1 Introduction

OHADI processes data from diverse source systems and loads the homogenized, consistent, complete, correct, and standardized data into HDWF for analysis.

2 General Security Principles

The following principles are fundamental to using any application securely.

2.1 Keeping Software Up To Date

One of the principles of good security practices is to keep all software versions and patches up to date.

2.2 Keeping Up To Date on the 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 to apply these patches as soon as they are released.

2.3 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® 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, HDI, and HMC.
- The password for the database listener. You must not configure a password for the database listener as that will enable remote administration. For more information, refer to *Removing the Listener Password of Oracle® Database Net Services Reference 11g Release 2 (11.2)*.

### 2.4 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.

Before executing DDL scripts to create HMC schema, a database user should be created with specified limited set of privileges. DBA access should not be given to the user.

### 3 Database Security Features

The following principles are fundamental to using any application securely.

#### 3.1 About Database Vault

Oracle Database Vault restricts access to specific areas in an Oracle database from any user, including users who have administrative access. For example, you can restrict administrative access to employee salaries, customer medical records, or other sensitive information.

#### 3.2 About Audit Vault

Oracle Audit Vault automates the audit collection, monitoring and reporting process. It turns 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.

#### 3.3 About Tablespace Encryption

Transparent Data Encryption is one of the three components of the Oracle Advanced Security option for Oracle Database 11.2.0.4 Enterprise Edition. It provides transparent encryption of stored data to support your compliance efforts. Applications do not have to be modified and will 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 to the Tablespace Encryption feature, eliminating the complex task of creating, managing and securing encryption keys.
3.4 Managing Default User Accounts
Schema owner should not be the user used for normal production; instead the account should be locked after the installation.

3.5 Closing All Open Ports Not in Use
Keep only the minimum number of ports open and close all ports that are not in use.

3.6 Disabling the Telnet Service
Oracle Healthcare Analytics Data Integration Configuration 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.

3.7 Disabling Other Unused Services
In addition to not using Telnet, the Oracle Healthcare Analytics Data Integration configuration 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 Oracle Healthcare Analytics Data Integration Configuration. 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, be sure to upgrade to the latest version of the protocol to provide the most up-to-date security for your system.

3.8 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.
3.9 Security Guidelines for Informatica Server

Since OHADI processes clinical and healthcare information that contains sensitive patient information, you must configure the Informatica server for maximum security. Follow the security guidelines provided in the Informatica user documentation.

3.10 Configuring Secure SQL NET

If Informatica is installed in a database server other than the server having HDWF schema, the data transfer will take place between two different database servers over a network. As HDWF contains sensitive clinical and healthcare data, you must secure the communication between database servers. Use Oracle® Net Manager to configure encryption to secure communication between database servers. Oracle provides different encryption algorithms to secure communication. Select an appropriate encryption algorithm. For more information, refer to Oracle® Database Advanced Security Administrator’s Guide 11g Release 2 (11.2).

4 Configuring Proxy Schema

OHADI supports data loading through a proxy user to protect business data. This is an optional configuration. If you do not want to load data through proxy user, you can skip this section. When configured, ETL uses proxy user to read data from the interface schema and write to the HDWF schema. It is important that the proxy user is created in the DB instance where HDWF is installed.

4.1 Configuring Proxy User

Perform the following steps for proxy user configuration:

1. Create a proxy schema user with an appropriate default tablespace with requisite quotas and temporary tablespace.

2. Log in to the SYSTEM user and execute the following scripts at the command prompt:
   @OHADI_PROXY_GRANT_SESSION_PRIVS.sql <name of the proxy schema>;
   @OHADI_PROXY_HDWF_GRANT_PRIVILEGES.sql <name of the interface schema> <name of the HDWF schema> <name of the metadata schema> <name of the proxy schema>;

3. Log in to the PROXY user and execute the following scripts at the command prompt:
   @OHADI_PROXY_CREATE_SYNONYMS.sql <name of the metadata schema> <name of the proxy schema>;}
4. Manually create the proxy schema relational connection <DI_PROXY_INFA_CONNECTION> in the Informatica workflow manager.

5. Configure the values of the following parameters:
   - $DBCONNECTION_ETL=<DI_PROXY_INFA_CONNECTION>
   - $DBCONNECTION_TARGET=<DI_PROXY_INFA_CONNECTION>
   - $DBCONNECTION_SOURCE=<DI_PROXY_INFA_CONNECTION>

   for the ETL parameter file, SIL_DI_Global_Param_File.prm, present at:
   - $PMSourceFileDir\$PMSourceFileDir\DI_HDWF_INITIAL_LOAD\$PMSourceFileDir\DI_HDWF_INCREMENTAL_LOAD\$PMSourceFileDir\DI_HDWF_INITIAL_LOAD_PARTY_AVAILABLE\$PMSourceFileDir\DI_HDWF_INCREMENTAL_LOAD_PARTY_AVAILABLE

6. For HLI, configure the following parameters in $PMSourceFileDir\HLI_ParameterFile.prm:
   - $DBCConnection_Target_HDI=<DI_PROXY_INFA_CONNECTION>
   - $DBCConnection_Config_HMC=<DI_PROXY_INFA_CONNECTION>

5 Switching to Default Configuration from Proxy Schema Configuration

Perform the following steps to revert proxy configuration:

1. Update the following parameters in the $PMSourceFileDir\SIL_DI_Global_Param_File.prm file:
   - $DBCONNECTION_ETL=<DI_ETL_INFA_CONNECTION>
   - $DBCONNECTION_TARGET=<DI_TARGET_INFA_CONNECTION>
   - $DBCONNECTION_SOURCE=<DI_SOURCE_INFA_CONNECTION>

---

**Note:** As initial load runs in the bulk mode, it is necessary to delete indexes and disable constraints before ETL execution and re-create the same after ETL execution. To do this, proxy user is assigned with the following privileges using the OHADI_PROXY_GRANT_SESSION_PREIVS.sql executed in Step 2:

- CREATE ANY INDEX
- DROP ANY INDEX
- ALTER ANY TABLE

These privileges can be revoked after the completion of the initial load or before starting the incremental load by logging into the SYSTEM user and executing the following script at the command prompt:

@OHADI_PROXY_HDWF_REVOKE_PRIV_INIT.sql <name of the proxy schema>;}
2. Copy the file to the OHADI folders mentioned in step 6.

3. For HLI, configure the following parameters in $PMSourceFileDir\HLI_ParameterFile.prm:
   - $DBConnection_Target_HDI=<DI_SOURCE_INFA_CONNECTION>
   - $DBConnection_Config_HMC=<DI_ETL_INFA_CONNECTION>

4. Log in to the OHADI repository through workflow manager and delete the relational connection created for proxy user.

5. Log in to the database as system user and delete proxy schema:

   sqlplus <sys user>@"(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)
   (HOST=<hostname>)(PORT=<port number>))(CONNECT_DATA=(SERVICE_NAME=<service_name>)))" as sysdba
   Enter the password when prompted.
   drop user <name of the proxy schema> cascade;

6 Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at

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.