System Administration Guide

Oracle® Health Sciences WebSDM and Empirica Study

Release 3.1.2

January 2013

Part Number: E38363-01

Copyright © 2000–2013, Oracle and/or its affiliates. All rights reserved.

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software -- Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This documentation may include references to materials, offerings, or products that were previously offered by Phase Forward Inc. Certain materials, offerings, services, or products may no longer be offered or provided. Oracle and its affiliates cannot be held responsible for any such references should they appear in the text provided.

Contents

CONFIDENTIAL ▪ Copyright © 2000–2013, Oracle and/or its affiliates. All rights reserved.

Copyright © 2000–2013, Oracle and/or its affiliates. All rights reserved.

1 Introduction

This guide describes required and optional tasks that are performed by a system administrator after WebSDM™/Empirica Study™ installation. It is intended for use by system administrators (or database administrators) who are familiar with Oracle relational databases and who host WebSDM/Empirica Study at their own installations, rather than contracting for this service from Oracle.

Note: Where this document refers to 'WebSDM', the statement is equally true for instantiations of the product that include Empirica Study. The term 'Empirica Study' can be freely substituted for 'WebSDM'.

This guide covers the following topics:

- System configuration
- User accounts and security
- Data loading
- Monitoring WebSDM

In addition to this guide, the following documentation resources are also available:

- *WebSDM/Empirica Study Windows 2003/2008 Server Installation Instructions* (the `WebSDM_Windows_Installation_Instructions.pdf` file provided on the installation CD).
- WebSDM help: all users can access the WebSDM™/Empirica Study™ online help system for detailed, context-sensitive information including step-by-step procedures for many of the topics covered in this guide. To access help, click **Help** on any page.

  In addition to the online help, you can typically access Release Notes, information on the WebSDM API, and other pertinent, customer-specific documents from the help: click **Show Table of Contents** in any help topic, and then open the "Release Notes and Other Documents" topic in the table of contents.

1.1 Product Overview

WebSDM (Web Submission Data Manager) is a web-based system that is designed to enhance the speed and quality of reviews done on clinical trial data that will be submitted to the Food and Drug Administration (FDA). Users load case report data files into WebSDM, which performs automated checks of the data to assure that it conforms to the Clinical Data Interchange Standards Consortium (CDISC) Study Data Tabulation Model (SDTM) electronic submission standard. Users can also use WebSDM features to query data and prepare reports.

CONFIDENTIAL ▪ Copyright © 2000–2013, Oracle and/or its affiliates. All rights reserved.

Empirica™ Study is an optional feature set that can be licensed along with WebSDM. Empirica Study supports the detection and evaluation of possible safety issues in clinical trial data. Requirements that apply to the Empirica Study feature set only are not covered by this guide.

1.2 WebSDM System Architecture

As a web-based system, the WebSDM application runs on a server that users can access with a web browser running on a client computer. WebSDM is a "thin-client" system, meaning that no components other than a web browser are required to be installed on the users' computers. All application processing occurs on the server.

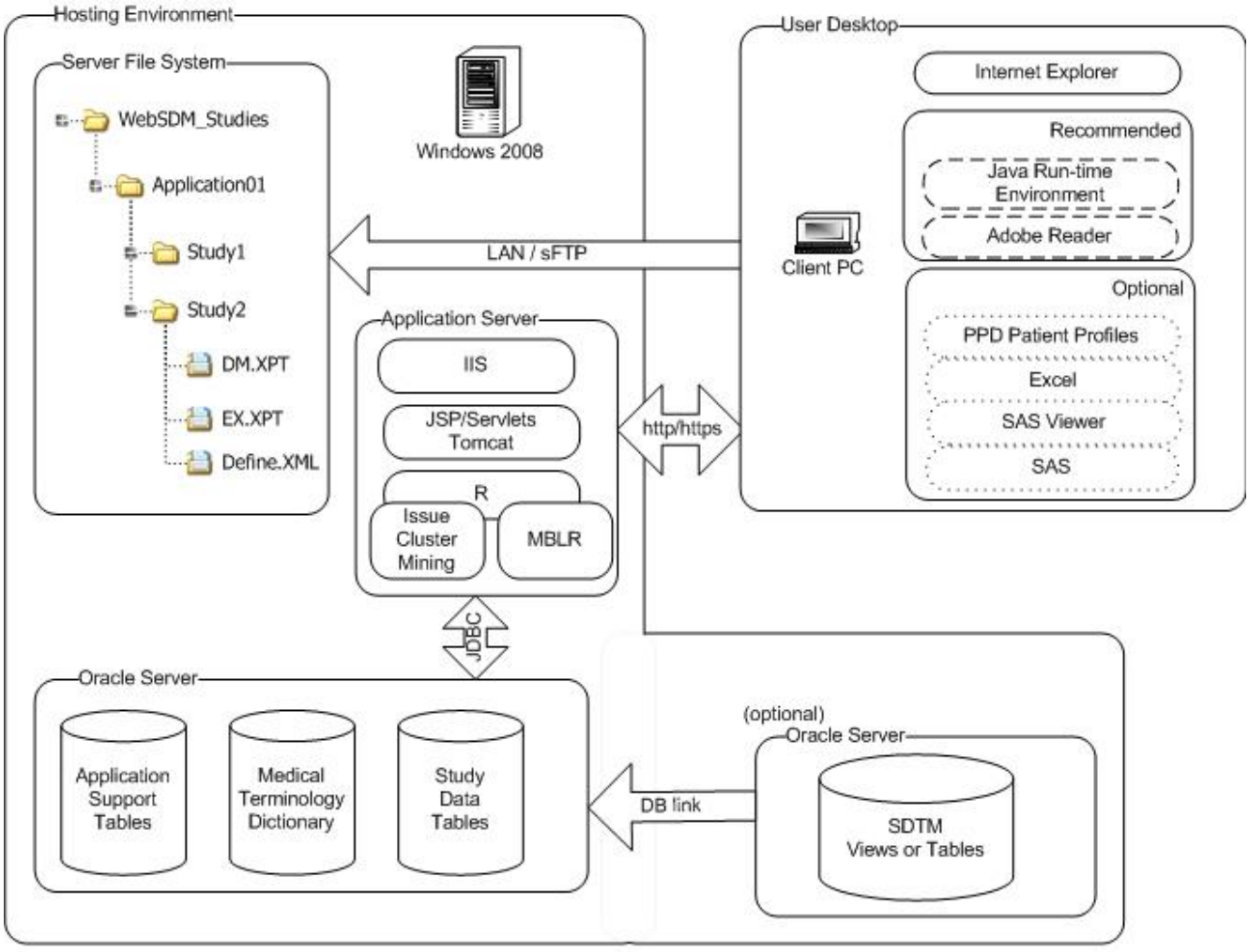
WebSDM uses an Oracle database, which often runs on the same physical server as the application server. In configurations with a very large number of users or a very large amount of data, the WebSDM server environment may include separate physical server machines for the application server and the Oracle database.

Though WebSDM does not require a client installation, there are several optional features that do. For more information, see Client Computer Setup.

Note: if your Oracle database does not run on the same physical server as the application server, both servers should be set to the same time zone.

CONFIDENTIAL ▪ Copyright © 2000–2013, Oracle and/or its affiliates. All rights reserved.

An illustration of the typical WebSDM system architecture follows.



Data can be loaded into the WebSDM server environment in two ways:

- SDTM data files in SAS transport (.xpt) format from a local or network accessible file system.
- From other Oracle schemas with data tables that conform to the SDTM standard.

2 System Configuration

This chapter covers the following sections::

- Server Setup
- Client Computer Setup
- Setup in WebSDM
- Installing MedDRA Versions

2.1 Server Setup

This section covers the following sub-sections:

- Required hardware and software
- Setting the session timeout period
- Configuring the properties file

2.1.1 Required hardware and software

The hardware requirements of the WebSDM server include:

- Windows/Intel Pentium Processor (32-bit or 64-bit)
- 2 x 2.8 GHz processors
- 4 GB of memory
- 250 GB disk (RAID 5 recommended)

Additional disk storage may be recommended depending on the size and number of studies that will be kept on the server.

Step-by-step instructions for WebSDM installation are provided in the *WebSDM/Empirica Study Windows 2003/2008 Server Installation Instructions* (WebSDM_Windows_Installation_Instructions.pdf). Instructions for periodic updates are provided in the *WebSDM/Empirica Study Windows 2003/2008 Server Upgrade Instructions* (WebSDM_Windows_Upgrade_Instructions.pdf).

This list provides an overview of required server software, which includes:

CONFIDENTIAL ▪ Copyright © 2000–2013, Oracle and/or its affiliates. All rights reserved.

- Windows 2003 Standard or Enterprise, Windows 2003 x64 Standard or Enterprise, or Windows 2008 Standard or Enterprise.

  Note: The 64-bit Itanium version is not supported.

- Single or multi-processor. For information about setting up a multi-processor server for WebSDM, see *System Tuning and Monitoring* (page 49).
- Oracle 10g (10.2.0.3 or higher) or 11g (11.2.0.2 or higher) database, using a single-byte database character set such as the WE8MSWIN1252, or using a multi-byte character set with NLS_LENGTH_SEMANTICS set to "CHAR".
- Oracle 10g (10.2.0.3 or higher) or 11g (11.2.0.2 or higher) client.
- If you will be implementing Single Sign-On, a server with the Oracle Access Manager (OAM) installed.
- Microsoft Internet Information Services (IIS) web server.
- Apache Tomcat 6.0.2.2 application server (provided on installation CD).
- An installation of the 32-bit version of R for Windows. R version 2.13.2 is downloadable from http://cran.r-project.org; licensing information for use of R can be found at http://www.r-project.org.
- A file compression and extraction utility for `.zip` files, such as WinZip.

In general, WebSDM functionality is independent of the database server configuration selected (that is, the operating system under which the database is running has no effect on WebSDM). There are two exceptions:

- For a database running under UNIX, the `direct_path` element in the `website.properties` file should be set to `0` (zero). By default, this file is in the following directory: `c:\Lincoln\apps\websdm\webapps\web_root\WEB-INF\classes\`. See *Configuring website.properties for background processes* (page 11).
- In WebSDM, the View Free Space page is only partially functional when the database is deployed to a machine other than the application server. See *Reviewing space consumption* (page 51).

2.1.2 Setting the session timeout period

WebSDM has a security feature that automatically cancels user sessions that have been inactive for a specified period of time. To configure the session timeout period and end inactive sessions automatically, you set a timeout interval in the `web.xml` file on the WebSDM server. You use an ASCII text editor such as Notepad to review and edit the `web.xml` file, which is found by default in the `C:\Lincoln\apps\websdm\webapps\web_root\WEB-INF` directory.

The <session-timeout> tag sets the maximum length of time for a session to remain inactive before the user is logged out automatically. For example, to set the session timeout period to 30 minutes you supply a value for this tag as follows:

```
<session-timeout>30</session-timeout>
```

Typically, a system administrator sets the session timeout period at installation and updates it as needed.

2.1.3 Configuring the properties file

The file website.properties contains site-specific configuration settings that allow WebSDM to establish database connections and locate external resources. The content of this file is usually set during WebSDM installation but may be modified at any time. By default, this file is in the following directory: c:\Lincoln\apps\websdm\webapps\web_root\WEB-INF\classes\.

The website.properties file contains configuration information used by WebSDM for connecting to the database and for certain foreground and background processes. You can use a text editor such as Notepad to open the file and edit the values for its elements

2.1.3.1 Configuring website.properties for database connection

Element	Description
user pass connect	Define the credentials and connection information needed for WebSDM to log in to the master database account. After installation, the values specified for user and pass match the credentials specified in the 2_create_oracle_user.sql script executed during WebSDM installation. The value specified for connect should be jdbc:oracle:oci8:@websdm, as illustrated above. You can also reset the values specified for these elements from within WebSDM. For more information, see *Setting the database connection for the WebSDM master account* (page 17). This procedure resets the values in the website.properties file only; it does not reset the actual database password.

2.1.3.2 Configuring website.properties for foreground processes

Element	Description
r_path	Defines the path to the R executable.
tablespace_datafileSpec	Used if a WebSDM site option is set to create a distinct tablespace for

Element	Description
tablespace_options	each registered application. For more information on WebSDM site options, see *Setting site options* (page 18), and consult a database administrator to confirm that the values specified for these elements are appropriate for your environment.

2.1.3.3 Configuring website.properties for background processes

Element	Description
serverid	This element should be set to 4.
logfile uselog loglevel	Define whether and how system events are logged. The value specified for logfile can be any valid file name on the WebSDM server. The recommended setting for uselog is true and for loglevel is error. *Note*: These elements control how background processes are logged, and are not affected by the WebSDM site option for Log Level.
process_dir	Specifies the name of a directory that WebSDM can use to store temporary files generated by the background processes.
sqlldr_path	Defines the path to the SQL*Loader executable, which is part of the Oracle client kit.
direct_path	To support a database running under UNIX, remove the # symbol from the beginning of this line to "un-comment" it.

2.1.4 Replacing the encryption key

The license.config file contains a site-specific key to encrypt/decrypt the master database account and the database passwords associated with the accounts created for new applications and studies/pools. Follow these steps to regenerate the key if it is lost or corrupted:

1. Stop the WebSDM service.
2. Navigate to <root>\Lincoln\apps\<instance>\webapps\web_root\WEB_INF\classes
3. Rename the existing license.config file to another name such as license.old
4. Navigate to <root>\Lincoln\apps\<instance>\bin
5. Use a text editor to open the file generate_keys.bat and review the values of INSTALL_ROOT and APPLICATION_DIR. If the installation root is other than the c drive, change the value of INSTALL_ROOT to the correct drive. If the WebSDM instance is other

CONFIDENTIAL ▪ Copyright © 2000–2013, Oracle and/or its affiliates. All rights reserved.

than websdm, change the value of APPLICATION_ROOT. If changes are needed, edit and save the file.

