Oracle® Health Sciences Information Gateway

CONNECT Gateway and Adapter Installation and Configuration Guide

Release 2.0.1

E37024-02

October 2013

ORACLE®

Oracle Health Sciences Information Gateway CONNECT Gateway and Adapter Installation and Configuration Guide, Release 2.0.1

E37024-02

Contents

3 Configuring the Oracle Health Sciences Information Gateway CONNECT Gateway and Adapter

A Running Oracle Health Sciences Information Gateway CONNECT Installer

B Configuring Oracle CONNECT Adapters with Oracle Components

C Creating and Importing Certificates Using the GlassFish Self-Signed Certificate Scripts

Preface

The Oracle Health Sciences Information Gateway (OHIG) leverages Integrating the Healthcare Enterprise (IHE) profiles, CONNECT reference architecture, Direct, and Oracle WebLogic to orchestrate secure, health policy-based exchanges over the Internet.

Audience

This document is intended for users who want to install and use OHIG to participate in standards-based health information exchange activities within their organizations or with other organizations.

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.

Related Documents

For more information, see the following documentation sets:

Oracle Health Sciences Information Gateway

- *Oracle Health Sciences Information Gateway CONNECT Gateway and Adapter Installation and Configuration Guide*
- *Oracle Health Sciences Information Gateway Cross Community Access Installation and Configuration Guide*
- *Oracle Health Sciences Information Gateway Cross Community Access User Guide*
- *Oracle Health Sciences Information Gateway Secure Health Email Installation and Configuration Guide*
- *Oracle Health Sciences Information Gateway Security Guide*

- *Oracle Health Sciences Information Gateway Release Notes*

Oracle Health Sciences Information Manager

- *Oracle Health Sciences Information Manager Health Record Locator Installation and Configuration Guide*
- *Oracle Health Sciences Information Manager Policy Engine Installation and Configuration Guide*
- *Oracle Health Sciences Information Manager Policy Monitor Installation and Configuration Guide*
- *Oracle Health Sciences Information Manager Health Record Locator User Guide*
- *Oracle Health Sciences Information Manager Security Guide*
- *Oracle Health Sciences Information Manager Release Notes*

Oracle Healthcare Master Person Index

- *Oracle Healthcare Master Person Index Australia Patient Solution User's Guide*
- *Oracle Healthcare Master Person Index United States Patient Solution User's Guide*
- *Oracle Healthcare Master Person Index United Kingdom Patient Solution User's Guide*
- *Oracle Healthcare Master Person Index Provider Index User's Guide*
- *Oracle Healthcare Master Person Index User's Guide*
- *Oracle Healthcare Master Person Index Installation Guide*
- *Oracle Healthcare Master Person Index Working With IHE Profiles User's Guide*
- *Oracle Healthcare Master Person Index Analyzing and Cleansing Data User's Guide*
- *Oracle Healthcare Master Person Index Data Manager User's Guide*
- *Oracle Healthcare Master Person Index Configuration Guide*
- *Oracle Healthcare Master Person Index Standardization Engine Reference*
- *Oracle Healthcare Master Person Index Configuration Reference*
- *Oracle Healthcare Master Person Index WebLogic User's Guide*
- *Oracle Healthcare Master Person Index Command Line Reports and Database Maintenance User's Guide*
- *Oracle Healthcare Master Person Index Loading the Initial Data Set User's Guide*
- *Oracle Healthcare Master Person Index Match Engine Reference*
- *Oracle Healthcare Master Person Index Message Processing Reference*

Conventions

The following text conventions are used in this document:

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 describes the minimum hardware and software requirements for installing Oracle Health Sciences Information Gateway (OHIG) CONNECT.

This chapter includes the following sections:

1.1 Hardware Requirements

The following are the hardware requirements for installing OHIG CONNECT Gateway and Adapter:

- 4 GB (4096 MB) of RAM
- 12 GB of Disk Space
- 16 GB of disk space for 64 bit

1.2 Software Requirements

The following are the software requirements for installing OHIG CONNECT Gateway and Adapter:

- Java 1.7 executable in path
- Oracle Database 10+ (11g Release 1)
- GlassFish Enterprise Server 2.1.1 Patch 16 or higher
- WebLogic Server 10.3.6.0 (11g Release 1)
- Oracle Enterprise Linux 5.5 or higher

Configuration Requirements

Apache Ant 1.8.2 executable in path

```
PATH=$PATH:<install_dir>/apache-ant-1.8.2/bin
```

Oracle Software Requirements

- Oracle Health Sciences Information Manager (OHIM) Record Locator 2.0 or higher
- Oracle Health Sciences Information Manager (OHIM) Policy Engine 2.0 or higher

- Oracle Healthcare Master Person Index (OHMPI) 2.0.1 or higher
- Oracle Healthcare Transaction Database (HTB) 6.1 or higher

1.3 Downloading Oracle Health Sciences Information Gateway CONNECT Gateway and Adapter

To download the Oracle Health Sciences Information Gateway CONNECT Gateway and Adapter, perform the following tasks:

1. Navigate to `http://edelivery.oracle.com`.
2. Enter your Registration information, accept the Agreement Terms by selecting the checkboxes, then click **Continue**.
3. From the **Select a Product Pack** drop-down menu, select **Health Sciences**.
4. From the **Platform** drop-down menu, select **Linux x86**.
5. Click **Go**.
6. Select **Oracle Health Sciences Information Gateway Media Pack**.
7. Click **Continue**.
8. Click **Download** for the following and save the files to your system:
   - **Oracle Health Science Information Gateway 2.0.1 CONNECT Gateway and Adapter**
9. Extract the files to view the *Oracle Health Sciences Information Gateway CONNECT Gateway and Adapter Installation and Configuration Guide* and get the compressed tar file (`*.tgz`).

2

Setting Up Oracle Health Sciences Information Gateway CONNECT Gateway and Adapter

This chapter provides general directions for setting up OHIG CONNECT. It contains the following topics:

2.1 Prerequisites

2.1.1 Prerequisites for Installing Common Oracle Health Sciences Information Gateway CONNECT

Perform the following steps for a common install of OHIG CONNECT:

1. Extract the installer .tgz file by executing the following commands:

```
$ tar -zxvf ohig_connect_installer.tgz
$ cd ohig_connect_installer
```

2. Create database tables by executing the following commands:

```
$ cd <install_dir>/addons/connect/oracle_db
$ sqlplus
SQL*Plus: Release 11.1.0.6.0 - Production on Thu Jul 19 12:34:18 2012
Enter user-name: sys as sysdba
Enter password:
SQL> @nhincdb_oracle.sql;
Commit complete.
SQL> quit
```

2.1.2 Prerequisites for WebLogic Oracle Health Sciences Information Gateway CONNECT Install

2.1.2.1 Setting up Java Secure Socket Extension (JSSE) Compatible Demo Trust and Identity Keystores

2.1.2.1.1 Creating Java Secure Socket Extension (JSSE) Compatible Keystores from DemoTrust.jks and DemoIdentity.jks

Example Environment Variables

```
MW_HOME=/home/hiauser/Oracle/Middleware
JAVA_HOME=/home/common/java/jdk1.7.0
JAVA_VENDOR=Sun
WL_SERVER_DIR=$MW_HOME/wlserver_10.3
WL_DOMAIN_DIR=$MW_HOME/user_projects/domains/domain1
```

Execute the following commands:

1. List the original demo truststore:

   ```
   $ keytool -list -keystore $WL_SERVER_DIR/server/lib/DemoTrust.jks -storepass
   DemoTrustKeyStorePassPhrase -v
   ```

2. List the original demo identity keystore:

   ```
   $ keytool -list -keystore $WL_SERVER_DIR/server/lib/DemoIdentity.jks -storepass
   DemoIdentityKeyStorePassPhrase -v
   ```

