Oracle® Health Sciences Information Manager

Security Guide

4.0
F50773-01
January 2022

Oracle Health Sciences Information Manager Security Guide, 4.0

F50773-01

Contents

Preface

This preface contains the following sections:

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.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Related resources

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

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.

1

Security Guidelines

This guide provides details on security guidelines and recommendations.

- Configure strong passwords
  Although the importance of passwords is well known, the following basic rule of security management is worth repeating: **Ensure all your passwords are strong**
- Restrict 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.
- Secure Policy Monitor
  You must secure Policy Monitor to protect data.
- Use two-way 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.
- Close unused open ports
  Keep only the minimum number of ports open. Close ports that are not in use.
- Keep Telnet service disabled for remote sessions
  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.
- Keep other unused services disabled
  To ensure security, disable unused services.
- Integrate application-generated logs
  Use a centralized log monitoring tool that collects application-generated logs from Oracle Health Sciences Information Manager.

Configure strong passwords

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.

Restrict 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

Secure Policy Monitor

You must secure Policy Monitor to protect data.

To secure Policy Monitor:

- Restrict the access to Policy Monitor directory and further restrict and control access to the following files: **Input parameter** and **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.

Use two-way 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.

For instructions on enabling SSL, see the Oracle WebLogic Server 12c guidelines or Enable SSL (for middle tier). 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/TLS Protocols in Oracle WebLogic Server - Disable SSL 2.0/3.0 and Enable TLS 1.x Options* (Doc ID 2162789.1) on My Oracle Support (https://support.oracle.comhttps://support.oracle.com). Oracle recommends that you disable the insecure SSL and TLS protocols, such as SSLv1, SSLv2, SSLv3, and TLSv1.0 and earlier.

Close unused open ports

Keep only the minimum number of ports open. Close ports that are not in use.

Configure HRL, PM, and XCA Gateway servers with only minimum number of required ports.

Keep Telnet service disabled for remote sessions

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.

Keep other unused services disabled

To ensure security, disable unused services.

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.

Integrate application-generated logs

Use a centralized log monitoring tool that collects application-generated logs from Oracle Health Sciences Information Manager.