Oracle® Healthcare Analytics Data Integration

Security Guide

Release 3.1 for Oracle Data Integrator

E63828-01

June 2015

This document contains the following sections:

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 practice 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:

Make sure 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 the section *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 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 Linux.
- 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 Configuring Secure SQL NET

If the Oracle Data Integrator (ODI) repository 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

Proxy schema is a schema through which you can access the main schemas like HDI (interface schema), HDM (HDWF schema), and HMC (metadata schema) with limited access. OHADI ETLs must be executed through a proxy schema. This is an optional feature. To use this feature, you must follow the steps in Section 4.1. This appendix provides information on how to execute ETLs using the proxy schema. It contains the following topics:

4.1 Executing ETLs Using a Proxy Schema

To execute ETLs using a proxy schema, perform the following steps:

1. Navigate to the ohadi_sql directory under OHADI Installation folder and open the command prompt.

   Note: If sqlplus does not work from command prompt, first set the ORACLE_HOME environment variable to Oracle's home directory and use the following syntax to connect to sqlplus:

   Linux:

   ```
   sqlplus <user>@"(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)
   (HOST=<hostname>)(PORT=<portnumber>))(CONNECT_DATA=(SERVICE_
   NAME=<service_name>)))"
   ```

   Enter the password when prompted.

2. Log in as SYS user in database with the following syntax from the command prompt and execute the scripts.

   ```
   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.

3. Create a proxy schema user within the same DB instance where HDWF 6.0 is installed, with an appropriate default tablespace with requisite quotas and temporary tablespace.

4. Execute the following scripts from the SYS user:

```
@OHADI_PROXY_GRANT_SESSION_PREIVS.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 PROXY_SCHEMA>;
```

5. Log in as <*PROXY_SCHEMA*> user in the database by executing the following command in the command prompt and execute the script:

```
sqlplus <proxy schema>@"(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)
(HOST=<hostname>)(PORT=<port number>))(CONNECT_DATA=(SERVICE_
NAME=<service_name>)))"
```

Enter the password when prompted.

```
@OHADI_PROXY_PACKAGE_CREATE_CONTEXT.sql;
```

6. Log in as HDWF user (for example, HDM) in the database using the following commands in the command prompt:

```
sqlplus <hdwf schema>@"(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)
(HOST=<hostname>)(PORT=<port number>))(CONNECT_DATA=(SERVICE_
NAME=<service_name>)))"
```

Enter the password when prompted.

```
@OHADI_PROXY_E_TABLE_SCRIPT_DI_TABLES.sql <name of the HDWF schema>;

@OHADI_PROXY_E_TABLE_SCRIPT_MDM_TABLES.sql;
```

7. Log in as Metadata user (for example, HMC) in the database using the following commands in the command prompt:

```
sqlplus <metadata schema>@"(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)
(HOST=<hostname>)(PORT=<port number>))(CONNECT_DATA=(SERVICE_
NAME=<service_name>)))"
```

Enter the password when prompted.

```
@OHADI_PROXY_E_TABLE_SCRIPT_RULE_TABLES.sql;

@OHADI_PROXY_UPDATE_GLBL_PARAM_TABLE.sql <name of the metadata schema>;
```

8. Log in as SYS user and execute the following script:

```
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.

```
@OHADI_HDWF_CONFIG_GRANT_PRIVILEGES.sql <name of the interface schema>
<name of the HDWF schema> <name of the metadata schema>
```