3. Create Java Secure Socket Extension (JSSE) compatible demo truststore:

   ```
   $ keytool -importkeystore -srckeystore $WL_SERVER_DIR/server/lib/DemoTrust.jks
   -destkeystore $WL_SERVER_DIR/server/lib/DemoTrustChangeit.jks -srcstoretype JKS
   -deststoretype JKS -srcstorepass DemoTrustKeyStorePassPhrase -deststorepass
   changeit
   ```

4. Create JSSE compatible demo identity keystore:

   ```
   $ keytool -importkeystore -srckeystore $WL_SERVER_
   DIR/server/lib/DemoIdentity.jks -destkeystore $WL_SERVER_
   DIR/server/lib/DemoIdentityChangeit.jks -srcstoretype JKS -deststoretype JKS
   -srcstorepass DemoIdentityKeyStorePassPhrase -deststorepass changeit -srcalias
   demoidentity -destalias demoidentity -srckeypass DemoIdentityPassPhrase
   -destkeypass changeit -noprompt
   ```

5. List JSSE compatible demo truststore:

   ```
   $ keytool -list -keystore $WL_SERVER_DIR/server/lib/DemoTrustChangeit.jks
   -storepass changeit -v
   ```

6. List JSSE compatible demo identity keystore:

   ```
   $ keytool -list -keystore $WL_SERVER_DIR/server/lib/DemoIdentityChangeit.jks
   -storepass changeit -v
   ```

2.1.2.1.2 Configuring Custom WebLogic Trust and Identity Keystores

1. Update WebLogic security through the console:
   a. Log into `http://localhost:7001/console/`.
   b. Navigate to **Home** > **Summary of Environment** > **Summary of Servers** > **AdminServer**.
   c. Under the **General** tab, enter the following values in the respective fields:

      Listener Port Enabled =true

      Listener Port =7001

      SSL Listener Port Enabled =true

      SSL Listener Port =7002
   d. Under the **Configuration/Keystores** tab, enter the following values in the respective fields:

      Custom Identity and Custom Trust =true

      Keystores =Custom Identity and Custom Trust

      Custom Identity Keystore =/home/hiauser/Oracle/Middleware/wlserver_10.3/server/lib/DemoIdentityChangeit.jks

      Custom Identity Keystore Type =JKS

      Custom Identity Keystore Passphrase =changeit

      Custom Trust Keystore =/home/hiauser/Oracle/Middleware/wlserver_10.3/server/lib/DemoTrustChangeit.jks

      Custom Trust Keystore Type =JKS

      Custom Trust Keystore Passphrase =changeit
   e. Under the **Configuration/SSL** tab, enter the following values in the respective fields:

      Private Key Location =from Custom Identity Keystore

      Private Key Alias =demoidentity

      Private Key Passphrase =changeit

      Certificate Location =from Custom Identity Keystore

      Trusted Certificate Authorities =from Custom Trust Keystore
   f. Under the **Advanced** tab, enter the following values in the respective fields:

      Select Hostname Verification =None

      Note: This setting is not recommended for the production environment.

      ---

2. Install shared libraries:
   - `jsf-1.2.war`
   - `jstl-1.1.2.war`

   Shared libraries can be found in `/home/hiauser/Oracle/Middleware/wlserver_10.3/common/deployable-libraries`.

Note: The following is required for OHIG CONNECT Universal Client GUI:

```
jsf-1.2.war
jstl-1.1.2.war
```

3. Edit WebLogic installation information:

Note: This script should be used to start WebLogic before and after deploying OHIG CONNECT.

```
$ cd <install_dir>/addons/connect/scripts
$ vi connect-start-weblogic.sh
```

4. Use the OHIG CONNECT WebLogic Start Script:

```
$ sh ./connect-start-weblogic.sh
```

2.1.3 Prerequisites for Testing Oracle Health Sciences Information Gateway CONNECT

1. Update firewall settings. For more information on updating firewall settings, refer to Setting up the Network on page 2-4.
2. Exchange certificates between gateway and adapter machines. For more information on exchanging information, refer to Exchanging Certificates on page 2-5.
3. Load sample documents.

```
$ cd <install_dir>/addons/connect/oracle_db $sqlplus
SQL*Plus: Release 11.1.0.6.0 - Production on Thu Jul 19 12:34:18 2012
Enter user-name: sys as sysdba
Enter password:
SQL> DROP TABLE nhincuser.document;
Table dropped.
SQL> quit
$ imp nhincuser/nhincpass file=populateTestData_oracle.dmp log=output.log
full=yes
Import terminated successfully without warnings.
```

2.2 Setting up the Network

This section provides information for the GlassFish network setup and the WebLogic network setup.

2.2.1 Setting up the GlassFish Network

Perform the following steps to setup the GlassFish network:

1. Allow external connections to http port and SSL http port by opening incoming ports:

```
# cd /etc/sysconfig/# vi iptables
```

2. Add the following lines:

```
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 8080 -j
ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 8181 -j
ACCEPT
```

3. Restart the service.

```
# service iptables restart
Flushing firewall rules: [OK ]
```

2.2.2 Setting up the WebLogic Network

Perform the following steps to setup the WebLogic network:

1. Allow external connections to http port and SSL http port by opening incoming ports:

```
# cd /etc/sysconfig/# vi iptables
```

2. Add the following lines:

```
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 7001 -j
ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 7002 -j
ACCEPT
```

3. Restart the service:

```
# service iptables restart
Flushing firewall rules: [OK ]
```

2.3 Exchanging Certificates

2.3.1 Exchanging GlassFish Certificates

Perform the following steps to exchange GlassFish certificates:

Example Environment Variables

```
JAVA_HOME=/home/common/java/jdk1.7.0
ANT_HOME=/home/common/ant/apache-ant-1.8.2
AS_HOME=/home/hiauser/SUNWappserver
JAVA_VENDOR=Sun

AS_SERVER_DIR=$AS_HOME
AS_DOMAIN_DIR=$AS_HOME/domains/domain1
```

1. Export the demo identity certificate:

```
$ keytool -export -keystore $AS_DOMAIN_DIR/config/identity.jks -storepass
changeit -alias identity -file <machine1_host_name>.cer
```

2. Copy the demo identity certificate remotely:

```
$ scp -rp <machine1_host_name>.cer hiauser@<machine2_host_
```

```
name>:/home/hiauser/downloads/certs
```

3. Copy the trusted identity certificate locally:

```
$ scp hiauser@<machine2_host_
name>:/home/hiauser/SUNWappserver/domains/domain1/config/<machine2_host_
name>.cer .
```

4. Import the trusted identity certificate:

```
$ keytool -import -keystore $AS_DOMAIN_DIR/config/cacerts.jks -storepass
changeit -alias <machine2_host_name> -file <machine2_host_name>.cer
-trustcacertsTrust this certificate? [no]: yes
```

5. List the truststore:

```
$ keytool -list -keystore $AS_DOMAIN_DIR/config/cacerts.jks -storepass changeit
-v
```

2.3.2 Exchanging WebLogic Certificates

Perform the following steps to exchange WebLogic certificates:

Example Environment Variables

```
MW_HOME=/home/hiauser/Oracle/Middleware
JAVA_HOME=/home/common/java/jdk1.7.0
JAVA_VENDOR=Sun

WL_SERVER_DIR=$MW_HOME/wlserver_10.3
WL_DOMAIN_DIR=$MW_HOME/user_projects/domains/domain1
```

1. Export the demo identity certificate:

```
$ keytool -export -keystore $WL_SERVER_DIR/server/lib/DemoIdentityChangeit.jks
-storepass changeit -alias demoidentity -file <machine1_host_name>.cer
```

2. Copy the demo identity certificate remotely:

```
$ scp -rp <machine1_host_name>.cer hiauser@<machine2_host_
name>:/home/hiauser/downloads/certs
```

3. Copy the trusted identity certificate locally:

```
$ scp hiauser@<machine2_host_name>:/home/hiauser/Oracle/Middleware/wlserver_
10.3/server/lib/<machine2_host_name>.cer .
```

4. Import the trusted identity certificate:

```
$ keytool -import -keystore $WL_SERVER_DIR/server/lib/DemoTrustChangeit.jks
-storepass changeit -alias <machine2_host_name> -file <machine2_host_name>.cer
-trustcacerts
```

5. List the truststore:

```
$ keytool -list -keystore $WL_SERVER_DIR/server/lib/DemoTrustChangeit.jks
-storepass changeit -v
```

2.4 Installing Oracle Health Sciences Information Gateway CONNECT Gateway and Adapter

Execute the following commands to install the CONNECT Gateway and Adapter:

```
$ tar -zxvf ohig_connect_installer.tgz
$ cd ohig_connect_installer
$ java -jar ohig_connect_installer.jar
```

To follow prompts, refer to Appendix A, "Running Oracle Health Sciences Information Gateway CONNECT Installer".

