Oracle® Health Sciences Cohort Explorer

Secure Installation and Configuration Guide

Release 1.0

E24988-02

September 2011

ORACLE®

Oracle Health Sciences Cohort Explorer Secure Installation and Configuration Guide, Release 1.0

E24988-02

Contents

4 Installing Oracle Health Sciences Cohort Explorer Reports

5 Verifying an Oracle Health Sciences Cohort Explorer Installation

A Configuring Oracle Identity Management for Oracle Health Sciences Clinical Development Center

B Oracle Healthcare Data Warehouse Foundation Tables

Index

Preface

This guide provides information about installing and configuring Oracle Health Sciences Cohort Explorer (OHSCE). It also provides information on the secure configuration of the products required for an OHSCE installation.

This preface contains the following topics:

Restricted Use License of Oracle Business Intelligence Enterprise Edition with Oracle Health Sciences Cohort Explorer

Oracle Health Sciences Cohort Explorer (OHSCE) is licensed with a Restricted Use (RU) license of Oracle Business Intelligence Enterprise Edition (OBIEE).

This RU license of OBIEE permits the following:

- Addition of procedures to be called out by ETL for custom implementation of HIPAA-mandated de-identification of existing shipped OHSCE Extract Transform Load (ETL), Dimensions or Facts.
- Extension of existing OHSCE staging tables.
- Addition of new OHSCE staging tables.

All other changes to the OHSCE data model or ETL require a Full Use OBIEE license.

Audience

This guide is meant for System and Database Administrators.

Users of this guide must also be familiar with the following:

- Oracle Databases
- The Oracle Data Integrator application (ODI)

- The Oracle Data Integrator Console application (ODI Console)
- Oracle Web Logic Servers (required for ODI console)

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.

Finding Information and Patches on My Oracle Support

Your source for the latest information about Oracle Health Sciences Cohort Explorer is Oracle Support's self-service Web site, My Oracle Support (formerly MetaLink).

Before you install and use an Oracle software release, always visit the My Oracle Support Web site for the latest information, including alerts, release notes, documentation, and patches.

Creating a My Oracle Support Account

You must register at My Oracle Support to obtain a user name and password account before you can enter the Web site.

To register for My Oracle Support:

1. Open a Web browser to http://support.oracle.com.
2. Click the **Register here** link to create a My Oracle Support account. The registration page opens.
3. Follow the instructions on the registration page.

Signing In to My Oracle Support

To sign in to My Oracle Support:

1. Open a Web browser to http://support.oracle.com.
2. Click **Sign In**.
3. Enter your user name and password.
4. Click **Go** to open the My Oracle Support home page.

Searching for Knowledge Articles by ID Number or Text String

The fastest way to search for product documentation, release notes, and white papers is by the article ID number.

To search by the article ID number:

1. Sign in to My Oracle Support at http://support.oracle.com.
2. Locate the Search box in the upper right corner of the My Oracle Support page.

3. Click the sources icon to the left of the search box, and then select Article ID from the list.
4. Enter the article ID number in the text box.
5. Click the magnifying glass icon to the right of the search box (or press the Enter key) to execute your search.

   The Knowledge page displays the results of your search. If the article is found, click the link to view the abstract, text, attachments, and related products.

In addition to searching by article ID, you can use the following My Oracle Support tools to browse and search the knowledge base:

- Product Focus — On the Knowledge page, you can drill into a product area through the Browse Knowledge menu on the left side of the page. In the Browse any Product, By Name field, type in part of the product name, and then select the product from the list. Alternatively, you can click the arrow icon to view the complete list of Oracle products and then select your product. This option lets you focus your browsing and searching on a specific product or set of products.
- Refine Search — Once you have results from a search, use the Refine Search options on the right side of the Knowledge page to narrow your search and make the results more relevant.
- Advanced Search — You can specify one or more search criteria, such as source, exact phrase, and related product, to find knowledge articles and documentation.

Finding Patches on My Oracle Support

Be sure to check My Oracle Support for the latest patches, if any, for your product. You can search for patches by patch ID or number, or by product or family.

To locate and download a patch:

1. Sign in to My Oracle Support at http://support.oracle.com.
2. Click the **Patches & Updates** tab.

   The Patches & Updates page opens and displays the Patch Search region. You have the following options:

   - In the Patch ID or Number is field, enter the primary bug number of the patch you want. This option is useful if you already know the patch number.
   - To find a patch by product name, release, and platform, click the Product or Family link to enter one or more search criteria.
3. Click **Search** to execute your query. The Patch Search Results page opens.
4. Click the patch ID number. The system displays details about the patch. In addition, you can view the Read Me file before downloading the patch.
5. Click **Download**. Follow the instructions on the screen to download, save, and install the patch files.

Finding Documentation on the Oracle Technology Network

The Oracle Technology Network Web site contains links to all Oracle user and reference documentation. To find user documentation for Oracle products:

1. Go to the Oracle Technology Network at

   http://www.oracle.com/technetwork/index.html and log in.

2. Mouse over the Support tab, then click the **Documentation** hyperlink.

   Alternatively, go to Oracle Documentation page at

   http://www.oracle.com/technology/documentation/index.html

3. Navigate to the product you need and click the link.

   For example, scroll down to the Applications section and click Oracle Health Sciences Applications.

4. Click the link for the documentation you need.

Related Documents

For more information, see the following documents in the *Oracle Business Intelligence Suite Enterprise Edition 11g Release 1 (11.1.1)* documentation set, the Oracle Health Sciences Clinical Development Center Release 3.1 SP1 documentation set, and the *Oracle Healthcare Data Warehouse Foundation Release 3.1* documentation set:

Oracle Health Sciences Cohort Explorer Documentation

The Oracle Health Sciences Cohort Explorer documentation set includes:

- *Oracle® Health Sciences Cohort Explorer Release Notes*
- *Oracle® Health Sciences Cohort Explorer Secure Installation and Configuration Guide*
- *Oracle® Health Sciences Cohort Explorer Administrator's Guide*
- *Oracle® Health Sciences Cohort Explorer User's Guide*
- *Oracle® Health Sciences Cohort Explorer Implementation Scripts Guide*

Oracle Business Intelligence Enterprise Edition Documentation

The *Oracle Business Intelligence Suite Enterprise Edition Online Documentation Library* documentation set includes:

- *Oracle® Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition 11g Release 1 (11.1.1)*
- *Oracle® Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition 11g Release 1 (11.1.1)*
- *Oracle® Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition 11g Release 1 (11.1.1)*
- *Oracle® Fusion Middleware Scheduling Jobs Guide for Oracle Business Intelligence Enterprise Edition 11g Release 1 (11.1.1)*
- *Oracle® Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition 11g Release 1 (11.1.1)*
- *Oracle® Fusion Middleware Developer's Guide for Oracle Business Intelligence Enterprise Edition 11g Release 1 (11.1.1)*
- *Oracle® Fusion Middleware Integrator's Guide for Oracle Business Intelligence Enterprise Edition 11g Release 1 (11.1.1)*

Oracle Health Sciences Clinical Development Center (CDC) Documentation

The Oracle Health Sciences Clinical Development Center documentation set includes:

- *Prerequisites Guidelines (Release 3.1 SP1)*

- *CDC-CDR 3.1 SP1 Client Installation Qualification for Windows*
- *CDC-CDR 3.1 SP1 Client Installation Qualification for Citrix*
- *CDC - SCE User Guide (Release 3.1 SP1)*
- *CDC - SCE Visual Learning Guide (Release 3.1 SP1)*
- *CDC 3.1 SP1 Server Installation Qualification for HP-UX*
- *CDC 3.1 SP1 Server Installation Qualification for UNIX*
- *CDC 3.1 SP1 Server Installation Qualification for Windows*
- *CDC-CDR 3.1 SP1 CDRWeb Installation Qualification for Unix*
- *CDC-CDR 3.1 SP1 CDRWeb Installation Qualification for Windows*
- *CDC-SCE 3.1 SP1 Client Installation Qualification for Citrix*
- *CDC-SCE 3.1 SP1 Client Installation Qualification for Windows*
- *CDC-SCE 3.1 SP1 Database Server Installation Qualification for Unix*
- *CDC-SCE 3.1 SP1 Database Server Installation Qualification for UNIX using Windows*
- *CDC-SCE 3.1 SP1 Database Server Installation Qualification for Windows*
- *CDC 3.1 SP1 Database Patch Installation Qualification*

Oracle Healthcare Data Warehouse Foundation Documentation

The Oracle Healthcare Data Warehouse Foundation 3.1 documentation set includes:

- *Oracle Healthcare Data Warehouse Foundation Release Notes*
- *Oracle Healthcare Data Warehouse Foundation Data Dictionary*
- *Oracle Healthcare Data Warehouse Foundation Glossary*
- *Oracle Healthcare Data Warehouse Foundation Programmer's Guide*
- *Oracle Healthcare Data Warehouse Foundation Electronic Technical Reference Manual*

Oracle Data Integrator Documentation

The Oracle Data Integrator documentation is a part of the *Oracle Fusion Middleware 11.1.1.5.0* documentation set and includes:

- *Oracle® Fusion Middleware Getting Started with Oracle Data Integrator 11g Release 1 (11.1.1)*
- *Oracle® Fusion Middleware Developer's Guide for Oracle Data Integrator 11g Release 1 (11.1.1)*
- *Oracle® Fusion Middleware Installation Guide for Oracle Data Integrator 11g Release 1 (11.1.1)*
- *Oracle® Fusion Middleware Application Adapters Guide for Oracle Data Integrator 11g Release 1 (11.1.1)*
- *Oracle® Fusion Middleware Knowledge Module Developer's Guide for Oracle Data Integrator 11g Release 1 (11.1.1)*
- *Oracle® Fusion Middleware Connectivity and Knowledge Modules Guide for Oracle Data Integrator 11g Release 1 (11.1.1)*

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1 Getting Started

This chapter includes the following sections:

1.1 System Requirements

Your systems must meet the requirements of the Oracle Health Sciences Cohort Explorer (OHSCE) application.

1.1.1 Operating Systems

The following operating systems are supported:

- Microsoft Windows
- Linux x86/x86-64
- Sun SPARC Solaris

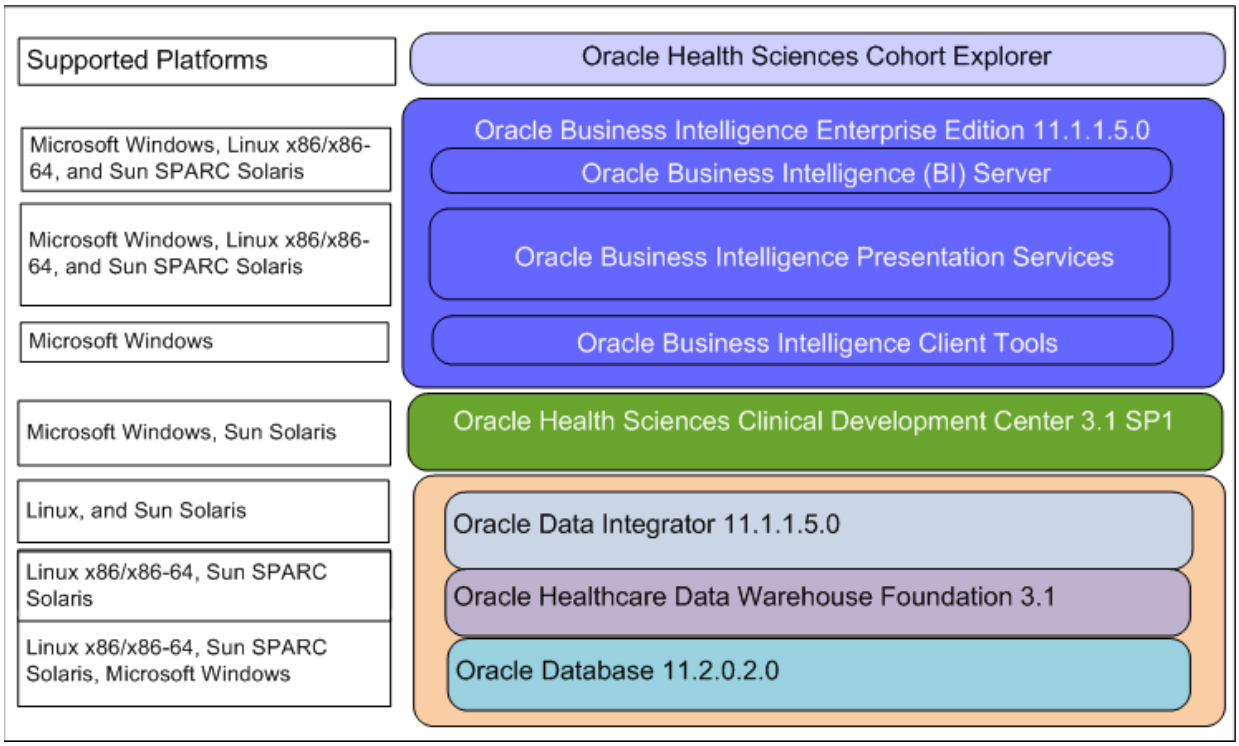
1.1.2 Browsers

OHSCE supports those Internet browsers supported by the Oracle Data Integrator (ODI). For details of browsers supported by ODI, refer to the *Oracle® Fusion Middleware Installation Guide for Oracle Data Integrator11g Release 1 (11.1.1)*

1.2 Technology Stack

The diagram below depicts the technology stack of OHSCE.

Figure 1–1 OHSCE Technology Stack



The required technology stack for Oracle Health Sciences Cohort Explorer consists of the following products:

- Oracle Database 11.2.0.1.0
- Oracle Healthcare Data Warehouse Foundation (HDWF) 3.1
- Oracle Data Integrator (ODI) 11.1.1.5.0
- Oracle Business Intelligence Enterprise Edition (OBIEE) 11.1.1.5.0
- Oracle Health Sciences Clinical Development Center (CDC) 3.1 SP1

1.3 General Security Principles

The following principles are fundamental to using any application securely.

1.3.1 Keep Software Up To Date

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

1.3.2 Keep Up To Date on 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 apply these patches as soon as they are released.

1.3.3 Configure 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.
- 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)*

1.3.4 Follow 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 Healthcare Data Warehouse Foundation (HDWF), the database user should be created with the specified limited set of privileges. DBA access should not be given to the user.

1.4 Before You Begin

This section describes the tasks that you must complete before you can install the Oracle Health Sciences Cohort Explorer (OHSCE) application.

1. Install Oracle Database 11.2.0.1.0 according to platform-specific installation instructions available at `http://www.oracle.com/pls/db112/portal.portal_db?selected=11&frame=`.
2. Install Oracle Healthcare Data Warehouse Foundation 3.1 according to instructions in the *Oracle® Healthcare Data Warehouse Foundation Release Notes*.

> **Note:** You must install the HDWF and OHSCE schemas on different databases.

Important: ■You must populate the Mandatory HDWF Code Types Table and the HDWF Physical Table for OHSCE to function correctly. Refer to Appendix B, "Oracle Healthcare Data Warehouse Foundation Tables" for the tables.

- Three OHSCE implementation scripts—`cohort_hdwf_test_data_load_v1.0.sql, cohort_hdwf_test_data_delete_v1.0.sql, and create_cxe_user_example.sql` are provided with this release. Refer the *Oracle® Health Sciences Cohort Explorer Implementation Scripts Guide* for details.

3. Install Oracle Data Integrator 11.1.1.5.0 according to the *Oracle® Fusion Middleware Installation Guide for Oracle Data Integrator*. Do not create ODI repositories during the installation.
4. Install Oracle Health Sciences Clinical Development Center 3.1 SP1 on the same instance as OHSCE, according to the *CDC-CDR 3.1 SP1 Client Installation Qualification* document.
5. Install Oracle Business Intelligence 11.1.1.5.0 according to *Oracle® Fusion Middleware Installation Guide for Oracle Business Intelligence*.

