Oracle® Healthcare Precision Medicine

Security Guide

Release 1.0

E74866-01

June 2016

This guide describes various security guidelines for installing Oracle Healthcare Precision Medicine (OHPM). Refer to the Oracle Technology Network (OTN) for the latest version of OHPM user documentation.

It contains the following topics:

1 General Security Principles

The following principles are fundamental to using any application securely.

1.1 Keeping Software Up To Date

One of the principles of good security practice is to keep all software versions and patches up to date. Ensure that you are current on CPUs.

1.2 Staying Up To Date on Latest Security Information Critical Patch Updates

Oracle continually improves its software and documentation. Critical Patch Updates are the primary means of releasing security fixes for Oracle products to customers with valid support contracts. They are released on the Tuesday closest to the 17th day of January, April, July and October. We highly recommend customers apply these patches as soon as they are released.

1.3 Configuring Strong Passwords on the Database

Although the importance of passwords is well known, the following basic rule of security management is worth repeating:

Ensure all your passwords are strong passwords.

You can strengthen passwords by creating and using password policies for your organization. For guidelines on securing passwords and for additional ways to protect passwords, refer to the *Oracle® Database Security Guide* specific to the database release you are using.

You should modify the following passwords to use your policy-compliant strings:

- Passwords for the database default accounts, such as SYS and SYSTEM.
- Passwords for the database application-specific schema accounts, such as HDM.
- Password for the database listener. You should not configure a password for the database listener as that will enable remote administration. For more information, refer to the *Removing the Listener Password* section of *Oracle® Database Net Services Reference 12c Release 12.1.0.2.0*

1.4 Following the Principle of Least Privilege

The principle of least privilege states that users should be given the least amount of privilege to perform their jobs. Overly ambitious granting of responsibilities, roles, grants — especially early on in an organization's life cycle when people are few and work needs to be done quickly — often leaves a system wide open for abuse. User privileges should be reviewed periodically to determine relevance to current job responsibilities.

2 Security Guidelines for Database Objects and Database Options

This section describes security guidelines for OHPM database objects and database options.

2.1 Oracle Healthcare Precision Medicine Objects

OHPM contains database objects. Use DDL scripts, PL/SQL procedures and functions to create database objects and DML scripts to create seed data. These files are available as part of the media pack.

The guidelines for installing and configuring the Oracle Database Server are available at the following location:

http://docs.oracle.com/database/121/nav/portal_11.htm

2.2 Oracle Database Options

Oracle Database includes options that provide additional security features. OHPM may include data that falls under HIPAA guidelines in the United States and similar guidelines elsewhere. These features can help you comply with those guidelines.

Database Vault

OHPM includes data that may fall under HIPAA or other regulations outside the United States. This data is highly sensitive and only those with a need to know should have access to it. To prevent unauthorized users from viewing the data, Oracle recommends that you use the Oracle Database Vault to limit access to the OHPM schema to the OHPM user.

Note: Database Vault requires a separate license.

Oracle Audit Vault

Oracle Audit Vault automates the audit collection, monitoring, and reporting process, turning audit data into a key security resource for detecting unauthorized activity.

Consider using this feature to satisfy compliance regulations such as SOX, PCI, and HIPAA, and to mitigate security risks. OHPM sets the client identifier in the database session to allow identification of the end user.

Note: Oracle Audit Vault requires a separate license.

Transparent Data Encryption

Transparent Data Encryption is one of the three components of the Oracle Advanced Security option for Oracle Database 112c. It provides transparent encryption of stored data to support your compliance efforts. If you employ Transparent Data Encryption, applications do not have to be modified and continue to work seamlessly as before. Data is automatically encrypted when it is written to the disk and automatically decrypted when accessed by the application. Key management is built in, eliminating the complex task of creating, managing and securing encryption keys.

Note: The Advanced Security Option is licensed separately from the database.

Tablespace Encryption

Tablespace Encryption is another component of the Oracle Advanced Security option for Oracle Database 12c. Tablespace encryption facilitates encryption of the entire tablespace contents, rather than having to configure encryption on a column-by-column basis. It encrypts data at the datafile level to keep users from viewing Oracle datafiles directly. Oracle recommends that you perform tablespace encryption for maximum protection.

User Management

WebLogic Server supports several authentication security providers, for example, LDAP. For more information, see the Oracle Fusion Middleware documentation for Administering Security for Oracle WebLogic Server at

http://docs.oracle.com/middleware/1213/wls/SECMG/default_atn.htm#SECMG174

OHPM supports any authentication security providers supported by WebLogic Server 12c (12.1.3).