2.5 Validating Oracle Health Sciences Information Gateway CONNECT using Universal Client

The OHIG CONNECT adapter comes with an internal implementation of MPI, Document Registry, and Document Repository services that are enabled by default. These services are available for testing purposes only.

To validate the CONNECT software on the OHIG Gateway and Adapter, perform the following steps:

1. Start the application server on both the gateway and adapter.
2. Validate the installation using the sample universal client distributed with the adapter:
   a. Launch the application by navigating to the following URL:

      `http://<adapter_host_ip >:7001/CONNECTUniversalClientGUI/`

   b. Search for patient with last name "Younger".
   c. If the installation is correct, this returns a page with the Patient ID for the patient.
   d. Click **PatientId** for additional details on the patient.
   e. The **Document** tab is now enabled and you can search for patient documents by date range. Search for date range 08/01/2000 to 08/01/2010.

2.6 Validating Oracle Health Sciences Information Gateway CONNECT using Soap UI Validation Suite

2.6.1 Running Validation Suite Tests

Perform the following steps to run validation suite tests:

1. Setup soapUI:

   ```
   $ cp <install_dir>/addons/connect/oracle_db/ojdbc6.jar to <soapui_install_
   dir>/bin/ext
   ```

2. Load soapUI tests:

   ```
   $ cd <config_nhin_dir>/ValidationSuite

   1-InternalSelfTest_g0-soapui-project.xml
   ```

```
1-InternalSelfTest_g1-soapui-project.xml
2-EndToEndSelfTest_g0-soapui-project.xml
2-EndToEndSelfTest_g1-soapui-project.xml
4-ConnectionManagerTest-soapui-project.xml
```

> **Note:** If running from an alternate machine, copy the /<config_nhin_dir> directory and edit the *.xml wsdl paths to reflect the new location.

3. Tar nhin directory:

```
$ cd <domain_config_dir>
$ tar cvf nhin.tar nhin
```

4. Copy the remote file:

```
$ scp hiauser@<remote_host>:<domain_config_dir>/nhin.tar .
```

3

Configuring the Oracle Health Sciences Information Gateway CONNECT Gateway and Adapter

This section describes how to do the configure the adapter to connect to Oracle services instead of the internal test services. This chapter contains the following topics:

3.1 Configuring the Adapter with Oracle Health Sciences Information Manager Health Record Locator

This section describes how to configure the adapter to connect to the Oracle Health Sciences Information Manager (OHIM) registry to Record Locator instead of the internal test document registry.

Prerequisite:

Configuration and validation specified in Section 2.5, "Validating Oracle Health Sciences Information Gateway CONNECT using Universal Client" on page 2-7 are completed successfully.

3.1.1 Installing Certificates

1. Log in to the adapter host. If not done already, create and import the certificate for the adapter host in to your application server's keystore. For details, refer to the following GlassFish or Weblogic application server documentation:

   Sun GlassFish Enterprise Server v2.1.1

   `http://docs.oracle.com/cd/E19879-01/index.html`

   Oracle® Fusion Middleware Securing Oracle WebLogic Server

   `http://docs.oracle.com/cd/E23943_01/web.1111/e13707/toc.htm`

2. Import the OHIM Health Record Location host's certificate or its CA's certification into your adapter application server's truststore.

3. Log in to the OHIM Health Record Locator host. If not done already, import the OHIM Health Record Locator's certificate into your application server's keystore.
4. Import the OHIG adapter host's certificate or its CA's certification into your OHIM Health Record Locator application server's truststore.

3.1.2 Configuring Oracle Health Sciences Information Gateway CONNECT Adapter with Oracle Registry

For information on configuring OHIG CONNECT Adapter with Oracle registry, refer to Section B.1, "Configuring Oracle Health Sciences Information Gateway CONNECT Adapter with Oracle Registry" in Appendix B, "Configuring Oracle CONNECT Adapters with Oracle Components".

3.1.3 Setting up Components

3.1.3.1 Loading Test Data in Oracle Health Sciences Information Manager Health Record Locator's Oracle Database

To load test data into Health Record Locator's Oracle Database, perform the following steps:

1. Log in to the OHIG adapter host.
2. Copy the file from `<install_dir>/addons/adapter/hrl/rls_oracle_db_scripts.zip` to the host where you have an SQL Plus client present in the PATH, and Bash or Sh shell is available. Extract the contents.
3. Log in to the host having SQL Plus, and change the directory to where you copied or extracted the files in the previous step.
4. Ensure that SQL Plus is available in the PATH, then run the script as follows:

   ```
   > bash loadTestData.sh
   ```

5. When prompted, enter information for the registry database host, port, SID, ADT user password, and HRLCORE user password.

3.1.4 Validating Adapter Configuration with Oracle Health Sciences Information Manager Health Record Locator

Perform the steps specified in Section 2.5, "Validating Oracle Health Sciences Information Gateway CONNECT using Universal Client" on page 2-7 to validate the adapter's configuration with OHMPI Health Record Locator. Apart from Universal Client UI, observe HRL logs during these steps to confirm Adapter is configured to connect to HRL.

3.2 Configuring the Adapter with Oracle Healthcare Master Person Index

This section describes how to configure the adapter to connect to OHMPI instead of the internal test patient master person index.

Prerequisite:

Configuration and validation specified in Section 2.5, "Validating Oracle Health Sciences Information Gateway CONNECT using Universal Client" on page 2-7 are completed successfully.

3.2.1 Installing Certificates

1. Log in to the adapter host. If not done already, create and import the certificate for the adapter host in to your application server's keystore. For details, refer to the following GlassFish or Weblogic application server documentation:

   Sun GlassFish Enterprise Server v2.1.1

   http://docs.oracle.com/cd/E19879-01/index.html

   Oracle® Fusion Middleware Securing Oracle WebLogic Server

   http://docs.oracle.com/cd/E23943_01/web.1111/e13707/toc.htm

2. Import the OHIM Health Record Location host's certificate or its CA's certification into your adapter application server's truststore.
3. Log in to the OHIM Health Record Locator host. If not done already, import the OHIM Health Record Locator's certificate into your application server's keystore.
4. Import the OHIG adapter host's certificate or its CA's certification into your OHIM Health Record Locator application server's truststore.

3.2.2 Configuring Oracle Health Sciences Information Gateway CONNECT Adapter with Oracle Master Person Index

For information on configuring OHIG CONNECT Adapter with Oracle MPI, refer to Section B.2, "Configuring Oracle Health Sciences Information Gateway CONNECT Adapter with Oracle Healthcare Master Person Index" in Appendix B, "Configuring Oracle CONNECT Adapters with Oracle Components".

3.2.3 Setting up Components

3.2.3.1 Creating Oracle Health Sciences Information Gateway CONNECT Test Patients

Note: Before proceeding with creating OHIG CONNECT test patients, ensure that you have already validated your configuration with OHIM HRL as described in Section 3.1.3, "Setting up Components" and Section 3.1.4, "Validating Adapter Configuration with Oracle Health Sciences Information Manager Health Record Locator".