Note: Oracle recommends that you enable HTTPS on middle-tier computers that host web services. Otherwise the trusted username and password become open to interception.

2

Installing the Oracle Health Sciences Cohort Explorer Schema

This chapter describes a secure installation of the Oracle Health Sciences Cohort Explorer (OHSCE) schema on either a Windows or Unix platform.

It includes the following sections:

The Master Install script is provided in the media pack.

A successful installation of the OHSCE schema creates the OHSCE data mart and seed data for OHSCE.

2.1 Security Guidelines for Database Objects and Database Options

This section describes Oracle Health Sciences Cohort Explorer database objects and database options.

2.1.1 About Oracle Health Sciences Cohort Explorer Database Objects

The Oracle Health Sciences Cohort Explorer contains database objects. Use DDL scripts and PL/SQL procedures and functions to create database objects; and DML scripts to create seed data.

While installing and configuring Oracle Database Server, follow the guidelines in *Oracle® Database 2 Day + Security Guide 11g Release 2 (11.2)*.

2.1.2 Oracle Database Options

The Oracle Database has options that provide additional security features. Oracle Health Sciences Cohort Explorer may include data that falls under HIPAA guidelines in the United States and similar guidelines elsewhere. These features can help comply with those guidelines.

2.1.2.1 Database Vault

Oracle Health Sciences Cohort Explorer includes data that may fall under HIPAA or other regulations outside the United States. These data are highly sensitive and only those with a need to know should have access to it. To prevent DBAs and others from

seeing the data, it is recommended that Oracle Database Vault be used to limit access to the HDWF schema to the HDWF user to prevent DBAs and other "superuser" accounts from accessing the data. Note that Database Vault requires a separate license.

2.1.2.2 Oracle Audit Vault

Oracle Audit Vault automates the audit collection, monitoring, and reporting process, turning 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. Note that Oracle Audit Vault requires a separate license.

2.1.2.3 Transparent Data Encryption

Transparent Data Encryption is one of the three components of the Oracle Advanced Security option for Oracle Database 11g Release 2 Enterprise Edition. It provides transparent encryption of stored data to support your compliance efforts. If you employ Transparent Data Encryption, applications do not have to be modified and 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, eliminating the complex task of creating, managing and securing encryption keys. Note that Transparent Data Encryption requires a separate license.

2.2 Prerequisites for Creating the Schema

You must ensure the following:

- Installation of the Oracle Health Sciences Clinical Development Center (CDC) 3.1 SP1 database.

  Refer to the document *CDC-SCE_3.1_SP1_Database_Server_Installation_Qualification_for_Windows* for details on a CDC database installation on MS Windows.

  Refer to the document *CDC-SCE_3.1_SP1_Database_Server_Installation_Qualification_for_UNIX_using_Windows* for details on a CDC database installation on UNIX.

  Note: Install OID 11.1.1.5.0 if you need to synchronize your user accounts using LDAP.

- Installation of the Oracle Health Sciences Clinical Development Center (CDC) 3.1 SP1 client.

  Refer to the appropriate document for details:

  CDC-SCE 3.1 SP1 Client Installation Qualification for Citrix
  CDC-SCE 3.1 SP1 Client_Installation Qualification for Windows
  CDC-SCE 3.1 SP1 Database Server Installation Qualification for UNIX using Windows

- Installation of the HDWF schema (created during the installation of Oracle Healthcare Data Warehouse Foundation 3.1).
- Creation of the main OHSCE data model user account with CREATE SESSION, CREATE TABLE and CREATE SYNONYM privileges.

Important: You must install the OHSCE schema on the same instance as the Oracle Health Sciences CDC database.

- No user is connected to the database.
- The user has passwords to the user accounts for the following:
  - OHSCE Data Model (OHSCE)
  - HDWF
  - GTMETA
  - SCESCHEMA
- The user knows the description of each parameter that is passed to the install_cxe.sql file. The install_cxe.sql script validates each of the nine expected parameters at the start of the script and exits if any of the parameters are incorrect.

  Provide the required parameters in the following sequence during the execution of the script:

  1. The name of the OHSCE schema user. This is not case-sensitive.
  2. The password of the OHSCE schema user. This is case-sensitive.
  3. The net manager configuration to connect to the OHSCE database instance.
  4. The GTMETA user password. The CDC database must be installed on the same instance as GTMETA. This is set to GTMETA after the installation of CDC. This parameter is case-sensitive.
  5. The SCESCHEMA user password. This is set to SCESCHEMA after the installation of CDC. This parameter is case-sensitive.
  6. The name of the HDWF schema user. This is not case-sensitive.
  7. The password of the HDWF schema user. This is case-sensitive.
  8. The net manager configuration to connect to the HDWF database instance. This is most likely a different instance than the OHSCE database instance.
  9. The name of the tablespace used to create indexes for the OHSCE schema. This parameter is used to specify the index tablespace.

2.3 Installation Files

Installation requires the following files:

- install_cxe.sql
- cohort_data_model.sql
- cohort_index_sequence.sql
- cohort_related_ddl.sql
- cohort_drop_indexes.sql
- load_seed_data.sql
- cohort_create_indexes.sql
- hdm_cd_repository_hier_v.sql
- load_cdc_data.sql

- c_load_param.sql
- c_load_de_identify.sql
- cohort_protocol_util.pks
- cohort_protocol_util.pkb
- cohort_revoke_grants.sql
- c_cohort_procedure_type.sql

2.4 Installing the Schema

Install and verify the installation of the schema:

1. Copy all the files listed in Section 2.3, "Installation Files" to the database server. Ensure that the files are placed in the same folder.

   Important: You must install OHSCE on the same instance as the Oracle Health Sciences CDC database.

2. Start SQLPLUS® in `/nolog` mode.
3. Execute the install_cxe.sql script using following command.

```
SQL>@install_cxe.sql  <CDM schema user name>
< CDM schema user password>
< Database Instance>
< GTMETA user password >
< SCESCHEMA user password >
< HDM schema user  name>
< HDM schema user password>
< Database Instance>
< Index tablespace name>
```

   The script installs the OHSCE database, creates a view in the HDWF schema and then integrates OHSCE with the CDC schema.

4. Review the install_cxe.log file that is created in the same folder after the installation.
5. Log into each schema as the schema owner to verify that all packages, stored procedures, functions, triggers, and views are valid in each of the OHSCE,HDWF, SCESCHEMA and GTMETA schemas.
6. Log in to SQL Developer with the OHSCE schema and verify the following:
   - All objects are created in the schema.
   - All records are correctly inserted into the C_LOAD_PARAM, C_LOAD_DATES, C_LOAD_DE_IDENTIFY and C_COHORT_PROCEDURE_TYPE tables.
7. Log in to the HDWF schema and verify that the HDM_CD_REPOSITORY_HIER_V view is created there.

3

Installing the Oracle Health Sciences Cohort Explorer ETL

This section describes the configuring of the master repository topology components and steps for updating existing topology components.

This chapter includes the following:

3.1 Security Guidelines for Oracle Data Integrator (ODI)

While installing and configuring the ODI Server, follow the guidelines documented in section "Managing the Security in Oracle Data Integrator" in the document *Oracle® Fusion Middleware Developer's Guide for Oracle Data Integrator 11g Release 1 (11.1.1)*.

This section includes the following:

3.1.1 Security Guidelines for Oracle Health Sciences Cohort Explorer ODI ETL Objects

The Cohort ETL objects consist of ODI Master Repository and the ODI Work Repository, which must be deployed in the ODI Server.

After deploying the ODI Master Repository, change all connection configurations as described in the *Oracle Health Sciences Cohort Explorer Installation Guide* to point to the customer database connection parameters.

The ODI Work Repository contains only metadata for Cohort ODI ETLs. The metadata is used within the context of the ODI Server, so follow the security guidelines applicable to the ODI Server while deploying these objects.

3.1.2 Managing Default User Accounts

Lock and expire default user accounts.

3.1.3 Closing All Open Ports Not in Use

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

3.1.4 Disabling the Telnet Service

Oracle Health Sciences Cohort Explorer 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.

3.1.5 Disabling Other Unused Services

Oracle Health Sciences Cohort Explorer 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.
- File transfer Protocol (FTP). This protocol is used for downloading or uploading files from the file server.

Therefore, restricting these services or information does not affect the use of Oracle Health Sciences Cohort Explorer. 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.

3.1.6 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:

- Enabling 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).
- Placing firewalls between servers so that only expected traffic can move between servers.

3.1.7 Enabling SSL

Due to the complexity in setting up SSL it is not enabled by default during installation. Communications between the browser and the application servers should be restricted to SSL. See the WebLogic 11g guidelines for instructions on enabling SSL.

3.2 Install an Oracle Data Integrator (ODI) Repository

Following are the installation steps:

- Download Zipped Files from the Installation Package
- Create a Database Schema
- Create an ODI Master Repository
- Create an ODI Work Repository
- Configure the ODI Physical Agent
- Configure the Physical Data Server
- Configure the Physical Schema
- Create a Database Link

3.2.1 Download Zipped Files from the Installation Package

Get the master repository and work repository zip files from the installation package. The file names are—Cohort_Explorer_ODI_Master_Repository.zip and Cohort_Explorer_ODI_Work_Repository.zip

3.2.2 Create a Database Schema

You must create a database schema for the ODI master repository and the ODI work repository. You may create different schemas for each repository if there is a business reason to do so. Oracle recommends creating a single schema for both repositories.

3.2.3 Create an ODI Master Repository

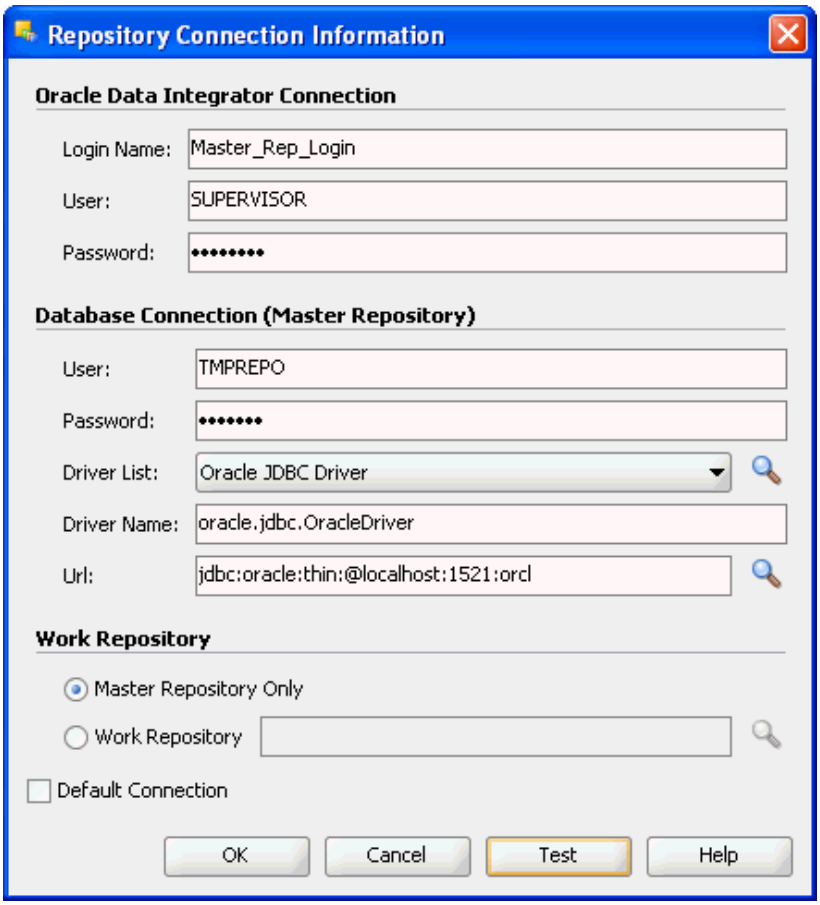
Creating an ODI master repository involves two steps:

- Creating a New ODI Repository Log In
- Importing the ODI Master Repository

3.2.3.1 Creating a New ODI Repository Log In

1. Open Oracle Data Integrator.
2. Select **File**, then **New**, then **Create a new ODI repository Login** in the **New Gallery** window.
3. Click **OK**. The **Repository Connection Information** window opens.
4. Enter values for all the properties as described below.

Figure 3–1 Repository Connection Information Window



Oracle Data Integrator Connection details:

Login name: Provide any value.

User: The default value is Supervisor.

Password: Provide any value.

Database Connection (Master Repository) details:

User: Provide the OHSCE data mart schema name in the database.

Password: Provide the OHSCE data mart schema password.

Driver List: Select Oracle JDBC Driver from the drop-down list.

Driver Name: Auto-populated when you select the Driver list.

URL: Use the search icon to get the URL format and provide the host, port and SID values of the master repository.

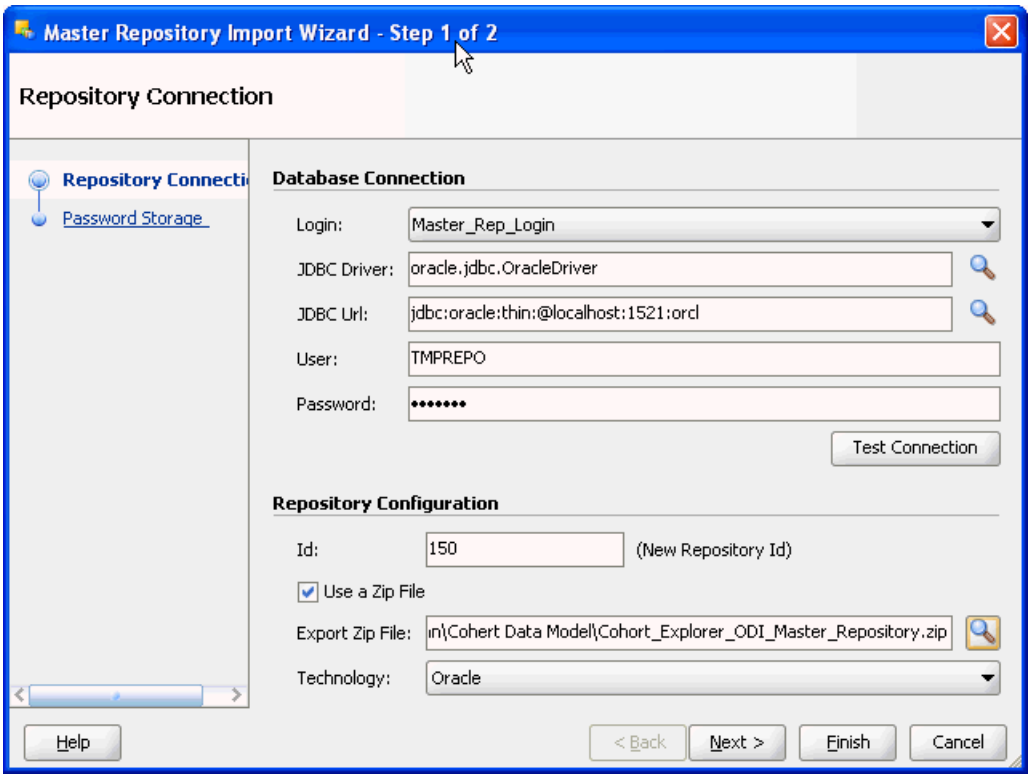
5. Select **Master Repository Only**.
6. Click **OK**. A login name is created with the name provided.

