, or create new roles if needed.

Granting permissions

When you assign users to roles, all users have the same set of permissions. Empirica Signal has many permissions that grant or restrict user access to different application features. Before assigning users to roles, review the permissions assigned to the roles to ensure users can perform all tasks relevant to their job responsibilities.

Publishing objects

You can control user access to objects, such as data mining 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 or who are superusers can publish objects that they or any users in their login group created.

For more information on user access control, see the Empirica Signal Help.