Perform the following steps to create OHIG CONNECT test patients:

1. Login to the OHMPI Master Index Data Manager (MIDM) web application.

   http://<ohmpi_host_url>:8080/PatientMIDM

2. A default user with MasterIndex.Admin,Administrator group privileges has already been created in the GlassFish file realm.

   User: mdm

   Password: mdm

3. In the **Source Record** tab, select **Add** and create the following patients in the MIDM:

```
System: SelfTest System 1
LocalID: D123401
FirstName: Gallow
LastName: Younger
SSN: 999-99-9999
Gender: Male
Date of Birth: 06/27/1999
Address Type: street address line
Address Line1: 123 Main street
City: LEESBURG
State Code: VA
Postal Code: 20176

System: SelfTest System 1
LocalID: D123407
FirstName: Jordy
LastName: LaForge
SSN: 999-99-9999
Gender: Female
Date of Birth: 11/14/1923
Address Type: delivery address line
Address Line1: 5804 Post Corners Trl
City: Centerville
State Code: VA
Postal Code: 20120

System: SelfTest System 1
LocalID: D123409
FirstName: Audrey
LastName: Kim
SSN: 999-99-9999
Gender: Female
Date of Birth: 03/14/1980
Address Type: street address line
Address Line1: 14701 Demming Drive
City: Gainsville
State Code: VA
Postal Code: 20155

System: SelfTest System 1
LocalID: D123402
FirstName: Anna
LastName: Schnur
SSN: 999-99-9999
Gender: Female
Date of Birth: 08/13/1956
Address Type: street address line
Address Line1: 312 HILL ROAD
City: HILLSBRO
State Code: MO
Postal Code: 37660
```

4. Note that the EUID returned on each of the above patients and update the PatientIDs in the NHINC and HRL databases by following the instructions below.

Updating the NHINC Database with New Patient IDs

1. Log into OHIG Adapter host.
2. Copy the file from `<install_dir>/addons/adapter/ohmpi/ohmpi_nhinc_db.tgz` to the host where you have an SQL Plus client present in the PATH and Bash or Sh shell is available. Extract the contents (for example, `tar -zxvf ohmpi_nhinc_db.tgz`).
3. Update script `nhinc3_upd_nhinc_patients.sh` with variable *oracleDBScriptsDir* pointing to the path where the above file was extracted.
4. Run the script `nhinc3_upd_nhinc_patients.sh`.

   ```
   > bash nhinc3_upd_nhinc_patients.sh
   ```

5. The script will prompt for the OHIG Oracle database host, port, SID, and NHINCUSER database user password.
6. When prompted, enter new patient IDs for the patients D123401/GallowYounger, D123407/Jordy LaForge, D123409/Audrey Kim, and D123402/AnnaSchnur.

Updating the HRL Database with New Patient IDs

1. Log in to OHIG Adapter host.
2. Copy the file from `<install_dir>/addons/adapter/ohmpi/ohmpi_rls_db.tgz` to the host where you have an SQL Plus client present in the PATH and Bash or Sh shell is available. Extract the contents (for example, `tar -zxvf hia11_ohmpi_rls_db.tgz`).
3. Update script `nhinc3_upd_rls_patients.sh` with variable *oracleDBScriptsDir* pointing to the path where the above file was extracted.
4. Run the script `nhinc3_upd_rls_patients.sh`.

   ```
   > bash nhinc3_upd_rls_patients.sh
   ```

5. The script will prompt for the OHIG Oracle database host, port, SID, and ADT and HRLCORE database users passwords.
6. When prompted, enter new patient IDs for the patients D123401/GallowYounger, D123407/Jordy LaForge, D123409/Audrey Kim, and D123402/AnnaSchnur.

3.2.4 Validating Adapter Configuration with Oracle Healthcare Master Person Index

Perform the steps specified in Section 2.5, "Validating Oracle Health Sciences Information Gateway CONNECT using Universal Client" on page 2-7 to validate the adapter's configuration with OHMPI. Apart from the Universal Client user interface, observe OHMPI logs during these steps to confirm that the adapter is configured to connect to OHMPI.

3.3 Configuring the Adapter with Oracle Health Sciences Transaction Database

This section describes how to configure the adapter to connect to the Oracle Health Sciences Health Transaction Database (HTB) instead of the internal test document repository.

Prerequisite:

Configuration and validation specified in Section 2.5, "Validating Oracle Health Sciences Information Gateway CONNECT using Universal Client" on page 2-7 are completed successfully.

3.3.1 Installing Certificates

1. Log in to the adapter host. If not done already, create and import the certificate for the adapter host in to your application server's keystore. Refer to the GlassFish or Weblogic application server documentation for details.

   Sun GlassFish Enterprise Server v2.1.1

   `http://docs.oracle.com/cd/E19879-01/index.html`

   Oracle® Fusion Middleware Securing Oracle WebLogic Server

   `http://docs.oracle.com/cd/E23943_01/web.1111/e13707/toc.htm`

2. Also import the HTB host's certificate or its CA's certification into your adapter application server's truststore.
3. Log in to the HTB host. If not done already, import the OHIM Health Record Locator's certificate into your application server's keystore.
4. Import the OHIG adapter host's certificate or its CA's certification into your HTB application server's truststore.

3.3.2 Configuring Oracle Health Sciences Information Gateway CONNECT Adapter with Oracle Repository

For information on configuring OHIG CONNECT Adapter with Oracle repository, refer to Section 3.3, "Configuring the Adapter with Oracle Health Sciences Transaction Database" in Appendix B, "Configuring Oracle CONNECT Adapters with Oracle Components".

A

Running Oracle Health Sciences Information Gateway CONNECT Installer

This appendix describes how to run the OHIG CONNECT installer. It contains the following topics:

A.1 Oracle Health Sciences Information Gateway CONNECT Adapter

Note: For the `connectadapter_host` or `connectgateway_host` properties, ensure that you provide a valid host name instead of **localhost** to avoid certificate exceptions.

A.1.1 GlassFish

```
$ cd <install_dir>
$ java -jar ohig_connect_installer.jar
Oracle HIG Connect Installer 2.0.1.0
-- Feature
Choose option install_feature (connect, connectadapter, connectgateway)
> connectadapter
-- Target
Choose option install_target (glassfish, weblogic)
> glassfish
-- Command
Choose option install_command (usage, version, install)
> install
-- Glassfish install directory
Enter glassfish_install_dir [#null]
> /home/hiauser/SUNWappserver
-- Glassfish domain name
Enter glassfish_domain_name [domain1]
>
-- Glassfish copy ojdbc jar to domain lib ext
Choose option glassfish_copy_ojdbc_jar_to_domain_lib_ext ([yes], no)
>
-- Start glassfish
Choose option start_glassfish ([yes], no)
```

```
> no
-- Glassfish admin username
Enter glassfish_admin_username [admin]
>
-- Glassfish admin password
Enter glassfish_admin_password [adminadmin]
>
-- Glassfish master password
Enter glassfish_master_password [changeit]
>
-- Glassfish admin port
Enter glassfish_admin_port [4848]
>
-- Glassfish jvm option -Xms
Enter glassfish_jvm_option_xms [512m]
>
-- Glassfish jvm option -Xmx
Enter glassfish_jvm_option_xmx [1024m]
>
-- Glassfish jvm option -XX:MaxPermSize
Enter glassfish_jvm_option_max_perm_size [256m]
>
-- Connect database host
Enter connect_db_host [localhost]
> hiadevdb
-- Connect database port
Enter connect_db_port [1521]
>
-- Connect database sid
Enter connect_db_sid [orcl]
>
-- Connect database nhinc username
Enter connect_db_nhinc_username [nhincuser]
>
-- Connect database nhinc password
Enter connect_db_nhinc_password [nhincpass]
>
-- Connect adapter host
Enter connectadapter_host [localhost]
>
-- Connect adapter http port
Enter connectadapter_http_port [8080]
>
-- Connect adapter https port
Enter connectadapter_https_port [8181]
>
-- Connect gateway host
Enter connectgateway_host [localhost]
>
-- Connect gateway http port
Enter connectgateway_http_port [8080]
>
-- Connect gateway https port
Enter connectgateway_https_port [8181]
>
-- Connect home community id
Enter connect_home_community_id [1.1]
>
-- Connect home community name
Enter connect_home_community_name [1.1]
```

```
>
-- Connect assigning authority id
Enter connect_assigning_authority_id [1.1]
>
-- Stop glassfish
Choose option stop_glassfish ([yes], no)
> no
```