3.2.3.2 Importing the ODI Master Repository

1. Open Oracle Data Integrator.
2. Select **File**, then **New**, then **Master Repository Import Wizard**.

3. Click **OK**. The **Master Repository Import Wizard** window opens.

Figure 3–2 Master Repository Import Wizard



4. Select the Database login name from the drop-down list. The other fields in the section get automatically updated.
5. Provide the repository ID in the **Repository Connection** section.

> **Note:** Each repository ID must be unique. ODI does not allow the import of a repository if its ID already exists.
>
> The repository zip files already contain the following IDs: 10, 0, 999, 100, 189, 111, 1, 11, 99, 900, 101, 666, 8, 600, 3, 892, 6, 66, 102, 103, 104, 105, 109, 110, 111, 199, 333, 777, 551, 512, 801, 802, 767, 803, 804, 805, 806, 807, 808, 809, 810, 811, 812, 813, 302, 303, 304, 305, 306. Provide IDs different from these while creating a repository.

6. Select the **Use Zip File** option and browse for the zip file containing the master repository.
7. Click **Finish**. The master repository is created.

3.2.4 Create an ODI Work Repository

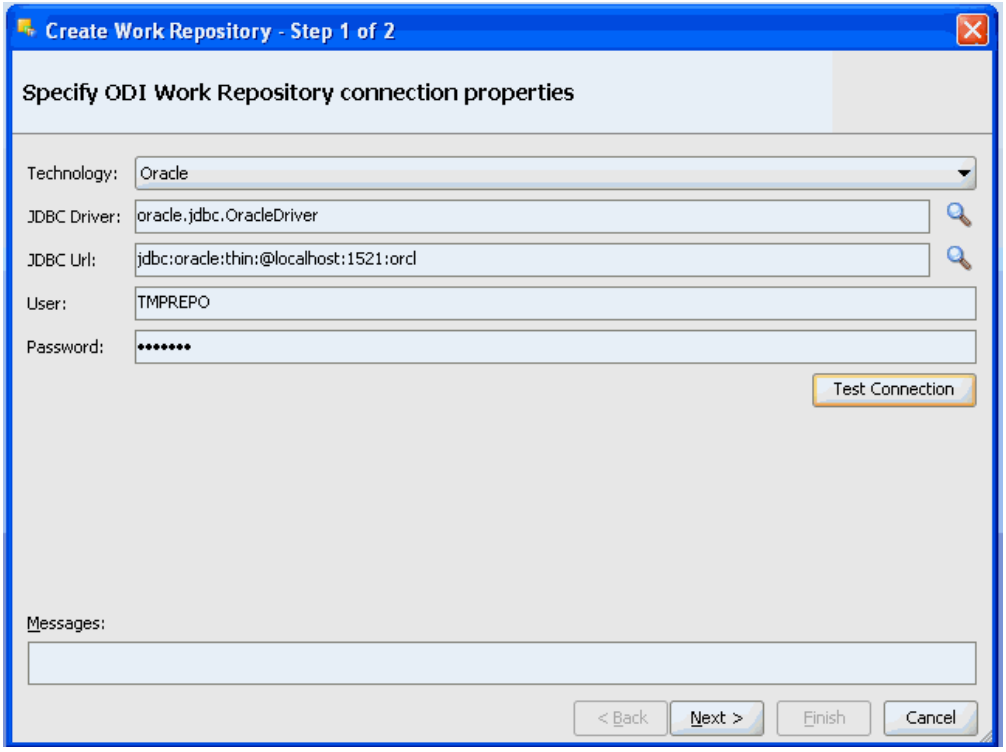
Creating an ODI work repository involves two steps:

- Creating a New ODI Work Repository
- Import the OHSCE Work Repository

3.2.4.1 Creating a New ODI Work Repository

1. Connect to the master repository.
2. Select **Topology**, then **Repositories**, right-click on **Work repositories**, and select **Create Work Repository**. A **Create Work Repository** window opens.

Figure 3–3 Create Work Repository Window-Step 1



3. Select the following values for these fields:

   Technology: Oracle

   JDBC Driver: Use the search icon to select **Oracle JDBC Driver**. The syntax is populated automatically.

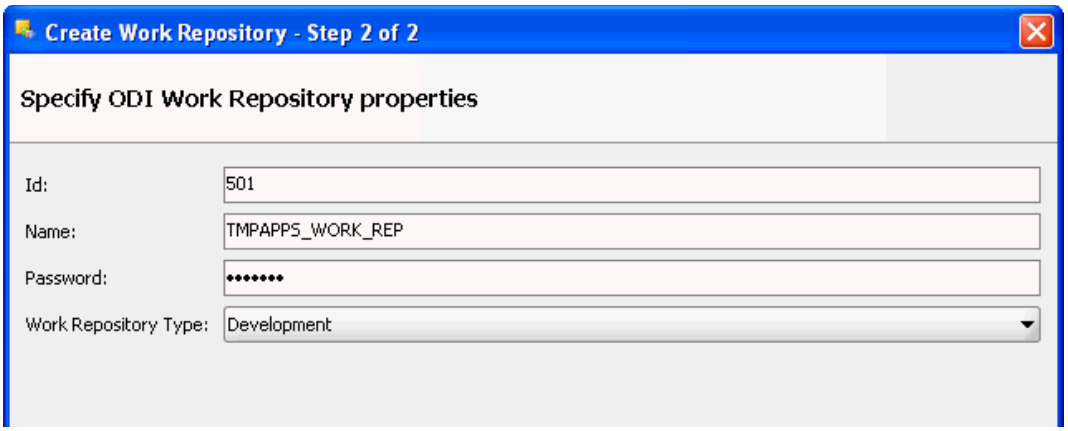
   JDBC URL: Use the search icon to get the URL format and provide the host, port and SID values of the work repository.

   User: Work repository schema user name

   Password: Work repository schema password

4. Click on **Test Connection** to verify whether or not the connection is successful. Click **Next**.

Figure 3–4 Create Work Repository Window-Step 2



5. Provide the necessary values for the fields in step 2 of the **Create Work Repository** window.

   ID: The Work Repository ID

   Note: Each repository ID must be unique. ODI does not allow the import of a repository if its ID already exists.

   The repository zip files already contain the following IDs: 10, 0, 999, 100, 189, 111, 1, 11, 99, 900, 101, 666, 8, 600, 3, 892, 6, 66, 102, 103, 104, 105, 109, 110, 111, 199, 333, 777, 551, 512, 801, 802, 767, 803, 804, 805, 806, 807, 808, 809, 810, 811, 812, 813, 302, 303, 304, 305, 306. Provide IDs different from these while creating a repository.

   Name: The name of the repository

   Password: The password for the repository

   Work Repository Type: Select the type of the work repository

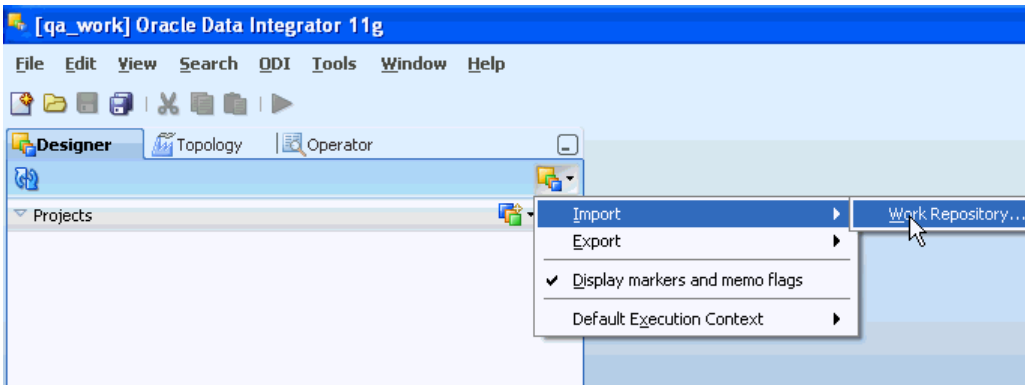
6. Click **Finish**. The work repository is created successfully. You are prompted to create a login name for the work repository.
7. Provide a login name for the work repository and click **OK**.

3.2.4.2 Import the OHSCE Work Repository

To import the OHSCE work repository into ODI:

1. Disconnect from the master repository.
2. Re-connect to the work repository with the login name created in the previous step.
3. Select the **Designer** tab, then select the **Connect Navigator icon** to select **Import**, then **Work repository** as shown below.

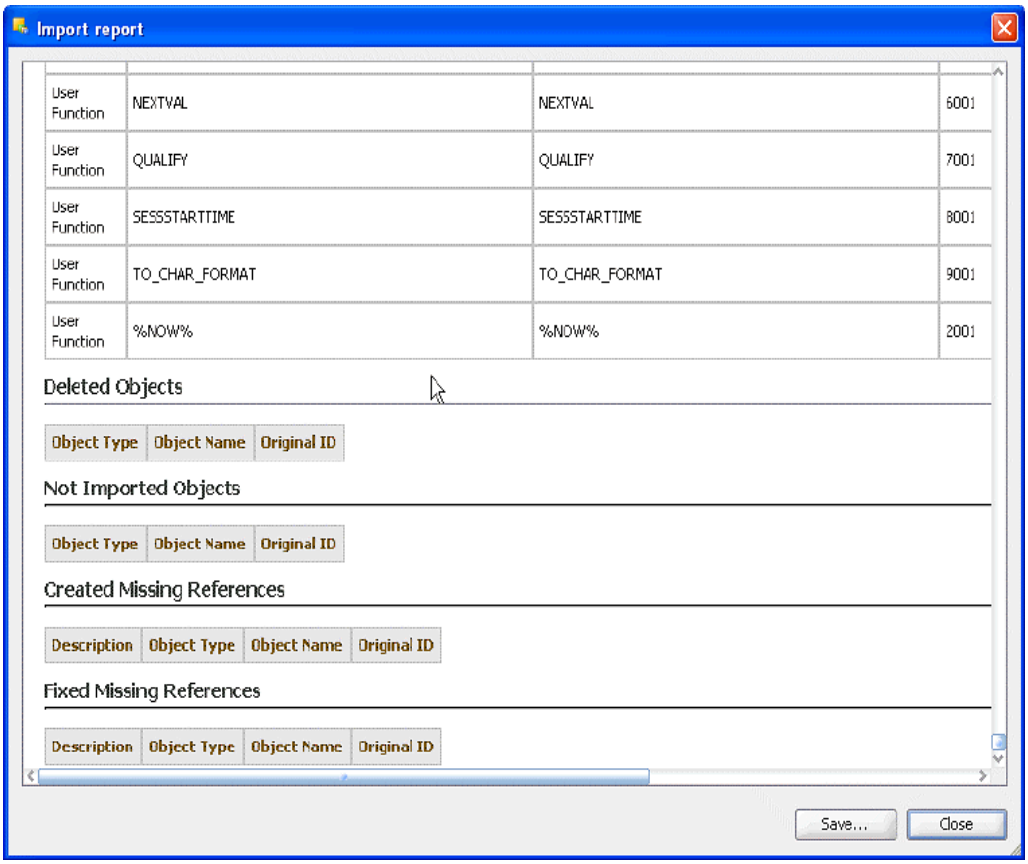
Figure 3–5 Import ODI Work Repository



4. The **Import work repository** window opens. Select the **Import Mode** as **Synonym Mode Insert**.
5. Select **Import from a zip File**.
6. Select the work repository zip file and click **OK**.

   During the import of the work repository, you are prompted to declare different work repository numbers in the master repository like in below screenshot. Click **OK** for each one of them. The **Import report** appears.

Figure 3–6 Import Report



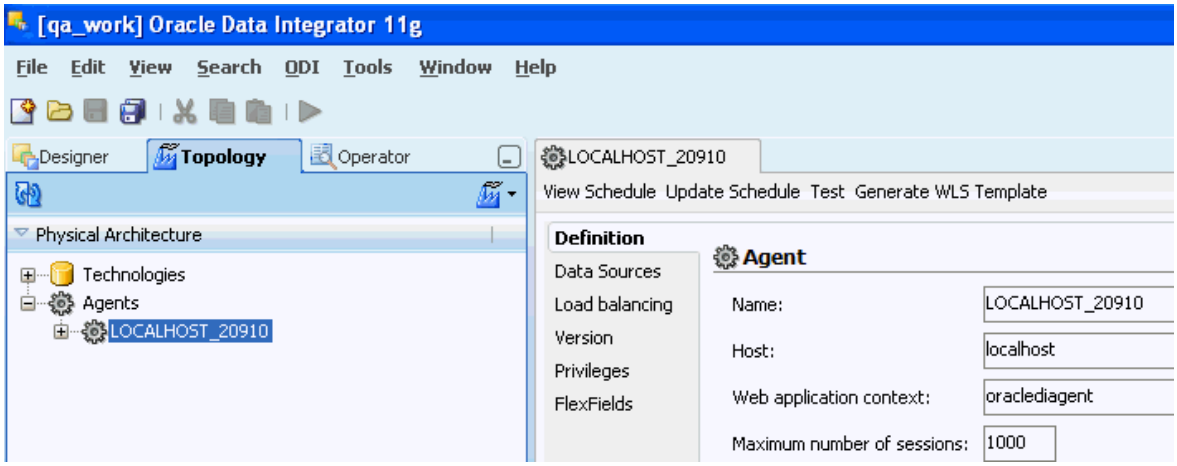
7. Click **Close**. The application is now installed successfully.

3.2.5 Configure the ODI Physical Agent

After a successful ODI installation, the ODI physical agent called LOCALHOST_20910, automatically appears. Modify the properties of the ODI agent as follows:

1. Select the **Topology** tab.
2. Navigate to **Physical Architecture**, then right-click on **Agents**, and finally select **LOCALHOST_20910**.
3. Edit the following:
   - **Name**: Enter a new name for the agent.
   - **Host**: Enter the host name where the ODI repository is installed.
   - **Port**: Enter a new port number or retain the default.
4. **Save** your changes. The new physical agent is created.