6. *(Windows 2008 server)* Right-click on the `generate_keys.bat` file, and then select **Run as administrator**.
   (Windows 2003 server) Double-click on the generate_keys.bat file.
7. Examine the script output, verify the last two lines are:

   ```
   [INFO] Generating C:\Linoln\apps\websdm\webapps\web_root\WEB-INF
                                                          \classes\license.config

   [INFO] Done
   ```

8. When prompted, type any key.
9. If the last two lines of script output are not as indicated, correct the error condition and repeat.
10. Navigate to `<root>\Lincoln\apps\<instance>\webapps\web_root\WEB_INF\classes`
11. Modify the properties of `license.config`, clearing the "Read Only" tick box.
12. Open `license.config`, with a text editor program such as Notepad and add the following line:

    `key_is_reset=true`

    Save this change.
13. Modify the security permissions of license.config, granting "Read" permission to websdm_app user and "Full" permissions to SYSTEM.
14. Modify the properties of `website.properties`, clearing the "Read Only" check box.
15. Open `website.properties` with a text editor program such as Notepad and look for a line that contains the string `encrypt_pass=`

    If no such line is found, or if it is found but is prefixed by the "#" character, skip to the next step. If the line is found and it is not prefixed by "#", then delete it.

    Change the line that contains "pass=", specifying the value of the WebSDM master account password in clear text. For example, if the password is "mypassword", the line should now be:

    pass=mypassword

    Save these changes.
16. Start the WebSDM service.
17. Log in to WebSDM using a superuser account.
18. If you made changes to `website.properties` above, then do the following:

CONFIDENTIAL ▪ Copyright © 2000–2013, Oracle and/or its affiliates. All rights reserved.

a. Click the **Settings** link, then click the **Set Database Connection** link.

b. Enter the appropriate value in the Password and Confirm Password fields and select the **Encrypt Password** check box.

c. Save these changes.

19. Log out of WebSDM.
20. Stop the WebSDM service.
21. Navigate to `<root>\Lincoln\apps\<instance>\webapps\web_root\WEB_INF\classes`
22. Open `license.config`, with a text editor program such as Notepad and delete the line:

    ```
    key_is_reset=true
    ```

    Save this change.
23. Modify the properties of `license.config`, selecting the **Read Only** check box.
24. Start the WebSDM service.

CONFIDENTIAL ▪ Copyright © 2000–2013, Oracle and/or its affiliates. All rights reserved.

2.1.5 Optional server setup

Optional server settings and software include the following:

- To support WebSDM email notification features, the SMTP mailer must be enabled.
- To provide secure connectivity from outside your corporate firewall, the secure HTTPS port may need to be enabled on the server. If users will always use WebSDM from a VPN account or from within your corporate firewall, this port can remain disabled.
- To change the location of database error messages, edit the `log4j.properties` file. WebSDM writes some database error messages to the location to which **log4j.appender.stdout.Target** points. By default, the location is **System.out**, which is written to Lincoln/apps/websdm/logs/stdout_<date>.log.

2.2 Client Computer Setup

This section covers the following sub-sections:

- Required hardware and software
- Optional computer setup

2.2.1 Required hardware and software

The minimum hardware requirements for each client machine are:

- Windows/Intel Pentium Processor
- 1 GHz processor
- 256 MB of RAM
- 1 GB available disk space (recommended)

Client computers require the following software applications to run WebSDM:

- Operating system: Microsoft® Windows® 7 or Windows XP
- Web browser: Microsoft Internet Explorer version 7.0 or 8.0

Preparatory steps that are required before users access WebSDM from a client computer follow.

CONFIDENTIAL ▪ Copyright © 2000–2013, Oracle and/or its affiliates. All rights reserved.

2.2.1.1 Allowing pop-up windows

Many WebSDM features, including the online help system, rely on pop-up windows to display information. Users who have pop-up blocking software installed or have the blocking feature enabled for Internet Explorer, must allow pop-up windows from the WebSDM site.

2.2.1.2 Enabling interactive DataMontage graphs

DataMontage is a third-party application that is bundled with WebSDM and installed on the server at installation. To enable DataMontage as a full-featured, interactive graphing applet, Java 6 or 7 must be installed on each user computer. Java is available at no cost from www.java.com. If Java is not available on a user's computer, DataMontage graphs can be produced as static JPEG images.

2.2.1.3 Setting other Internet Explorer options

For optimal results, the following settings should be verified for Internet Explorer on each client computer: from the Tools menu, select **Internet Options** and then click the Advanced tab. In the Printing section, "Print background colors and images" should be checked. In the Security section, "Do not save encrypted pages to disk" should be cleared.

2.2.2 Optional computer setup

Additional software applications that are recommended to support optional WebSDM features include:

- SAS Viewer 9.1
- Microsoft Excel
- WinZip
- Adobe Reader
- Base SAS 9.1.3
- PPD® Patient Profiles version 3.0

2.2.2.1 Enabling PPD Patient Profiles

To produce graphical patient profiles, WebSDM provides the option to use PPD Patient Profiles, which is available under separate license from Pharmaceutical Product Development, Inc. (PPD) and installed on individual client computers.

To enable PPD Patient Profiles version 3.0 and assure that the **PPD Patient Profiles** links in WebSDM launch this application correctly, on each client computer you:

- Create or modify the Windows environment variable CGPP_MEM to define the amount of RAM (in MB) used for short-term tasks. The average optimum value is approximately 75% of available RAM.

To set this variable, open the Windows Control panel and double-click System. On the Advanced tab click **Environment Variables**.

- Define a location for temporary files (`*.dat`, `*.dsc`, `*.dsn`, and `*.bin`) created by the application. The CG_SERVER_ TEMPDIR preference specifies a directory location for these files. This directory should be emptied occasionally so that excessive file accumulation does not occur. If you do not define a location for temporary files, WebSDM places the files on your desktop.

For step-by-step instructions, refer to the "Configuring PPD Patient Profiles" topic in the WebSDM help.

Note: For **PPD Patient Profiles** links to appear in WebSDM, the "Enable PPD Patient Profiles" site option must be set for your installation. See *Setting site options* (page 18).

PPD Patient Profiles is a third-party application provided and supported by Pharmaceutical Product Development, Inc. (PPD); further information about PPD Patient Profiles and contact information is available at www.ppdi.com.

2.3 Setup in WebSDM

After WebSDM is installed, you use the WebSDM user interface to:

- Set up database connection information for the WebSDM master account.
- Customize site options for your installation, including how tablespaces will be managed and the level of logging to use for system events.
- Enable standard reports by loading sample data.

During installation a single user account is provided with the username **admin** and a predefined password to allow administrative access to WebSDM. You can use this *"Superuser"* account, or set up a new *Superuser* account, to perform these setup activities in WebSDM. For more information on WebSDM user accounts, see *User Accounts and Security* (page 24).

This section covers the following sub-sections:

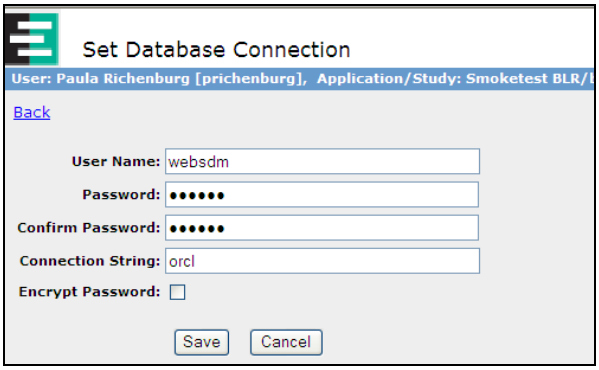
- Setting the database connection for the WebSDM master account
- Setting site options
- Setting up standard reports

CONFIDENTIAL ▪ Copyright © 2000–2013, Oracle and/or its affiliates. All rights reserved.

2.3.1 Setting the database connection for the WebSDM master account

The WebSDM master account is an Oracle account that is created at installation to contain WebSDM support tables. To encrypt the password that is set for the WebSDM master account, or to register a change to the WebSDM master account password in the `website.properties` file, you use a *Superuser* account. Log in to WebSDM as a *Superuser* and update the connection information for the WebSDM master account.

Caution: To reset the database password, you must perform the following **in addition to** using the ALTER USER command in SQLPlus to change the password. If you do not perform both procedures, WebSDM may become unusable.



To set the database connection: Click Settings / Set Database Connection.

Checking the "Encrypt Password" option is required for a secure installation.

After you click **Save**, additional links appear so that you can modify the database connection information or force a new WebSDM login to test the connection.

Note: The information that appears on this page is initially read from, and subsequently written to, the `website.properties` file. You can specify connection information by using this administrative option or by editing the `website.properties` file, which by default is in the following directory: `c:\Lincoln\apps\websdm\webapps\web_root\WEB-INF\classes\`. However, if you selected the Encrypt Password option and you need to register a change to the WebSDM master account password, you must change the password using the Set Database Connection page, rather than editing the `website.properties` file.

2.3.1.1 Configuring website.properties for database connection

The `website.properties` file contains configuration information used by WebSDM to connect to the database, and to perform certain foreground and background processes. You can use a text editor, such as Notepad, to open the file and edit the values for its elements.

 ▪ Copyright © 2000–2013, Oracle and/or its affiliates. All rights reserved.

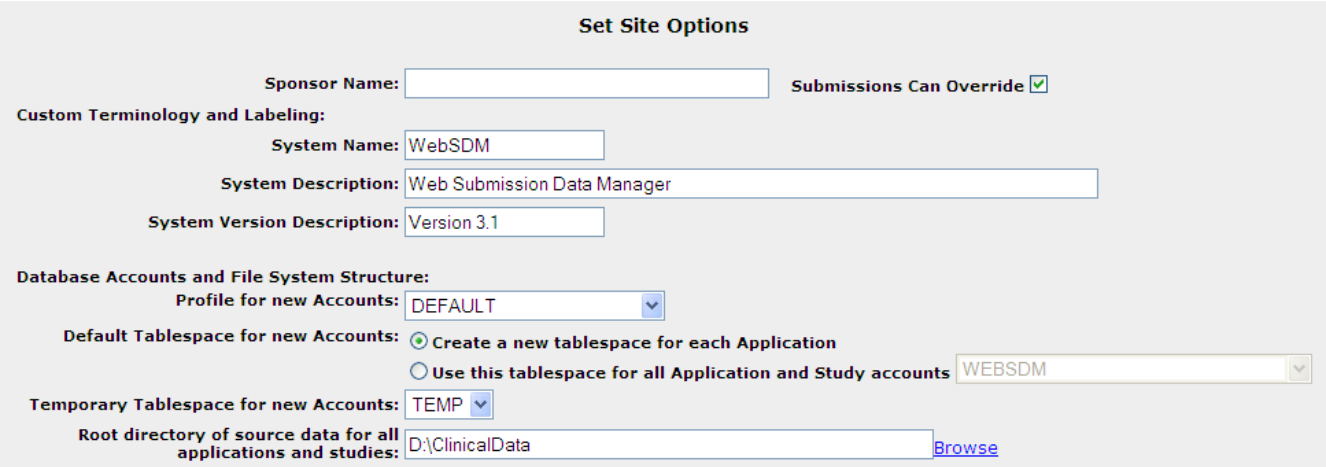
Element	Description

`user`
`pass`
`connect`
	Define the credentials and connection information for WebSDM to log in to the master database account. After installation, the values specified for `user` and `pass` must match the credentials specified in the 2_create_oracle_user.sql script executed during WebSDM installation. The value specified for connect should be jdbc:oracle:oci8:@websdm.

2.3.2 Setting site options

When you install WebSDM, default values are supplied for all of the system-wide WebSDM site options. Typically, you update the WebSDM site options to customize the application immediately after installation.

To update all of the site options, you log in with a *Superuser* account, click **Settings** at the top of any page, and then click **Set Site Options**. (non-superusers with the *Administer Users* permission can also access this page, but can update only the site options for password restrictions.)



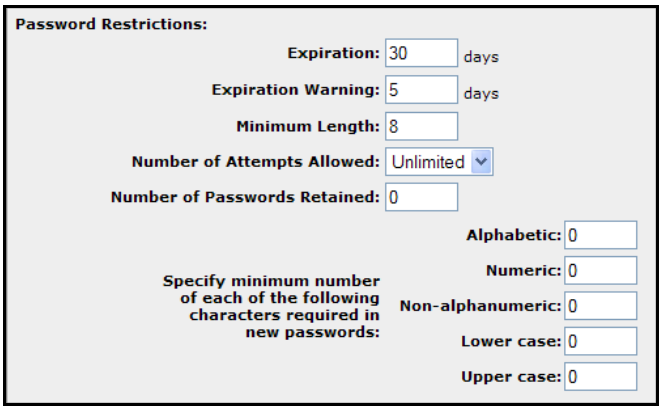
To set site options: Click Settings / Set Site Options.

Site Option	Description
Sponsor Name Submissions Can Override	These options define a default sponsor name for submissions (known as applications in WebSDM), and whether or not users will be able to override that default when registering individual applications. If you will be using studies from multiple sponsors, check "Submissions Can Override". For more information, see *Data Loading* (page 35).
Custom Terminology and Labeling	The options in this section customize information about the WebSDM application that appears in the user interface. • The System Name appears in the title of pop-up windows. • The System Description appears on the Login page, in the title of the main application window, on the Home page, and in the title of pop-up windows. • The System Version Description appears on the Login and Home pages.
Database Accounts and File System Structure	In this section, you select the tablespaces and profile to be assigned to the database accounts that get created for studies. Oracle databases are pre-configured with a profile named DEFAULT. If your database has additional profiles defined, you should choose the one that is best suited for use by the database accounts that get created when applications and studies are registered. Guidelines for profiles to be assigned to WebSDM study accounts are in Appendix A. The setting for Default Tablespace determines whether a single, common tablespace is used for all study-specific database accounts or a distinct tablespace is used for each application's study accounts. The option to "Create a new tablespace for each Application" is recommended. If you want to "Create a new tablespace for each Application", you should: • Verify that the WebSDM master account has been

CONFIDENTIAL ▪ Copyright © 2000–2013, Oracle and/or its affiliates. All rights reserved.