A.1.2 WebLogic

```
$ cd <install_dir>
$ java -jar ohig_connect_installer.jar
Oracle HIG Connect Installer 2.0.1.0
-- Feature
Choose option install_feature (connect, connectadapter, connectgateway)
> connectadapter
-- Target
Choose option install_target (glassfish, weblogic)
> weblogic
-- Command
Choose option install_command (usage, version, install)
> install
-- Start weblogic
Choose option start_weblogic ([yes], no)
> no
-- Weblogic install directory
Enter weblogic_install_dir [#null]
> /home/hiauser/Oracle/Middleware
-- Weblogic jdk directory
Enter weblogic_jdk_dir [/home/common/java/jdk1.7.0] based on [${install_java_
home}]
>
-- Weblogic server name
Enter weblogic_server_name [AdminServer]
>
-- Weblogic domain name
Enter weblogic_domain_name [domain1]
>
-- Weblogic domain directory
Enter weblogic_domain_dir [/home/hiauser/Oracle/Middleware/user_
projects/domains/domain1] based on [${weblogic_install_dir}${/}user_
projects${/}domains${/}${weblogic_domain_name}]
>
-- Weblogic admin username
Enter weblogic_admin_username [weblogic]
>
-- Weblogic admin password
Enter weblogic_admin_password [welcome1]
>
-- Weblogic admin protocol
Enter weblogic_admin_protocol [t3]
>
-- Weblogic host
Enter weblogic_host [localhost]
>
-- Weblogic admin port
Enter weblogic_admin_port [7001]
>
```

```
-- Connect database host
Enter connect_db_host [localhost]
> hiadevdb
-- Connect database port
Enter connect_db_port [1521]
>
-- Connect database sid
Enter connect_db_sid [orcl]
>
-- Connect database nhinc username
Enter connect_db_nhinc_username [nhincuser]
>
-- Connect database nhinc password
Enter connect_db_nhinc_password [nhincpass]
>
-- Connect gateway host
Enter connectgateway_host [localhost]
>
-- Connect gateway http port
Enter connectgateway_http_port [7001]
>
-- Connect gateway https port
Enter connectgateway_https_port [7002]
>
-- Connect adapter host
Enter connectadapter_host [localhost]
>
-- Connect adapter http port
Enter connectadapter_http_port [7001]
>
-- Connect adapter https port
Enter connectadapter_https_port [7002]
>
-- Connect home community id
Enter connect_home_community_id [1.1]
>
-- Connect home community name
Enter connect_home_community_name [1.1]
>
-- Connect assigning authority id
Enter connect_assigning_authority_id [1.1]
>
-- Stop weblogic
Choose option stop_weblogic ([yes], no)
> no
```

A.2 Oracle Health Sciences Information Gateway CONNECT Gateway

Note: For the `connectadapter_host` or `connectgateway_host` properties, ensure that you provide a valid host name instead of **localhost** to avoid certificate exceptions.

A.2.1 GlassFish

```
$ cd <install_dir>
$ java -jar ohig_connect_installer.jar
Oracle HIG Connect Installer 2.0.1.0
-- Feature
Choose option install_feature (connect, connectadapter, connectgateway)
> connectgateway
-- Target
Choose option install_target (glassfish, weblogic)
> glassfish
-- Command
Choose option install_command (usage, version, install)
> install
-- Glassfish install directory
Enter glassfish_install_dir [#null]
> /home/hiauser/SUNWappserver
-- Glassfish domain name
Enter glassfish_domain_name [domain1]
>
-- Glassfish copy ojdbc jar to domain lib ext
Choose option glassfish_copy_ojdbc_jar_to_domain_lib_ext ([yes], no)
>
-- Start glassfish
Choose option start_glassfish ([yes], no)
> no
-- Glassfish admin username
Enter glassfish_admin_username [admin]
>
-- Glassfish admin password
Enter glassfish_admin_password [adminadmin]
>
-- Glassfish master password
Enter glassfish_master_password [changeit]
>
-- Glassfish admin port
Enter glassfish_admin_port [4848]
>
-- Glassfish jvm option -Xms
Enter glassfish_jvm_option_xms [512m]
>
-- Glassfish jvm option -Xmx
Enter glassfish_jvm_option_xmx [1024m]
>
-- Glassfish jvm option -XX:MaxPermSize
Enter glassfish_jvm_option_max_perm_size [256m]
>
-- Connect database host
Enter connect_db_host [localhost]
> hiadevdb
-- Connect database port
Enter connect_db_port [1521]
>
-- Connect database sid
Enter connect_db_sid [orcl]
>
-- Connect database nhinc username
Enter connect_db_nhinc_username [nhincuser]
>
-- Connect database nhinc password
Enter connect_db_nhinc_password [nhincpass]
>
```

```
-- Connect adapter host
Enter connectadapter_host [localhost]
>
-- Connect adapter http port
Enter connectadapter_http_port [8080]
>
-- Connect adapter https port
Enter connectadapter_https_port [8181]
>
-- Connect gateway host
Enter connectgateway_host [localhost]
>
-- Connect gateway http port
Enter connectgateway_http_port [8080]
>
-- Connect gateway https port
Enter connectgateway_https_port [8181]
>
-- Connect home community id
Enter connect_home_community_id [1.1]
>
-- Connect home community name
Enter connect_home_community_name [1.1]
>
-- Connect assigning authority id
Enter connect_assigning_authority_id [1.1]
>
-- Stop glassfish
Choose option stop_glassfish ([yes], no)
> no
```

A.2.2 WebLogic

```
$ cd <install_dir>
$ java -jar ohig_connect_installer.jar
Oracle HIG Connect Installer 2.0.1.0
-- Feature
Choose option install_feature (connect, connectadapter, connectgateway)
> connectgateway
-- Target
Choose option install_target (glassfish, weblogic)
> weblogic
-- Command
Choose option install_command (usage, version, install)
> install
-- Start weblogic
Choose option start_weblogic ([yes], no)
> no
-- Weblogic install directory
Enter weblogic_install_dir [#null]
> /home/hiauser/Oracle/Middleware
-- Weblogic jdk directory
Enter weblogic_jdk_dir [/home/common/java/jdk1.7.0] based on [${install_java_
home}]
>
-- Weblogic server name
Enter weblogic_server_name [AdminServer]
>
```

```
-- Weblogic domain name
Enter weblogic_domain_name [domain1]
>
-- Weblogic domain directory
Enter weblogic_domain_dir [/home/hiauser/Oracle/Middleware/user_
projects/domains/domain1] based on [${weblogic_install_dir}${/}user_
projects${/}domains${/}${weblogic_domain_name}]
>
-- Weblogic admin username
Enter weblogic_admin_username [weblogic]
>
-- Weblogic admin password
Enter weblogic_admin_password [welcome1]
>
-- Weblogic admin protocol
Enter weblogic_admin_protocol [t3]
>
-- Weblogic host
Enter weblogic_host [localhost]
>
-- Weblogic admin port
Enter weblogic_admin_port [7001]
>
-- Connect database host
Enter connect_db_host [localhost]
> hiadevdb
-- Connect database port
Enter connect_db_port [1521]
>
-- Connect database sid
Enter connect_db_sid [orcl]
>
-- Connect database nhinc username
Enter connect_db_nhinc_username [nhincuser]
>
-- Connect database nhinc password
Enter connect_db_nhinc_password [nhincpass]
>
-- Connect gateway host
Enter connectgateway_host [localhost]
>
-- Connect gateway http port
Enter connectgateway_http_port [7001]
>
-- Connect gateway https port
Enter connectgateway_https_port [7002]
>
-- Connect adapter host
Enter connectadapter_host [localhost]
>
-- Connect adapter http port
Enter connectadapter_http_port [7001]
>
-- Connect adapter https port
Enter connectadapter_https_port [7002]
>
-- Connect home community id
Enter connect_home_community_id [1.1]
>
-- Connect home community name
```

```
Enter connect_home_community_name [1.1]
>
-- Connect assigning authority id
Enter connect_assigning_authority_id [1.1]
>
-- Stop weblogic
Choose option stop_weblogic ([yes], no)
> no
```