Figure 3–7 Configuring the ODI Physical Agent



3.2.6 Configure the Physical Data Server

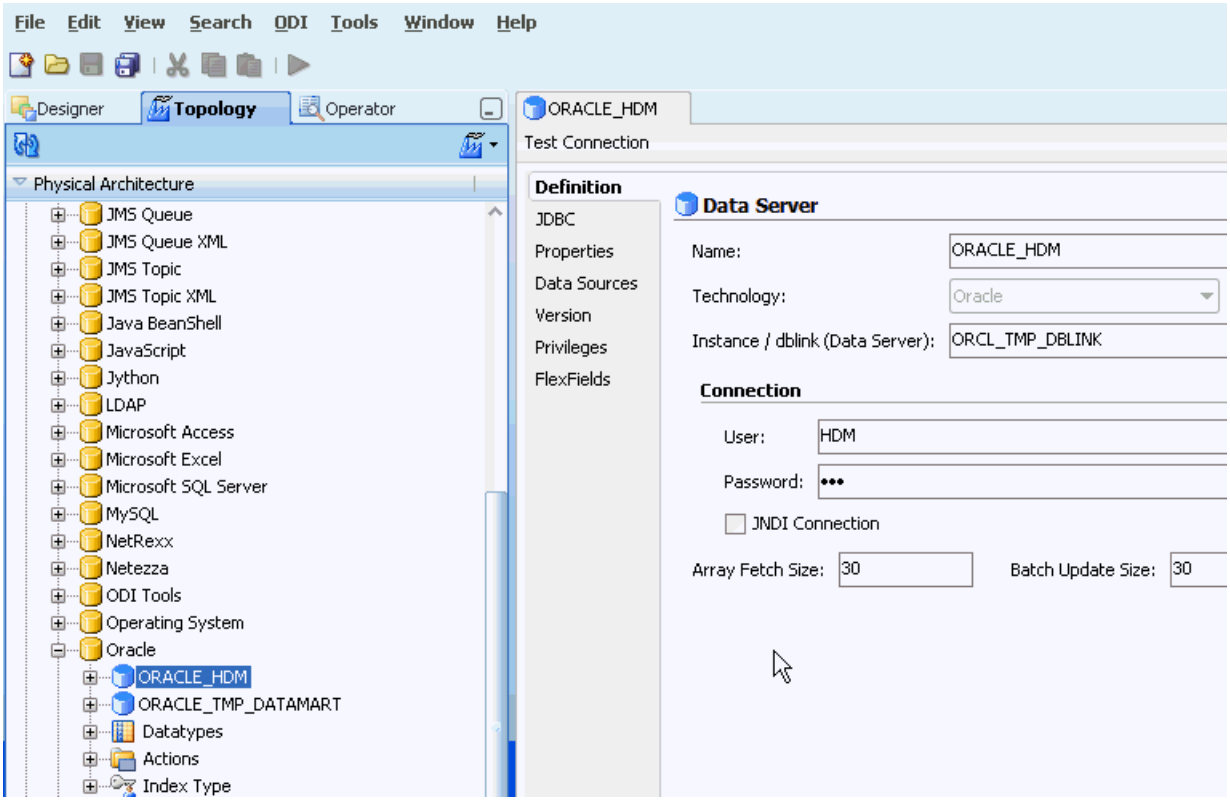
During the installation the following physical data servers are created automatically:

- ORACLE_HDM
- ORACLE_TMP_DATAMART

Configure these data servers as described below:

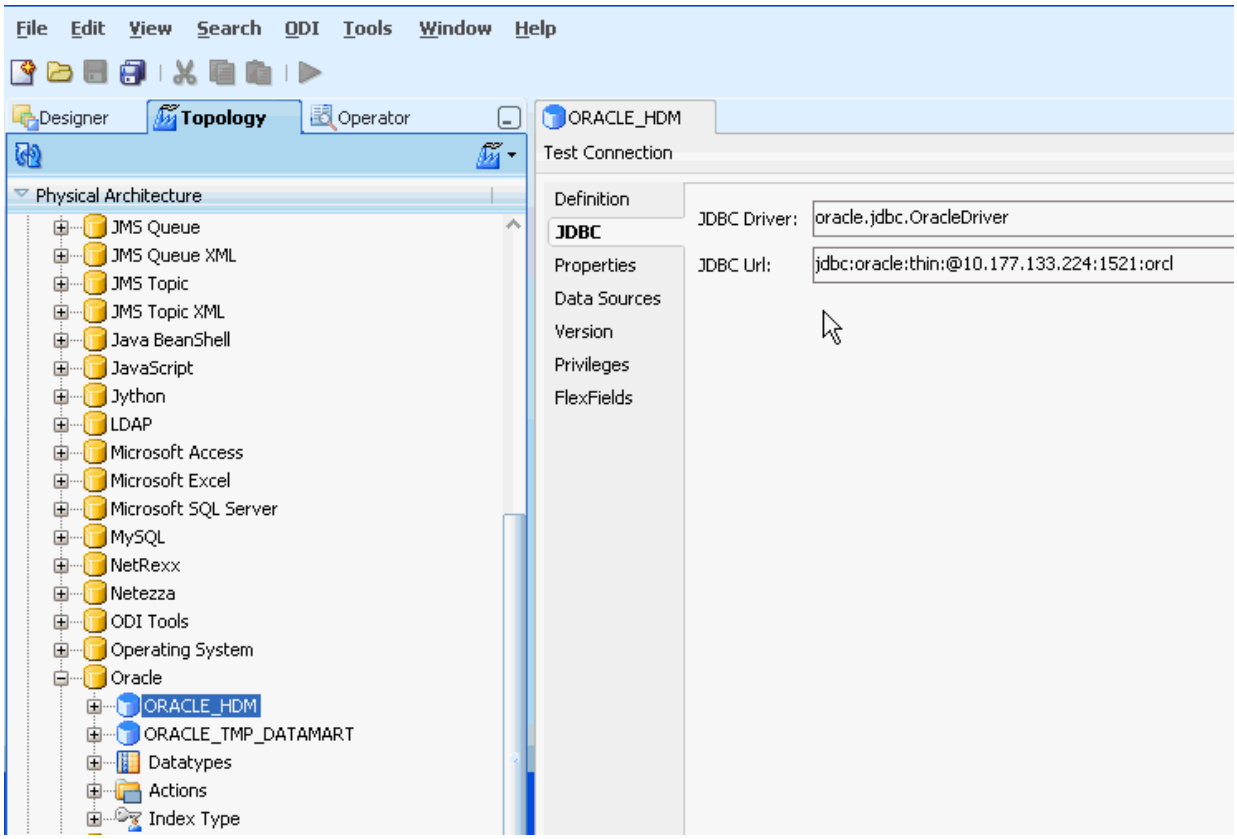
1. In the **Topology** tab, under the **Physical Architecture** tab, expand **Oracle**, select the physical data server created for **HDM** and double-click on it. You see the Definition details for the HDM data server as seen in the following screenshot.

Figure 3–8 Configuring the Physical Data Server



2. Update Definition tab properties as follows:
   - Connection User name and Password: Provide the user name and password for connecting to the HDM schema.
   - Instance/ DBlink (data server): Enter *NET_SERVICE_NAME*. This is the TNS entry name of the HDM schema
3. Update the JDBC tab properties of the system containing HDM schema:
   - **JDBC Driver:** The field is automatically populated.
   - **JDBC URL:** Provide the host, port and SID of the HDWF schema.

Figure 3–9 Configuring JDBC Properties of the Physical Data Server



4. Click the **Test Connection** button to test whether or not the values are correct.
5. Click **Save** on the menu bar. The existing Physical Data Server ORACLE_HDM is updated.
6. Repeat steps from 1 to 5 on the physical data server ORACLE_TMP_DATAMART, created for the OHSCE data mart.

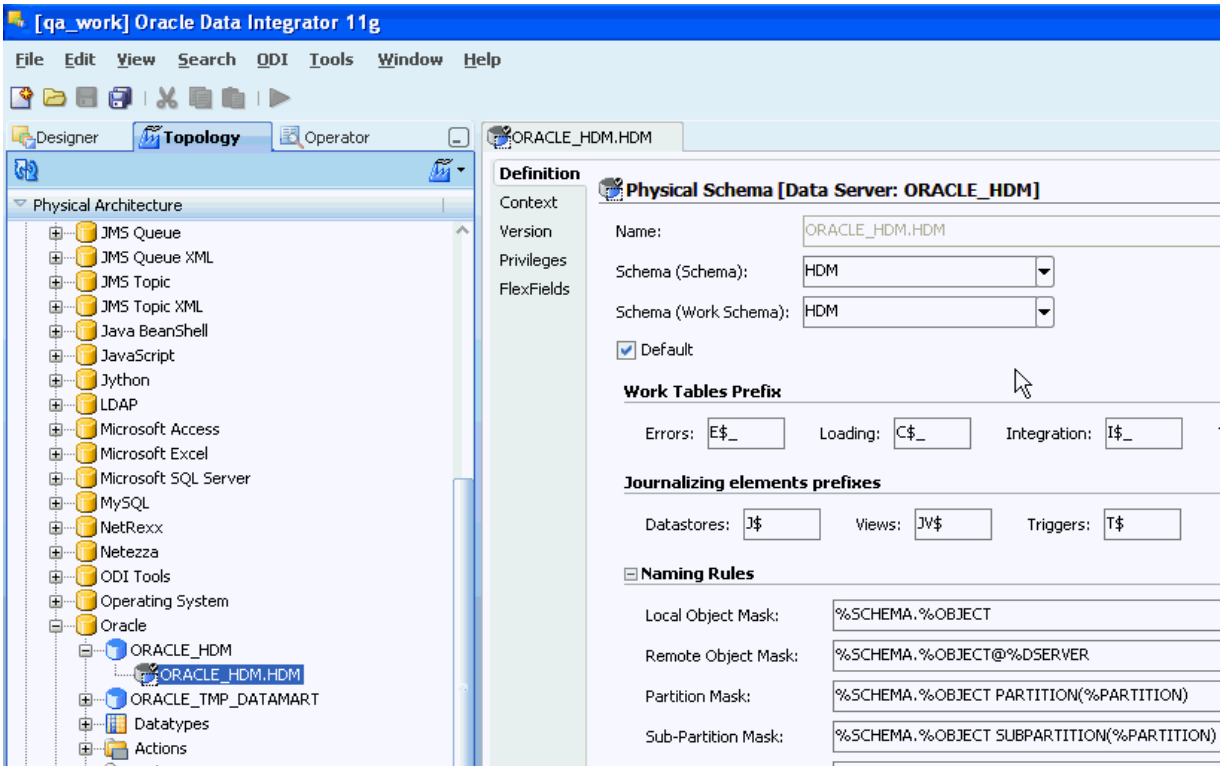
3.2.7 Configure the Physical Schema

The installation of OHSCE creates two schemas: ORACLE_HDM.HDM and ORACLE_TMP_DATAMART.TMPAPPS.

To update the existing physical schema:

1. Connect to the master repository and navigate to **Topology, Technologies**, then **Oracle**.

Figure 3–10 Configuring the Physical Schema



2. Double-click on **ORACLE_HDM** and provide the **Connection** details (User and password).
3. Navigate to the **JDBC** tab and provide the JDBC URL (the server where the data base is installed).
4. Click **Save**.
5. Repeat the above steps for ORACLE_TMP_DATAMART.
6. Double-click on ORACLE_HDM.TRCHDM, select Source schema name from the **Schema** and **Work Schema** drop-down lists.
7. Repeat the above steps for ORACLE_TMP_DATAMART.CDM.

Note: For further references on Topology configuration, follow the these ODI guides:

Oracle® Fusion Middle ware Getting Started with Oracle Data Integrator 11g Release 1 (11.1.1)

Oracle® Fusion Middleware Developer's Guide for Oracle Data Integrator 11g Release 1 (11.1.1)

3.2.8 Create a Database Link

ODI requires a database link between the source (HDWF Schema) and the target OHSCE data mart schema; to move data from the source to temporary tables that are created in the target.

For details, refer to ODI architecture in the *Oracle® Data Integrator User's Guide.*

To create a database link:

1. Connect to the ODI Work Repository.
2. Copy the TNS string from the HDM tnsnames.ora in the HDWF schema to the tnsnames.ora of the OHSCE Data Mart Schema.
3. Open the Initial Setup folder within the Execution Plans folder in ODI. The Initial Setup folder contains a **Create DBLink** task.
4. Right-click the package **Create DBLink** and select **Execute**.

3.3 Revoke Unnecessary Grants on the OHSCE Schema

For security purposes, you must revoke all unnecessary grants on the OHSCE schema. You need DBA privileges to perform this action.

1. Run the command `select * from session_privs` to find out all the privileges granted on the database.
2. Run the following script from the SQL Plus prompt: `cohort_revoke_grants.sql`. The script prompts you for the OHSCE schema name. The script revokes all grants except the following three grants that are necessary for the ETL execution:
   - grant CREATE SESSION to cdm;
   - grant CREATE SYNONYM to cdm;
   - grant CREATE TABLE to cdm;

4

Installing Oracle Health Sciences Cohort Explorer Reports

This chapter presents an overview of the Oracle Health Sciences Cohort Explorer (OHSCE) reports installation process. It also describes the OHSCE reports related installation tasks that you must complete. This chapter includes the following topics:

Note: The rest of the instructions in Section 4.2 assume that OBIEE is installed on Windows in the c:\Oracle\MiddleWare\instances\instance1\bifoundation and on UNIX in the /Oracle/MiddleWare/instances/instance1/bifoundation folders.

4.1 Security Guidelines for Oracle Business Intelligence Enterprise Edition (OBIEE)

While installing and configuring the OBIEE Server, you should follow guidelines in the document *Oracle® Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition 11g Release 1 (11.1.1)*.

4.1.1 Security Guidelines for Oracle Business Intelligence Enterprise Edition Report Objects

Oracle Health Sciences Cohort Explorer Report Objects consist of Cohorts RPD and Webcat, which is deployed in the OBIEE server.

RPD and Webcat contain only the metadata for analytical reports which is used in the context of the OBIEE Server. Therefore, follow the security guidelines applicable for OBIEE server while deploying these objects.

4.1.2 Managing Default User Accounts

Lock and expire default user accounts.

4.1.3 Checking External Links that May Expose Account Data

It is possible to add customized links to web applications that are deployed in a web server. Through this mechanism, any information that can be made available through a URL can be made accessible to OHSCE users. In addition, your customized links may support passing session parameters, such as the log-in user ID, and currently selected Product, Program, Study and Site to a URL. By passing these session parameters, you can access Web pages specific to you current selections on these attributes. However, you should be aware that in links that access external Web sites, passing account data and session information may pose a security risk.

4.1.4 Closing All Open Ports Not in Use

Keep only the minimum number of ports open. You should close all ports not in use.

4.1.5 Disabling the Telnet Service

Oracle Health Sciences Cohort Explorer 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.

4.1.6 Disabling Other Unused Services

In addition to not using Telnet, the Oracle Health Sciences Cohort Explorer 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 Health Sciences Cohort Explorer. 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.

4.1.7 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.

4.1.8 Enabling SSL

Due to the complexity in setting up SSL it is not enabled by default during installation. Communications between the browser and the application servers should be restricted to SSL. See the WebLogic 11g guidelines for instructions on enabling SSL.

4.2 Installing Oracle Health Sciences Cohort Explorer Reports

OHSCE reports installation consists of the following two components:

- Policy Store Migration on page 4-3
- Repository Installation on page 4-4

4.2.1 Policy Store Migration

Perform the following steps to migrate the policy in Oracle WebLogic:

1. Create a folder for PolicyStore Migration
   - Windows—<*DRIVE*>:\> PolicyStoreMigration
   - UNIX—/PolicyStoreMigration
2. Create sub-folders for Cohort Explorer and current production instances.
   - Windows —<*DRIVE*>:\> PolicyStoreMigration\Cohort

     <*DRIVE*>:\> PolicyStoreMigration\Prod
   - UNIX—/PolicyStoreMigration/Cohort

     UNIX—/PolicyStoreMigration/Prod
3. Copy system-jazn-data.xml supplied with OHSCE to the Cohort folder.
4. Copy the system-jazn-data.xml from the
   - Windows—*{Middleware_Home}*/ user_projects/domains/bifoundation_ domain/config/fmwconfig folder to the Prod folder.
   - UNIX—/*{Middleware_Home}*\ user_projects\domains\bifoundation_ domain\config\fmwconfig folder to the Prod folder.

   Note: Oracle recommends that you take a backup of all the files before merging the policies.
5. Copy the jps-config-policy.xml supplied with OHSCE to the PolicyStoreMigration folder.
6. Open the jps-config-policy.xml file. Edit the **location** attribute value in the <serviceInstance> tag for source and target to reflect the actual paths in your environment. The following changes must be reflected in jps-config-policy.xml
   - <serviceInstance name="srcpolicystore.xml" provider="policystore.xml.provider" location="C:\PolicyStoreMigration \Cohort ">

- <serviceInstance name="policystore.xml" provider="policystore.xml.provider" location="C:\PolicyStoreMigration \Prod ">

7. Open a command prompt. Run the Oracle WebLogic Scripting Tool (WLST).
   - Windows—*{Middleware_Home}*/Oracle_BI1/common/bin/wlst.cmd
   - Unix—*{Middleware_Home}*/Oracle_BI1\common\bin\wlst.sh
8. Run the following command in offline interactive mode,

```
migrateSecurityStore(type="appPolicies", srcApp="obi",
configFile="C:/PolicyStoreMigration/jps-config-policy.xml",
src="sourceFileStore", dst="targetFileStore",
overWrite="false")
```

9. The merged PolicyStore file is now available in the Prod folder. The PolicyStore should contain the following roles in addition to others:
   - CE-Administrator
   - CE-Physician
   - CE-Researcher
   - CE-LimitedAccess
   - CE-Developer
10. Stop Oracle WebLogic Server.
11. Copy the merged system-jazn-data.xml from Prod folder to
    - Windows—*"{Middleware_Home}*/user_projects/domains/bifoundation_domain/config/fmwconfig
    - Unix—*"{Middleware_Home}*\user_projects\domains\bifoundation_domain\config\fmwconfig
12. Start Oracle WebLogic Server.