Site Option	Description
	granted the CREATE TABLESPACE and DELETE TABLESPACE database privileges. (These privileges are granted at installation by the `2_create_oracle_user.sql` script. If those permissions are not granted to the WebSDM master account, the "Create a new tablespace for each Application" option is disabled.) • Consult a database administrator to verify that the `website.properties` file contains appropriate definitions for the `tablespace_datafileSpec` and `tablespace_options` elements. (By default, this file is in the `c:\Lincoln\apps\websdm\webapps\web_root\WEB-INF\classes\` directory.) You also specify a root directory on the server for the clinical trial data and metadata of all applications and studies. Users registering applications and studies can browse within the specified directory only. For more information, see *Data Loading* (page 35).

The next section of the Site Options page defines password restrictions which, when saved, apply to all newly created WebSDM user accounts. Typically, minimum password requirements are defined at installation to comply with organizational security requirements and are updated only as needed.

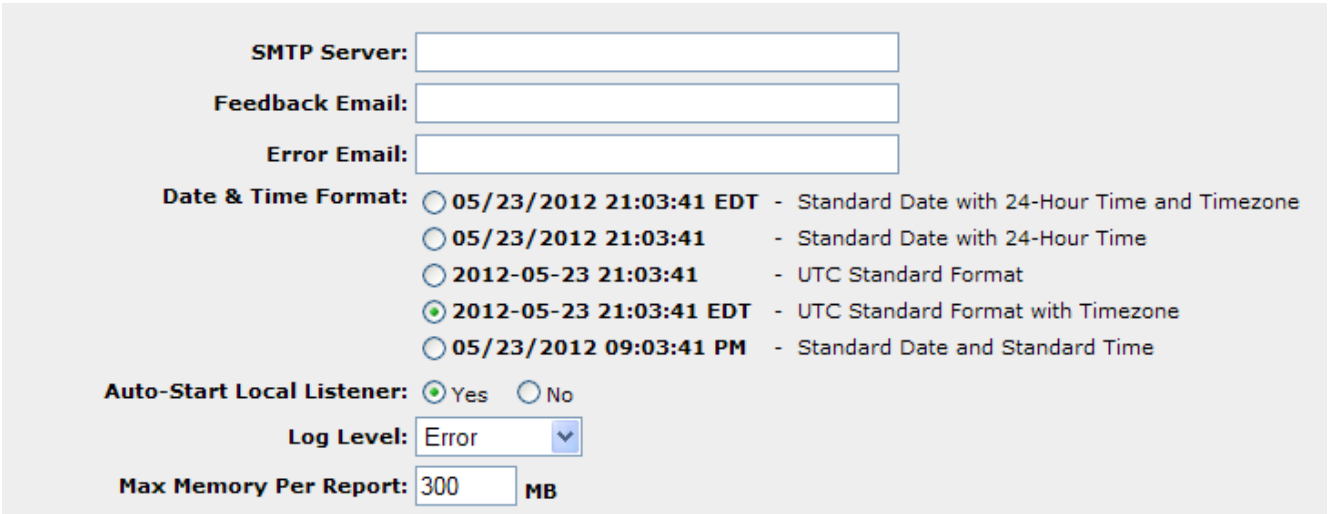


To set site options: Click Settings / Set Site Options.

CONFIDENTIAL ▪ Copyright © 2000–2013, Oracle and/or its affiliates. All rights reserved.

Site Option	Description
Expiration Expiration Warning	These options define the length of time in days that a password will be valid (the default is 0 to indicate no expiration), and the number of days prior to expiration to provide a warning at login that the password is about to expire.
Minimum Length	This option defines the minimum password length. You can specify a maximum of 64 characters. The default is 8.
Number of Attempts Allowed	This option specifies the number of password attempts allowed at login prior to automated disabling of the account. The default is Unlimited. See *Disabling and enabling user accounts* (page 33) for information on re-enabling accounts.
Number of Passwords Retained	This option defines the number of passwords to retain for each user. New passwords are required to be unique within this set. The default is 0.
Alphabetic Numeric Non-alphanumeric Lower case Upper case	These options specify minimum requirements for the inclusion of upper and lower case letters, numbers, and special characters in the password string. For each of these fields, the default is 0 to indicate that no minimum of that type is required.

On the next part of the Site Options page you define the following:



To set site options: Click Settings / Set Site Options.

CONFIDENTIAL ▪ Copyright © 2000–2013, Oracle and/or its affiliates. All rights reserved.

Site Option	Description
SMTP Server Feedback Email Error Email	These options specify the SMTP server address and the email addresses for feedback and issue reporting. The default value for Feedback Email and Error Email is **websdm_bugs@phaseforward.com**. To enable automated email notifications to new users when user accounts are created, the SMTP server must be defined before user accounts are set up. See *Creating a user account* (page 31).
Date & Time Format	These options allow you to select a preferred format for presenting dates and times.
Auto-Start Local Listener	This option defines whether a listener process should start automatically (if stopped) when a loading and checking run is submitted. The recommended setting is "Yes" to ensure that loading and checking runs initiated after a system reboot will run. For more information, see *System Tuning and Monitoring* (page 49).
Log Level	With this option, you specify the level of logging to use for system events. The recommended level is "Error".
Max Memory Per Report	Define the maximum amount (MB) of memory that a single report is allowed to use when executing. Typically set to a value that is no larger than 768 MB. Before changing this option, you may want to consult with Oracle. For more information, see *System Tuning and Monitoring* (page 49).

In addition, certain system features can be enabled or disabled for all WebSDM users. Of these features, only those that provide options for listing subjects and subject-level detail within a study, called "second-level drilldown" in WebSDM, should generally be enabled by a system administrator.

These features are:

Site Option	Description
Allow Subject Comment/Review/ Exclusion	Check to include a section for recording reviewer input when users access subject details from the Subject Lists tab; clear to prevent this section from appearing.

CONFIDENTIAL ▪ Copyright © 2000–2013, Oracle and/or its affiliates. All rights reserved.

Site Option	Description
Enable PPD Patient Profiles	Check to provide the option to view PPD Patient Profiles graphs of subject data; clear to prevent this option from displaying. This feature also requires the purchase and installation of a third-party software application on each client machine. See *Enabling PPD Patient Profiles* (page 15).
Enable Second Level Drilldown on Subjects Page	Check to provide hyperlinked subject IDs to show subject details in a separate window when a subject list appears in WebSDM; clear to provide hyperlinks only on the Subject Lists tab or in a report. The recommended setting is checked.
Enable Download Subject Details	Check to provide a **Download** link on pages in which subject details appear in a separate browser window. If cleared, no option to download subject details is offered.

Checkboxes for other settings in this section of the Site Options page are applicable in certain situations only, and should be cleared on most systems unless otherwise directed by Oracle.

2.3.3 Setting up standard reports

To enable the standard report definitions that are delivered with WebSDM, you must install sample data that is provided on the installation CD and the MedDRA version 11.0 account. In WebSDM, you register the LTI application and then load and check its SAMP1_312 study. This study uses the SDTM 3.1.2 standard and its data is coded to MedDRA 11.0. You must obtain MedDRA files from the MSSO by subscription.

Optionally, you can also load and check these studies in the LTI application:

- SAMP1 uses the SDTM 3.1 standard
- SAMP1_311 uses the SDTM 3.1.1 standard

Only the SAMP1_312 study is required to enable the standard reports.

For more information on registering and then loading and checking data see *Data Loading* (page 35).

2.4 Installing MedDRA Versions

You will need to install each version of MedDRA used by the studies that you plan to load into WebSDM. In addition, even if your own studies do not use MedDRA version 11.0, you will need to install version 11.0 since it is used by the LTI sample study. For instructions, see the Setting Up MedDRA Accounts section in the *WebSDM/Empirica Study Windows 2003/2008 Server Installation Instructions*.

CONFIDENTIAL ▪ Copyright © 2000–2013, Oracle and/or its affiliates. All rights reserved.

3 User Accounts and Security

The different types of WebSDM users can be categorized as follows:

- Clinical data reviewers browse, query, and review clinical data.
- Data managers load clinical data and check it for compliance with the CDISC SDTM standard.
- Administrators manage user access and provide application support.
- *Superusers* perform system monitoring, configuration, and administrative activities.

Initially, Oracle provides a single default user account for WebSDM with *Superuser* privileges. This account has the username **admin** and a predefined password. This user account should be edited to provide an email address for the system administrator. See *Editing user accounts* (page 32).

For compliance with US FDA 21 CFR Part 11, each WebSDM user must log in with a unique username and password. When you set up each new username in WebSDM:

- You control access to data objects (that is, to the studies and study pools within applications) by assigning the username to a login group. Once created, data objects can be published to one or more login groups. At least one login group should be created before you set up usernames. See *Setting Up Login Groups* (page 25).
- You control access to WebSDM options and features by assigning permissions to the username.

This section provides information on how to set up login groups, the permissions that you can assign, how to define sets of permissions called user roles, and how to manage user accounts.

Additional options for security can also be set for your installation:

- Minimum requirements for password structure can be specified using WebSDM. See *Setting site options* (page 18).
- A timeout period for inactive user sessions can be set on the WebSDM server. See *Setting the session timeout period* (page 9).

This chapter covers the following sections:

- Setting Up Login Groups
- Setting User Permissions
- Setting Up User Roles
- Managing User Accounts

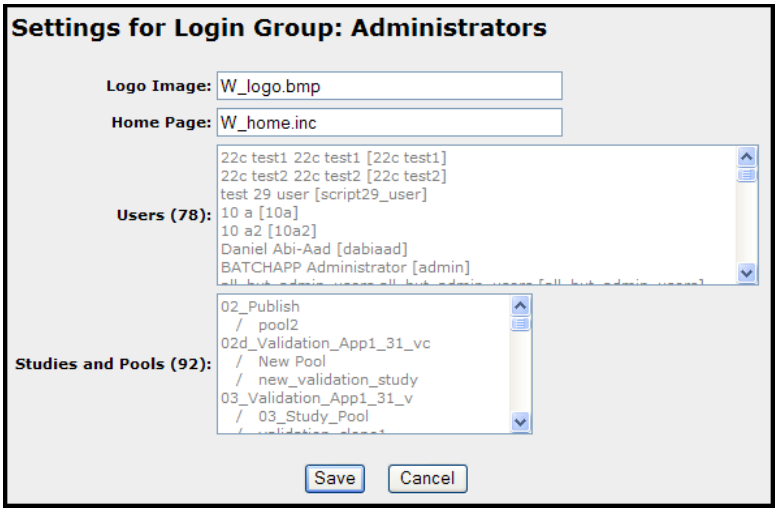
CONFIDENTIAL ▪ Copyright © 2000–2013, Oracle and/or its affiliates. All rights reserved.

3.1 Setting Up Login Groups

In WebSDM, login groups perform two separate functions: they control user access to data, and they allow customization of the WebSDM home page and logo.

All of the users at an installation can belong to the same login group, or users who are working on different submissions or studies can be assigned to different groups. At installation, WebSDM provides one predefined or standard login group named **Administrators** that contains the single initial user account **admin**. Before setting up user accounts at least one additional login group should be created.

A user with the *Administer Users* permission can set up a login group, assign users to the group, and specify the logo and home page to display when users in that group log in to WebSDM.



To define settings for a login group: Click Settings / Edit Login Group. Then click Create New Login Group or Edit.

3.1.1 Controlling access to data

To control access to data, studies and study pools can be "published" individually to different login groups. When a study is published, only users in the specified login group(s) are given access to the data. See *Publishing studies with "Completed" runs* (page 44).

Access to other WebSDM objects, including subject lists, report definitions, and report outputs, is also controlled through a similar publication mechanism.

CONFIDENTIAL ▪ Copyright © 2000–2013, Oracle and/or its affiliates. All rights reserved.

3.1.2 Customizing WebSDM

For each login group a different logo image and html file for the WebSDM "Home" page can be specified:

- Each image file that you intend to use as a logo must be located in the `C:\Lincoln\apps\websdm\webapps\web-root\image` directory. By default, the `E_logo.gif` file (the Empirica logo) is used as the logo for the Administrators login group. You can replace this default with your own company logo, or any other image, in the login groups you create. Image files must be in .bmp or .gif format and appropriately sized: WebSDM displays the logo in a 150 x 100 pixel space, and the image will be forced to fit.

(The screenshots in this document show `E_logo.gif`, the logo for Empirica products.)

- Each web page file that you intend to use as a custom home page must be located in the `C:\Lincoln\apps\websdm\webapps\web-root\customhomes` directory. Such pages should provide html appropriate for embedding within a pair of `<body>…</body>` tags, and can contain text, images, links to a company intranet or external web site, and so on. The default home page, `W_home.inc`, is appropriate for WebSDM installations.

Note: If the default paths for WebSDM files were changed during installation, these files may be located in a different directory path.