B

Configuring Oracle CONNECT Adapters with Oracle Components

This appendix contains the following topics:

B.1 Configuring Oracle Health Sciences Information Gateway CONNECT Adapter with Oracle Registry

1. Log into the OHIG adapter.
2. Edit the file `<config_nhin_dir>/internalConnectionInfo.xml`.

   GlassFish example:

   ```
   <glassfish_install_dir>/domains/<domain_
   name>/config/nhin/internalConnectionInfo.xml
   ```

   WebLogic example:

   ```
   <weblogic_install_dir>/user_projects/domains/<domain_
   name>/config/nhin/internalConnectionInfo.xml
   ```

3. Edit or create the business service `adapterxdsbdocregistrysoap12`. Ensure `<accessPoint>` is defined as:

   ```
   <accessPoint useType="endPoint">http://<oracle_registry_host_
   ip>:8080/hrl/regsvc</accessPoint>
      <categoryBag>
        <keyedReference tModelKey="uddi:nhin:versionofservice" keyName=""
   keyValue="1.0"/>
        <keyedReference tModelKey="CONNECT:adapter:apilevel" keyName=""
   keyValue="LEVEL_a0"/>
            </categoryBag>
   ```

> **Note:** If you have selected non-default home community ID (other than 1.1) for the HIG installation, ensure that you provide an appropriate value for the businessKey attribute of the businessService element.
>
> For example, if you have selected home community ID as 4.4, the businessKey value should be set to `uddi:testnhieonenode:4.4`.

4. Edit or create the business service `adapterxdsbdocregistry`. Change to the `<accessPoint>` from:

```
<accessPoint useType="endPoint">http://<adapter_host_
ip>:8080/CONNECTAdapter/DocumentRegistry_Service</accessPoint>
```

to

```
<accessPoint useType="endPoint">http://<adapter_host_
ip>:8080/CONNECTAdapterDocRegSoap12/AdapterDocRegistry2Soap12Service</accessPoi
nt>
  <categoryBag>
    <keyedReference tModelKey="uddi:nhin:versionofservice" keyName=""
keyValue="1.0"/>
    <keyedReference tModelKey="CONNECT:adapter:apilevel" keyName=""
keyValue="LEVEL_a0"/>
  </categoryBag>
```

5. Edit the file `<config_nhin_dir>/repository.properties` and edit or create the following property:

```
convertPnR2SOR=true
```

> **Note:** The property `convertPnRSOR` should only be set to `true` when using the internal test repository with Oracle Registry.

6. Restart the application server.

B.2 Configuring Oracle Health Sciences Information Gateway CONNECT Adapter with Oracle Healthcare Master Person Index

1. Log into the OHIG adapter host.
2. Edit the file `<config_nhin_dir>/internalConnectionInfo.xml`.

   GlassFish example:

```
<glassfish_install_dir>/domains/<domain_
name>/config/nhin/internalConnectionInfo.xml
```

   WebLogic example:

```
<weblogic_install_dir>/user_projects/domains/<domain_
name>/config/nhin/internalConnectionInfo.xml
```

3. Edit or create the business service `adaptercomponentmpiservice`. Change the `<accessPoint>` from:

```
<accessPoint useType="endPoint">http://<adapter_host_
ip>:8080/Adapter/PatientDiscovery/A_0/AdapterComponentMpiService</accessPoint>
```

to

```
<accessPoint useType="endPoint">http://<adapter_host_
ip>:8080/AdapterComponentIheMpi/AdapterComponentMpiService</accessPoint>
```

4. Edit or create the business service `adaptercomponentmpisecuredservice`. Change the `<accessPoint>` from:

```
<accessPoint useType="endPoint">https://<adapter_host_
ip>:8181/Adapter/PatientDiscovery/A_
0/AdapterComponentMpiSecuredService</accessPoint>
```

to

```
<accessPoint useType="endPoint">https://<adapter_host_
ip>:8181/AdapterComponentIheMpi/AdapterComponentMpiSecuredService</accessPoint>
```

5. Edit the file `<config_nhin_dir>/AdapterComponentIheMpiConfig.properties` and edit or create the following property:

```
ihempi.pdq.v3.endpoint.url=http://<oracle_mpi_host_ip>:8080/PDQSupplier_
Service/PDQSupplier
```

6. Restart the application server.

B.3 Configuring Oracle Health Sciences Information Gateway CONNECT Adapter with Oracle Repository

1. Log into the OHIG adapter.
2. Edit the file `<config_nhin_dir>/internalConnectionInfo.xml`.

   GlassFish example:

```
<glassfish_install_dir>/domains/<domain_
name>/config/nhin/internalConnectionInfo.xml
```

   WebLogic example:

```
<weblogic_install_dir>/user_projects/domains/<domain_
name>/config/nhin/internalConnectionInfo.xml
```

3. Edit or create the business service `adapterxdsbdocrepositorysoap12retrieve`. Ensure `<accessPoint>` is defined as:

```
<accessPoint useType="endPoint">https://<oracle_repository_host_
ip>:7778/XDS/xdsrepositoryb_Soap12</accessPoint>
   <categoryBag>
       <keyedReference tModelKey="uddi:nhin:versionofservice" keyName=""
keyValue="1.0"/>
```

```
      <keyedReference tModelKey="CONNECT:adapter:apilevel" keyName=""
keyValue="LEVEL_a0"/>
    </categoryBag>
```

Note: If you have selected non-default home community ID (other than 1.1) for the HIG installation, ensure that you provide an appropriate value for the businessKey attribute of the businessService element.

For example, if you have selected home community ID as 4.4, the businessKey value should be set to `uddi:testnhieonenode:4.4`.

---

4. Edit or create the business service adapterxdsbdocrepositorysoap12pnr. Ensure `<accessPoint>` is defined as:

```
<accessPoint useType="endPoint">https://<oracle_repository_host_
ip>:7778/XDS/xdsrepositoryb/iti41</accessPoint>
   <categoryBag>
      <keyedReference tModelKey="uddi:nhin:versionofservice" keyName=""
keyValue="1.0"/>
      <keyedReference tModelKey="CONNECT:adapter:apilevel" keyName=""
keyValue="LEVEL_a0"/>
    </categoryBag>
```

Note: If you have selected non-default home community ID (other than 1.1) for the HIG installation, ensure that you provide an appropriate value for the businessKey attribute of the businessService element.

For example, if you have selected home community ID as 4.4, the businessKey value should be set to `uddi:testnhieonenode:4.4`.

---

5. Edit or create the business service `adapterxdsbdocrepository`. Change the `<accessPoint>` from:

```
<accessPoint useType="endPoint">http://<adapter_host_
ip>:8080/CONNECTAdapter/DocumentRepository_Service</accessPoint>
```

to

```
<accessPoint useType="endPoint">http://<adapter_host_
ip>:8080/CONNECTAdapterDocReposSoap12/AdapterDocRepository2Soap12Service</acces
sPoint>
   <categoryBag>
     <keyedReference tModelKey="uddi:nhin:versionofservice" keyName=""
keyValue="1.0"/>
     <keyedReference tModelKey="CONNECT:adapter:apilevel" keyName=""
keyValue="LEVEL_a0"/>
   </categoryBag>
```

6. Ensure to comment-out the business service adapterxdsbdocrepositorysoap12 element.
7. Restart the application server.

Note: To avoid the exception, *javax.net.ssl.SSLException: Received fatal alert: illegal_parameter*, execute the following steps.

