Oracle® Health Sciences Life Sciences Warehouse

Security Guide

Release 3.0
F32375-01
October 2020

Oracle Health Sciences Life Sciences Warehouse Security Guide, Release 3.0

F32375-01

Copyright © 2017, 2020, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government’s use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

1 Oracle LSH and Oracle DMW Security

Access to Oracle Support

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

Preface

This preface contains the following sections:

Related resources

All documentation and other supporting materials are available on the Oracle Help Center.

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.

1

Oracle LSH and Oracle DMW Security

This guide includes the following sections:

- Introduction
- User Security Features
- Application Security Features
- Security Configuration Features
- Oracle DMW Secure Development

Introduction

This guide presents security guidelines and recommendations for Oracle Life Sciences Data Hub (Oracle LSH) and Oracle Health Sciences Data Management Workbench (Oracle DMW). It 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

When you set up user accounts as described in "Setting Up User Accounts" in the *Oracle Life Sciences Data Hub System Administrator's Guide*, use the information in the following topics to securely configure users in Oracle LSH:

- User Password Security
- Database User Account Security

- TMS User Security

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

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

The Oracle LSH user database accounts have a session timeout with a default setting of 24 hours. A public API is provided to permit an administrator to modify the timeout value, but the maximum value permitted is 24 hours. This setting applies to all database accounts in the Oracle LSH instance. You cannot set a different timeout for each account. If the database accounts are not used to connect Oracle DMW to another application, but are used by individuals to occasionally connect to the database to query data, then a shorter timeout provides greater security for your environment

For more details, 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.

> **Note:**
>
> For more information on security features, see "User Security Features" and "Designing a Security System" in the *Oracle Life Sciences Data Hub Implementation Guide*.

The following topics provide information to securely configure user security in the Oracle LSH and Oracle DMW applications:

- Roles, Rights, and User Groups
- Data Blinding and Masking
- Object Security
- Auditing and Monitoring

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 on the object's subtype.

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

For more information, see "Setting Up Object Security" in the *Oracle Life Sciences Data Hub System Administrator's Guide*.

Auditing and Monitoring

This section contains the following topics:

- Data Auditing
- Oracle DMW Discrepancy Auditing

Data Auditing

In Oracle LSH, you can select a data processing type that provides an audit trail of changes made to the data. With Oracle LSH audited data, you can recreate the state of data in the table at any previous point in time using data snapshots. The audit trail never deletes data. But, it records each change to each record over time, including data deletions.

Oracle DMW maintains a full audit trail for all changes made to data. You can display the most recent Oracle DMW data in the Oracle DMW application. Data from the audit trial is visible in Oracle LSH.

Oracle DMW Discrepancy Auditing

Oracle DMW maintains a full audit trail for all changes made to data discrepancies either manually or programmatically. 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.

Security Configuration Features

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

- Secure Installation
- Security for Third-Party Applications

Secure Installation

This section contains the following topics to securely install Oracle LSH and Oracle DMW:

- Secure the Database Context

- Secure Installation with HTTPS
- Secure the WebLogic Server
- Secure Access to APIs
- Oracle DMW File Watcher Security
- DP Server Security

Secure the Database Context

Use Transparent Data Encryption (TDE) to encrypt the tablespaces holding your LSH/DMW data. See "Securing Stored Data Using Transparent Data Encryption" in the *Oracle Database Advanced Security Administrator's Guide* (https://docs.oracle.com/cd/E11882_01/network.112/e40393/asotrans.htm#ASOAG600).

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.

You can use HTTPS to encrypt and protect communication between the client desktop and the Oracle LSH and Oracle DMW application server. You can also configure the transmission of data from source systems and Oracle LSH and Oracle DMW to use encrypted communication protocols.

You can install Oracle LSH and Oracle DMW to use HTTP, but Oracle recommends that you use HTTPS with data encryption using Transport Layer Security (TLS) 1.2 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*
- *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*.

Oracle DMW 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 restricting the access permissions on the Linux directories and files and by limiting the number of user groups that have write or execute access to the file share.

For more information, see the *Oracle Health Sciences Data Management Workbench Installation Guide*.

DP Server Security

The DP Server process creates directories for each job. 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 Linux 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 more information, see the *Oracle Life Sciences Data Hub Installation Guide*.

Security for Third-Party Applications

Oracle LSH can be integrated with 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 topic describes how to secure these integrations:

- Secure Oracle Business Intelligence Enterprise Edition Integration

Secure Oracle Business Intelligence Enterprise Edition Integration

To secure the OBIEE applications that are integrated with Oracle LSH, 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.

For more information, 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*.

Oracle DMW Secure Development

This section provides an overview of the security options for customers who will use Oracle DMW user database accounts to access the Oracle DMW and Oracle LSH

public views and Application Programming Interfaces (called Oracle DMW APIs in this document). For further information on these views and APIs, see the "Introduction to Oracle DMW APIs" in the *Oracle Health Sciences Life Sciences Warehouse API Guide*.

The recommendations in this document are not exhaustive and no guarantee is given that implementing all the suggestions in this document provides sufficient protection for all security threats. The reason for this disclaimer is that you cannot delegate responsibility for secure application development to a third party or a single document. This document is to help developers be aware of the security tools and features that they can use to implement application security. This document does not replace a formal code review process.