4.2.2 Repository Installation

Perform the following steps to install the OHSCE reports on Windows and Unix:

1. Place the OracleHeathSciencesCohortExplorer.rpd in the following folder:
   - Windows—<*DRIVE*>:\> Oracle\MiddleWare\instances\instance1\bifoundation\OracleBIServerComponent\coreapplication_obis1\repository
   - UNIX—Oracle/MiddleWare/instances/instance1/bifoundation/OracleBIServerComponent/coreapplication_obis1/repository
2. Unzip OracleHealthSciencesCohortExplorer.zip in the following folder:
   - Windows—<*DRIVE*>:\>\Oracle\MiddleWare\instances\instance1\bifoundation\OracleBIPresentationServicesComponent\coreapplication_obips1\catalog
   - UNIX—Oracle/MiddleWare/instances/instance1/bifoundation/OracleBIPresentationServicesComponent\coreapplication_obips1/catalog
3. Unzip help.zip in:
   - Windows—<*DRIVE*>:\Oracle\MiddleWare\Oracle_BI1\bifoundation\web\app\res\s_blafp\help

- UNIX—Oracle/MiddleWare/Oracle_BI1/bifoundation/web/app/res/s_blafp/help

4. Unzip help.zip in:
   - Windows—<Drive>:\Oracle\MiddleWare\user_projects\domains\bifoundation_domain\servers\bi_server1\tmp_WL_user\analytics_11.1.1\7dezjl\war\res\s_blafp\help
   - UNIX—Oracle/MiddleWare/user_projects/domains/bifoundation_domain/servers/bi_server1/tmp/_WL_user/analytics_11.1.1/7dezjl/war/res/s_blafp/help
5. In the Oracle BI Administration Tool, open the newly installed Oracle BI repository (OracleHealthSciencesCohortExplorer.rpd) in the offline mode to configure static variables and connections.

   Note: The OBIEE BI Administration Tool is supported only on Windows. If OHSCE is installed on Unix, copy OracleHealthSciencesCohortExplorer.rpd to a Windows system to perform modifications described in the following sections. Once the modifications are complete, copy the OracleHealthSciencesCohortExplorer.rpd back to the Unix system.

   a. In the Oracle BI Administration Tool, select **File**, then **Open**, and then **Offline**.
   b. Navigate to the OracleHealthSciencesCohortExplorer.rpd, and then click **Open**.
   c. In the Open Offline dialog box, enter the of repository password to log into the OracleHealthSciencesCohortExplorer.rpd file. The default password is 'cohort'. You can change the password by clicking **File**, then **Change Password**. Enter the old password and then the new password. Confirm the new password.
   d. Click **OK**.
6. In the Oracle BI Administration Tool, select **Manage** and then **Variables**.
7. In the Variable Manager dialog box, expand the **Repository** and then **Variable** in the left pane. Then click **Static**.
8. Double-click and modify the following static variables:

Table 4–1 Static Variables

Variable Name	Instruction
OLAP_DSN	Enter the value of the database name
OLAP_USER	Enter the value of the database schema
ConsentTypeCode	Enter the value of the type code for Consent
ConsetStatusCode	Enter the value of the type code for Consent Status
MinEventDate	Enter the approximate date when the first patient event was noted. This is used as the reference date in the Patient Event Timelines Chart in Patient Timelines Tab in the Cohort Explorer dashboard.

9. Click **OK** after each modification.
10. Close the Variable Manager.

11. Modify the connection pools in the RPD as following:
    a. In the physical layer, expand the OracleHealthScienceCohortExplorer node and double-click the connection pool.
    b. Change the password to the password of the schema user.
    c. Click **OK**.
12. In the physical layer, double -click the OracleHealthScienceCohortExplorer node.
13. Click the **Features** tab. Navigate to the SORT_ORDER_LOCALE feature. If both the value and the default are the same, change the value to **english-uk**.
14. From the File menu, select **Save** to save the rpd.
15. Navigate to \Oracle\Middleware\instances\instance1\config\OracleBIPresentationServicesComponent\coreapplication_obips1
16. Open instanceconfig.xml in an editor and make the following changes:
    a. Locate the `Cube` section, in which you must modify the following elements:
       – `CubeMaxRecords`: Set this value to the number of specimen instances (number of rows in W_EHA_SPECIMEN_PATIENT_H) in the facility, if the specimen instances are greater than the number of patients in the facility. If not, set this value to the number of patients in the facility.
       – `CubeMaxPopulatedCells`: Set this value to the number of specimen instances (number of rows in W_EHA_SPECIMEN_PATIENT_H) in the facility, if the specimen instances are greater than the number of patients in the facility. If not, set this value to the number of patients in the facility.
    b. Locate the `Table` section in which you must modify `MaxVisibleRows`. Set this value to an approximate of the number of patients in the facility * Number of event types per patient
    c. Locate the Pivot Table section, in which you must modify `MaxVisibleRows`. Set this value to the number of specimen instances (number of rows in W_EHA_SPECIMEN_PATIENT_H) in the facility, if the specimen instances are greater than the number of patients in the facility. If not, set this value to the number of patients in the facility.
17. Save and close instanceconfig.xml.
18. Log in to Fusion Middleware Control (https://<host>:7001/em).
19. Expand the **Business Intelligence** folder and select the **coreapplication** node.
20. Navigate to the **Repository** tab of the **Deployment** page.
21. Click on **Lock and Edit Configuration**.
22. In the **Upload BI Server Repository** section, click the **Browse** button to select the **OracleHeathSciencesCohortExplorer.rpd**.
23. Enter the repository password (*cohort*) in **Repository Password** and **Confirm Password** fields. The default password is 'cohort'. If you have changed the password in step 5c, enter the new password.
24. Enter the location of the OracleHealthSciencesCohortExplorer catalog in the **BI Presentation Catalog** section.
25. Click **Apply** and then click **Activate Changes**.

26. Select the **Capacity Management** tab and then **Performance**. In the section **Maximum Number of Rows Processed When Rendering a Table View**, increase the number of rows to an approximate of the number of patients in the facility * Number of event types per patient.
27. Click **Apply**, and then **Activate Changes**.
28. Select the **Overview** tab and click the **Restart** button, then click **Yes**.
29. Open your browser and sign in to OBIEE.
30. Select **Cohort Explorer** from the **Dashboards** drop-down list.
31. Click **Edit Dashboard** under the **Summary** tab.
32. Select **Edit Analysis** for report biospecimen_samples_r.
    a. Select the **Criteria** tab, then click on **Show/Hide Selection Steps Pane**.
    b. Under the section **Specimen - Anatomical Site**, edit the first step **Start with...** to include the Anatomical Sites you want to see in report.
    c. Save the report.
33. Click **Apply**.
34. Return to the Business Intelligence Overview page and click **Restart**.
35. Click **Yes**.

4.3 Accessing Oracle Health Sciences Cohort Explorer

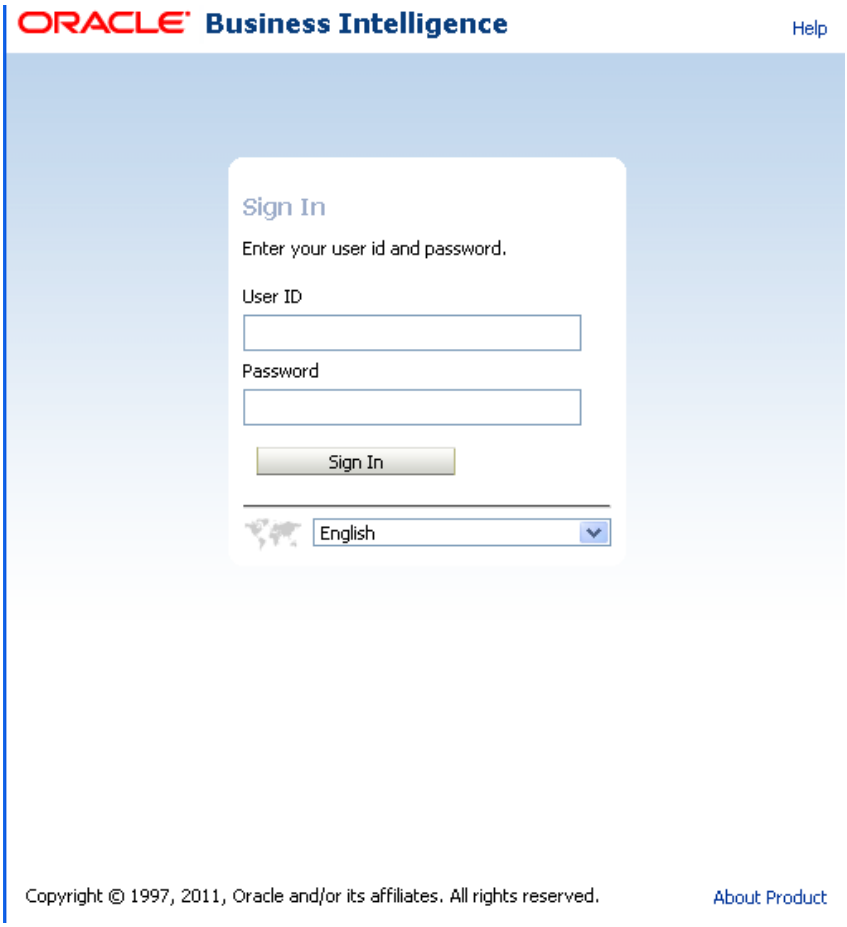
Your security privileges determine what reports you can see and what you can do in OHSCE. To log in to OHSCE, you must have a browser on your computer and a URL, username, and password provided by your company.

4.3.1 Logging In

1. Open your browser and enter the URL provided by your company.

   Figure 2-1 displays the OHSCE login page.

Figure 4–1 Oracle Health Sciences Cohort Explorer Login Page



2. Enter the following user ID and password.

   Username: `Administrator`

   Password: *`Enter the password`*.

3. Click **Login**.

   After your login credentials are authenticated, your default dashboard page is displayed.

4.3.2 Viewing a Dashboard

Perform the following steps to view a dashboard:

1. Log in to OHSCE.
2. Select Cohort Explorer dashboard.
3. Select a dashboard page.

5

Verifying an Oracle Health Sciences Cohort Explorer Installation

This chapter describes the components of the application after a successful installation. Verify that they are available after installation.

This chapter includes the following sections:

5.1 OHSCE Database Components

After a successful installation of the Master Install Script, you can view the following components in the Oracle HSCE data mart schema.

- The following 33 data model tables containing patient-related medical information. When ODI packages are executed, data is loaded into these tables from HDWF:

  W_EHA_ANATOMICAL_SITE_D
  W_EHA_CONSENT_D
  W_EHA_CONSENT_PATIENT_H
  W_EHA_CONSENT_STATUS_D
  W_EHA_DIAGNOSIS_D
  W_EHA_DIAGNOSIS_STATUS_D
  W_EHA_DIAGNOSTIC_TEST_D
  W_EHA_DIAGTST_PATIENT_H
  W_EHA_DIAGTST_PROC_DHL
  W_EHA_DIAGTST_SPEC_DHL
  W_EHA_DIAGTST_SUBADM_DHL
  W_EHA_DX_PATIENT_H
  W_EHA_ETHNICITY_D
  W_EHA_ETHN_PATIENT_H
  W_EHA_MEDICATION_D
  W_EHA_PATIENT_HISTORY_D
  W_EHA_PROCEDURE_D
  W_EHA_PROCEDURE_TYPE_D
  W_EHA_PROC_PATIENT_H
  W_EHA_PROC_SUBADMN_DHL
  W_EHA_PROC_TYPE_PROC_DHL
  W_EHA_PROTOCOL_D
  W_EHA_PROTOCOL_PATIENT_H
  W_EHA_PT_HISTORY_PT_H

W_EHA_RACE_D
W_EHA_RACE_PATIENT_H
W_EHA_RESEARCH_PATIENT_D
W_EHA_RESEARCH_PATIENT_F
W_EHA_SPECIMEN_D
W_EHA_SPECIMEN_PATIENT_H
W_EHA_SUBADMN_PATIENT_H
W_EHA_UOM_D
W_USER_D

- The following configuration tables used by ETL:

  C_COHORT_PROCEDURE_TYPE
  C_LOAD_PARAM
  C_LOAD_DATES
  C_LOAD_DE_IDENTIFY
- The following view used by ETL:

  W_EHA_RESEARCH_PATIENT_V
- The following procedures used by ETL:

  ETL_POSTPROCESSOR()
  NAV_RECORD_UPDATE()
  SEED_NA_RECORDS()
  SEED_NOT_AVAILABLE_RECORDS()
- The following functions used by ETL:

  CUSTOM_HDM_DATE_DE_IDENTIFY()
  CUSTOM_HDM_NUMBER_DE_IDENTIFY()
  CUSTOM_HDM_STRING_DE_IDENTIFY()
  GETCOLDATATYPE()

5.2 ODI Repository Components

This section describes the organization of an ODI project in this application. All related ODI objects are organized within ODI folders in a particular hierarchy. Each folder contains various objects as described below.

This section describes the following:

- ODI Master Repository Components
- ODI Work Repository Components

5.2.1 ODI Master Repository Components

The ODI master repository contains topology information such as contexts, physical architecture components such as agents, technologies and logical architecture components such as agents and technologies.

Topology information:

- Contexts— Global
- Physical Architecture Agents: LOCALHOST_20910
- Physical Architecture Technologies: ORACLE_HDM, ORACLE_DATAMART, ORACLE_TEMP_DATAMART
- Logical Architecture Agents: LOCALHOST_20910
- Logical Architecture Technologies: ORACLE_SOURCE, ORACLE_TARGET

You can choose to use the existing topology and update it according to your system and database configurations, or create a new set of these components. See the sections on configuration for instructions.

5.2.2 ODI Work Repository Components

This repository contains ODI objects such as folders, packages, interfaces, variables, sequences and functions organized in the following manner:

The project **OracleHealthcareAnalytics** under the **Project** tab, contains the following folders:

- **Execution Plans** containing the following sub folders.

  Initial Setup
  Level1_Load_User_Dimension
  Level2_Load_All_Other_Dimensions_And_Patient_Fact
  Level3_Load_All_Bridge_Tables
  Level4_Load_Unspecified_Records_For_Bridge_Tables
  Level5_Load_Protocol_Tables
  Master_Execution_plan
- **Mappings** containing the following sub folders.

  Dimensions
  Facts
- **Variables** containing 73 variables.

  Dimensions
  Facts
- **Sequence** containing 31 sequences.

  Dimensions
  Facts
- **User Functions** containing one function—**UserWID**.

  LKM TMP APPS Oracle to Oracle (DBLINK)
  CKM Oracle
  IKM TMP APPS Oracle Control Append
  IKM TMP APPS Oracle Incremental Update

The **Models** tab contains a folder—**Oracle Healthcare Analytics**, which in turn contains 3 models.