3 Revoking Unnecessary Grants

For security purposes, you must revoke all unnecessary grants on the schema (grants that are needed during installation and are not required during runtime).

4 Disabling Unnecessary Operating System Level Services

This section suggests various unused operating system level services that you can disable to improve security.

4.1 Disabling the Telnet Service

OHPM does not use the Telnet service.

Telnet listens on port 23 by default. If the Telnet service is available on any computer, Oracle recommends that you disable Telnet in favor of Secure Shell (SSH). Telnet, which sends clear-text passwords and user names through a log-in, is a security risk to your servers. Disabling Telnet tightens and protects your system security.

4.2 Disabling Other Unused Services

OHPM does not use the following services or information for any functionality:

- Simple Mail Transfer Protocol (SMTP). This protocol is an Internet standard for E-mail transmission across Internet Protocol (IP) networks.
- Identification Protocol (identd). This protocol is generally used to identify the owner of a TCP connection on UNIX.
- Simple Network Management Protocol (SNMP). This protocol is a method for managing and reporting information about different systems.
- File transfer Protocol (FTP). This protocol is used for downloading or uploading files from the file server.

Therefore, restricting these services or information does not affect the use of OHPM. If you are not using these services for other applications, Oracle recommends that you disable these services to minimize your security exposure. If you need SMTP, identd, or SNMP for other applications, upgrade to the latest version of the protocol to provide the most up-to-date security for your system.

5 Designing Multiple Layers of Protection

When designing a secure deployment, design multiple layers of protection. If a hacker should gain access to one layer, such as the application server, this should not automatically give them easy access to other layers, such as the database server.

Providing multiple layers of protection may include:

- Enabling only those ports required for communication between different tiers, for example, only allowing communication to the database tier on the port used for SQL*NET communications, (1521 by default).
- Placing firewalls between servers so that only expected traffic can move between servers.

6 Security Guidelines for Oracle Data Integrator

While installing and configuring the Oracle Data Integrator (ODI) Server, follow the guidelines documented in section *Managing Security in Oracle Data Integrator* in the document *Oracle® Fusion Middleware Developer's Guide for Oracle Data Integrator 12c.*

7 Security Guidelines for the Middle Tier

This section describes the security guidelines for the OHPM middle tier.

7.1 Removing Unused Applications from WebLogic

Currently, the WebLogic Server installation includes the entire JDK and some additional WebLogic Server development utilities (for example, wlsvc). These development programs are not needed at runtime and can be safely removed. The following are recommendations for making a WebLogic Server installation more secure:

- Do not install the WebLogic Server sample applications.
- Delete development tools, such as the Configuration Wizard and the jCOM tools.
- Delete the Derby database, which is bundled with WebLogic Server for use by the sample applications and code examples as a demonstration database.

For more details, refer to the Determining Your Security Needs section in *Oracle® Fusion Middleware Securing a Production Environment for Oracle WebLogic Server 12c (12.1.3)*

7.2 Enabling TLS

To create an unique private identity key and trust certificate, TLS is not enabled by default during the installation. Communications between the browser and the application servers should be restricted to TLS.

It is optional to enable TLS, but Oracle recommends TLS for a production environment.

To enable TLS:

1. Log into WebLogic Server Administration Console.
2. Click the **Environment** node in the Domain Structure pane and click **Servers** in Environment table.
3. Click the server where you deployed the .ear file.
4. Click the **Configuration** tab.
5. Click the **General** tab.
6. If Save is disabled, click **Lock & Edit** in the Change Center pane.
7. Select the **SSL Listen Port Enabled** check box and enter a port number.
8. To disable non-SSL port, deselect the **Listen Port Enabled** check box.
9. Click **Save.**
10. Click **Activate Changes** in the Change Center pane, if it is enabled.
11. Click the **Control** tab.
12. Click the **Start/Stop** tab.
13. Click **Restart SSL**
14. Click **Yes.**

    The *TLS channels have been successfully restarted.* message appears.