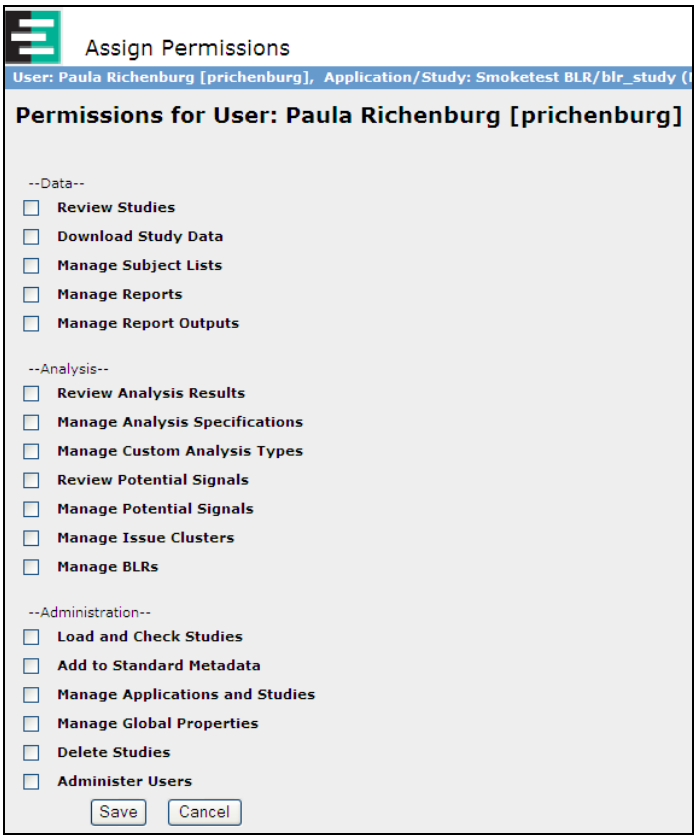
3.2 Setting User Permissions

WebSDM controls access to its options and features with permissions. As a security measure, a user can only access a WebSDM option or feature after the associated permission is assigned to that user's account.

When you create or edit user accounts, permissions can be assigned individually or through a user role.

CONFIDENTIAL ▪ Copyright © 2000–2013, Oracle and/or its affiliates. All rights reserved.

A user with the *Administer Users* permission can assign individual permissions to users.



To assign permissions: Click Settings / Edit Users. Click for a user, select Edit, and click Assign Permissions.

Note: WebSDM *Superusers* can perform all WebSDM functions and access system administration features and options that are not provided by permissions. Only those users who need to perform system administration functions should be assigned the *Superuser* attribute. Typically, only one or two *Superusers* are identified per installation.

3.2.1 Permissions for working with data

Permission	Allows the user to:
Review Studies	View all information about studies that can be accessed from the Domains tab. View subject lists, report definitions, and report outputs that have been published to the user's login group. (This permission is necessary for most users: it provides a minimum level of system access.)

 ▪ Copyright © 2000–2013, Oracle and/or its affiliates. All rights reserved.

Permission	Allows the user to:
Download Study Data	Download all clinical data for a study domain from the Clinical Data page, which is accessed from the Domains tab. Download report output after running a report definition or viewing a previously saved output.
Manage Subject Lists	Create, copy, rename, and delete subject lists, edit subject lists and publish them to others.
Manage Reports	Create, edit, and copy report definitions, and distribute the XML of a report definition by email.
Manage Report Outputs	Save the results of running a report definition as report output, edit the attributes of report outputs, and publish or delete saved outputs.

3.2.2 Permissions for administration

Permission	Allows the user to:
Load and Check Studies	Initiate the loading and checking of study data, and view the status of these processes on the Run History tab.
Add to Standard Metadata	Load and edit customer-defined rules and error messages for checking study data.
Manage Applications and Studies	On the Setup tab, register, edit, and update properties for applications, studies, and study pools, and publish studies and study pools to login groups. A study or study pool can be deleted by the user who registered it, a user with the *Delete Studies* permission, or a *Superuser*. An application can be deleted only by a *Superuser*.
Manage Global Properties	Create and manage event lists and define test identifiers system-wide, in addition or as an alternative to managing these properties at the individual application or study level.
Delete Studies	Delete studies and study pools. The user who registered a study or study pool can delete that object without explicitly having this permission.
Administer Users	Create and edit users, login groups, and roles. Set site options related to user passwords.

CONFIDENTIAL ▪ Copyright © 2000–2013, Oracle and/or its affiliates. All rights reserved.

Permission	Allows the user to:
	View the User Activity Audit Trail and list of currently logged in users. Send messages to users.

3.3 Setting Up User Roles

In WebSDM, roles are collections of user permissions that have been selected and grouped under an identifying name. As a result, defining one or more user roles can streamline the process of setting up new users.

WebSDM supplies the following built-in roles (individual permissions are described in the *Setting User Permissions* section above):

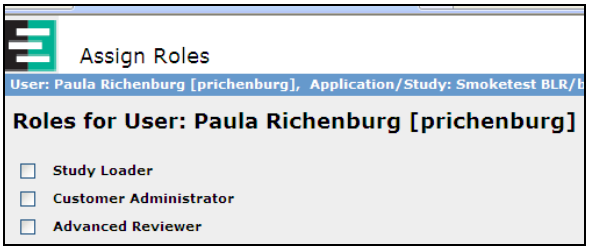
Role	Description	Permissions Assigned
Reviewer	Offers a basic level of data access.	*Review Studies* *Download Study Data* *Manage Subject Lists* *Manage Reports* *Manage Report Outputs*
Advanced Reviewer	Offers the data access of the Reviewer role, plus additional capabilities.	*Review Studies* *Download Study Data* *Manage Subject Lists* *Manage Reports* *Manage Report Outputs* *Manage Applications and Studies* *Manage Global Properties* *Manage Advanced Application and Study Properties*
Study Loader	Provides administrative capabilities for data loading, and also offers minimal data review access.	*Review Studies* *Download Study Data* *Load and Check Studies* *Manage Applications and Studies* *Manage Global Properties* *Delete Studies*

CONFIDENTIAL ▪ Copyright © 2000–2013, Oracle and/or its affiliates. All rights reserved.

Role	Description	Permissions Assigned
Customer Administrator	Assigns all permissions to a user, providing access to user management and data review features and administrative capabilities for data loading.	*Review Studies* *Download Study Data* *Manage Subject Lists* *Manage Reports* *Manage Report Outputs* *Load and Check Studies* *Manage Applications and Studies* *Manage Global Properties* *Delete Studies* *Administer Users*

A user with the *Administer Users* permission can modify these built-in roles and define additional roles for your installation as needed. To create, edit, or delete roles click **Settings** then **Edit Roles**.

A user with the *Administer Users* permission can also assign roles to users as needed.



To assign roles: Click Settings / Edit Users. Click for a user, select Edit, and click Assign Roles.

Note: Additional roles may be supplied for installations with Empirica Study features.

3.4 Managing User Accounts

WebSDM users with the *Administer Users* permission can create, edit, enable or disable, and delete user accounts. To review a list of all current WebSDM user accounts click **Settings** then **Edit Users**.

For information on the permissions that can be assigned to user accounts, see *Setting User Permissions* (page 26).

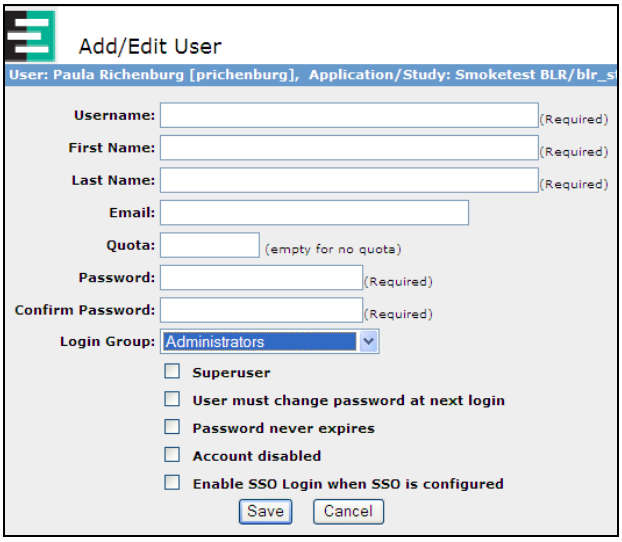
If you are implementing Single Sign-On, you must contact Oracle for assistance in creating user accounts in Oracle Access Manager (OAM). For more information, see the *Configuring Single Sign-On for WebSDM/Empirica Study* topic in the WebSDM/Empirica Study Help.

Note: In WebSDM, *Superusers* can perform all WebSDM functions and access system administration features and options that are not linked to permissions. Only those users who need to perform system administration functions should be assigned the *Superuser* attribute. Typically, only one or two *Superusers* are identified per installation.

3.4.1 Creating a user account

To create user accounts in WebSDM, a user must have the *Administer Users* permission. Before creating a user account, the following information should be available:

- The username to assign.
- The user's first name, last name, and (optional) email address. The user's email address is used to notify the user when the account is created, for notifications that loading and checking runs are complete, and for messages sent to all WebSDM users.
- The password restrictions defined for your installation (minimum length, character types, and so on) as site options. See *Setting site options* (page 18).
- The user's login group, which determines the study data that can be accessed. See *Setting Up Login Groups* (page 25).
- The permissions or user role(s) the user will require. See *Setting User Permissions* and *Setting Up User Roles* (page 29).

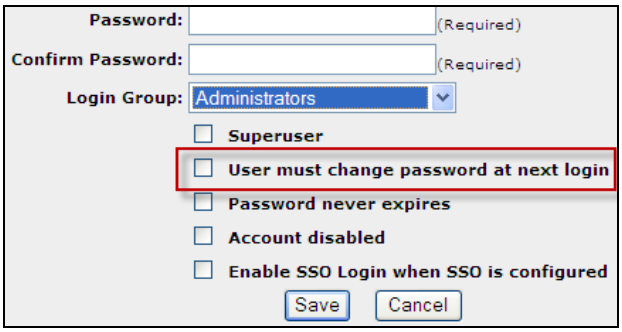


To add a user: Click Settings / Edit Users. Then click Add a New User.

The Quota field is reserved for future use.

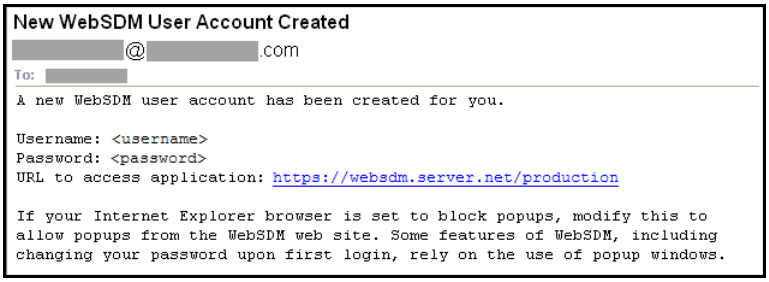
CONFIDENTIAL ▪ Copyright © 2000–2013, Oracle and/or its affiliates. All rights reserved.

If your standard operating procedures require users to change an assigned password when they log in to a new user account, check the "User must change password at next login" option each time you create an account, and make sure that pop-up blocking software installed on users' computers has been modified to allow pop-up windows for your WebSDM URL.



To require a password change: Click Settings /Edit Users . Click Add a New User or click for a user and select Edit.

When you click **Save**, WebSDM automatically generates an email message that is sent to the address defined for this new user:



After you click **Save**, additional links appear at the bottom of this page. To assign the role(s) or individual permissions that will provide access to the functions that the user will perform in WebSDM, you click:

- **Assign Roles**
- **Assign Permissions**

For more information, see *Setting Up User Roles* (page 29) and *Setting User Permissions* (page 26).

3.4.2 Editing user accounts

To edit user accounts, a WebSDM user must have the *Administer Users* permission, or be a superuser. Updates can be made to a user's:

- First and last names
- Email address

 ▪ Copyright © 2000–2013, Oracle and/or its affiliates. All rights reserved.

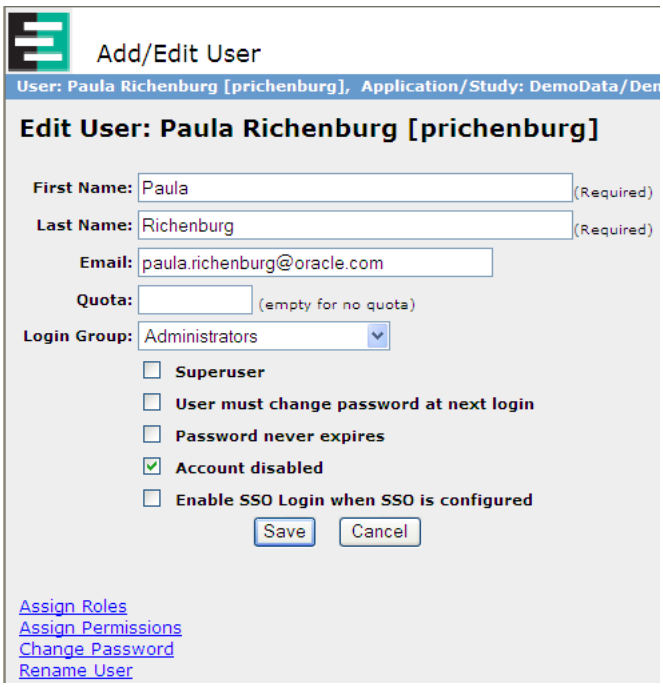
- Login group
- Account status (enabled or disabled)
- Roles
- Permissions
- Password
- Username

You can change the username by renaming the user. For more information on renaming users, see the *Renaming a User* topic in the WebSDM Help.

3.4.3 Disabling and enabling user accounts

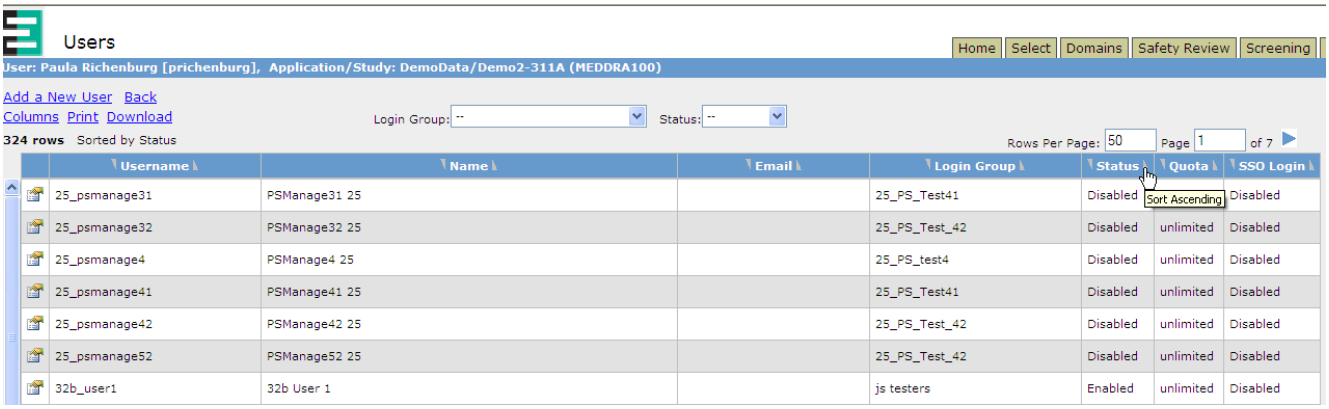
User access to WebSDM can be disabled manually by a user with the *Administer Users* permission. It can be disabled automatically after expiration or after a user's repeated attempts to enter a password in excess of the permitted number of attempts.