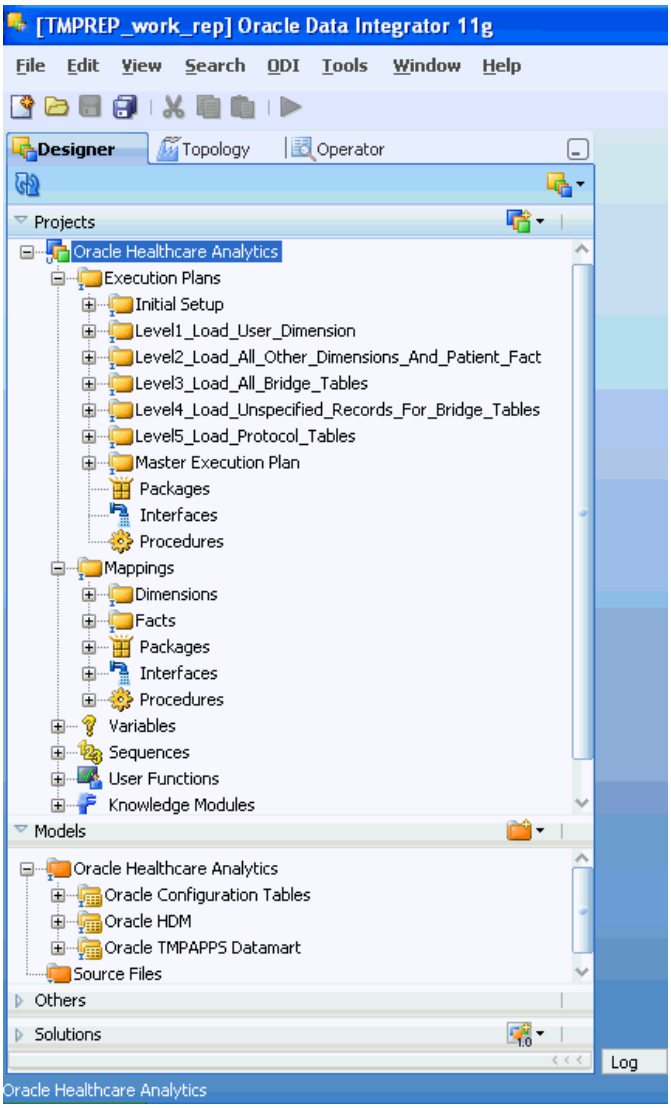
- Oracle Configuration Tables
- Oracle HDM
- Oracle TMPAPPS Data mart

The **Others** tab contains 8 Global User Functions as follows:

- TO_CHAR_FORMAT()
- %NOW%()
- ADD_TO_DATE()
- SESSSTARTTIME()
- COALESCE()
- NEXTVAL()
- GET_SCEN_NAME()
- QUALIFY()

The screenshot depicts the organization structure described above for the W_EHA_ANATOMICAL_SITE_D table.

Figure 5–1 Organization Structure of an ODI Work Repository



A

Configuring Oracle Identity Management for Oracle Health Sciences Clinical Development Center

This appendix includes the following topics:

A.1 Installing the Prerequisite Software

Complete the following pre-installation tasks before you install Oracle Identity Management (OID):

1. Install Oracle 11*g*R2 RDBMS.
2. Create a Database (for example, DB001) using the following parameters:
   - character set=AL32UTF8
   - processes = 500
   - OPEN_CURSOR=600

   Set the SYS and SYSTEM password set to `Password`

   Note: Any database name or password provided in this document is merely an example. Provide your own names and passwords.

3. Download and install Oracle WebLogic Server version 10.3.4.0.
4. Download and install Oracle Identity Management 11*g* (OID) version 11.1.1.2.0.
5. Download and install the Oracle Fusion Middleware Family for Identity Management 11*g* (OID) version 11.1.1.5.0 patch.
   a. Select the **Install Software only** option when installing OID.
   b. Click **Next** and complete the installation.

Note: When installing OID (LDAP server), we assume you have:

- Installed all software on the same machine. If you use different computers, replace *localhost* references.
- Used MS Windows as your operating system. The steps to install OID on Unix and Linux are different.

Perform the following steps:

- "Configure Oracle Identify Management" on page 2
- "Create an LDAP User" on page 2

A.1.1 Configure Oracle Identify Management

After installing all the prerequisite software, navigate to the following directory and execute the Config.bat file to configure OID:

c:\Oracle\Middleware\Oracle_IDM1\Bin

The following settings were used for the purpose of testing:

Table A–1 Settings Used to Configure OID

Settings	Parameter	Value
WebLogic Settings	Create Domain Password Domain Name Web Logic Server directory	weblogic weblogic1 IDMDomain c:\Oracle\Middleware\wlserver_10_3
OID Settings	Oracle Instance Name Oracle Identity Federation Component (OIF) Auto Port Configuration LDAP V3 name Space Virtual Directory Admin Admin Password	asinst_1 Deselect Select c=oracle, dc=com cn=orclAdmin Password123
Specify Schema Database	Connect String User Password	localhost: 1521:db001 sys Password123
OID Configuration	ODS Schema Password ODSSM Schema Password	Password123 Password123
Create Oracle Internet Directory	Realm Admin Password	dc=oracle, dc=com cn=orclAdmin Password123

A.1.2 Create an LDAP User

You only need perform the following steps to authenticate LDAP with the CDC application.

This section contains the following topics:

- "Creating an LDAP User Using Command Line Tools" on page 3
- "Creating an LDAP User Using the Self-Service Console" on page 4

You can create or modify a user and its attributes by using either command line tools or Oracle Internet Directory's self service console, (`http://host:port/odsm` for 11*g* and `http://host:port/oiddas` for 10*g*).

For more information about the Oracle Internet Directory, refer the *Oracle® Fusion Middleware Administrator's Guide* located at `http://download.oracle.com/docs/cd/E14571_01/oid.1111/e10029/toc.htm`.

A.1.2.1 Creating an LDAP User Using Command Line Tools

Before creating an LDAP user, execute the following bind command on command prompt to authenticate to a directory server:

```
ldapbind -h <OID_host> -p <non_SSLport> -D cn=<OID_superuser> -w
<OID_superuser_password>
```

where:

- **h** specifies the host name of the directory server
- **p** specifies the port number of the directory server
- **D** specifies the bind DN, the user authenticating to the directory.
- **cn** specifies the admin username provided during installation
- **w** specifies the bind password in simple authentication

```
ldapadd -h <OID_host> -p <nonSSLport> -D cn=<OID_superuser> -w
<OID_superuser_password> -f orcl.ldif
```

where:

- **p** specifies the port number of the directory server
- **D** specifies the bind DN, the user authenticating to the directory
- **cn** specifies the bind username provided during installation
- **w** specifies the bind password in simple authentication
- **f** specifies the LDAP Data Interchange Files containing attributes of a user.

  A sample orcl.ldif file has the following content:

  dn: cn=cdctest,cn=users,dc=oracle,dc=com

  objectclass: inetorgperson

  objectclass: orcluserv2

  objectclass: orcluser

  givenname: cdctest

  sn: cdctest

  orcltimezone: Asia/Mumbai

  mail: username@domain.com

  uid: cdctest

  userpassword: <<Password for the user>>

  orclactivestartdate: 20080310000000z

  orclisenabled: ENABLED

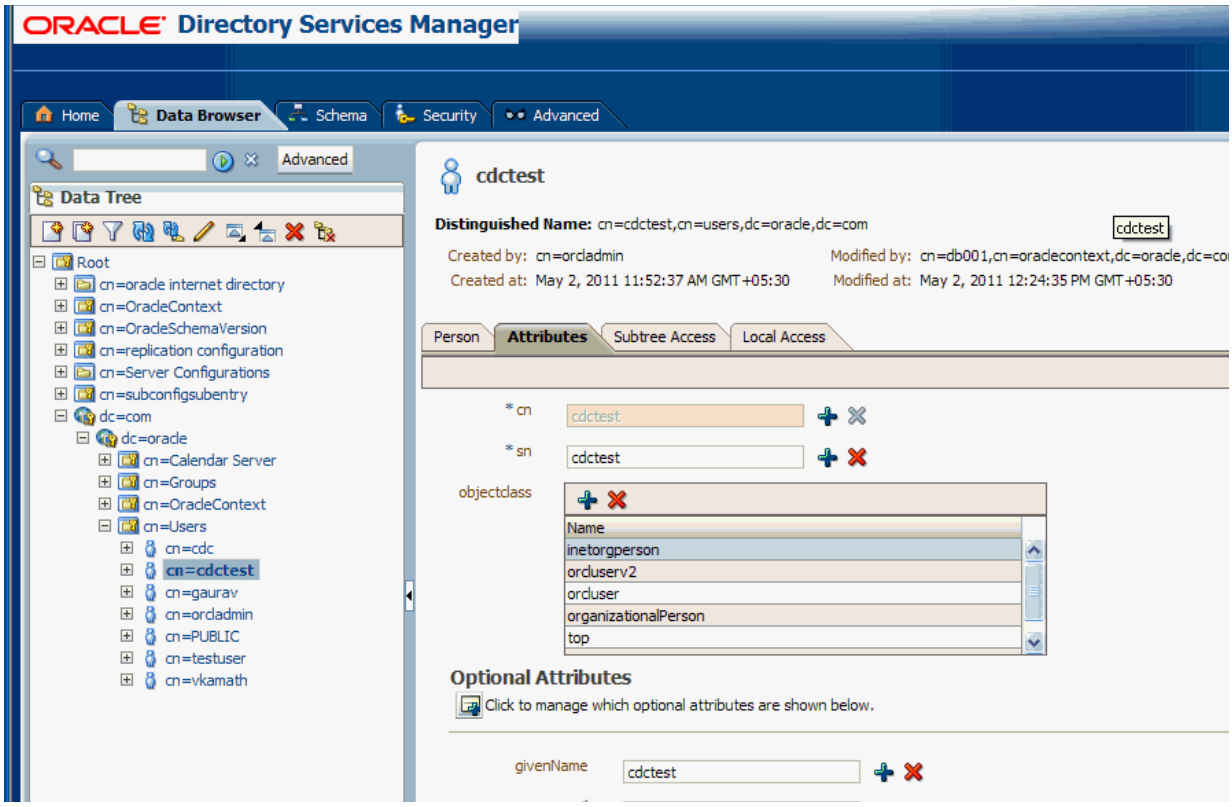
Refer the *Oracle® Fusion Middleware Administrator's Guide for Oracle Internet Directory* for details.

A.1.2.2 Creating an LDAP User Using the Self-Service Console

An LDAP user can view the user information using the OID self-service console. A user can add, modify, or delete user attributes using this console or the command line tool.

Figure A–1 depicts the Self-Service Console used to create an LDAP user.

Figure A–1 Creating an LDAP User Using Self-Service Console



A.2 Install the Oracle Health Sciences Clinical Development Center 3.1 SP1 Client

Install the CDC client using the instructions below. This section contains the following topics:

A.2.1 Prerequisites

- Ensure that no previous installation of the CDC-SCE 3.1 SP1 client exists.
- Ensure relevant software prescribed in the Oracle Health Sciences CDC Prerequisites Guideline document are installed.

- Ensure that the CDC-SCE 3.1 SP1 Database Server Installation Qualification Protocol is executed successfully.
- Install the Oracle Client version 11.2.0.1.0 (32 bit).
- Install the JRE 1.6 (32 bit) and set its path in the environment variables of your local machine.
- Obtain a copy of the approved SCESetupRCPPlugin.exe file for the installation of the Oracle Health Sciences CDC application.

A.2.2 Installing the Oracle Health Sciences Clinical Development Center (CDC) Client

1. Copy the SCESetupRCPPlugin.exe file to a temporary directory on the client machine.
2. Double-click on the SCESetupRCPPlugin.exe file. The **CDC Setup: Installation Folder** window opens.

   You may specify a destination folder. The default destination folder is C:\Program Files\Oracle Health Sciences\CDC.
3. Click **Install**. A CDC Setup confirmation message, **Install for All Users?** is displayed.
4. Click **Yes**. The CDC Setup dialog box closes when installation is complete.
5. Click **Close**. The **CDCSetup: Completed** window closes.
6. Double-click on the CDC shortcut on the desktop or navigate to **Start**, then **Programs**, then **Oracle Health Sciences**, then **CDC**, then select **CDC Client**. The **Oracle Health Sciences CDC Login** window opens.
7. Click **Edit**. The **Login Preferences** dialog opens.
8. Enter the following values:
   - **Server** — Host name
   - **Port**—Port name
   - **Database**—Database name
9. Click **OK**.The **Login Preferences** dialog closes.
10. Use Control+Shift to return to the **Oracle Health Sciences CDC Login** window.
11. Enter *sceadmin* in the **User** and **Password** fields in the **Oracle Health Sciences CDC Login** window.
12. Click **OK**. The **Please select the root folder for SCE Source Control** window opens.
13. Select the working folder and click **OK**. You are logged in successfully to the Oracle Health Sciences CDC Client application.
14. Close the **Oracle Health Sciences CDC Client** window to exit the application.
15. Launch the Oracle Health Sciences Security Manager application from **Start**, then select **Programs**, then **Oracle Health Sciences**, then **CDC**, then select **Security Manager**. The **Login to CDC Security Manager** window opens.
16. Click **Edit DB**. The **Edit Database preference** dialog opens.
17. Edit the Database URL string from jdbc:oracle:thin:@localhost:1521:ORCL to `jdbc:oracle:thin:@<Database server name >:<Database`

Port>:<Database name>, entering the same values for **Server, Port** and **Database** parameters as provided earlier in Step 8.

18. Click **OK**.
19. Login to the Oracle Health Sciences CDC Security Manager as **sceadmin**.
20. Close the window to exit the CDC Security Manager.
21. Launch the Oracle Health Sciences CDC application from **Start**, then select **Programs**, then **Oracle Health Sciences**, then **CDC**, then select the **CDC Client**. Else, click on the desktop CDC shortcut.
22. Login to Oracle Health Sciences CDC with the created user name and password.

A.3 Configuring Your Single Sign-On (SSO) ID with Oracle Business Intelligence Enterprise Edition

This section includes the following tasks:

- "Install Prerequisites for SSO ID Configuration" on page 6
- "Configure Your Database to Use the Directory" on page 6
- "Register Your Database with the Directory" on page 7
- "Create Credentials for a Oracle Health Sciences Clinical Development Center User on the LDAP Server" on page 8

A.3.1 Install Prerequisites for SSO ID Configuration

To configure your SSO ID, you need:

- Oracle 11gR2 RDBMS.
- Weblogic server 10.3.4.0.
- Oracle Identity Management version 11.1.1.5.0

Refer "Installing the Prerequisite Software" on page 1 for details.

A.3.2 Configure Your Database to Use the Directory

Follow the instructions below to configure your database. Relevant information is also available at http://download.oracle.com/docs/cd/E11882_01/network.112/e10744/getstrtd.htm#CBHDDECG.

1. Start NetCA using the netca command.

   On Windows, you can also start NetCA from the Start menu—Select **Start,** then **All Programs**, then **OracleHomeName**, **Configuration and Migration Tools**, **Net Configuration Assistant**.

   On Unix, you can start NetCA using the following command—$ORACLE_HOME/bin/netca.

   The **Oracle Net Configuration Assistant's Welcome** screen is displayed.
2. Select **Directory Usage Configuration** and click **Next.** The **Directory Type** screen is displayed.
3. Select **Oracle Internet Directory** as the **Directory Type** and click **Next.** The **Directory Location** screen is displayed.
4. Enter details of your directory location.

- **Hostname**: The Oracle Internet Directory server hostname.
- **Port**: The LDAP non-SSL and SSL port numbers. Replace these port numbers with 3060 and 3131 respectively.
- **SSL Port**: The SSL port number.

