Oracle® Health Sciences Information Gateway

Security Guide

Release 2.0.1

E37114-02

October 2013

This guide describes important security management options for Oracle Health Sciences Information Gateway (HIG).

1 Introduction

This guide presents the following security guidelines and recommendations:

- Configuring Strong Passwords on the Database
- Changing the Default Apache James Server's Root Password
- Restricting Access to Sensitive Files and Directories
- Securing the Oracle Databases
- Using SSL
- Configuring Other Apache James Parameters to Secure Health Email Server
- Closing All Unused Open Ports
- Keeping Telnet Service Disabled for Remote Session
- Keeping Other Unused Services Disabled

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 JAMESUSER and DIRECTUSER.

> **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 Changing the Default Apache James Server's Root Password

To prevent unauthorized access to Apache James Admin Console, Oracle recommends that you change the James admin password (sometimes referred to as the "root" password) immediately after configuring the Oracle Secure Health Email server. Oracle has extended the Apache James Server to read encrypted password stored in config.xml.

To change and encrypt the password, refer to the *Secure Health Email Installation and Configuration Guide Release 2.0.1, section H, Password Encoding*.

Since the administrative passwords are present in the Apache James config.xml file (<james_home>/apps/james/SAR-INF/config.xml), the OS user should have readable permissions on the Apache James server.

4 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:

- Apache James:

  Below files have encrypted passwords or reference to them.

  - `config.xml` file under `<james_home>apps/james/SAR-INF`
  - `beans.xml` under `<james_home>/bin/`
  - `config.properties` under `<james_home>/bin/`

- Log files are stored under the following directories:

    - `<james_home>/temp/`
    - `<james_home>/apps/james/logs/`
- GlassFish:
    - `<GlassFish_home>/domains/<domain_name>/config/domain.xml`
    - `<GlassFish_home>/domains/<domain_name>/logs`

5 Securing the Oracle Databases

The Oracle Secure Health Email server deals with sensitive and personal information. It is recommended to take all necessary steps to secure the Oracle database used for storing emails, inbox, as well as database used as OHIM Public Key Directory, for storing keys, certificates, and trust anchors of users.

Oracle recommends securing these database servers. Use TDE (Transparent Data Encryption) to protect the credentials and email stores. Note that TDE is part of the Oracle Advanced Security Option and is an additional cost. To protect this information from the DBA, use the Oracle Data Vault (also an additional cost option).

6 Using SSL

Oracle recommends to configure the Oracle Secure Health Email server to be used with SSL connections. The following are the configuration steps:

- Edit ssl server socket factory and update it with the correct keystore path and passwords.
- Enable both smtpserver and pop3server for TLS use.
- If you are connecting to remote SMTP gateway or SMTP server through SSL, ensure to specify javax.net.ssl.SSLSocketFactory to be used as socket factory by "ExtendedRemoteDelivery" mailet.

For more details, refer to *Oracle Secure Health Email Installation and Configuration Guide, Release 1.2, E22884-01* and the following Apache James 2.3.2 Wiki pages:

- `http://james.apache.org/server/2.3.2/usingTLS.html`
- `http://james.apache.org/server/2.3.2/smtp_configuration.html`
- `http://james.apache.org/server/2.3.2/pop3_configuration.html`

Oracle recommends using two-way SSL while using GlassFish or WebLogic application servers. CONNECT Gateway, Adapters, and XCA Gateway applications are standard Java EE application and can utilize an industry standard security infrastructure and framework. There is no configuration required on the applications. The application Server (WebLogic or GlassFish) 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_3DES_EDE_CBC_SHA for TLS authentication.

7 Configuring Other Apache James Parameters to Secure Health Email Server

The Secure Health Email Server is built on top of Apache James Server and the VM template is configured with the following parameter to improve security. Oracle recommends that you continue to use the following configurations.

config.xml (<james_home>/apps/james/SAR-INF/) file elements.

Table 1 Apache James Parameters

XPath to Configuration Element	Description
/config/smtpserver/handler/authRequired	Enables SMTP authentication
/config/smtpserver/handler/authorizedAddresses	Authorizes specific addresses or networks
/config/smtpserver/handler/verifyIdentity	Verifies sender addresses, ensuring that the sender address matches the authenticated user

8 Closing All Unused Open Ports

Keep only the minimum number of ports open. You should close ports that are not in use. Configure Secure Health Email server with only minimum number of required ports.

If you are using standard SMTP and POP3 ports then you may want to open port 25 and 110. If you change these default standard ports in Apache James configuration file, ensure you close unused standard ports.

9 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.

10 Keeping Other Unused Services Disabled

Secure Health Email server, CONNECT Gateway, Adapter, and XCA Gateway servers does 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.
- **Network News Transfer Protocol (NNTP)**: Apache James 2.3.2 server supports NNTP apart from SMTP and POP3 protocols. NNTP is an Internet application protocol used for transporting Usenet news articles between news servers and for reading and posting articles by end-user client applications.

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 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 Gateway Security Guide, Release 2.0.1
E37114-02