You edit user accounts individually to enable a disabled account or manually disable an account.



To disable or enable a user account: Click Settings / Edit Users. Then click for a user and select Edit.

The status of each user account displays in the Status column of the table of user accounts that appears when you click **Settings** then **Edit Users**.



To identify disabled user accounts: Click Settings / Edit Users. Then click the up arrow in the Status column heading.

3.4.4 Deleting user accounts

User accounts can be deleted by a user with the *Administer Users* permission. This procedure is recommended only when a user account has never been used to log in to WebSDM or perform any WebSDM tasks. To prevent access to WebSDM, an account can be disabled instead of deleted. See *Disabling and enabling user accounts* (page 33).

To delete a user account, click **Settings** and then **Edit Users** . Then click  for the user and select **Delete**. The user who deletes the account becomes the owner of any applications, studies, loading and checking runs, subject lists, report definitions, or report outputs that were originally created by the deleted user account. As a result, it is recommended that the user who is deleting the account be in the same login group as the user who is being deleted, as this will allow uninterrupted access to published objects by other users in the group.

If the deleted user is currently logged in, that user can continue working; however, once the user logs out, the user will not be able to log in again.

After a user account is deleted, it cannot be used to log in to WebSDM. However, the username continues to appear on the User Activity Audit Trail with "(deleted)" appended to it. See *Auditing user activity* (page 48).

You can add a new user account with the same username and other information as a previously deleted account.

CONFIDENTIAL ▪ Copyright © 2000–2013, Oracle and/or its affiliates. All rights reserved.

4 Data Loading

SDTM-formatted study data may be loaded into WebSDM and Empirica Study from SAS v5 transport files, or from tables or views in an Oracle database. Loading study data from an external database source – either Oracle Health Sciences InForm or Oracle Life Sciences Data Hub – requires establishing a database link. See the Appendices in *WebSDM/Empirica Study Windows 2003/2008 Server Installation Instructions* (the `WebSDM_Windows_Installation_Instructions.pdf` file provided on the installation media) or contact Oracle for further details on loading study data stored in an Oracle database.

To prepare for loading studies stored as SAS `.xpt` transport files, you set up server directories for the SDTM source data. You then copy study data files to the directories you have set up on the application server and use WebSDM to load the data by:

- Registering an application
- Registering the studies in the application
- Setting up a loading and checking run for the studies

This chapter covers the following sections:

- Data Directory Setup
- Registering Applications and Studies
- Loading and Checking Data
- Deleting Applications

4.1 Data Directory Setup

At installation, files for the WebSDM application are installed by default to the `C:\Lincoln\apps\websdm` directory. Data for submissions, or "applications" as they are called in WebSDM, and their component studies can be stored either on the same drive as the WebSDM application files or on a different drive. A local drive other than `C:\` is recommended.

Typically, sites designate a single directory (such as the `submissions` directory in the examples that follow) that will contain all application and study directories and files for use in WebSDM. Within WebSDM, the location of this root directory should be specified as a site option before you register applications. When you specify the root directory, users with the *Manage Applications and Studies* permission can browse within, but not above, the defined directory and its subdirectories. Application or study data stored in any other directory on the server cannot be loaded into WebSDM. See *Setting site options* (page 18).

Some restrictions apply to the selection of a root directory:

- The root directory for submissions should *not* be the same as or under the working directory. (The working directory is parent to the `procs` folder identified by `process_dir` in website.properties, section 2.1.3.3 above). So, for example, if `process_dir=D:\websdm\procs` and the working directory location is `D:\websdm`, then an appropriate location for the root directory would be a different folder on `D:` such as `D:\ClinicalData`.

- If the `C:\` drive must be used for storing clinical data (for example, if the server is not partitioned into multiple drives), then the root directory for submissions should *not* be located beneath the `C:\Lincoln` directory.

When users "register" an application in WebSDM, all of the studies for that application can also be registered automatically if the application and its study data use a directory structure that conforms to the FDA's 1999 electronic New Drug Application (eNDA) standard or to the International Conference on Harmonisation's electronic Common Technical Document (eCTD) specification. Examples of each of these directory structures follow.

4.1.1 eNDA standard

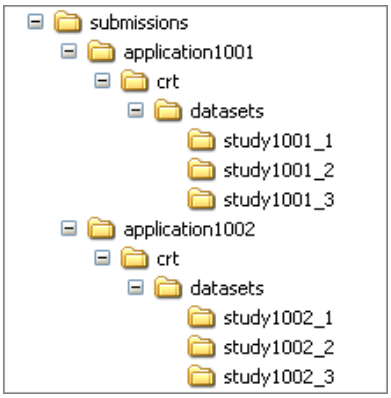
The eNDA standard directory structure is:

```
\<application name>
    \crt
        \datasets
            \<study name 1>
            \<study name 2>
```

Each `<study name n>` folder must contain the SAS transport files (`.xpt` files) for the clinical trial data, and may also contain a `define.xml` file. The `define.xml` file defines standard metadata models for case report tabulation and analysis data.

To use WebSDM's **Generate Metadata** feature that allows you to generate a new `define.xml` file, the `<study name n>` folder must be writeable.

For example:



4.1.2 eCTD specification

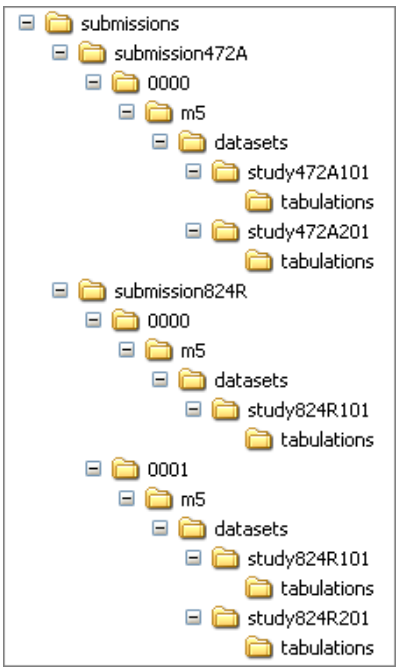
The eCTD directory structure specification is:

```
\<application name>
    \<nnnn submission number>
        \m5
            \datasets
                \<study name 1>
                    \tabulations
                \<study name 2>
                    \tabulations
```

Each `<nnnn submission number>` folder name is a unique, four-digit identifying number for the application: the name of the folder for the initial submission should be `0000`, the next submission should be `0001` folder, and so on. The `tabulations` folder must contain the SAS transport files for the clinical trial data and can also contain a `define.xml` file.

CONFIDENTIAL ▪ Copyright © 2000–2013, Oracle and/or its affiliates. All rights reserved.

For example:



To use WebSDM's **Generate Metadata** feature that allows you to generate a new `define.xml` file, the `tabulations` folder must be writeable.

4.2 Registering Applications and Studies

An application in WebSDM is used to group a set of related studies. For example, an application might consist of the set of studies that will be submitted together to a regulatory agency in support of a New Drug Application. An application contains data and metadata for one or more studies, which could be different studies or multiple versions of the same study.

Before you register an application or study, you:

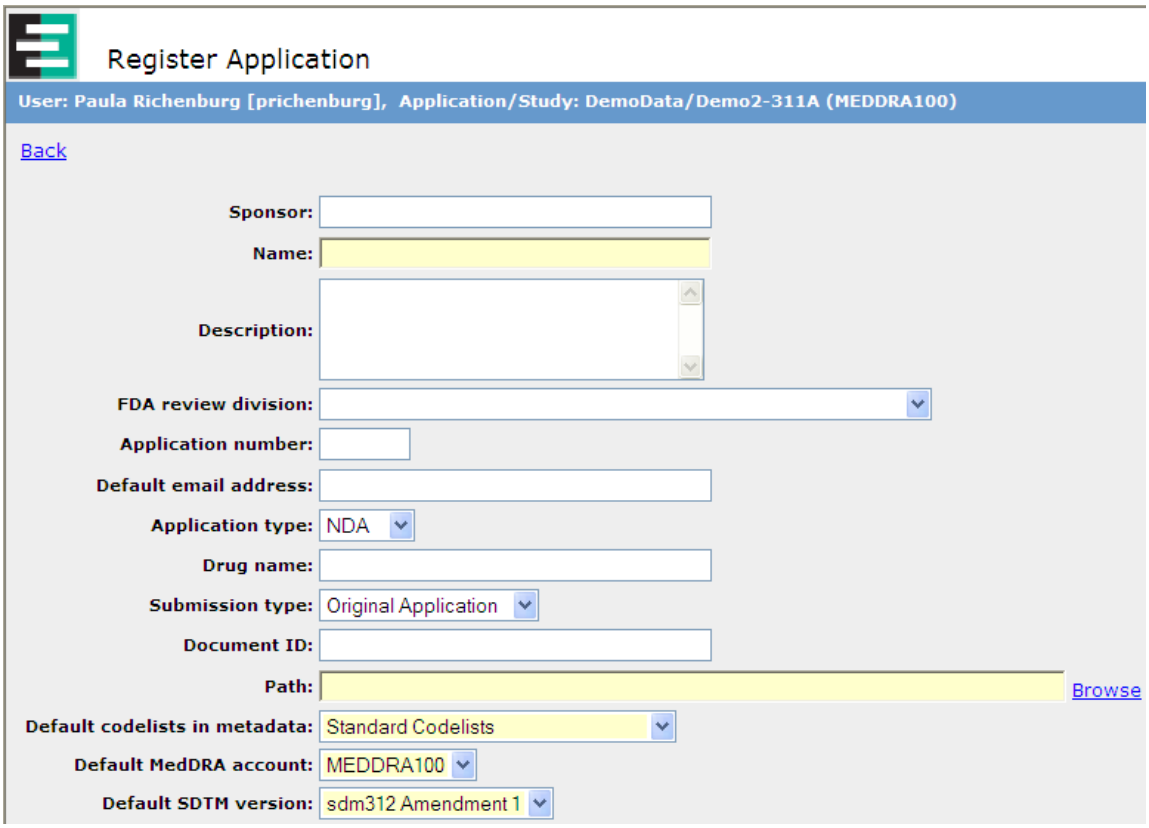
- Set up data directories on the server (required only for studies whose data source type is SAS transport files).
- Identify which CDISC SDTM version the data uses.
- Identify which version(s) of the MedDRA coding thesaurus the data uses, and verify that those version(s) are installed on the WebSDM server. See *Installing MedDRA Versions* (page 23).

  To check which MedDRA versions are currently installed from within WebSDM, on the Setup tab click **Applications** then **Register Application**. The page that appears includes a Default MedDRA account drop-down list with every currently accessible MedDRA account.
- Determine whether a `define.xml` file is available for each study.

 ▪ Copyright © 2000–2013, Oracle and/or its affiliates. All rights reserved.

4.2.1 Registering an application

Registering an application in WebSDM identifies the location of the directories that contain the source files for the studies in that application. Users with the *Manage Applications and Studies* permission can register an application.



To register an application: On the Setup tab, click Applications. Then click Register Application.

The registration process collects descriptive data for the application, including an identifying name and description for use within WebSDM, the submission type, and so on. In the Path field, you specify the location of the application's source data.

You also specify the following to be used by default for the application's studies.

- Default codelists in metadata: Indicates the default rule governing how codelists will be assembled for system-generated `define.xml` files.
- Default MedDRA account: The name of the Oracle account that contains the version of MedDRA to use by default for each study.
- Default SDTM version: The version of CDISC SDTM to associate by default with the application's studies.

The default values supplied for the application can be overridden for individual studies as needed.

CONFIDENTIAL ▪ Copyright © 2000–2013, Oracle and/or its affiliates. All rights reserved.

A WebSDM site option controls whether or not a new Oracle tablespace is created for each application, or a single, specified tablespace is used for all applications. For more information, see *Setting site options* (page 18).

4.2.2 Automated study registration

After you supply all information to register an application and click **OK**, WebSDM analyzes the directory tree structure found in the supplied path. If the directory structure follows the eNDA standard or eCTD specification, an Auto-Register studies page appears to present these options for registering each study found:

- Defer study registration.
- Use the `define.xml` file for study metadata if found in the directory (if more than one is supplied for a study, you can select any one of them).
- Generate a `define.xml` metadata file using SDTM standard codelists for variables that are subject to CDISC controlled terminology.
- Generate a `define.xml` metadata file using SDTM standard codelists for variables that are subject to CDISC controlled terminology and data-driven codelists for variables that are subject to sponsor-defined controlled terminology.