5. Click **Next.** The **Select Oracle Context** screen is displayed.
6. Select the default Oracle Context to use. You must select this if there are multiple identity management realms on the directory server.
7. Click **Next.** The **Directory Usage Configuration: Done** screen is displayed.
8. Confirm that the directory usage configuration is successfully completed. Click **Next**.
9. Click **Finish.**

   NetCA creates an ldap.ora file in the $ORACLE_HOME/network/admin directory. This is the $ORACLE_HOME\network\admin directory in Windows. The ldap.ora file stores the connection information details about the directory.

A.3.3 Register Your Database with the Directory

Use the Database Configuration Assistant (DBCA) tool to register the database with the Oracle Internet Directory.

1. Start DBCA using the DBCA command.

   On Windows, you can also start DBCA from the **Start** menu:

   Click **Start**, then **All Programs**, then **Oracle - OracleHomeName, Configuration and Migration Tools**, and finally **Database Configuration Assistant**.

   On Unix, you can start DBCA using the following command: $ORACLE_HOME/bin/dbca.

   The **Welcome** screen is displayed.
2. Click **Next**. The **Database Configuration Assistant:Operations** screen is displayed.
3. Select **Configure Database Options**. Click **Next**.The **Database** screen appears.
4. Select the database name that to configure. If you are not using operating system authentication, you might also be asked to enter SYS user credentials.
5. Click **Next**. The **Management Options** screen is displayed.
6. Select **Keep the database configured with Database Control** if you want to continue using Database Control to manage the database. You can also choose to use Grid Control to manage the database.
7. Click **Next**. The **Security Settings** screen is displayed.
8. Select **Keep the enhanced 11g default security settings** and click **Next**. The **Network Configuration** screen is displayed.
9. Select **Yes, register the database** to register the database with the directory:
   a. Enter the distinguished name (DN) of a user who is authorized to register databases in Oracle Internet Directory.
   b. Enter the password for the directory user.

c. Enter a wallet password to protect the wallet. The wallet password that you specify is different from the database password.

d. Re-enter the password in the **Confirm Password** field. Click **Next**.

Note: The database uses a randomly generated password to log in to the directory. This database password is stored in an Oracle wallet that you can also use to store certificates for SSL connections.

The **Database Components** screen is displayed.

10. Click **Next.** The **Connection Mode** screen is displayed.
11. Select **Dedicated Server Mode** or **Shared Server Mode**.
12. Click **Finish.** The **Confirmation dialog box** appears.
13. Click **OK**.

Note: The default wallet is created in the $ORACLE_BASE/admin/database_sid/wallet directory.

Verify that automatic login for the wallet is enabled by checking for the **cwallet.sso** file in the wallet directory. If the file is not present, open the wallet using Oracle Wallet Manager, and use the option to enable automatic login.

Note: During the Net configuration you might get an **Anonymous Bind** error. If so, change the attribute value of `orclAnonymousBindsFlag = 1`.

Use the following command and file:

Command: `ldapmodify -D cn=orcladmin -q -p portNum -h hostname -f ldif File. For example, ldapmodify -D cn=orcladmin -q -p port Num -h localhost -f modfile.ldif`

Create a file (modfile.ldif) using admin to OID server that contains:

```
dn: cn=oid1,cn=osdldapd,cn=subconfigsubentry

Changetype: modify

replace: orclAnonymousBindsFlag

OrclAnonymousBindsFlag: 1
```

A.3.4 Create Credentials for a Oracle Health Sciences Clinical Development Center User on the LDAP Server

Follow this procedure to create CDC user credentials on the LDAP server.

1. Create a CDC user using the security manager and assign the protocol_admin role. While creating a CDC user, select the **Use Database Authentication** option.

   Refer to section "Create an LDAP User" on page 2 for details.

2. Create a user on the LDAP server with the same name as the CDC user. Refer to section "Create an LDAP User" on page 2 for details.
3. Create the Oracle Internet Directory (OID) user and its attributes by using either command line tools or OID's self service console (`http://host:port/odsm for 11g and http://host:port/oiddas for 10g`).

   Download the *Oracle® Fusion Middleware Administrator's Guide for Oracle Internet Directory* at `http://download.oracle.com/docs/cd/E14571_01/oid.1111/e10029/toc.htm`.

   Refer to section "Create an LDAP User" on page 2 for details. We recommend that you create an OID user using command line tools.
4. Login to the database as System manager.
5. Edit the CDC user to be able to identify it globally. The identification needs to include the "distinguished name" of the user. Execute the following command:

   ```
   Alter user cdctest identified globally as
   'cn=cdctest,cn=users,dc=oracle,dc=com';
   ```

   where; the USER_NAME is replaced with the correct user account and DISTINGUISH_NAME is replaced with the LDAP information.

After completing all the configuration, you can log in to the CDC client as well as the database application using LDAP password authentication.

A.4 Configuring Oracle Business Intelligence Enterprise Edition (OBIEE) with Oracle Internet Directory (OID)

This section includes the following topics:

A.4.1 Install the Prerequisite Software

Complete the following tasks:

1. Install Oracle 11g RDBMS.
2. Create Database DB003, with AL32UTF8, processes = 500 and OPEN_CURSOR=600
3. Obtain RCU. It is available either on its own installation CD-ROM in the `bin` directory, or in a .zip file on Oracle Technology Network (OTN): `http://www.oracle.com/technology/software/products/middleware/htdocs/111110_fmw.html`

A.4.2 Configure the Database

After creating a user, configure the database to use the LDAP directory.

For more information, refer to Chapter 2, "Getting Started with Enterprise User Security ", of the *Oracle® Database Enterprise User Security Administrator's Guide 11gRelease 2 (11.2)*. The guide is available for download at:

http://download.oracle.com/docs/cd/E11882_01/network.112/e10744/getstrtd.htm#CBHDDECG

Perform steps mentioned in Sections 2.1 and 2.2 to configure and register your database.

> **Tip:** When you perform Netconfiguration, you may get the Anonymous Bind error. Change the attribute value of orclAnonymousBindsFlag to 1. Use the following command:
>
> ```
> ldapmodify -D cn=orcladmin -q -p portNum -h hostname
> -f ldif File
> ```
>
> A sample .ldif file has the following content:
>
> dn: cn=oid1,cn=osdldapd,cn=subconfigsubentry
>
> Changetype: modify
>
> replace: orclAnonymousBindsFlag
>
> OrclAnonymousBindsFlag: 1

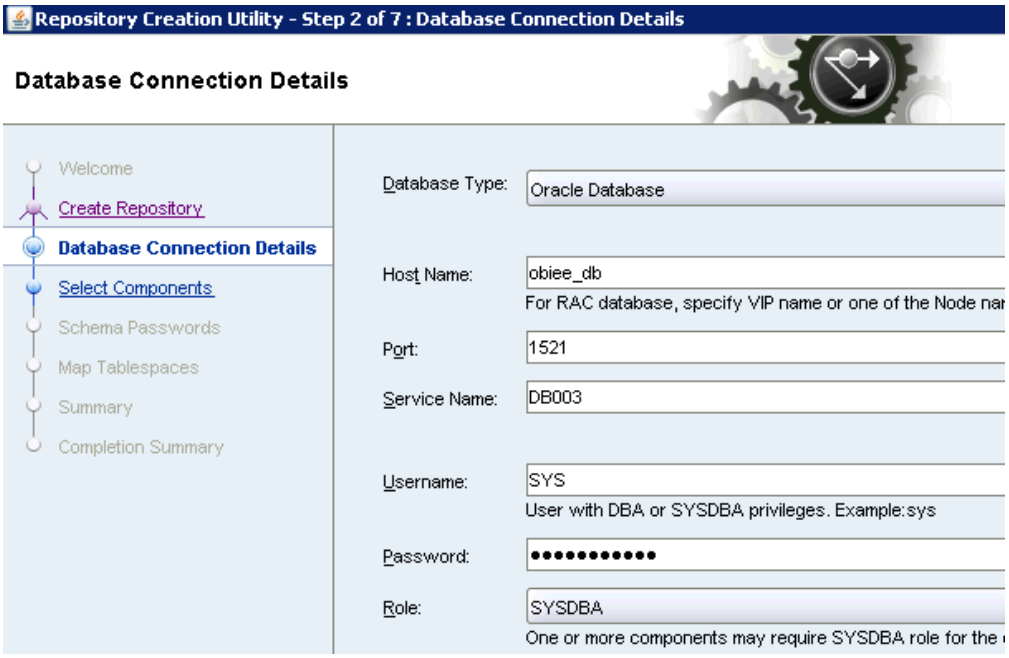
A.4.3 Run the Repository Creation Utility (RCU) to Create Oracle Business Intelligence Database Schemas

You can run RCU locally from the CD-ROM or your RCU_HOME, or remotely. If you are not allowed to install components in the database server, you can run RCU directly from the CD.

To create the Oracle Business Intelligence schemas using RCU:

1. Do either of the following:
   - If you downloaded and extracted the RCU .zip file, access the `bin` directory in the RCU_HOME.
   - If you have the RCU CD-ROM, insert the CD-ROM into your computer and access the `bin` directory.
2. Start RCU. In Unix:**/rcu**. In Windows: **rcu.bat**. The **Welcome** screen opens.
3. Click **Next**. The **Create Repository** screen opens.
4. In the **Create Repository** screen, select **Create** and then click **Next**. The **Database Connection Details** screen opens.
5. In the **Database Connection Details** screen, select the type of database on your system. You must create the Oracle Business Intelligence schemas on this database. Enter the necessary credentials for RCU to be able to connect to your database.

Figure A–2 Repository Creation Utility-Database Connection Details



6. Click **Next**. The **Checking Prerequisites** screen opens. After checking is complete with no errors, click **OK** to close the screen and proceed to the **Select Components** screen

7. In the **Select Components** screen, near the top of the screen, select **Create a new Prefix**. The default prefix is **DEV**. Enter another prefix if you prefer.

   Oracle Business Intelligence 11g Installer automatically creates schema names in the format prefix_schemaname. For example, if you enter the prefix BI, Oracle Business Intelligence 11g Installer creates a schema named BI_BIPLATFORM.

   Important: Make a note of these schema names and the prefix values from this screen. You need them to configure your products later in the installation process.

   ---

8. Click the plus sign (+) next to the Business Intelligence component group. Select **Business Intelligence Platform** (a check mark appears next to it). This action automatically selects the Metadata Services (MDS) schema (under the AS Common Schemas group), which is also required by Oracle Business Intelligence.

   If you have another MDS schema installed to use with Oracle Business Intelligence, deselect the **Metadata Services (MDS)** check box and ignore the warning message that appears in the **Messages** box.

   Do not click the **Oracle AS Repository Components check box** because this configures RCU to install many other schemas that are not required by Oracle Business Intelligence.

9. Click **Next.** The **Checking Prerequisites** screen opens. After the checking is complete with no errors, click **OK** to close the screen and proceed to the **Schema Passwords** screen.

10. In the **Schema Passwords** screen, select **Use same password for all schemas**. Enter and confirm a password for the schemas.

11. Click **Next** to proceed to the **Map Tablespaces** screen. In the **Map Tablespaces** screen, confirm the schema names.Click **Next** to create the tablespaces for the schemas.

    After the tablespaces are created with no errors, click **OK** to close the screen and proceed to the **Summary** screen.

12. In the **Summary** screen, click **Create**. The **Create** screen opens and RCU creates the schemas. After the schemas are created with no errors, the **Completion Summary** screen opens.

13. In the **Completion Summary** screen, click **Close**.

A.4.4 Install Oracle Business Intelligence Enterprise Edition (OBIEE) 11g

Follow the instructions below to install OBIEE 11g.

1. Download the latest OBIEE 11g (11.1.1.5.0) from:

   http://www.oracle.com/technetwork/middleware/bi-enterprise-edition/downloads/bus-intelligence-11g-165436.html

2. Extract the downloaded copy into two different folders.

3. Download and use OBIEE installation instructions from:

   https://debaatobiee.wordpress.com/tag/obiee-11g-install-guide/

   or

   http://download.oracle.com/docs/cd/E12839_01/install.1111/e12002/oid.htm#CIHHFIGC

   The following is a sample of OBIEE settings:

   - **Administrator details**

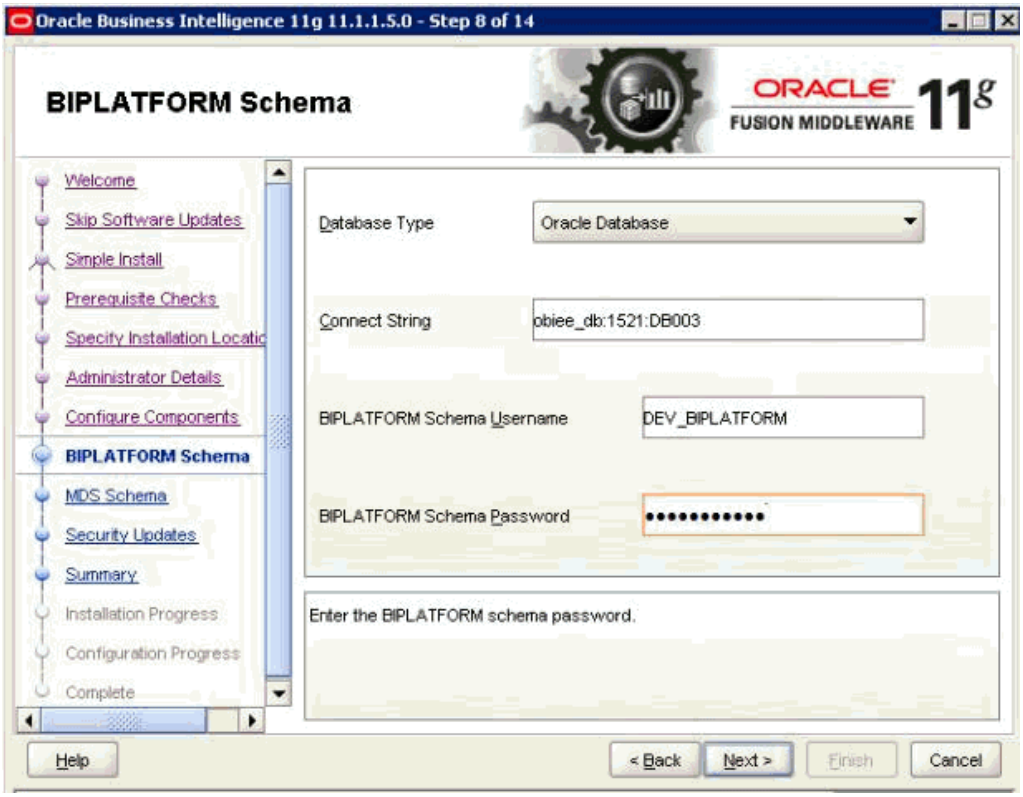
     Username: weblogic

     Password: weblogic1

     Confirm Password: weblogic1

   - BIPLATFORM Schema

Figure A–3 Biplatform Schema Settings

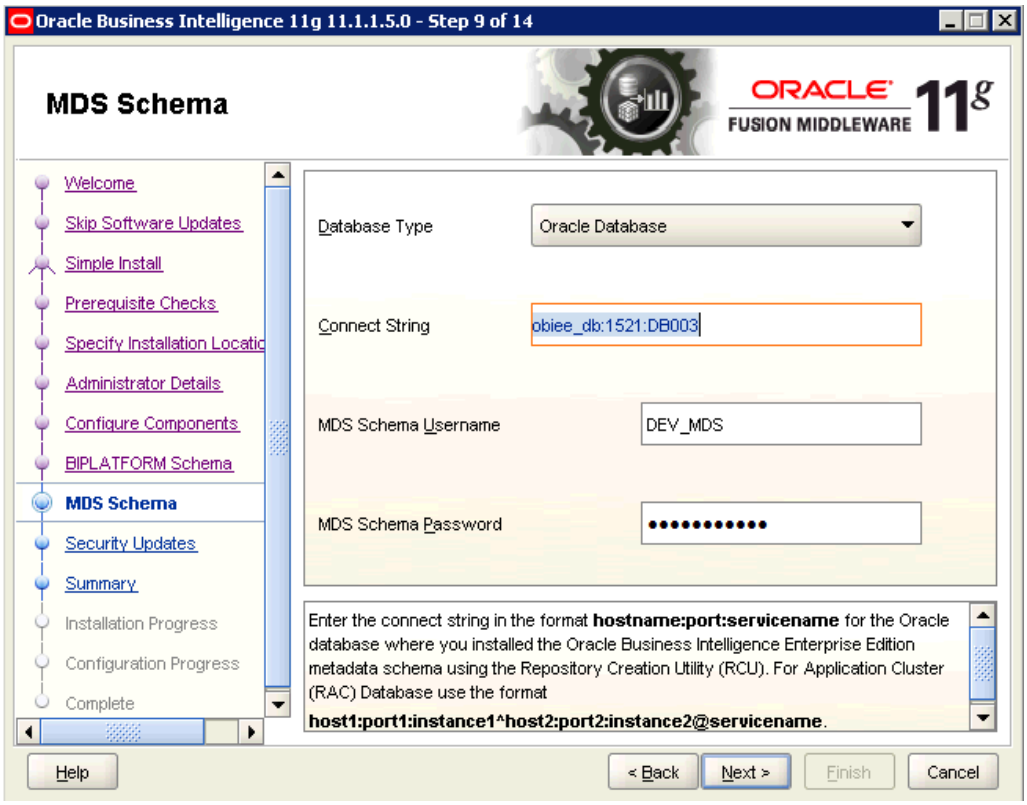


Enter the following details and click **Next**.

