Oracle Health Sciences Life Sciences Warehouse

Security Guide

Release 2.4

E52295-01

May 2014

This guide describes essential security management options for the following applications:

- Oracle Life Sciences Data Hub 2.4
- Oracle Health Sciences Data Management Workbench 2.4

Introduction

This guide presents security guidelines and recommendations for the Oracle Life Sciences Data Hub (Oracle LSH) and Oracle Health Sciences Data Management Workbench (Oracle DMW) applications, and includes the following sections:

- User Security Features
- Application Security Features
- Security Configuration Features

In addition, see the following documents for security configuration instructions:

- *Oracle Health Sciences Data Management Workbench Installation Guide*
- *Oracle Health Sciences Data Management Workbench User's Guide*
- *Oracle Life Sciences Data Hub System Administrator's Guide*
- *Oracle Life Sciences Data Hub Installation Guide*
- *Oracle Life Sciences Data Hub Application Programming Interface Guide*
- *Oracle Life Sciences Data Hub Implementation Guide*
- *Secure Configuration Guide for Oracle E-Business Suite*
- *Oracle Fusion Middleware Understanding Security for Oracle WebLogic Server*
- *Oracle Fusion Middleware Securing Oracle WebLogic Server*
- *Oracle Fusion Middleware Information Roadmap for Oracle WebLogic Server*

User Security Features

Use the following information to securely configure users in the Oracle LSH application.

See "Setting Up User Accounts" in the *Oracle Life Sciences Data Hub System Administrator's Guide* for instructions on creating users.

User Password Security

Oracle recommends that you use the profile settings described in this section to provide optimal security in login password usage in Oracle LSH:

- **Password case sensitivity:** You must set this profile to Insensitive if you are using Oracle LSH Programs of type Business Intelligence Publisher to enable users to log in to BI Publisher using their single sign-on credentials.
- **Password length requirement:** This profile determines the minimum number of characters required in a user's Oracle LSH login password. The default setting is 5. Oracle recommends a setting of 8 or more for use with Oracle LSH.
- **"Hard to guess" requirement:** This profile enforces requirements that make it more difficult to guess what another user's password might be. These requirements come as a package; you must either accept or reject the whole. Oracle recommends a setting of Yes (to accept the package) for use with Oracle LSH.
- **"Forgot your password?" functionality:** For Oracle LSH, Oracle recommends a setting of 40 for the Local Login Mask profile. This setting displays a "Forgot your password?" link on the Login page. If the user clicks this link, the system loads a page where the user can enter his or her username.

  The user then receives an email stating, "Password reset requires approval." The user needs to click one of the choices "Approve" or "Reject" that automatically generate an email response. If the user ignores the notification, the request expires in four hours.
- **Limit on log-in attempts:** This profile option determines the maximum number of logins a user can attempt before the user's account is disabled. To reinstate the account a system administrator must unlock the account and reset the password. For example, if the value set is 3, it will lock the account if the user enters incorrect password 3 times.
- **Time limit on password reuse after resetting a password:** This profile will set the minimum number of days that a user must wait after changing his or her password before being allowed to reuse a password. The user can use the new password once and then must wait the number of days you set before he or she can reuse the password.

  For example, if the value of this profile is set to 5, a user who changes his or her password cannot reuse the password until 5 days after they reset.

  If the profile value is set to the number 0, then there is no restriction on password reuse.

See "Setting Password Requirements" in the *Oracle Life Sciences Data Hub System Administrator's Guide*.

To change their own passwords, both Oracle LSH and Oracle DMW users must use Preferences in Oracle LSH. See the Oracle Life Sciences Data Hub User's Guide and the *Oracle Health Sciences Data Management Workbench User's Guide*

Database User Account Security

To limit user access to the Oracle LSH database, you must create an Oracle LSH database account for users who need access to the Oracle LSH database through an external system or remote database. Oracle LSH allows you to create an Oracle LSH database account to allow only the users you select to access the database.

See "Database Accounts for Use in Definition" in the *Oracle Life Sciences Data Hub System Administrator's Guide*.

TMS User Security

Users who will run Oracle LSH APIs that insert, delete, or modify Oracle LSH classification hierarchies and terms (LSH Classification Admin tasks) need security access for their Oracle LSH database account to the Oracle Thesaurus Management System (TMS) instance that is installed as part of Oracle LSH.

See "Setting Up TMS Security for Users" in the *Oracle Life Sciences Data Hub System Administrator's Guide*.

Application Security Features

Oracle LSH and Oracle DMW include security features that allow you to control user access to user interface pages, study data, and objects and operations.

Use the following information to securely configure user security in the Oracle LSH and Oracle DMW applications.

See "User Security Features" and "Designing a Security System" in the *Oracle Life Sciences Data Hub Implementation Guide*.

Roles, Rights, and User Groups

Users are allowed to perform an operation on an object or output when they:

- belong to a user group that is assigned to the object or output either explicitly or by inheritance
- and are assigned to a role within that user group that allows the operation on the object.

You must define user groups and assign users to roles within the groups. In Oracle DMW, predefined roles are available for use with both Oracle DMW and Oracle LSH. You can edit the predefined roles as necessary.

Users must also have an application role that allows them to access particular pages in the user interface.

See the *Oracle Life Sciences Data Hub System Administrator's Guide* and the *Oracle Health Sciences Data Management Workbench User's Guide*.

Data Blinding and Masking

Oracle LSH and Oracle DMW provide data blinding functionality. To see blinded data, a user must have the following privileges:

- Normal access to the table: belonging to a user group that has access to the table, with a role in the context of that user group that allows Read privileges on the data.
- An application role that allows access to blinded data across all studies and tables.