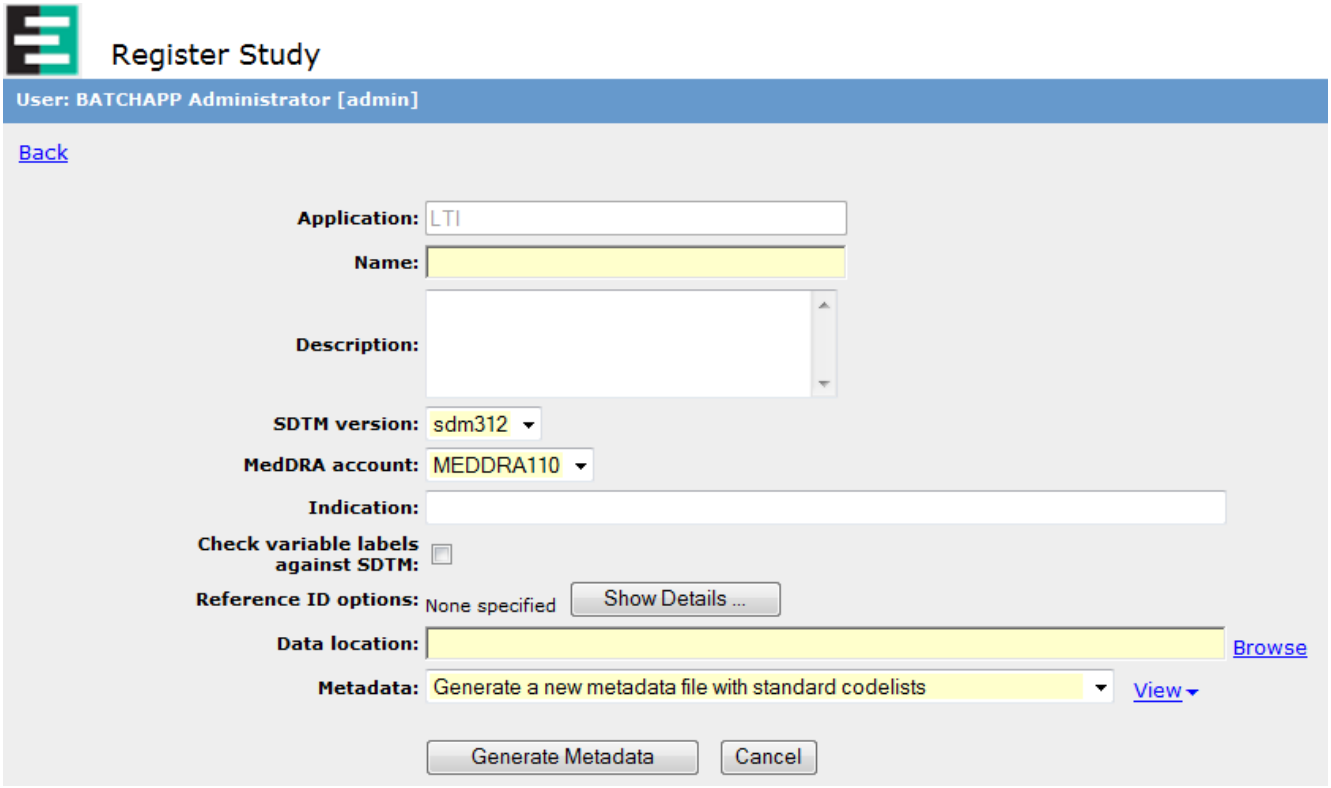
As a result, you can automatically register the application's studies even if `define.xml` files are not present to supply study metadata.

4.2.3 Manual study registration

You also have the alternative in WebSDM to register studies manually at another time. You can register a study manually if you want to defer study registration, if the directory structure does not comply with a standard format, or if you want to add a new study to an existing application.

When manually registering a study based on an Oracle data source type – Oracle Health Sciences InForm or Oracle Life Sciences Data Hub – you can create the study directory from within WebSDM. A study directory is required to hold metadata, even if the study's clinical data comes from an Oracle database source.

CONFIDENTIAL ▪ Copyright © 2000–2013, Oracle and/or its affiliates. All rights reserved.



To register a study: On the Setup tab, click Studies / Pools. Then click Register Study.

For more information on setting up directories for WebSDM source data, see *Data Directory Setup* (page 36).

4.2.4 Naming split domain and supplemental files

For study data that complies with the SDTM version 3.1.2 or 3.1.3 standard, data comprising a single domain can be loaded into WebSDM from multiple `.xpt` files, referred to as a "split domain." The recommended naming convention for such split domain files is `xxnn`, where `xx` represents the abbreviated name of the data domain and `nn` represents a two-character alphanumeric suffix.

The SDTM version 3.1.2 and 3.1.3 standards also allow data to be loaded from supplemental data files. The recommended naming convention for supplemental data files is `SUPPxx`, where `xx` represents the abbreviated domain name that requires the supplemental data. Supplemental files can also be split; if split, the files should be named using the format `SUPPxxnn`, where `nn` represents a two-character alphanumeric suffix.

 ▪ Copyright © 2000–2013, Oracle and/or its affiliates. All rights reserved.

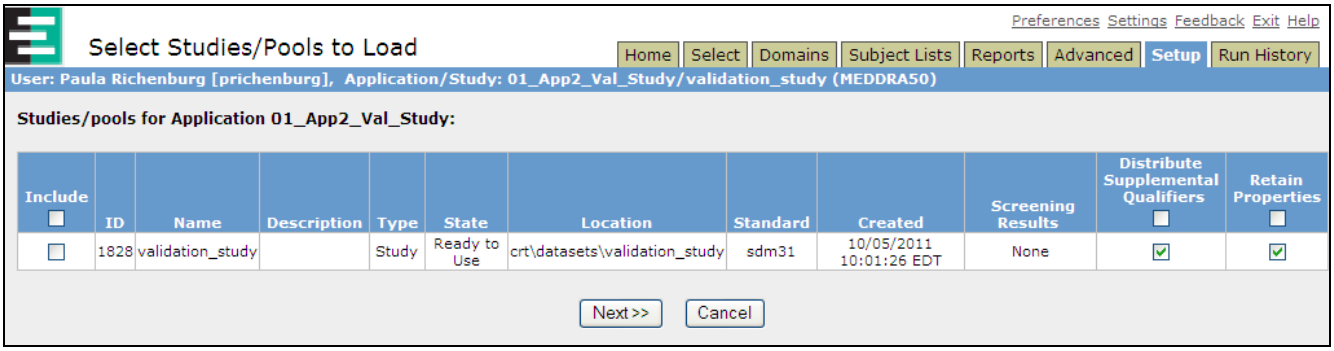
For example, adverse event data that is supplied by a set of two `.xpt` files and two supplemental files should have names such as the following:

```
AE01.xpt
AE02.xpt
SUPPAE01.xpt
SUPPAE02.xpt
```

4.3 Loading and Checking Data

After studies (or study pools) are registered, a user with the *Load and Check Studies* permission can initiate a loading and checking run. This batch process:

- **Loads data**: The loading process uses metadata from the `define.xml` file to load clinical data from the SAS transport (`.xpt`) files in the study's path into the WebSDM database. This process transforms ISO standard dates into true Oracle datetime format and derives other variables as well.
- **Checks data**: WebSDM applies a set of standard checks to the data to determine compliance with the version of the CDISC SDTM indicated in the study's associated `define.xml` file. The standard checks augmented by any supplemental rules optionally defined by users with the *Add to Standard Metadata* permission. If the study data does not meet the condition specified by a standard or supplemental check, WebSDM generates an error message.



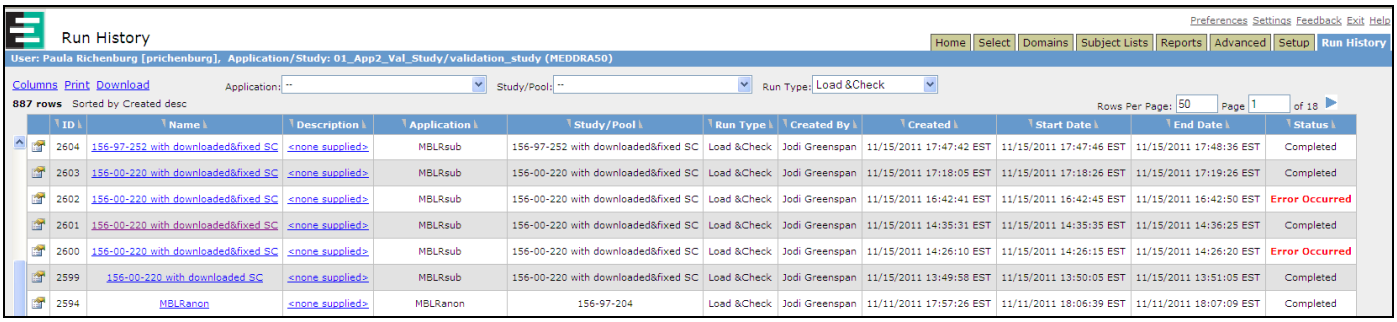
To load and check an application's studies: On the Setup tab, click Applications. Then click for an application and select Load.

The loading and checking process runs in the background as a batch job, and can optionally generate an email message to notify the initiating user when the job is complete. The current status of a study's loading and checking process, from **Not Loaded** to **Ready to Use**, can be monitored. To review the State value of studies in an application, on the Setup tab click **Studies / Pools**.

CONFIDENTIAL ▪ Copyright © 2000–2013, Oracle and/or its affiliates. All rights reserved.

4.3.1 Reviewing load status

After a user submits a loading and checking run, the run appears in the table presented by the Run History tab. The status for the run is blank while the run is in progress, and then it is updated automatically to **Error Occurred** or **Completed**.

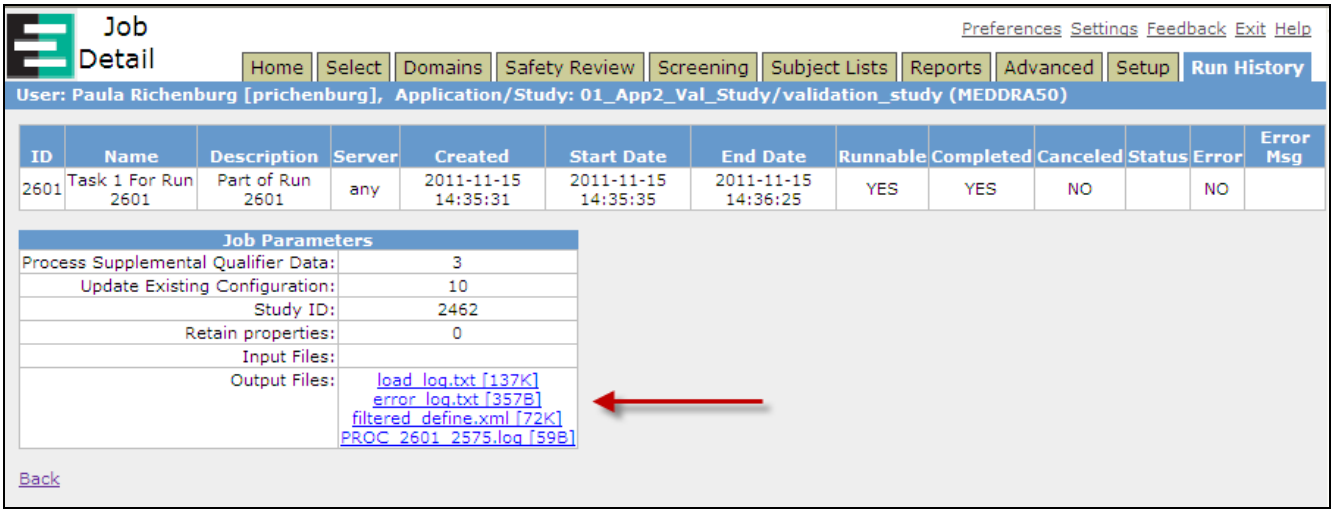


To review a load and check run: Click the Run History tab.

Users can also cancel a run that is in progress by clicking for the run and selecting **Cancel**. These runs appear with a status of **Cancelled**.

4.3.2 Working with "Error Occurred" runs

A loading and checking run fails (Error Occurred status) if the required SAS transport (`.xpt`) files are missing or faulty, or if the `define.xml` file is badly constructed. The `error_log.txt` file lists the error that caused the run to fail.



To review a failed run: On the Run History tab, click <run name>. Then click <job name> and error_log.txt.

To resolve load problems, you may need to regenerate the `.xpt` files or the `define.xml` file for the study, replace the files in the study's path with the new files, and then re-run the loading and checking

run. You can also view the additional files provided, load_log.txt, filtered_define.xml, and PROC_*job-id_log-id*.log, for additional information that can help in resolving load problems.

Note: The SAS System Viewer can be useful for inspecting the content of `.xpt` files. This application is distributed without charge: see www.sas.com.

If the problem stems from a sponsor-provided `define.xml` file, you may need to edit this file to correct any errors before re-submitting the loading and checking run.

4.3.3 Publishing studies with "Completed" runs

After a study has been registered and loaded, it can be published. Until a study is published it can be accessed only by its owner (that is, the person who registered the study). At installations where a team of users is responsible for reviewing and correcting errors found when loaded data is checked, a study can, and typically should, be published as soon as its loading and checking run is complete.

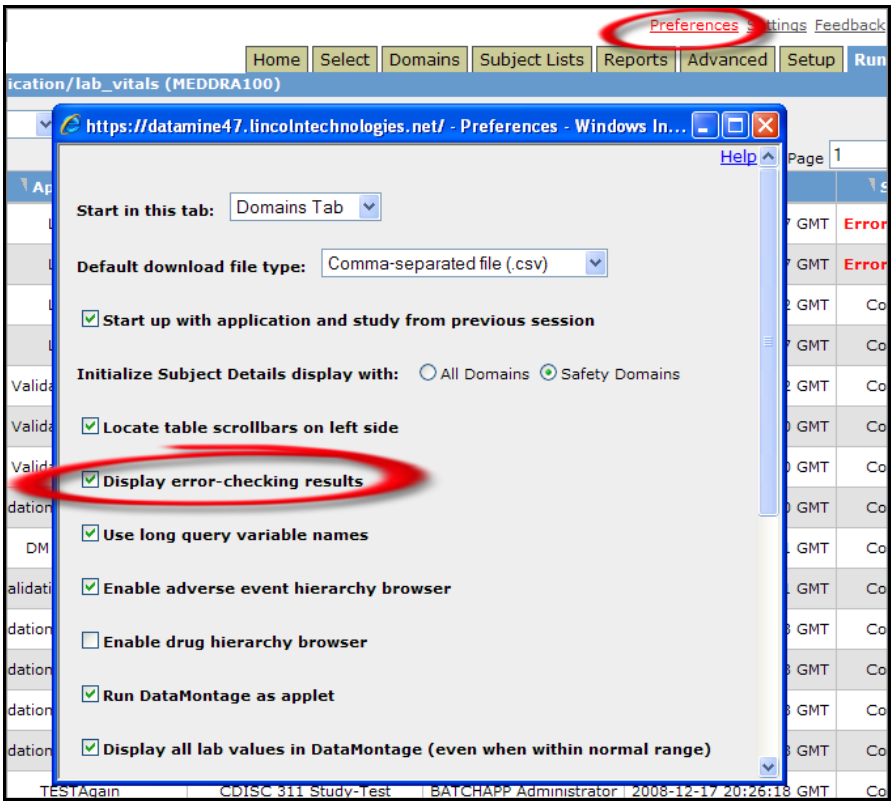
Users with the *Manage Applications and Studies* permission can publish studies to their own login groups. Users who also have the *Administer Users* permission can publish studies to any login group.

