Oracle® Healthcare Master Person Index

Security Guide

Release 4.0

E68425-01

February 2016

This document provides the security guidelines that must be followed to use the Oracle Healthcare Master Person Index (OHMPI) application. It includes the following sections:

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.

1.2 Keeping 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 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® WebLogic Portal 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 RXI.
- The password for the database listener. Oracle recommends that you do not configure a password for the database listener as that will enable remote administration. For more information, refer to *Oracle® Database Net Services Reference 12c Release 1 (12.1)*.

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.

1.5 Managing Default User Accounts

Lock and expire default user accounts.

1.6 Closing All Open Ports Not in Use

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

1.7 Disabling the Telnet Service

OHMPI does not use the Telnet service.

By default, Telnet listens on port 23.

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.

1.8 Disabling Other Unused Services

In addition to not using Telnet, OHMPI 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.

Restricting these services or information does not affect the use of OHMPI. 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, ensure that you upgrade to the latest version of the protocol to provide the most up-to-date security for your system.

1.9 Designing for 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, that should not automatically give them easy access to other layers, such as the database server.

Providing multiple layers of protection may include:

- Enable 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).
- Place firewalls between servers so that only expected traffic can move between servers.

1.10 Enabling SSL

Due to the complexity in setting up SSL it is not enabled by default during installation. Communications between the browser and the application servers should be restricted to SSL. For instructions on enabling SSL, see the Oracle WebLogic Server 12c guidelines or Section 4.2, "Enabling SSL".

You must start the Oracle WebLogic Server with a parameter to exclude SSL 2.0 and/or SSL 3.0 to in order to mitigate the SSL V3.0 "Poodle" Vulnerability, CVE-2014-3566. For more information, see *How to Change SSL Protocols (to Disable SSL 3.0) in Oracle Fusion Middleware Products* (Doc ID 1936300.1) on My Oracle Support (`https://support.oracle.com`). Oracle recommends that you disable the insecure SSL and TLS protocols, such as SSLv1, SSLv2, SSLv3, and TLSv1.0 and below.

2 Protected Health Information

OHMPI may include protected health information (PHI) that falls under HIPAA guidelines in the United States and similar guidelines elsewhere. If you have concerns over such data, the configuration measures can help you comply with those guidelines by masking sensitive information. To mask the sensitive data (PHI) within MIDM application, you must configure the Master Index Data Manager Security. For information on MIDM Security, see *Oracle Healthcare Master Person Index Data Manager User's Guide*.

3 Security Guidelines for Database Objects and Database Options

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

3.1 Oracle Database Options

The Oracle Database has options that provide additional security features. OHMPI 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

OHMPI includes data that may fall under HIPAA or other regulations outside the United States. These data are highly sensitive and only those with a need to know should have access to it. To prevent DBAs and others from seeing the data, Oracle recommends that Oracle Database Vault must be used to limit access to the OHMPI schema for the OHMPI user to prevent DBAs and other "superuser" accounts from accessing the data.

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.

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 11gR2 (11.2.0.1.0) and Oracle Database 12cR1 (12.1.0.2.0) Enterprise Editions. 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 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 11gR2 (11.2.0.1.0) and Oracle Database 12cR1 (12.1.0.2.0) Enterprise Editions. 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 data file level to keep users from viewing the oracle data files directly. Oracle recommends that you perform tablespace encryption for maximum protection.

4 Security Guidelines for the Middle-Tier

After you import the projects, ensure that the data source connection, JMS Servers, and JMS Topics are created in Oracle WebLogic Server console and the user(s) created in Oracle WebLogic Server are assigned to the MasterIndex.Admin group.

4.1 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 Release 3 (12.1.3)*.

4.2 Enabling SSL

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

To enable SSL:

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 OHMPI_App.ear.
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 "SSL 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 Release 3 (12.1.3)*.

4.3 Configuring SSL

To setup SSL, 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).

For more details, refer to Configuring SSL section in *Oracle® Fusion Middleware Securing Oracle WebLogic Server 12c Release 3 (12.1.3)*.

4.4 Allowing Only Known Host

Allowing only known IP's to access the OHMPI application would prevent it to be crawled by search engines and only let customers access the application. This can be done by restricting access from customer's public IP's.

For more information, see *Access Control section in Oracle® Fusion Middleware Administrator's Guide* for Oracle HTTP Server Release 1 (11.1.1). (`http://docs.oracle.com/cd/E23943_01/web.1111/e10144/security.htm#CDDBCEJI`).

4.5 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 to turn 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 *Oracle® Fusion Middleware Securing Oracle WebLogic Server 12c Release 3 (12.1.3)*.

4.6 Creating MIDM User Accounts for Web Service on WebLogic

In the following steps you create the `MasterIndex.Admin` group, and then create a new user:

1. On the left panel, under Domain Structure, expand **Services**, and then choose **Security Realms**.
2. In the table on the Summary of Security Realms panel, click **myrealm**, which is the name of the realm.

   The Settings for myrealm panel appears.
3. Select the **Users and Groups** tab and then click **Groups**.
4. In the Groups table, click **New**.
5. In the Name field, type `MasterIndex.Admin` (if it does not exist) and click **OK**.
6. On the Settings for myrealm panel, select **Users and Groups** and then **Users**.
7. In the Users table, click **New**.

8. Type `MasterIndex.WSUser` and a password of your choice for the new user that you are creating.

9. Click **OK**.

10. Select **User Group**.

11. To add the user you created, drag **MasterIndex.Admin** from the **Available** list to the **Chosen** list.

4.7 Setting Up the User for MIDM Access Using WebLogic

In the following steps you create the MasterIndex.Admin and Administrator groups, and then create a new user within the two groups. Use the user you create for MIDM access using the WebLogic Admin Console.

