Secure Configuration Guide

Oracle® Health Sciences WebSDM and Empirica Study

Release 3.1.2

January 2013

Part Number: E38369-01

Contents

About this guide

This guide provides guidance and recommendations on installing, configuring, and managing WebSDM and Empirica Study 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 WebSDM and Empirica Study installation guide and user documentation.

Audience

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

- Install and configure WebSDM and Empirica Study 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

WebSDM/Empirica Study is a web application designed to work with clinical trial data in the Clinical Data Interchange Standards Consortium (CDISC) Study Data Tabulation Model (SDTM) format. The Web Submission Data Manager (WebSDM) component allows you to validate case report data for compliance with the CDISC *Study Data Tabulation Model Implementation Guide*. The Empirica Study component is an optional set of features supporting the detection and evaluation of possible safety issues in study data. When your organization implements WebSDM/Empirica Study, 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 WebSDM and Empirica Study 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 aspect of complexity, such as non-alphabetical characters.

- Keep passwords secure.

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. Should you need to update user accounts, send users their username and password in separate email messages.

- 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 WebSDM and Empirica Study.

Installing and configuring your system securely

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 Internet Information Services (IIS)

The standard WebSDM/Empirica Study 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`

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 and configuring WebSDM/Empirica Study

The WebSDM/Empirica Study 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 WebSDM/Empirica Study:

Execute scripts without passwords on the command line

Where it is required to authenticate to your Oracle database during the WebSDM/Empirica Study 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 WebSDM/Empirica Study 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 WebSDM/Empirica Study 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 for files you have edited.

Encrypt the master database password

The WebSDM/Empirica Study installation instructions include steps to encrypt the master database password. To ensure a secure installation, follow the procedures in *WebSDM/Empirica Study Windows 2003/2008 Server Installation Instructions* to encrypt the database password.

Enable only what is required

When you have completed the WebSDM/Empirica Study installation, you should disable features that you will not use, such as PPD Patient Profiles or Empirica Study features.

Route email to a secure address

In WebSDM/Empirica Study, provide secure email addresses for the Feedback Email and Error Email site options. Consider providing email addresses that are not routed over the internet.

Establish best practices for downloading data

WebSDM/Empirica Study 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 WebSDM/Empirica Study.

Replace the encryption key if compromised or corrupted

WebSDM/Empirica Study uses an encryption key to protect the database passwords associated with the accounts created for new applications and studies/pools, and the master database account. Follow the procedures in *WebSDM/Empirica Study System Administration Guide* to replace the encryption key if it is compromised or corrupted.

WebSDM/Empirica Study security features

WebSDM/Empirica Study provides three main security features to help you secure your system:

- Authentication

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

- Auditing

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

- User Access Control

  WebSDM/Empirica Study provides several default roles to which you can assign users. You can also create new roles or assign individual permissions to restrict user access to only the features that are appropriate for their job responsibilities. WebSDM/Empirica Study also provides publishing capabilities to restrict user access to objects.

- User Session Timeout

  WebSDM/Empirica Study automatically cancels user sessions that have been inactive for a specified period of time. The WebSDM/Empirica Study installation instructions include instructions for changing the default timeout period.

Authentication

Authentication methods

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

- **Local**—User information stored in WebSDM/Empirica Study is used for authentication.
- **Single Sign-On**—User information stored in Oracle® Access Manager is used for authentication.

With local authentication, WebSDM/Empirica Study 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, WebSDM/Empirica Study sends an account lockout email notification to your site administrator.

For more information on configuring and implementing authentication methods, see the WebSDM/Empirica Study Help.

Password requirements

WebSDM/Empirica Study 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. WebSDM/Empirica Study provides the following password options and default values:

- Expiration — 0 days
- Expiration Warning — 7 days
- Minimum Length — 8 characters
- Number of Attempts Allowed — Unlimited
- Number of Passwords Retained — 0
- Minimum Alphabetic — 0
- Minimum Numeric — 0
- Minimum Non-alphanumeric — 0
- Minimum Lowercase —
- Minimum Uppercase —

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

Disabling user accounts

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

Auditing

The WebSDM/Empirica Study auditing feature is a standard feature that cannot be disabled. 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 unauthorized actions or misuse.

WebSDM/Empirica Study maintains audited user activity indefinitely. You cannot modify or delete audit records through WebSDM/Empirica Study.

For more information on auditing, see the WebSDM/Empirica Study Help.

User access control

WebSDM/Empirica Study 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, those users have the same set of permissions. WebSDM/Empirica Study provides 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.

You can also assign users to roles, and then supplement individual users with specific permissions.

Publishing studies and other objects

You control user access to studies and other objects by publishing them 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 that they have created. Those users can publish objects only to other users in their own login group.

Users with the *Administer Users* permission or who are superusers can publish objects that they or any other users created.

For more information on user access control, see the WebSDM/Empirica Study Help.