To publish a study: On the Setup tab click Studies / Pools. Then click for a study and select Publish.

Note: Each study in an application must be published individually. Publishing one study in an application does not have the effect of publishing any of the other studies in that application.

4.3.4 Reviewing checking results in "Completed" runs

You can review the checking results for a run whose status is Completed. To review the results of structure and consistency checks, a user must select the "Display error-checking results" user preference.



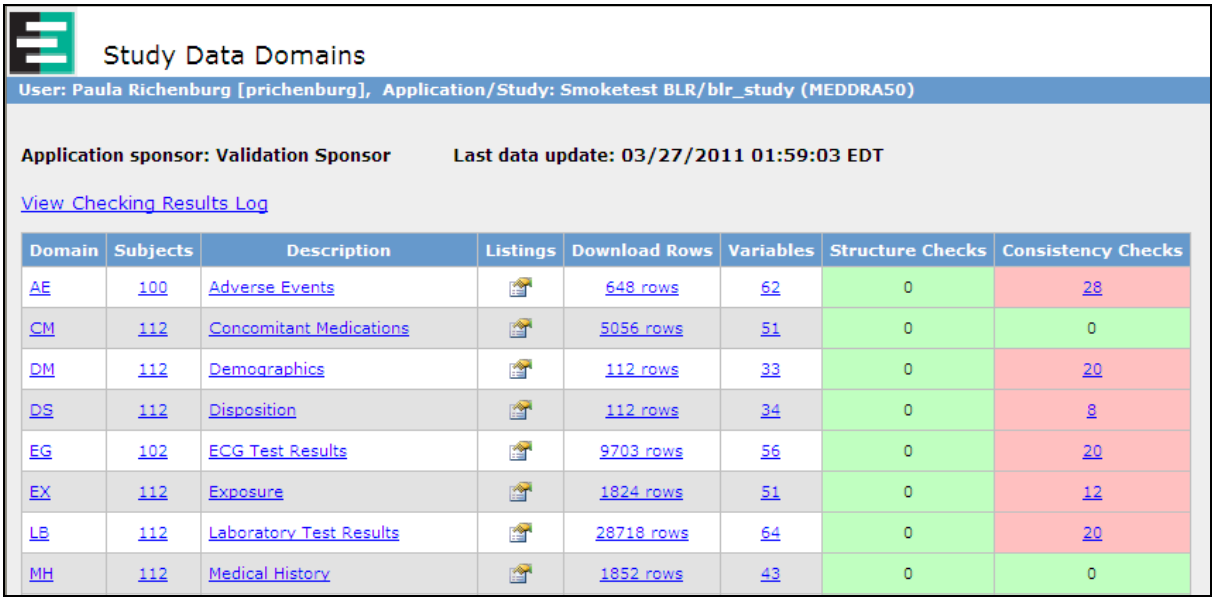
To set a user preference: Click Preferences.

After this preference is set, when the user logs in to WebSDM, selects the application and study, and navigates to the Domains tab, two additional columns appear in the table:

- The Structure Checks column displays a count of errors found in the metadata of each domain in the study. Click the linked count for details on these checking results.
- The Consistency Checks column displays a count of errors found in the clinical data of each domain. Click the linked count for details on these checking results.

The cells in these columns are color-coded by the severity of the error(s) found.

CONFIDENTIAL ▪ Copyright © 2000–2013, Oracle and/or its affiliates. All rights reserved.



Study Data Domains

User: Paula Richenburg [prichenburg], Application/Study: Smoketest BLR/blr_study (MEDDRA50)

Application sponsor: Validation Sponsor Last data update: 03/27/2011 01:59:03 EDT

View Checking Results Log

Domain	Subjects	Description	Listings	Download Rows	Variables	Structure Checks	Consistency Checks
AE	100	Adverse Events		648 rows	62	0	28
CM	112	Concomitant Medications		5056 rows	51	0	0
DM	112	Demographics		112 rows	33	0	20
DS	112	Disposition		112 rows	34	0	8
EG	102	ECG Test Results		9703 rows	56	0	20
EX	112	Exposure		1824 rows	51	0	12
LB	112	Laboratory Test Results		28718 rows	64	0	20
MH	112	Medical History		1852 rows	43	0	0

To review counts of structure and data errors: Click the Domains tab.

4.4 Deleting Applications

If you need to delete an application, a *Superuser* can do so from within WebSDM: navigate to the Setup tab, click  for the application, and select **Delete**. All related Oracle accounts are deleted, as is the application-level tablespace (if there is one).

If WebSDM is unable to remove all of the datafiles associated with the Oracle tablespace created for the application and its studies, a warning message appears. In such a case, you should manually delete the datafile(s) listed by the warning message from the WebSDM database. If a datafile is not deleted and a new application is later created with the same name as that of the deleted application, an error message redisplays the names of the datafiles that must be deleted.

CONFIDENTIAL ▪ Copyright © 2000–2013, Oracle and/or its affiliates. All rights reserved.

5 Monitoring WebSDM

In WebSDM, options are available to help you monitor the activities of individual users and the system as a whole. WebSDM also offers options for reviewing and tuning the system, including restarting the listener.

This chapter covers the following sections:

- User Monitoring and Messaging
- System Tuning and Monitoring

5.1 User Monitoring and Messaging

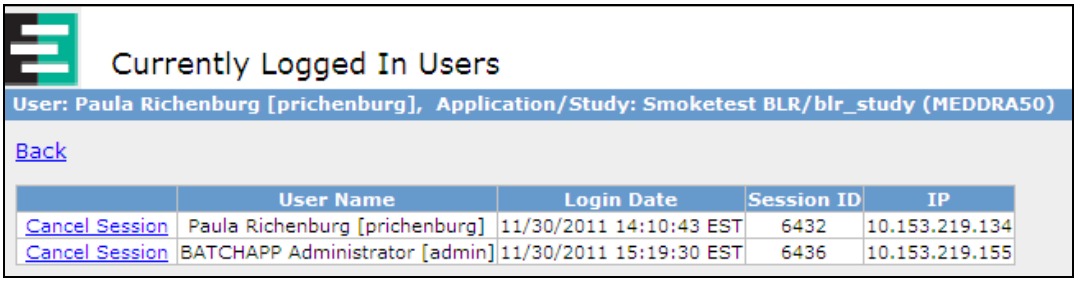
When users with the *Administer Users* permission click **Settings** in WebSDM, they can access options to:

- **View Currently Logged In Users**
- **View User Activity Audit Trail**
- **Send Message to All Users**

This section describes how these options can be used to research user activity and provide information to WebSDM users.

5.1.1 Reviewing current users

Before system maintenance activities or as a security measure, a list of currently logged in users can be produced.



To review current users: Click Settings / View Currently Logged In Users.

This option also allows you to find and cancel orphan sessions, which may be created when a user closes the browser application without having first logged out of WebSDM.

CONFIDENTIAL ▪ Copyright © 2000–2013, Oracle and/or its affiliates. All rights reserved.

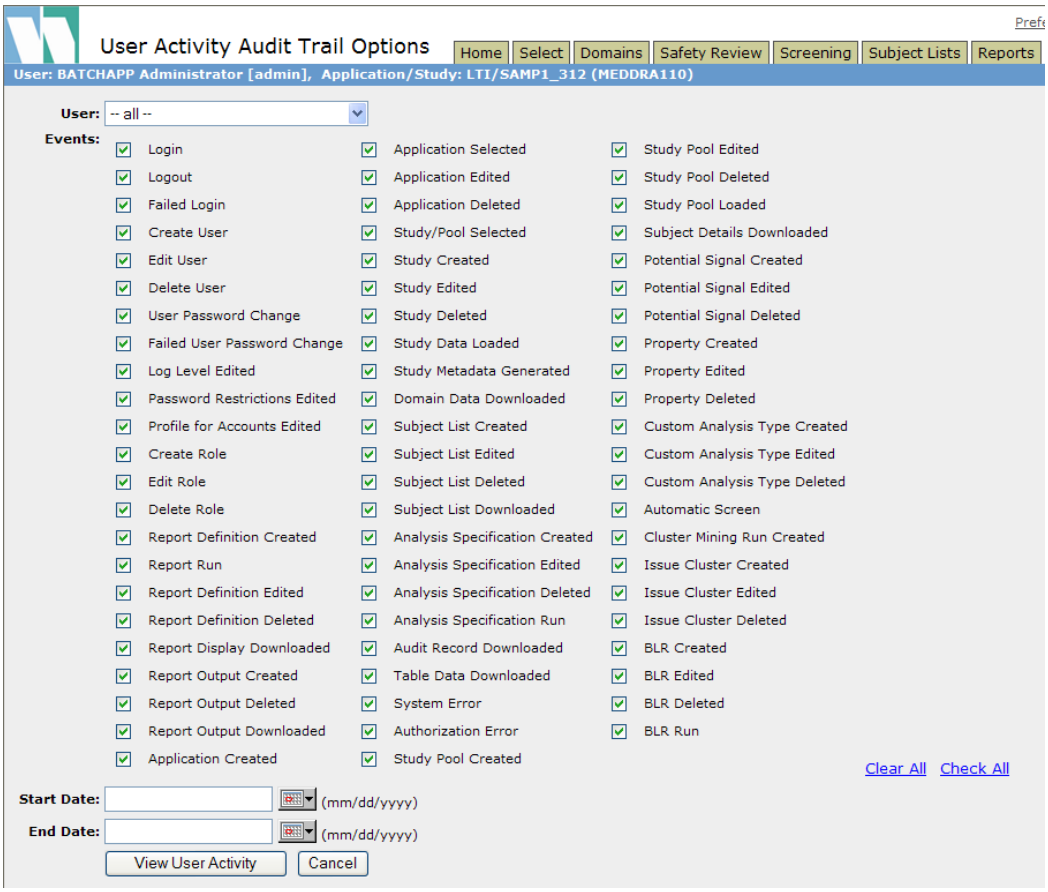
Note: User sessions are automatically terminated after a period of inactivity (as described in *Setting the session timeout period*). If you cancel the session of an active user, that user will lose any unsaved work.

5.1.2 Auditing user activity

The User Activity Audit Trail produces a report of user activity. You can review activity for:

- A single user or all users
- Specific system activities or all activities
- A single date, a date range, or a complete history from WebSDM installation to the present

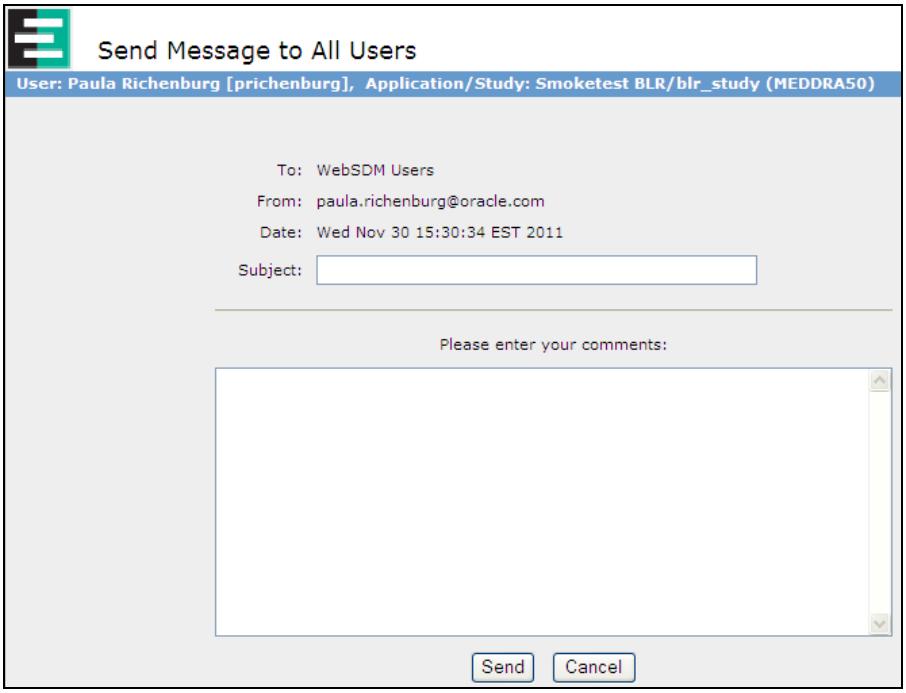
You can print or download the report that is produced for future reference.



To review user activity: Click Settings / View User Activity Audit Trail.

5.1.3 Sending a message to all users

A message can be sent to notify WebSDM users of upcoming activities such as system shutdowns, upgrades, or other issues.



To send a message: Click Settings / Send Message to All Users.

WebSDM sends the message to all enabled user accounts that have a valid associated email address.

5.2 System Tuning and Monitoring

WebSDM provides a user interface for performing system tuning and monitoring functions. A *Superuser* can click **Settings** in WebSDM to:

- Set up a multi-processor server by defining the number of background processors.
- Review space consumption for the Oracle tablespace used by the WebSDM master account.
- Restart the WebSDM listener process manually.

