Oracle® Health Sciences Information Manager

Security Guide

Release 3.0

E61285-01

March 2015

This guide describes important security management options for Oracle Health Sciences Information Manager (HIM).

1 Introduction

This guide presents the following security guidelines and recommendations:

- Section 2, "Configuring Strong Passwords on the Database"
- Section 3, "Restricting Access to Sensitive Files and Directories"
- Section 4, "Securing Policy Monitor"
- Section 5, "Using SSL"
- Section 6, "Closing All Unused Open Ports"
- Section 7, "Keeping Telnet Service Disabled for Remote Session"
- Section 8, "Keeping Other Unused Services Disabled"

ORACLE

2 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.

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.
- Database application-specific schema accounts, such as ADT, HRLCORE, LOG, DUSB, XPID, ARRUSER, and GATEWAY.

> **Note:** Ensure that you do not set a password for the database listener in the listener.ora file. The local operating system authentication will secure the listener administration. The remote listener administration is disabled when the password is not set. This prevents brute force attacks on the listener password.

3 Restricting Access to Sensitive Files and Directories

Oracle recommends limiting the access to the files and directory containing sensitive information. In Linux environment, default files and directories to 740 or 640 permissions as applicable.

Some of the sensitive files are listed below:

- <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

4 Securing Policy Monitor

To secure Policy Monitor:

- Restrict the access to Policy Monitor directory and further restrict and control access to the following files:
  - Input parameter
  - Key and Trust stores
- Always encrypt passwords in input parameter file(s) using AES or RSA ciphers.
- Avoid using UDP server in production. Oracle recommends using TLS server.
- Never use TCP server in production.

5 Using SSL

Oracle recommends using two-way SSL while using WebLogic Application Server. HRL and XCA Gateway applications are standard Java EE applications and can utilize an industry standard security infrastructure and framework. There is no configuration required on the applications. The WebLogic Application Server provides SSL service. For more information about configuring SSL, see the Application Server's documentation.

When SSL or TLS is configured, it is recommended to use TLS_RSA_WITH_AES_128_CBC_SHA cipher instead of SSL_RSA_WITH_DES_EDE_CBC_SHA for TLS authentication.

Oracle recommends that you disable the insecure SSL and TLS protocols, such as SSLv1, SSLv2, SSLv3, and TLSv1.0 and below.

6 Closing All Unused Open Ports

Keep only the minimum number of ports open. You should close ports that are not in use. Configure HRL, PM, and XCA Gateway servers with only minimum number of required ports.

7 Keeping Telnet Service Disabled for Remote Session

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

8 Keeping Other Unused Services Disabled

HRL, PM, and XCA Gateway servers do not use following protocols, services, or information for its functionality:

- **Identification Protocol (identd)**: Identifies the owner of a TCP connection on UNIX.
- **Simple Network Management Protocol (SNMP)**: Manages and reports information about different systems.
- **File Transfer Protocol (FTP)**: Transfers or copies file from one host to another. FTP is inherently insecure and should be disabled.

9 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.

Oracle Health Sciences Information Manager Security Guide, Release 3.0
E61285-01

Copyright © 2012, 2015, Oracle and/or its affiliates. All rights reserved.

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, the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. 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 Xeon 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, Opteron, the AMD logo, and the AMD Opteron 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.