GlassFish

Add the following JVM options from Glassfish admin console and restart the server:

- `-Dcom.sun.net.ssl.enableECC=false`
- `-Djsse.enableSNIExtension=false`

WebLogic

Add the following JVM options to the OHIG Connect WebLogic script:

- `-Dcom.sun.net.ssl.enableECC=false`
- `-Djsse.enableSNIExtension=false`

To set these JVM options, perform the following steps:

1. Navigate to the scripts directory using the following command:

   ```
   $ cd <install_dir>/addons/connect/scripts
   ```

2. Open the script file using the following command:

   ```
   $ vi connect-start-weblogic.sh
   ```

3. Add the following commands before the `export JAVA_OPTIONS` command:

   ```
   JAVA_OPTIONS="$JAVA_OPTIONS -Dcom.sun.net.ssl.enableECC=false"
   JAVA_OPTIONS="$JAVA_OPTIONS -Djsse.enableSNIExtension=false"
   ```

4. Save the changes and restart the server.

C

Creating and Importing Certificates Using the GlassFish Self-Signed Certificate Scripts

This appendix describes how to create and import certificates using the GlassFish self-signed certificate scripts. It contains the following topics:

C.1 Installing Self-signed Certificates on Oracle Health Sciences Information Gateway CONNECT Adapter

Perform the following steps to install self-signed certificates on the OHIG CONNECT adapter:

1. Log in to the adapter machine.
2. Stop the application server using the following commands:
   a. `> cd <glassfish_install_dir>/bin`
   b. `> asadmin stop-domain <domain_name>`
3. Navigate to the directory `<install_dir>/addons/connect/scripts` using the following command:

   ```
   > cd <install_dir>/addons/connect/scripts
   ```
4. Execute `create-and-import-selfsigned-certs.sh` to install the self-signed certificate.

   ```
   > sh create-and-import-selfsigned-certs.sh
   ```

   This performs the following:
   - creates the keystore for the private internal key
   - exports the certificate that will authenticate the internal key
   - imports the trusted certificates into the truststore
   - provides these certificates to the server to use for authentication purposes
5. Install the certificates from the other components that will communicate with the Adapter (Gateway, OHMPI, HPE, HPM, HRL, HTB, and so on).

6. Copy the certificate of the component machine <COMPONENT_HOSTNAME.cer> to the <glassfish_install_dir>/domains/<domain_name>/config folder.
7. Navigate to and execute <install_dir>/addons/connect/scripts/import-others-cert.sh. When prompted by the scripts, enter the machine hostname (it should match the cert file you copied to the config folder without .cer suffix).

   ```
   > bash import-others-cert.sh
   ```

C.2 Installing Self-signed Certificates on Oracle Health Sciences Information Gateway CONNECT Gateway

Perform the following steps to install self-signed certificates on the OHIG CONNECT gateway:

1. Log in to the gateway machine.
2. Stop the application server using the following commands:
   a. `> cd <glassfish_install_dir>/bin`
   b. `> asadmin stop-domain <domain_name>`
3. Navigate to the directory <install_dir>/addons/connect/scripts using the following command:

   ```
   > cd <install_dir>/addons/connect/scripts
   ```
4. Execute create-and-import-selfsigned-certs.sh to install the self-signed certificate.

   ```
   > sh create-and-import-selfsigned-certs.sh
   ```

   This performs the following:
   - creates the keystore for the private internal key
   - exports the certificate that will authenticate the internal key
   - imports the trusted certificates into the truststore
   - provides these certificates to the server to use for authentication purposes
5. Install the adapter machine certificate.
6. Copy the adapter machine certificate of <ADAPTER_ HOSTNAME.cer> to the <glassfish_install_dir>/domains/<domain_name>/config folder.
7. Navigate to and execute <install_dir>/addons/connect/scripts/import-others-cert.sh. When prompted by the scripts, enter the adapter machine hostname (it should match with the cert file you copied to the config folder without .cer suffix).

   ```
   > bash import-others-cert.sh
   ```

C.3 Avoiding a Java Security Certificate Exception

To avoid a java.security.cert.CertificateException you must ensure that your OHIM host names are not fully qualified.

To Make the Hostname Not Fully Qualified

1. Set the OHIM and OHIG host names to be not fully qualified.

2. Add aliases for all hosts.
3. Regenerate and reimport the certificates.
4. Restart all the servers.
5. Test that you do not have a Java security certificate exception.

D

Examples for Setting up Oracle Health Sciences Information Gateway CONNECT

This appendix contains the following topics:

D.1 Environment Settings

D.1.1 Example GlassFish Directories

GlassFish Home

```
/home/hiauser/SUNWappserver
```

GlassFish Domain Directory

```
/home/hiauser/SUNWappserver/domains/domain1
```

GlassFish NHIN Config Directory

```
/home/hiauser/SUNWappserver/domains/domain1/config/nhin
```

Log Directory

```
/home/hiauser/SUNWappserver/domains/domain1/logs/
```

GlassFish Bin Directory

```
/home/hiauser/SUNWappserver/bin
```

D.1.2 Example GlassFish Commands

Environment Variables

```
AS_HOME=/home/hiauser/SUNWappserver
JAVA_HOME=/home/common/java/jdk1.7.0
JAVA_VENDOR=Sun
```

```
$ cd /home/hiauser/SUNWappserver/bin
$ asadmin start-domain domain1
$ asadmin stop-domain domain1
```

D.1.3 Example WebLogic Directories

WebLogic Home

```
/home/hiauser/Oracle/Middleware
```

WebLogic Server Directory

```
/home/hiauser/Oracle/Middleware/wlserver_10.3
```

WebLogic Domain Directory

```
/home/hiauser/Oracle/Middleware/user_projects/domains/domain1
```

WebLogic NHIN Config Directory

```
/home/hiauser/Oracle/Middleware/user_projects/domains/domain1/config/nhin
```

Demo Certificate Directory

```
/home/hiauser/Oracle/Middleware/wlserver_10.3/server/lib/
```

Log Directory

```
/home/hiauser/Oracle/Middleware/user_
projects/domains/domain1/servers/AdminServer/logs/
```

WebLogic Bin Directory

```
/home/hiauser/Oracle/Middleware/user_projects/domains/domain1/bin
```

D.1.4 Example WebLogic Commands

Environment Variables

```
MW_HOME=/home/hiauser/Oracle/Middleware
JAVA_HOME=/home/common/java/jdk1.7.0
JAVA_VENDOR=Sun

$ cd /home/hiauser/Oracle/Middleware/user_projects/domains/domain1/bin
$ startWebLogic.sh
$ stopWebLogic.sh
```

D.1.5 Example GlassFish /home/hiauser/.bashrc

```
# .bashrc

# Source global definitions
if [ -f /etc/bashrc ]; then
        . /etc/bashrc
fi

# User specific aliases and functions
umask 027

# User specific environment and startup programs
JAVA_HOME=/home/common/java/jdk1.7.0
ANT_HOME=/home/common/ant/apache-ant-1.8.2
AS_HOME=/home/hiauser/SUNWappserver
JAVA_VENDOR=Sun
```

```
AS_SERVER_DIR=$AS_HOME
AS_DOMAIN_DIR=$AS_HOME/domains/domain1

PATH=$JAVA_HOME/bin:$PATH:$HOME/bin:/sbin:.:$AS_HOME/bin:$ANT_HOME/bin

export PATH JAVA_HOME ANT_HOME AS_HOME AS_SERVER_DIR AS_DOMAIN_DIR

alias start="sh /home/hiauser/SUNWappserver/bin/asadmin start-domain domain1"
alias stop="sh /home/hiauser/SUNWappserver/bin/asadmin stop-domain domain1"
alias log="tail -f /home/hiauser/SUNWappserver/domains/domain1/logs/server.log"
```