1. On the left panel, under Domain Structure, expand **Services**, and then choose **Security Realms**.

2. In the table on the Summary of Security Realms panel, click **myrealm**, which is the name of the realm.

   The Settings for myrealm panel appears.

3. Select the **Users and Groups** tab and then click **Groups**.

4. In the Groups table, click **New**.

5. In the Name field, type `MasterIndex.Admin` and click **OK**.

6. In the Groups table, click **New**.

7. In the Name field, type `Administrator` and click **OK**.

8. On the Settings for myrealm panel, select **Users and Groups** and then **Users**.

9. In the Users table, click **New**.

10. Type a name and a password for the new user you are creating and click **OK**.

11. Select **User Group**.

12. To add the two groups you created to the user you created, from the Available list, drag **MasterIndex.Admin** to the **Chosen** list, and then drag Administrator to the **Chosen** list.

5 Restricting Access to Sensitive Files and Directories

Oracle recommends that you limit the access to the files and directory containing sensitive information. In Linux environment, default the files and directories to 750 or 640 permissions, as applicable.

The following are the sensitive files:

- <WebLogic_Home>/user_projects/domains/<domain_name>/config/config.xml
- <WebLogic_Home>/user_projects/domains/<domain_name>/config/*
- <WebLogic_Home>/user_projects/domains/<domain_name>/servers/AdminServer/logs
- <WebLogic_Home>/user_projects/domains/<domain_name>/servers/<ManagedServerName>/logs

- <WebLogic_Home>/user_projects/domains/<domain_name>/<OHMPI_OracleWallet_Files>
- IBML and Profiler directories
- Real-time Loader installation directories
- Directories where MPI and RM database scripts are copied, updated, and executed
- Relationship Management MPI Agent Wallet files
- IHE HL7v2 folder

6 Finding Information and Patches on My Oracle Support

Your source for the latest information about OHMPI is Oracle Support's self-service Web site My Oracle Support (formerly MetaLink).

Before you install and use OHMPI, always visit the My Oracle Support Web site for the latest information, including alerts, White Papers, installation verification (smoke) tests, bulletins, and patches.

6.1 Creating My Oracle Support Account

You must register at My Oracle Support to obtain a user name and password account before you can enter the website.

To register for My Oracle Support:

1. Open a Web browser to `https://support.oracle.com`.
2. Click the **Register here** link to create a My Oracle Support account. The registration page opens.
3. Follow the instructions on the registration page.

6.2 Signing In to My Oracle Support

To sign in to My Oracle Support:

1. Open a Web browser to `https://support.oracle.com`.
2. Click **Sign In.**
3. Enter your user name and password.
4. Click **Go** to open the My Oracle Support home page.

6.3 Finding Information on My Oracle Support

There are many ways to find information on My Oracle Support.

6.3.1 Searching by Article ID

The fastest way to search for information, including alerts, White Papers, installation verification (smoke) tests, and bulletins is by the article ID number, if you know it.

To search by article ID:

1. Sign in to My Oracle Support at `https://support.oracle.com`.
2. Locate the Search box in the upper right corner of the My Oracle Support page.

3. Click the sources icon to the left of the search box, and then select **Article ID** from the list.
4. Enter the article ID number in the text box.
5. Click the magnifying glass icon to the right of the search box (or press the Enter key) to execute your search.

   The Knowledge page displays the results of your search. If the article is found, click the link to view the abstract, text, attachments, and related products.

6.3.2 Searching by Product and Topic

You can use the following My Oracle Support tools to browse and search the knowledge base:

- Product Focus — On the Knowledge page under Select Product, type part of the product name and the system immediately filters the product list by the letters you have typed. (You do not need to type "Oracle.") Select the product you want from the filtered list and then use other search or browse tools to find the information you need.
- Advanced Search — You can specify one or more search criteria, such as source, exact phrase, and related product, to find information. This option is available from the **Advanced** link on almost all pages.

6.4 Finding Patches on My Oracle Support

Be sure to check My Oracle Support for the latest patches, if any, for your product. You can search for patches by patch ID or number, or by product or family.

To locate and download a patch:

1. Sign in to My Oracle Support at `https://support.oracle.com`.
2. Click the **Patches & Updates** tab. The Patches & Updates page opens and displays the Patch Search region. You have the following options:
   - In the **Patch ID or Number is** field, enter the number of the patch you want. (This number is the same as the primary bug number fixed by the patch.) This option is useful if you already know the patch number.
   - To find a patch by product name, release, and platform, click the **Product or Family** link to enter one or more search criteria.
3. Click **Search** to execute your query. The Patch Search Results page opens.
4. Click the patch ID number. The system displays details about the patch. In addition, you can view the Read Me file before downloading the patch.
5. Click **Download.** Follow the instructions in the patch Read Me to install the patch.

7 Finding Oracle Documentation

The Oracle Web site contains links to all Oracle user and reference documentation. You can view or download a single document or an entire product library.

7.1 Finding Oracle Health Sciences Documentation

To get user documentation for Oracle Health Sciences applications, go to the Oracle Health Sciences documentation page at:

http://www.oracle.com/technetwork/documentation/hsgbu-154445.html

Always check the Oracle Health Sciences Documentation page to ensure you have the latest updates to the documentation.

7.2 Finding Other Oracle Documentation

To get user documentation for other Oracle products:

1. Go to the following Web page:

   http://www.oracle.com/technology/documentation/index.html

   Alternatively, you can go to http://www.oracle.com, point to the Support tab, and then click **Documentation**.

2. Scroll to the product you need and click the link.
3. Click the link for the documentation you need.

8 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 Master Person Index Security Guide, Release 4.0
E68425-01