Oracle® Healthcare Data Repository

Secure Configuration Guide

Release 8.0

E98319-01

February 2019

The *Secure Configuration Guide* provides an overview of the security features provided with the Oracle® Healthcare Data Repository application, including details about the general principles of application security, and how to install, configure, and use the Healthcare Data Repository application securely.

This guide is for users who install and configure the Healthcare Data Repository application.

- Security Overview
- Secure installation and configuration
- Security Features
- Documentation Accessibility

1 Security Overview

- Application security overview
- General security principles

1.1 Application security overview

To ensure security in the Healthcare Data Repository application, carefully configure all system components:

- Firewalls
- Load balancers
- Virtual Private Networks (VPNs)

1.2 General security principles

Require complex and secure passwords

Any user who is configured in the WebLogic server where HDR application is deployed can access its APIs. It is recommended that strong password is used for the WebLogic user account that will be used to access HDR APIs.

Keep passwords private and secure

Tell users never to share passwords, write down passwords, or store passwords in files on their computers.

Lock computers to protect data

Encourage users to lock computers that are left unattended.

Provide only the necessary rights to perform an operation

Create necessary user roles for users accessing the application developed using HDR APIs to provide necessary access control to access different types of clinical data stored in HDR.

2 Secure installation and configuration

- Installation overview
- Post-installation configuration

2.1 Installation overview

Use the information in this chapter to ensure the Healthcare Data Repository application is installed and configured securely. For information about installing and configuring the Healthcare Data Repository application, see the *Installation Guide*.

Secure Socket Layer (SSL)

To encrypt the transmission of data between the application server and the applications that consume HDR APIs, you must enable the Secure Socket Layer (SSL) port on the HDR managed server and obtain an X.509 certificate using your company certificate store or a third party to configure the HDR managed server SSL certificates.

Configure strong database passwords

When you install the Healthcare Data Repository application, a system database administrator user is created. Only a system database administrator can perform the installation. Ensure all your database schema passwords for HDR, ETS and HDR_CONFIG users are strong passwords.

Close all unused ports

Keep only the minimum number of ports open. You should close all ports not in use.

The Healthcare Data Repository application uses the following ports:

- WebLogic admin server SSL port for users who administer the HDR application.
- WebLogic managed server SSL port for accessing the HDR.

Disable all unused services

Disable all unknown, unused services running on the HDR WebLogic instance.

2.2 Post-installation configuration

Restrict access to Healthcare Data Repository server machines

Allow only administrator and system accounts access to the Healthcare Data Repository application server and database server machines.

Limit the number of users with access to the server machines. Disable or delete any unnecessary users.

Configure strong user passwords

Configure password options to require a secure level of complexity. For example, a minimum required password length of 8 characters requires users to create more secure and complex passwords than a minimum required password length of 6 characters.

3 Security Features

- User security features
- Application security features
- Data security features

3.1 User security features

Login security

Users must enter their user names and passwords to access the HDR APIs during each client request.

If either a user name or password is incorrect, an error message appears, but does not tell the user the value that is incorrect. Therefore, if someone else is using the account to attempt to log in, the message does not confirm either a user name or password.

No data loss after a session transaction

All HDR services are stateless and none of the services maintain any kind of session information after the API call ends.

Automatically deactivated user accounts

UserLockout can be enabled for the HDR WebLogic user. Refer to `https://docs.oracle.com/middleware/12213/wls/WLACH/pagehelp/Securitysecurityrealmrealmuserlockouttitle.html`.

Security event logs

User authentication logging for HDR application can be done by configuring the WebLogic Auditing Provider. Refer to `https://docs.oracle.com/middleware/12213/wls/SECMG/audit.htm#SECMG137`.

3.2 Application security features

Oracle Healthcare Data Repository relies on WebLogic user authentication to access all its APIs. There is no authorization mandated since more elaborate user authentication and authorization are implemented in the application developed using HDR APIs.

Default user

The Healthcare Data Repository application installs the WebLogic admin user by default. During the installation, you configure a password for this user.

Oracle recommends that you create administrator accounts for individual users and delete the system user after the initial application configuration.

3.3 Data security features

Protecting study objects

You can protect a library or a study to prevent users from making changes to study objects that you do not want to be modified.

When you protect a study or library, changes cannot be made to study objects or to the structure of the study or library.

When a study object is protected, its icon changes to reflect its protected state.

For more information, see the *Implementation Guide*.

Audit trails for data security

Audit trails are comprehensive records that include information about each change that occurs in the Healthcare Data Repository application.

The audit trail for the Healthcare Data Repository application records each change, and for each change:

- Person who made the change.
- Date and time of the change.

You cannot modify data in an audit trail. For more information, see the *User Guide*.

4 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 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.

Oracle Healthcare Data Repository Secure Configuration Guide, Release 8.0
E98319-01

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.