You must also configure SSL, identity, and trust. For more information, refer to *Oracle® Fusion Middleware Securing Oracle WebLogic Server 12c (12.1.3).*

7.3 Configuring TLS

To set up TLS, perform the following steps:

1. Obtain an identity (private key and digital certificates) and trust (certificates of trusted certificate authorities) for WebLogic Server. Use the digital certificates, private keys, and trusted CA certificates provided by WebLogic Server, the CertGen utility, the keytool utility, or a reputable vendor such as Entrust or Verisign to perform this step.
2. Store the identity and trust. Private keys and trusted CA certificates which specify identity and trust are stored in keystores.
3. Configure the identity and trust keystores for WebLogic Server in the WebLogic Server Administration Console.
4. Set SSL configuration options for the private key alias and password in the WebLogic Server Administration Console. Optionally, set configuration options that require the presentation of client certificates (for two-way SSL).
5. As per Oracle Software Security standards, it is recommended that you disable *weak SSL cyphers*, that is, TLS lower than v1.1 and SSL v3 and v2.

For more details, refer to Configuring SSL section in *Oracle® Fusion Middleware Securing Oracle WebLogic Server 12c (12.1.3)*.

7.4 Protecting User Accounts

WebLogic Server defines a set of configuration options to protect user accounts from intruders. In the default security configuration, these options are set for maximum protection. You can use the Administration Console to modify these options on the **Configuration** > **User Lockout** page.

As a system administrator, you have the option of turning off all the configuration options, increasing the number of login attempts before a user account is locked, increasing the time period in which invalid login attempts are made before locking the user account, and changing the amount of time a user account is locked. Remember that changing the configuration options lessens security and leaves user accounts vulnerable to security attacks. For more details, refer to Configuring Security for a WebLogic Domain section in *Oracle® Fusion Middleware Securing Oracle WebLogic Server 12c (12.1.3)*.

7.4.1 Password Validation Providers

WebLogic Server includes a Password Validation provider, which is configured by default in each security realm. The Password Validation provider manages and enforces a set of configurable password composition rules, and is automatically invoked by a supported authentication provider whenever a password is created or updated for a user in the realm. When invoked, the Password Validation provider performs a check to determine whether the password meets the criteria established by the composition rules. The password is then accepted or rejected as appropriate. For more information on the Password Validation provider, see the *Oracle® Fusion Middleware Administering Security for Oracle WebLogic Server 12c (12.1.3)*.

8 Protecting Data

Data is vulnerable at many points in any computer system, and many security techniques and types of functionality can be employed to protect it.

9 Setting Up Fine Grain Audit Policy

The OHPM application has 3 different schemas:

- Schema for OHPM
- Application schema used by the Oracle Health Sciences Translational Research application user interface

Oracle recommends that only the OHPM schemas have audit policies. There is no need to log unwarranted access to the application schema. The package used to create each policy is the DBMS_FGA package. This package lets you create specific policies for each table. Oracle recommends that the policy names match each table name that is to be audited. This allows for simple identification of audit policies for each table. The audit policies must be defined for `INSERT`, `DELETE`, or `UPDATE` operations.

To move PHI data in the OHPM Schema, Oracle recommends that you have auditing enabled for `Select` operations. Also, the columns that are audited must be left `NULL` to audit all columns that are accessed. The default value for any column change must be left as is. The mode used to record information must be set to DB + extended or XML extended in order to log the exact SQL statement and bind variables. This is important to detect which data may is affected. Refer to the Oracle database documentation, for a detailed description of the DBMS_FGA package.

There are initialization parameters to specify where the audit logs are stored. Oracle recommends that the audit logs be stored in a separate tablespace and preferably on a different disk so as to not interfere with other database operations which may need high throughput of the disks with real data. Information about parameters for audit log storage can also be found in the Oracle database documentation.

Oracle recommends that a general audit mode be set to audit each logon to the database as the actual DBA password could be compromised and you may want to disable audit policies. Setting up an audit policy to log all log on operations to the database is always a very good idea in production databases.

Here is an example of the SQL to set up an audit policy:

```
begin
DBMS_FGA.ADD_POLICY(
object_schema=>'ODB',
object_name=>'W_EHA_GENE',
policy_name=>'W_EHA_GENE',
enable=>true,
statement_types=>'INSERT,UPDATE,DELETE'
);
end;
```

For more information on setting up the audit policy, refer to *Oracle Database Online Documentation 11g Release 2 (11.2)* at http://www.oracle.com/pls/db112/homepage.

10 Disclaimer

The Oracle Healthcare Precision Medicine software is only a search tool and is not intended to, and must not replace the clinician's judgment or experience. Furthermore, the healthcare professional using this search tool should employ their professional judgment concerning the reliability and accuracy of the information in the various knowledge databases that are employed or selected as content for reports generated using Oracle Healthcare Precision Medicine.

11 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 Precision Medicine Security Guide, Release 1.0
E74866-01