In Oracle LSH, blinding is at the table level only. Blinded tables are partitioned, with the real data in one partition and dummy data in the other. Only users with special privileges can view any real data in the table at all.

In Oracle DMW you can mark data as blinded at the table, column, row, or cell level and specify masking values for the sensitive data. Only users with special privileges can view any real data, but all users with normal Read privileges and user group access to the table can see the real, nonblinded data and the masking values for the sensitive data.

In both products, each time a user with special privileges requests to view real, blinded data, the system audits the event.

When data is blinded, it is hidden in the Oracle LSH and Oracle DMW user interfaces and databases, discrepancy records, and in export or job outputs unless a user with the required blinding application role and normal access to the table(s) explicitly requests to view the real data.

If your study contains Personal/Protected Health Information (PHI), Oracle recommends that you blind all PHI.

Object Security

Each time a user tries to perform an operation on a defined object, the system runs a check that compares the security privileges of the user with the security requirements of the object.

A user can operate on an object only if both these conditions are met:

- The user belongs to an active user group that is assigned to that object, either explicitly or through inheritance.
- The user has a role in that user group that permits the operation o the object's subtype.

In addition, Oracle DMW includes predefined roles that are available for use with Oracle LSH, and control user access to specific objects and operations for those objects.

See "Setting Up Object Security" in the *Oracle Life Sciences Data Hub System Administrator's Guide*.

Auditing and Monitoring

Oracle LSH and Oracle DMW maintain a full audit trail for all changes made to data discrepancies either manually or programatically. The audit trail records the user name, data changed, and timestamp of the change. The audit trail is read-only and cannot be modified by any user.

In addition, a user with the appropriate privileges can download a file containing discrepancy information. This action is audited with user identification, timestamp and a complete copy of the downloaded file.

Security Configuration Features

Use the following information to securely configure the Oracle LSH and Oracle DMW applications.

Secure Installation

Use the following information to securely install the Oracle LSH and Oracle DMW applications.

Secure Installation with HTTPS

By default, the Oracle LSH and Oracle DMW installation is configured to use HTTPS, which requires the use of a trusted signed certificate.

HTTPS can be used to encrypt and protect communication between the client desktop and the Oracle LSH and Oracle DMW application server. Transmission of data from source systems and Oracle LSH and Oracle DMW can also be configured to use encrypted communication protocols.

It is also possible to install Oracle LSH and Oracle DMW to use HTTP.

Oracle recommends that you use HTTPS and a trusted signed certificate.

Secure the WebLogic Server

For information on securing the WebLogic Server, see:

- *Oracle Fusion Middleware Securing Oracle WebLogic Server*
- Oracle Fusion Middleware Securing a Production Environment for Oracle WebLogic Server
- "Security" in *Oracle Fusion Middleware Information Roadmap for Oracle WebLogic Server*

Secure Access to APIs

Oracle LSH includes a set of APIs that enable you to do most of the things you can do through the user interface, including creating, modifying, and installing objects. You can call Oracle LSH APIs from source code in a defined Program in Oracle LSH. In this case, no additional security or setup is required.

To run any API package from a tool outside of Oracle LSH, such as SAS, SQL Developer, or SQL*Plus, your system administrator must configure security settings including setting up a database account and a TMS account with specific privileges. In addition, you can use a PL/SQL wrapper or the security API functionality.

See the *Oracle Life Sciences Data Hub Application Programming Interface Guide*.

File Watcher Security

The files that are placed on a remote file share for detection by File Watcher must have restricted access to prevent investigators and others from seeing data they should not see, such as blinded data. Ensure that the file share is secure by limiting the number of user groups that have write or execute access to the file share.

See the *Oracle Health Sciences Data Management Workbench Installation Guide*.

DP Server Security

The DP Server process creates directories for each job, and the job directory can contain information that may be sensitive to your organization. Oracle recommends that you grant full access to the OS directory only to the Oracle user who runs the DP Server process, and the external processing engine user who writes into the job directory as part of the job execution (for example, the OS user who runs the Informatica Integration service process).

See the *Oracle Life Sciences Data Hub Installation Guide*.

Security for Third-Party Applications

Oracle LSH and Oracle DMW can be integrated with Informatica and the Oracle Business Enterprise Edition (OBIEE) applications including BI Publisher and applications used for visualization such as BI Server, BI Presentation Services, and OBIEE Answers. The following section describes how to secure these integrations.

Secure Informatica Integration

If Oracle LSH and Oracle DMW are integrated with Informatica, Oracle recommends that you secure the job directories to which Informatica publishes files. To do so, make sure that you only allow a few users write or execute permissions for the job directories.

See "Securing Informatica Job Directories" in the *Oracle Life Sciences Data Hub Installation Guide* and "Setting Up Security for Informatica" in the *Oracle Life Sciences Data Hub System Administrator's Guide*.

Secure Oracle Business Intelligence Enterprise Edition Integration

To secure the OBIEE applications that are integrated with Oracle LSH or Oracle DMW, consider the following:

- User groups, roles, and rights that you configure in Oracle LSH determine the data that users can access in the OBIEE applications when the OBIEE application is launched from within Oracle LSH.
- When a user launches an OBIEE application from outside of Oracle LSH, blinded and noncurrent data is not available, regardless of the user's privileges.
- Each Presentation Server must be installed on a different computer and have a unique URL. You can use this setup to control what users can see in OBIEE.

See "Security Configuration" in the *Oracle Life Sciences Data Hub System Administrator's Guide*. In addition, see "Setting Up Oracle Business Intelligence Visualizations" and "Setting Up Security for Oracle Business Intelligence Publisher" in the *Oracle Life Sciences Data Hub System Administrator's Guide*.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

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

Security Guide, Release 2.4
E52295-01