9. Log in again as SYS user and execute the following script:

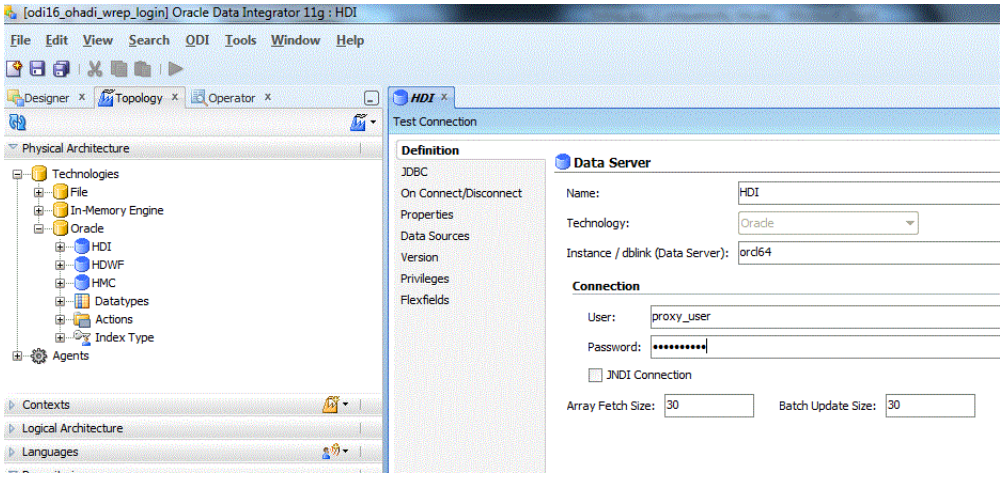
```
sqlplus <sys user>@"(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)
(HOST=<hostname>)(PORT=<port number>))(CONNECT_DATA=(SERVICE_
NAME=<service_name>)))" as sysdba
```

Enter the password when prompted.

```
@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 PROXY_SCHEMA>;
```

10. In ODI, log in to OHADI work repository and navigate to **Topology > Physical Architecture > Technologies > Oracle**.
11. Click the HDI data server. Modify the following options:
    - User - <name of the proxy schema>
    - password - <password of the proxy schema>

Figure 1 Modify the Options for the HDI Data Server



12. Repeat step 11 for HDWF and HMC data servers.
13. Save the repository.
14. Execute the OHADI ETLs.

4.2 Executing ETLs Using Proxy Schema for HLI

Proxy schema is a schema through which you have limited access to the main schemas like HDI (interface schema) and HMC (metadata schema). HLI ETLs must also be executed through a proxy schema. This is an optional feature. To use this feature, perform the following steps once:

1. Traverse to the hli_sql directory under HLI installation folder and open the command prompt.

> **Note:** If sqlplus does not work from command prompt, first set the ORACLE_HOME environment variable to Oracle's home directory and use the following syntax to connect to sqlplus:
>
> Linux:
>
> ```
> sqlplus <user>@"(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)
> (HOST=<hostname>)(PORT=<portnumber>))(CONNECT_DATA=(SERVICE_
> NAME=<service_name>)))"
> ```
>
> Enter the password when prompted.

2. Log in as SYS user in database from the command prompt and execute the following scripts:

```
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.

3. Create a proxy schema user within the same DB instance where HDWF 6.0 is installed, with an appropriate default tablespace with requisite quotas and temporary tablespace.
4. Log in as HDI user in database and execute the following scripts:

```
sqlplus <HDI user>@"(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)
(HOST=<hostname>)(PORT=<port number>))(CONNECT_DATA=(SERVICE_
NAME=<service_name>)))"
```

Enter the password when prompted.

```
@ HLI_PROXY_E_DDL.sql
```

5. Disconnect <*HDI user*> user.
6. Log in as SYS user.

```
sqlplus <sys user>@"(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)
(HOST=<hostname>)(PORT=<port number>))(CONNECT_DATA=(SERVICE_
NAME=<service_name>)))" as sysdba
```

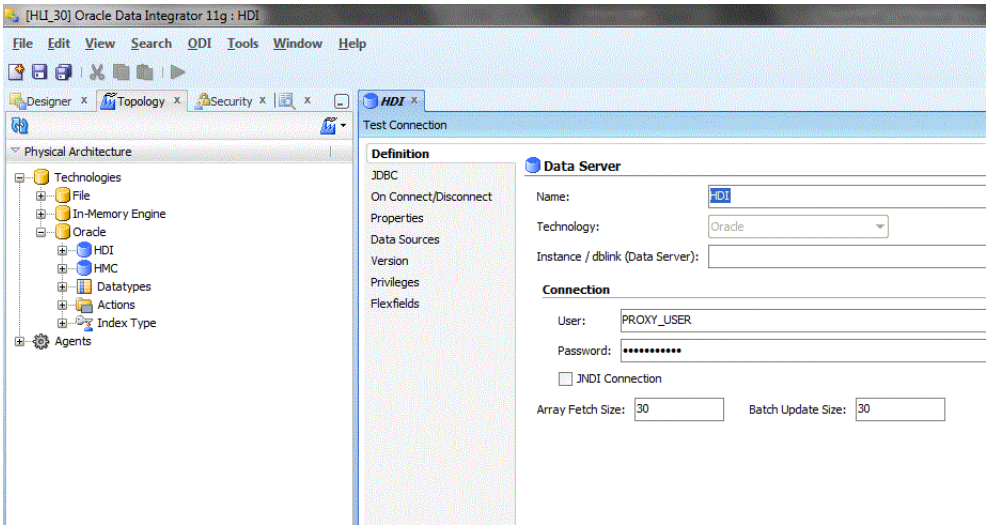
Enter the password when prompted.

7. Run the following script:

```
@ HLI_PROXY_HDWF_GRANT_PRIVILEGES.sql <name of the interface schema>
<name of the metadata schema> <name of the proxy schema PROXY_SCHEMA>;
```

8. In ODI:
   a. Log in to HLI work repository.
   b. Navigate to **Topology** > **Physical Architecture** > **Technologies** > **Oracle**.
   c. Click the HDI data server.
   d. Modify the following options as shown in the screenshot.
   - User - name of the proxy schema
   - password - password of the proxy schema

Figure 2 Modifying the HDI Connection Settings



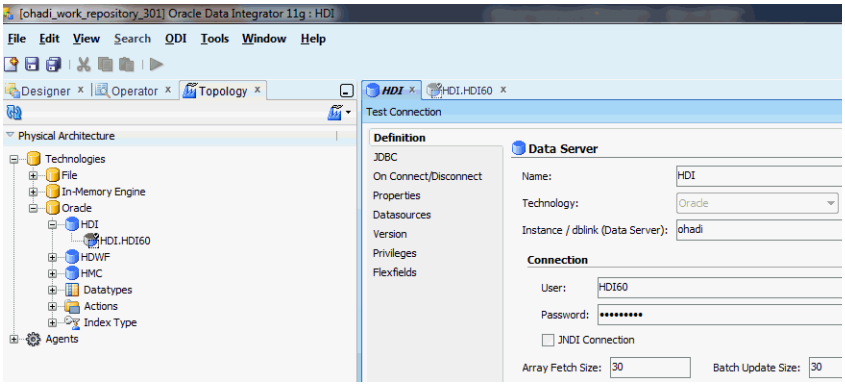
9. Repeat step 8 for the other data server HMC.
10. Save the repository.
11. Execute HLI ETLs.

5 Switching to Default Configuration from Proxy Schema Configuration

To revert the proxy schema configuration to the default schema configuration, perform the following steps:

1. In ODI, log in to OHADI or HLI work repository, and navigate to T**opology > Physical Architecture > Technologies > Oracle**.
2. Click the HDI data server. Modify the following options:
   - User - <name of the HDWF Interface schema name>
   - password - <password of the HDWF Interface schema>

Figure 3 Test Connection



3. Repeat step 2 for HDWF and HMC schema.

4. Save the configuration in the repository.
5. Log in as SYS user in database with the following syntax from the command prompt and execute the scripts.

```
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 PROXY_SCHEMA> cascade;
```

6. Log in as Metadata user (for example, HMC) in the database using the following commands in the command prompt:

```
sqlplus <metadata user>@"(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)
(HOST=<hostname>)(PORT=<port number>))(CONNECT_DATA=(SERVICE_
NAME=<service_name>)))"
```

   Enter the password when prompted.

```
@ OHADI_PROXY_REVERT_GLBL_PARAM_TABLE.sql <name of the metadata
schema>;
```

7. For OHADI, make sure to execute the following global packages before executing any transactional ETL:
   - PKG_Global_Refresh_Variables
   - PKG_Global_Refresh_Procedure

6 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 Healthcare Analytics Data Integration Security Guide, Release 3.1 for Oracle Data Integrator
E63828-01