Database Type
Connect String
BIPLATFORM Schema Username
BIPLATFORM Schema Password

- MDS Schema:

Figure A–4 MDS Schema Settings



Enter the following details and click **Next** to complete the installation.

Database Type
Connect String
MDS Schema Username
MDS Schema Password

During the installation, you may be asked to enter the Disk path before you can proceed with the installation.

A.4.5 Configure OBIEE with OID for Authentication

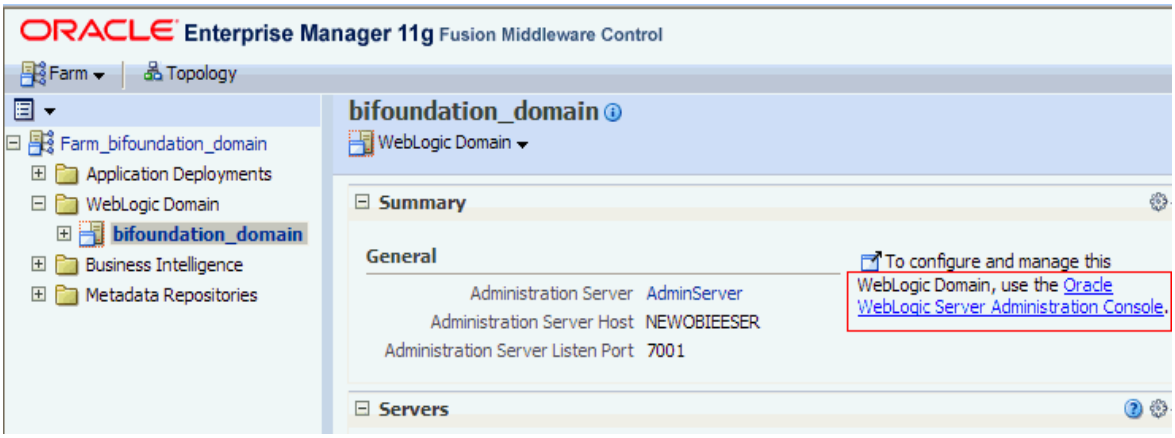
To configure OBIEE with OID:

1. Use the following link to download configuration instructions.

   `http://download.oracle.com/docs/cd/E14571_01/bi.1111/e10543/privileges.htm`

2. Use the Enterprise Manager Link to access the **Oracle Weblogic Server (WLS) Administration Console**. The User Name is **weblogic,** password is **weblogic1**.

Figure A–5 Enterprise Manager Link to Oracle WLS Console



3. In the Oracle WebLogic Server Administration Console, click **Lock & Edit** in the **Change Center**.
4. Select **Security Realms** from the left pane and click **myrealm**.
5. Select the **Providers** tab, then select the **Authentication** subtab.
6. Click **New** to launch the **Create a New Authentication Provider** page.
7. Enter values in the **Create a New Authentication Provider** page:
8. Click the new Authenticator Provider in the **Name** column to display the Settings for <*Authentication Provider Name*> page.
9. Select the **Configuration\Common** tab, and use the **Control Flag** drop-down list to select **SUFFICIENT**. Click **Save**.
10. Select the **Provider Specific** tab. Specify details for the **Connection, Users, Static and Dynamic Groups**, and **General Area** under the Provider Specific tab.
11. Click **Save**.
12. At the main **Settings for myrealm** page, select the **Providers** tab, then select the **Authentication** subtab.
13. Click **Reorder** to open the Reorder Authentication Providers page.
14. Select the name of the Oracle Internet Directory authentication provider (for example, MyOIDDirectory) and use the arrow buttons to move it into the first position in the list. Click **OK**.
15. Click DefaultAuthenticator in the **Name** column to view the **Settings for DefaultAuthenticator** page.
16. Select the **Configuration\Common** tab, and use the **Control Flag** drop- down list to select **SUFFICIENT**, then click **Save**.

A.4.6 Configure the User Name Attribute in the Identity Store

To configure the User Name attribute:

1. In **Oracle Enterprise Manager - Fusion Middleware Control**, navigate to \Weblogic domain\bifoundation_domain in the navigation pane.
2. Right-click **bifoundation_domain** and select **Security**, then select **Security Provider Configuration** to view the Security Provider Configuration page.

3. In the **Identity Store Provider** area, click **Configure** to display the Identity Store Configuration page.
4. In the **Custom Properties** area, use the **Add** option to add the following two **Custom Properties**:

   User.login.attr and **username.attr**
5. Click **OK** to save changes.
6. Restart the Admin Server.

A.4.7 Verify OID Users and Groups in the WebLogic Console

You must add the OID user to the BISystem/BIAdministrators Application Role.

1. In the **Fusion Middleware Control** target navigation pane, go to the Oracle WebLogic Server domain in which Oracle Business Intelligence is installed. For example, bifoundation_domain.
2. Go to the **Application Roles** page in Fusion Middleware Control.
3. In the **Select Application Stripe to Search** list, select **OBI** from the list. Click the search arrow to the right of the **Role Name** field.
4. Select **BIAdministrators** Application Role and click **Edit**. You can also choose to edit other OBIEE-specific roles displayed in the list.
5. In the **Edit Application Role** page, click **Add Group**/**Add User**.
6. In the **Add User** dialog, search for the trusted user created in Oracle Internet Directory. Use the shuttle controls to move the trusted user name (**BIAdministrators**) from the **Available Users** list to the **Selected Users** list.
7. Click **OK**. The trusted user (**BIAdministrators**) contained in Oracle Internet Directory is now a member of the BISystem Application Role.
8. Add the trusted user's credentials to the **oracle.bi.system** credential map.
9. From the Fusion Middleware Control target navigation pane, expand the form, then expand **WebLogic Domain**, and select **bifoundation_domain**.
10. From the WebLogic Domain menu, select **Security**, then **Credentials**.
11. Open the **oracle.bi.system** credential map, select **System User** and click **Edit**.
12. In the **Edit Key** dialog, enter BISystemUser (or name you selected) in the **User Name** field. In the **Password** field, enter the trusted user's password that is contained in Oracle Internet Directory.
13. Click **OK**.
14. In **WebLogic Console**, click **myrealm** to view the **Settings** for <Realm> page, select the **Roles and Policies** tab, and add the new System user to the **Global Admin Role**.
15. Start the Managed Servers. The new trusted user from Oracle Internet Directory is configured for Oracle Business Intelligence.

Note: If you have created a trusted OID Group, then in the **Add Group** option, select the corresponding group and include it in an **Application Role**. This ensures that OID users under the same group automatically get included in the Application Role.)

---

16. Create the **BISystem** user in OID.

B

Oracle Healthcare Data Warehouse Foundation Tables

This appendix includes the following sections:

B.1 Mandatory Oracle Healthcare Data Warehouse Foundation Code Types Table

Oracle Healthcare Data Warehouse Foundation (HDWF) mandatory Code Types require configuration from source system(s) to populate respective Cohort data mart tables.

Table B–1 Mandatory HDWF Code Types Tables

OHSCE Data Mart Table(s)	Code Type	Description	Sample Value
W_EHA_RESEARCH_PATIENT_D	ADDRESS_STATUS_CODE	The coded representation of the status of the address.	For example, current, active, and inactive.
W_EHA_RESEARCH_PATIENT_D	ADDRESS_TYPE	The type of address.	For example, Mailing, Business, and Home.
W_EHA_UOM_D	AGE_AT_FIRST_ONSET_UOM_CODE	The coded representation of the unit of measure for the age at first onset value as it pertains to the diagnosis.	For example, Years, Months, Days, and Hours.
W_EHA_ANATOMICAL_SITE_D W_EHA_SPECIMEN_PATIENT_H	ANATOMICAL_SITE_CODE	The coded representation of the anatomical site for the diagnosis, specimen, etc.	For example, Arterial system structure.
W_EHA_CONSENT_STATUS_D	CONSENT_STATUS_CODE	The coded representation of the status of the consent form.	For example, Active, and Not Active.
W_EHA_CONSENT_D	CONSENT_TYPE	The coded representation of the type of the consent.	For example, Surgical, Study, Blood Products, and Special Procedure.
W_EHA_RESEARCH_PATIENT_D	COUNTRY_CODE	The coded representation of the country in which the patient is located.	For example, United States, and Canada.
W_EHA_DIAGNOSIS_D W_EHA_DX_PATIENT_H	DIAGNOSIS_CODE	The coded representation of the diagnosis.	For example, Leukemia.
W_EHA_DIAGNOSIS_STATUS_D W_EHA_DX_PATIENT_H	DIAGNOSIS_STATUS_CODE	The coded representation of the status of the diagnosis.	For example, recurrent, active, and not active.

Table B–1 (Cont.) Mandatory HDWF Code Types Tables

OHSCE Data Mart Table(s)	Code Type	Description	Sample Value
W_EHA_DIAGNOSTIC_TEST_D W_EHA_DIAGTST_PATIENT_H W_EHA_DIAGTST_SPEC_DHL W_EHA_DIAGTST_SUBADM_DHL	DIAGNOSTIC_ TEST_CODE	The coded representation of the diagnostic test.	For example, Chest x-ray.
W_EHA_UOM_D	DOSE_UOM_CODE	The coded representation of the unit of measure of the dose of substance administered.	For example, milligrams and grams.
W_EHA_ETHNICITY_D	ETHNICITY_CODE	The coded representation that best describes the ethnic origin of the patient.	For example, "1" = Spanish/Hispanic Origin, "2" = Not of Spanish/Hispanic Origin, "9" = Unknown
W_EHA_UOM_D	FREQUENCY_ UOM_CODE	The coded representation of the units of measure for the substance frequency.	For example, BID = Twice a Day.
W_EHA_ETHNICITY_D	GENDER_CODE	The coded representation that best describes the gender of the patient.	For example, "M" = Male, "F" = Female.
W_EHA_DIAGTST_PROC_DHL	INTERVENTION_ OBSERVATION_ RELATIONSHIP_ TYPE	The coded representation of the relationship type between the diagnostic test and respective results.	For example, Resulting.
W_EHA_RESEARCH_PATIENT_D	MARITAL_STATUS_ CODE	The coded representation of the patient's marital (civil) status.	For example, Married and Unmarried.
W_EHA_MEDICATION_D W_ EHA_SUBADMN_PATIENT_H W_ EHA_PROC_SUBADMN_DHL	MEDICATION_ CODE	The coded representation of the generic names associated with a medication.	For example, the second segment of numbers in an NDC. 451 from 50580-451-03 signifies 500 mg Acetaminophen.
W_EHA_UOM_D	OBSERVATION_ VALUE_UOM_ CODE	The coded representation of the unit or measure of a numeric value for an test result.	For example, mg/dl.
W_EHA_PATIENT_HISTORY_D	PATIENT_ HISTORY_CODE	The coded representation of the representation of the type of Patient History.	For example, Tobacco Use, Alcohol Use.
W_EHA_PROCEDURE_D W_EHA_ PROC_PATIENT_H W_EHA_ PROC_SUBADMN_DHL W_EHA_ DIAGTST_PROC_DHL	PROCEDURE_ CODE	The coded representation of the procedure.	For example, brain tumor resection.
W_EHA_RACE_D	RACE_CODE	The coded representation that best describes the race of the party.	For example, "01" = White, "02" = African American (Black), "03" = Native American (American, Indian/Eskimo/Aleut), "04" = Asian, "05" = Native Hawaiian or Other Pacific Islander, "88" = Other Race, "99" = Unknown
W_EHA_DIAGTST_SUBADM_DHL W_EHA_PROC_SUBADMN_DHL	RELATED_ INTERVENTION_ RELATIONSHIP_ TYPE	The coded representation of the relationship type between the diagnostic test or procedure (intervention) and medications or results respectively.	For example, Pre, Intra and Post Intervention Medication; or Pre, Intra, Post Intervention Diagnostic Test.
W_EHA_UOM_D	SPECIMEN_ QUANTITY_UOM_ CODE	The coded representation of the units for measure for the amount of specimen collected.	For example, millimoles/liter, and mg/dL.

Table B–1 (Cont.) Mandatory HDWF Code Types Tables

OHSCE Data Mart Table(s)	Code Type	Description	Sample Value
W_EHA_SPECIMEN_D	SPECIMEN_TYPE_ CODE	The coded representation of the type of Specimen.	For example, Blood, Urine, and Sputum.
W_EHA_RESEARCH_PATIENT_D	STATE_CODE	The coded representation of the code for state within a country.	For example, AZ, CO, MO, and CA.
W_EHA_RESEARCH_PATIENT_D	POSTAL_CODE	The coded representation of the Zip Code assigned by the Postal Service to the patient's principal residence.	For example, 33101.

B.2 Oracle Healthcare Data Warehouse Foundation Physical Table

You must load the following HDWF physical tables for OHSCE to function properly.

Table B–2 HDWF Physical Tables

HDWF Physical Table Name	HDWF Logical Entity Name
HDM_CD_HIER	Code Hierarchy
HDM_CD_REPOSITORY	Code Repository
HDM_CD_REPOSITORY_CD_TYP	Code Repository Code Type
HDM_CD_SYS	Code system
HDM_CD_TYP	Code Type
HDM_CNRN	Concern
HDM_CNRN_ANATSITE	Concern Anatomical Site
HDM_CNSNT	Consent
HDM_IND_PRTY	Individual Party
HDM_IND_PRTY_ETHN	Individual Party Ethnicity
HDM_IND_PRTY_RC	Individual Party Race
HDM_INTVN	Intervention
HDM_INTVN_OBSV	Intervention Observations
HDM_INTVN_SUBST	Intervention Substance
HDM_OBSV	Observation
HDM_PRTY_ADDR	Party Address
HDM_PT	Patient
HDM_PT_HX	Patient History
HDM_RELTD_INTVN	Related Intervention
HDM_SPCMN	Specimen
HDM_SUBADMN	Substance Administration
HDM_SUBST_HX	Substance History

Index

P

R

S

T

U

V