D.1.6 Example WebLogic /home/hiauser/.bashrc

```
# .bashrc

# Source global definitions
if [ -f /etc/bashrc ]; then
        . /etc/bashrc
fi

# User specific aliases and functions
umask 027

# User specific environment and startup programs
JAVA_HOME=/home/common/java/jdk1.7.0
ANT_HOME=/home/common/ant/apache-ant-1.8.2
MW_HOME=/home/hiauser/Oracle/Middleware
JAVA_VENDOR=Sun

WL_SERVER_DIR=$MW_HOME/wlserver_10.3
WL_DOMAIN_DIR=$MW_HOME/user_projects/domains/domain1

PATH=$JAVA_HOME/bin:$PATH:$HOME/bin:/sbin:.:$MW_HOME/bin:$ANT_HOME/bin

export PATH JAVA_HOME ANT_HOME MW_HOME WL_SERVER_DIR WL_DOMAIN_DIR

alias start="sh $WL_DOMAIN_DIR/bin/startWebLogic.sh"
alias stop="sh $WL_DOMAIN_DIR/bin/stopWebLogic.sh"
alias log="tail -f $WL_DOMAIN_DIR/servers/AdminServer/logs/AdminServer.log"
```

D.2 Creating and Importing a Self-Signed Certificate

Perform the following steps to create a self-signed certificate:

1. Create the identity keystore:

   ```
   $ keytool -genkey -keystore keystore.jks -storepass changeit -keypass changeit
   -alias identity -dname "CN=MyHostname, OU=FOR TESTING ONLY, O=MyOrganization,
   L=MyTown, S=MyState, C=US" -keyalg RSA -keysize 2048
   ```

2. Export the identity keystore certificate:

   ```
   $ keytool -export -keystore keystore.jks -storepass changeit -alias identity
   -file identity.cer
   ```

3. Import the identity keystore certificate:

   ```
   $ keytool -import -keystore truststore.jks -storepass changeit -alias identity
   -file identity.cer -trustcacerts
   ```

4. List the identity keystore:

```
$ keytool -list -keystore keystore.jks -storepass changeit -v
```

5. List the truststore:

```
$ keytool -list -keystore truststore.jks -storepass changeit -v
```

E

References

This section provides links to supporting documentation and resources.

E.1 CONNECT

Please visit the following links for more information about CONNECT software and documentation:

CONNECT Release Home

http://developer.connectopensource.org/display/NHINR33/Release+3.3+Home

CONNECT Software Documentation

http://developer.connectopensource.org/display/NHINR33/Software+Documentation

CONNECT Architecture Overview

http://developer.connectopensource.org/display/NHINR33/Architecture+Overview

CONNECT Interface Description Document

http://developer.connectopensource.org/display/NHINR33/Interface+Description+Document

CONNECT Universal Client GUI User Manual

http://developer.connectopensource.org/display/NHINR33/UC+GUI+User+Manual

Using the CONNECT Solution to support Health Information Exchange

http://developer.connectopensource.org/display/NHINR33/Using+the+CONNECT+Solution+to+Support+Health+Information+Exchange+(HIE)

CONNECT Specifications

http://www.connectopensource.org/product/connect-nhin-specs

F

Acronyms

This section provides a list of commonly used acronyms.

F.1 Acronyms

CCD
Continuity of Care Document

CDA
Clinical Document Architecture

DER
Distinguished Encoding Rules

HIE
Health Information Exchange

HIO
Health Information Organization

HL7
Health Level 7

IHE
Integrating the Healthcare Enterprise

NAV
Notification Of Document Availability

NHIE
Nationwide Health Information Exchange

NHIN
Nationwide Health Information Network

NHIO
Nationwide Health Information Organization

OHIG
Oracle Health Sciences Information Gateway

OHIM
Oracle Health Sciences Information Manager

SAML
Security Assertion Markup Language

VM
Oracle Virtual Machine

WSDL
Web-Service Definition Language

XDM
Cross-Enterprise Document Media Interchange

Glossary

This section provides definitions of commonly used words.

CONNECT

Is a software solution that supports health information exchange that implements Nationwide Health Information Network (NHIN) standards and governance to make sure that health information exchanges are compatible with other exchanges being set up throughout the country. It enables public and private organizations to participate in the NHIN by leveraging their existing health information systems.

CONNECT Adapter

The portion of the CONNECT architecture that encapsulates the components most likely to be customized or replaced by an organization implementing CONNECT.

CONNECT Gateway

The portion of the CONNECT architecture that encapsulates the components most likely to be use as-is by an organization without modification. These components are primarily responsible for orchestrating information exchange with the NHIN.

Health Information Exchange

Health Information Exchange is an entity that enables the movement of health-related data among entities within a state, a region, or a non-jurisdictional participant group, which might include "classic" regional health information organizations at regional and state levels, Health Information Organization integrated delivery systems and health plans, or health data banks that support health information exchange.

Health Information Organization

Health Information Organization is an organization that enables the movement of health-related data among entities, evolving as a replacement term for health information exchange or HIE. Healthcare Information Technology Standards Panel Or simply HITSP, a cooperative partnership between the public and private sectors formed and supported by ONC for the purpose of harmonizing and integrating standards that will meet clinical and business needs established by AHIC use cases for sharing information among organizations and systems.

Integrating the Healthcare Enterprise

Integrating the Healthcare Enterprise is an initiative by healthcare professionals and industry to improve the way computer systems in healthcare share information, promoting and coordinating the use of established standards such as DICOM and HL7 to address specific clinical need in support of optimal patient care. The Nationwide Health Information Network is being developed by ONC to provide a secure,

nationwide, interoperable health information infrastructure that will connect providers, consumers, and others involved in supporting health and healthcare.

Nationwide Health Information Network

Nationwide Health Information Network is a set of standards, services and policies that enable secure health information exchange over the Internet. The network will provide a foundation for the exchange of health information across diverse entities, within communities and across the country, helping to achieve the goals of the HITECH Act. This critical part of the national health IT agenda will enable health information to follow the consumer, be available for clinical decision making, and support appropriate use of healthcare information beyond direct patient care so as to improve population health.

Nationwide Health Information Network Gateway

Within the CONNECT solution, the implementation of the core NHIN services and service interface specifications, comprising the CONNECT gateway and CONNECT adapter. The NHIN health information exchange or NHIE, a health information exchange that implements the NHIN architecture, processes, and procedures, is accredited as a participant of the NHIN.

Oracle Virtual Machine

Oracle Virtual Machine is a platform that provides a fully equipped environment for better leveraging the benefits of virtualization technology. Oracle VM enables you to deploy operating systems and application software within a supported virtualization environment.

Oracle Virtual Machine Manager

Oracle Virtual Machine Manager provides the user interface, which is a standard ADF (Application Development Framework) web application, to manage Oracle VM Servers. It manages virtual machine lifecycle, including creating virtual machines from installation media or from a virtual machine template, deleting, powering off, uploading, deployment and live migration of virtual machines. It manages resources, including ISO files, virtual machine templates, and sharable hard disks.

Oracle Virtual Machine Server

Oracle Virtual Machine Server allows a self-contained virtualization environment designed to provide a lightweight, secure, server-based platform for running virtual machines. Oracle VM Server is based upon an updated version of the underlying Xen hypervisor technology, and includes Oracle VM Agent.

Oracle Virtual Machine Template

Oracle Virtual Machine Template provides an innovative approach to deploying a fully configured software stack by offering pre-installed and pre-configured software images. Use of Oracle VM templates eliminates the installation and configuration costs, and reduces the ongoing maintenance costs helping organizations achieve faster time to market and lower cost of operations.

Security Assertion Markup Language

Security Assertion Markup Language is an XML-based standard for exchanging authentication and authorization data between security domains.

Web Services Description Language

Web Services Description Language is an XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information.

XML Schema

XML Schema is a means for defining the structure, content, and semantics of XML documents.

Index