Guidelines are presented here to assist in mitigating common security risks when customers are using the Oracle DMW APIs. The Open Web Application Security Project (OWASP) publishes the OWASP Top 10 to identify some of the most critical application security risks. This document briefly describes each Top 10 risk and Oracle DMW mitigation strategies, and encourages you to extend these strategies to secure your applications and environments that use Oracle DMW APIs. For the OWASP Foundation's description of the OWASP Top 10 Application Security Risks, see:https://www.owasp.org/index.php/Top_10-2017_Top_10.

This section contains the following topics:

Injection

SQL Injection can occur when untrusted data is used in a command or query. If an attacker sends hostile data, this can result in executing harmful commands or in unauthorized access of data.

To prevent injection when you write you own PL/SQL code to access the Oracle DMW APIs, your code should:

- Use parameterized queries. Use prepared statements rather than generating dynamic SQL.
- Use bind variables. Use bind variables to enter input values into SQL statements.
- Validate user input. White list input validation is preferred to ensure that the input is an expected value. As appropriate for different data types: check the input length, check for a permitted value, check for proper format, check for permitted characters, and/or check minimum and maximum value ranges.

Broken Authentication

Access control weaknesses can lead to unauthorized data access either by attackers or by users obtaining access to data they are not authorized to view.

To counter attacker access, use strong passwords. Create a policy for password length and complexity. See "Choosing A Secure Password": https://www.oracle.com/technetwork/database/security/secure-passwords-082531.html

Each Oracle DMW API user should have a private user account to access the Oracle DMW database. The database account is associated with and has the same object-level security as the Oracle DMW user account. Database users should not share credentials. Sharing credentials can provide a user with privileges beyond their Oracle DMW application user account and provide access to data that the user isn't authorized to view.

Sensitive Data Exposure

Attackers may obtain unauthorized access to poorly protected sensitive data. Caution should be used to hide sensitive information from unauthorized users.

When using the Oracle DMW APIs, the SQL*Net connection to the database should be secured with cryptographic controls such as a VPN tunnel.

Clinical trial data stored in Oracle DMW may contain blinded data, which shouldn't be viewed by some application users. By default, the blinded data is not returned to the user through the Generic Visualization Business Areas (GVBA) access. The user must specifically request access to the blinded data through one of the API calls, and is granted access only if the appropriate "blind break" privileges have been granted to the user. Access to blinded data is audited in the Oracle DMW application.

When initializing access to a GVBA using the API procedure CDR_PUB_API_GVA.setInitializeBa, users cannot set incompatible blinding access types for different business areas during the same session. If this is attempted, an error occurs. In order to modify the blinding access type, the user must reset the business area access by calling the appropriate Generic Visualization Business Areas (GVBA) procedure, and then initialize each business area using the same blinding access type.

Users who are allowed to view data, especially blinded data, should be careful to ensure that the data is never displayed to colleagues who should not see it, either because the data is blinded or because it belongs to a study or clinical data model where they do not have access.

XML External Entities (XXE)

The Oracle DMW application uses internally generated XML to communicate between different parts of the application. It uses an XML Schema to constrain the structure and content of messages.

Broken Access Control

In some applications, the UI controls function-level access by exposing only the functionality where access has been granted and hiding functionality where the user

has not been granted access. Without database-level access control, an attacker who has partial access to the application might be able to gain access to an unauthorized function.

For API access, the Oracle DMW security privileges determine which actions a user is authorized to perform on Oracle DMW objects and security is verified in the Oracle DMW application database code before the action is performed. Oracle recommends that you set up user roles based on the principle of least privilege. Users should have only the minimum privileges necessary to perform their function.

Your code that uses the Oracle DMW views and APIs should properly enforce access privileges for application functions at the level of the business logic in your program. The default behavior in an application should be to deny access to application functions unless the access is granted explicitly.

Use of the Oracle DMW API is often to view data in a graphical or analysis application. Oracle recommends that you create your Oracle DMW application user with privileges to view data (view-only), so the corresponding database user will be restricted to view-only privileges for the data. See "Use or create object security roles" in the *Oracle Health Sciences Data Management Workbench Administration Guide*.

Security Misconfiguration

Attackers can take advantage when the security configuration is incorrect or incomplete to obtain unauthorized access to an application. The entire technology stack must be configured properly, and processes should be in place to detect misconfigurations-missing patches, accounts with default passwords, insecure settings in frameworks or libraries, etc.

The Oracle DMW application hosted by Oracle Managed Cloud Services is deployed in a secure hosted environment following Oracle policy and procedures.

Ensure that your on-premise configuration, which makes use of Oracle DMW APIs and views, does not contain opportunities for an attacker to gain unauthorized access to the system. Take care to secure database accounts, files, directories, servers, the network, and other data access channels outside of the API domain.

Cross-Site Scripting

Cross-site scripting is not applicable for access to the Oracle DMW API.

Insecure Deserialization

Oracle recommends that your code, which makes use of the Oracle DMW views and API, does not accept serialized objects from untrusted sources or that only primitive data types are permitted in such serialized objects.

Components with Known Vulnerabilities

Oracle recommends that you apply updates including the relevant Critical Patch Updates to your Oracle DMW environment when they become available. Oracle Critical Patch Updates are described at: https://www.oracle.com/technetwork/topics/security/alerts-086861.html.

Insufficient Logging and Monitoring

Oracle recommends event logging and monitoring of the environment where Oracle DMW is deployed to enable detection and response to suspicious activity in a timely manner.