This section describes the options you select to perform these tasks.

This section also includes the procedure for restarting the WebSDM service, which you perform on the host server.

CONFIDENTIAL ▪ Copyright © 2000–2013, Oracle and/or its affiliates. All rights reserved.

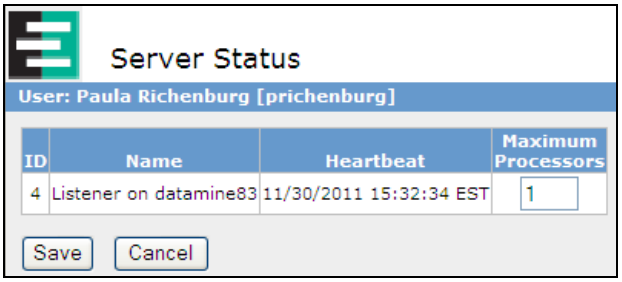
5.2.1 Setting up a multi-processor server

WebSDM utilizes two different kinds of computer processing:

- Foreground or interactive processing, as for specifying loading and checking runs
- Background or batch processing, as for executing loading and checking runs

If WebSDM is running on a single-processor server, that server performs both kinds of processing. If WebSDM is installed on a multi-processor server, one of the processors should be used for foreground processing, and the other(s) for background processing. Within WebSDM, you can set the maximum number of processors to use for background processing. This setting controls the number of loading and checking runs that can be executed concurrently.

For example, if there are three processors on the WebSDM server you would set the maximum number of (background) processors to two. Two runs can be executed at the same time on such a server.



To set the number of background processors: Click Settings / View Server Status.

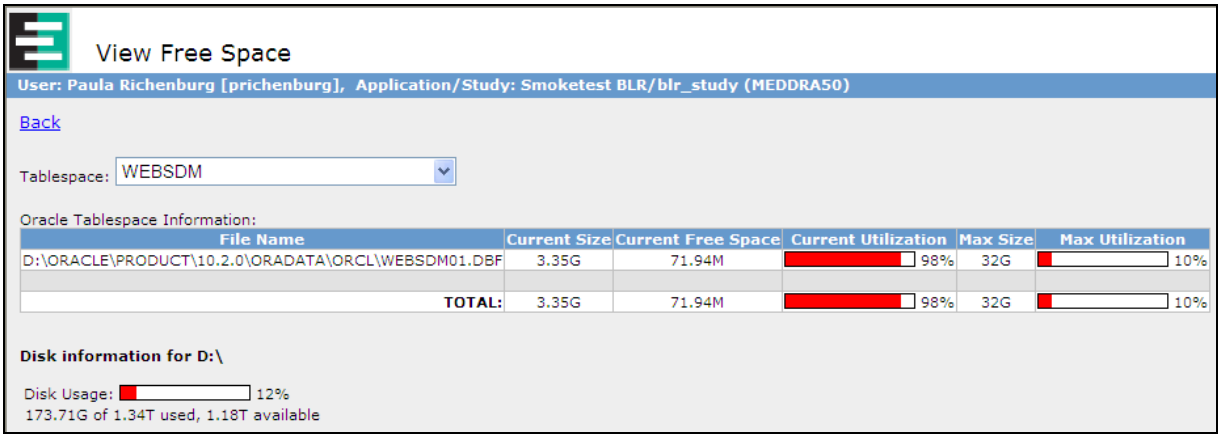
A WebSDM *Superuser*, such as the default "**admin**" user account, can access this option and define the number of background processors.

For a dedicated server, the maximum for background processing should be set to one less than the number of processors on the server. For a shared server, a smaller maximum is recommended.

Note: The heartbeat value shown by this option is for the WebSDM listener process, which checks for any background processes initiated by loading and checking runs. The listener starts up automatically with WebSDM and its heartbeat is updated every 2-30 seconds. If the listener stops, it can be restarted manually. See *Restarting the listener* (page 51).

5.2.2 Reviewing space consumption

On an ongoing basis, *Superusers* can check the remaining space for the Oracle tablespace used by the WebSDM master account.



To check server space: Click Settings / View Free Space.

This feature may be useful for monitoring the Max Utilization level of a tablespace: when it approaches a threshold predefined by your installation, such as 75%, additional datafiles may need to be allocated.

This option displays information for the tablespace used by the WebSDM master account only. To review the utilization of tablespaces used by application and study-level accounts or MedDRA dictionary accounts, Oracle DBA tools must be used.

Note: The "Disk information" section of this page is reliable only in configurations where the database and the application server are running on the same server.

5.2.3 Restarting the listener

The WebSDM listener process identifies background processes and assigns them to server processors for execution. In WebSDM, background processes are initiated by the submission of loading and checking runs. The listener process may terminate unexpectedly when it encounters an error, or may be stopped by a system operator.

A *Superuser* can restart the web server's WebSDM listener process manually from within WebSDM. To restart the listener, click **Settings** then **Restart Listener**.

Database connection and configuration information for the listener is saved in the WebSDM `website.properties` text file. For more information on editing this file, which is found by default in the `c:\Lincoln\apps\websdm\webapps\web_root\WEB-INF\classes\` directory, see *Configuring website.properties for background processes* (page 11).

Note: If the Auto-Start Local Listener site option is set to allow automatic restart, WebSDM checks the listener heartbeat value and, if the listener process is not running, restarts it automatically. See *Setting site options* (page 18).

5.2.4 Restarting the WebSDM service

For the WebSDM application to be accessible to users, the WebSDM service must be running. The WebSDM service may stop due to an OS failure or a problem with the availability of the database.

To start the WebSDM service on the host Windows server:

1. Log on to the Windows server as an Administrator.

2. Either open a command window and enter the following command:

   ```
   net start <service name>
   ```

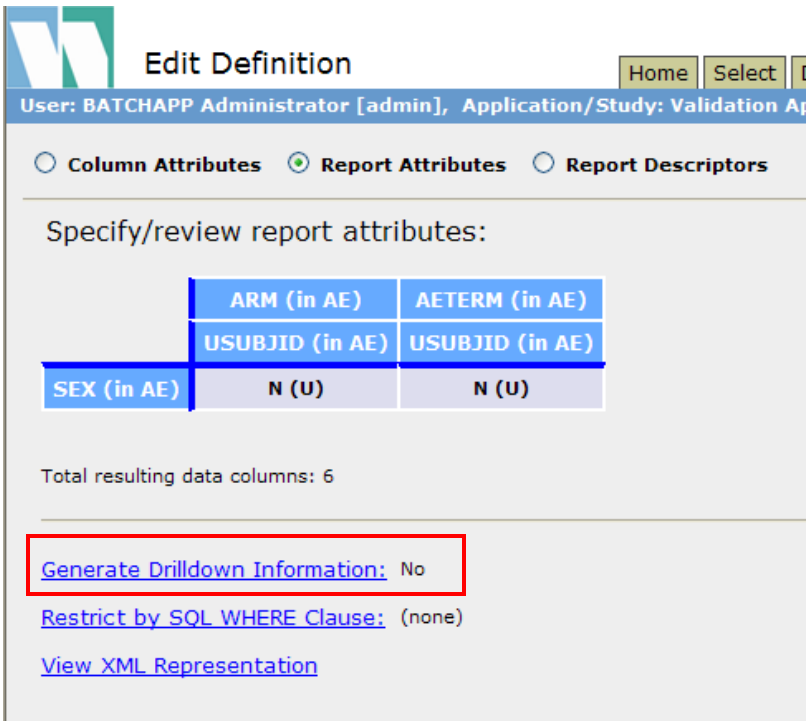
   or right-click on the server's desktop My Computer icon and select **Manage**, expand the **Services and Applications** node and click **Services**, then right-click on the **websdm** service and select **Start**.

*Note***:** At installation, the name given to this service by default is "websdm". If a different name was supplied at your installation, use that name instead.

5.2.5 Allocating memory for reports

The site option Max Memory Per Report allows you to specify the amount of memory that will be allocated to running each report. The default value is 300 MB, which is generally sufficient for moderately-sized studies.

If most reports run successfully but a specific report definition does not complete, you may be able to decrease that particular report's memory demands by editing its attributes. Edit the Report Definition; select the Report Attributes page, and set the **Generate Drilldown Information** option to No.



When a report does not have enough memory to run, this message will display:

> **The report could not be displayed for the following reasons:**
>
> **System error occurred. Contact your system administrator.**

If this message occurs with some regularity (for example, when running reports on a very large study), you can increase the memory allocated to reports by setting the **Max Memory Per Report** site option to a value higher than the default 300 MB. It is recommended that the value not exceed 768 MB.

CONFIDENTIAL ▪ Copyright © 2000–2013, Oracle and/or its affiliates. All rights reserved.

Appendix A: Profile for Study Accounts

WebSDM creates a database account for each application and study that is registered. The accounts associated with studies own the tables that contain the clinical data comprising a study – these tables are created and populated during loading and checking runs. The accounts associated with applications are reserved for future use.

WebSDM assigns a fixed password for these accounts. That password was generated via the use of a random password generating utility, specifying the following criteria:

- The password is 10 characters long.
- The password contains at least one alphabetic character.
- The password contains at least one number.
- The password contains at least one non-alphanumeric character.

WebSDM does not support the expiration or resetting of the password for these accounts. If your site has installed a new version of WebSDM and your database is configured with a DEFAULT profile that imposes limits on the duration of passwords or that uses a password verifying function more restrictive than the criteria specified above, you must define an additional profile and use the appropriate WebSDM site option (described in *Setting site options*) to associate that profile with the application and study accounts.

Note: If your site has upgraded from a previous release of WebSDM that did not allow specification of an additional profile, do not create an additional profile or modify the DEFAULT profile.

The following script (when executed while connected to the database as the SYS user) creates a profile that is suitable for the application and study accounts:

```
CREATE OR REPLACE FUNCTION verify_websdm_acct_pw
(username varchar2,
  password varchar2,
  old_password varchar2)
  RETURN boolean IS
   n boolean;
   m integer;
   differ integer;
   isdigit boolean;
   ischar  boolean;
   ispunct boolean;
   digitarray varchar2(20);
   punctarray varchar2(25);
   chararray varchar2(52);

BEGIN
   digitarray:= '0123456789';
   chararray:= 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ';
   punctarray:='!"#$%&()``*+,-/:;<=>?_';
```

```
-- Check for the minimum length of the password
   IF length(password) < 10 THEN
      raise_application_error(-20002, 'Password length less than 10');
   END IF;

   -- Check if the password is too simple. A dictionary of words may be
   -- maintained and a check may be made so as not to allow the words
   -- that are too simple for the password.
   IF NLS_LOWER(password) IN ('welcome', 'database', 'account', 'user', 'password', 'oracle',
'computer', 'abcd') THEN
      raise_application_error(-20002, 'Password too simple');
   END IF;

   -- Check if the password contains at least one letter, one digit and one
   -- punctuation mark.
   -- 1. Check for the digit
   isdigit:=FALSE;
   m := length(password);
   FOR i IN 1..10 LOOP
      FOR j IN 1..m LOOP
         IF substr(password,j,1) = substr(digitarray,i,1) THEN
            isdigit:=TRUE;
             GOTO findchar;
         END IF;
      END LOOP;
   END LOOP;
   IF isdigit = FALSE THEN
      raise_application_error(-20003, 'Password should contain at least one digit, one character and one
punctuation');
   END IF;
   -- 2. Check for the character
   <<findchar>>
   ischar:=FALSE;
   FOR i IN 1..length(chararray) LOOP
      FOR j IN 1..m LOOP
         IF substr(password,j,1) = substr(chararray,i,1) THEN
            ischar:=TRUE;
             GOTO findpunct;
         END IF;
      END LOOP;
   END LOOP;
   IF ischar = FALSE THEN
      raise_application_error(-20003, 'Password should contain at least one digit, one character and one
punctuation');
   END IF;
   -- 3. Check for the punctuation
   <<findpunct>>
   ispunct:=FALSE;
   FOR i IN 1..length(punctarray) LOOP
      FOR j IN 1..m LOOP
         IF substr(password,j,1) = substr(punctarray,i,1) THEN
            ispunct:=TRUE;
             GOTO endsearch;
         END IF;
      END LOOP;
   END LOOP;
   IF ispunct = FALSE THEN
      raise_application_error(-20003, 'Password should contain at least one digit, one character and one
punctuation');
   END IF;

   <<endsearch>>
   -- Everything is fine; return TRUE ;
   RETURN(TRUE);
END;
/

create profile WEBSDM_STUDIES_PROFILE limit
```

```
COMPOSITE_LIMIT  UNLIMITED
SESSIONS_PER_USER  UNLIMITED
CPU_PER_SESSION  UNLIMITED
CPU_PER_CALL  UNLIMITED
LOGICAL_READS_PER_SESSION  UNLIMITED
LOGICAL_READS_PER_CALL  UNLIMITED
IDLE_TIME  UNLIMITED
CONNECT_TIME  UNLIMITED
PRIVATE_SGA  UNLIMITED
FAILED_LOGIN_ATTEMPTS  5
PASSWORD_LIFE_TIME  UNLIMITED
PASSWORD_REUSE_TIME  UNLIMITED
PASSWORD_REUSE_MAX  UNLIMITED
PASSWORD_LOCK_TIME  UNLIMITED
PASSWORD_GRACE_TIME  UNLIMITED
PASSWORD_VERIFY_FUNCTION verify_websdm_acct_pw
;
```

After creating a profile, use **Settings / Set Site Options** in WebSDM to associate it with application and study accounts. Use the **Profile for New Accounts** setting in the "Database Accounts and File System Structure" section to select it.

For more information, see the Oracle Database Security Guide, 10g Release 2, Chapter 7 Security Policies, Section Password Complexity Verification, or Oracle Database Security Guide, 11g Release 2, Chapter 3, Configuring Authentication, Section Customizing Password Complexity Verification.

CONFIDENTIAL ▪ Copyright © 2000–2013, Oracle and/or its affiliates. All rights reserved.