Oracle® Health Sciences Information Manager

Cross Community Access Installation and Configuration Guide

Release 3.0

E61376-01

March 2015

This guide discusses how to install and configure the Oracle® Health Sciences Information Manager (OHIM) Cross Community Access (XCA) Gateway.

1 Getting Started

This section describes the minimum hardware and software requirements for installing XCA Gateway.

1.1 Hardware Requirements

The following are the minimum hardware requirements for installing XCA Gateway:

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

1.2 Software Requirements

The following are the software requirements for installing XCA Gateway:

- Java 1.7 executable in path (for installer)
- Oracle JDK 1.7.0_45+ and WebLogic Server 11g Release 1 (10.3.6.0) or WebLogic Server 12c Release 2 (12.1.2)
- Oracle Database 11g Release 2 (11.2.0.4.0) or Oracle Database 12c Release 1 (12.1.0.2.0)
- Oracle Enterprise Linux 5.5 or higher

1.2.1 Configuration Requirements

- Apache Ant 1.8.2 executable in path

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

1.3 Downloading Oracle Health Sciences Information Manager XCA Gateway

To download the Oracle Health Sciences Information Manager XCA Gateway, perform the following tasks:

1. Navigate to http://edelivery.oracle.com.

2. Enter your Registration information, accept the Agreement Terms by selecting the check boxes, 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 Manager Media Pack**.
7. Click **Continue**.
8. Click **Download** for the following and save the files to your system:
   - **Oracle Health Sciences Information Manager 3.0 XCA Gateway**
9. Extract the files to view the *Oracle Health Sciences Information Manager Cross Community Access Installation and Configuration Guide* and get the compressed tar file (`*.tgz`).

2 Preparing Database Schemas in Linux

To prepare database schemas in Linux, perform the following:

1. Copy and unzip script files. Ensure SQL Plus is present in PATH.

   Execute the following commands:

   a. `cd <install_dir>/ohim_xca_installer/addons/xcagateway/oracle_db/`

   b. `unzip gateway_oracle_db_scripts.zip`

   c. `cd gateway_oracle_db_scripts`

2. (Optional step) If SQL Plus is not available, copy the zip file `gateway_oracle_db_scripts.zip` to the host system where SQL Plus and Bash or Sh shell are available.

   For example,

   ```
   scp <install_dir>/ohim_xca_installer/addons/xcagateway/oracle_
   db/gateway_oracle_db_scripts.zip user@sql_plus_host:/tmp/
   ```

3. Log in to the host system where you copied the zip file. Execute the following commands to unzip the file:

   a. `cd /tmp`

   b. `unzip gateway_oracle_db_scripts.zip`

   c. `cd gateway_oracle_db_scripts`

   Note: Update the SQL script `create_tblspc_users.sql` with your Oracle Database (DB) specific Tablespace information.

4. Run the `> bash ./create_tblspc_users.sh` script.
5. Enter database connection information and password for GATEWAY user when prompted.
6. Return to the host system where you are installing the XCA Gateway.

3 Running the XCA Gateway Installer

To run the XCA Gateway installer, perform the following:

1. Extract the tgz file.
2. Configure the XCA Gateway.

   XCA configuration will be split into two properties files inside the application server, **IG.Properties** and **RG.Properties**.

   The location of the properties files is `<application-server-home>/<user_projects>/domains/<domain-name>/config/xca/`.

4 Installing the XCA Gateway

Execute the following commands to install the XCA Gateway:

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

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

5 Configuring Initiating Gateway

5.1 Providing Local Home Community ID of the Initiating Gateway

Enter the following community IDs for configuring Initiating Gateway (IG):

- `localHomeCommunityId_IG=`
- `localHomeCommunityId_XCPD=`

5.2 Configuring the Repository for Initiating Gateway

Prerequisite: Get the repository unique ID and repository URL for retrieving document transactions.

Update the configuration file as follows:

Syntax: `RepositoryUniqueId=RepositoryURL`

For example,

```
#1.3.6.1.4.1.21367.13.40.39=http://<hostname>:<port>/services/xdsrepositoryb
```

5.3 Enabling the Grouping Option with Local Document Consumer

Prerequisite to enable grouping: Get the local community registry URL for Stored Query and Repository URL for retrieving document.

Set the following `INGWGroupedWithDocumentConsumer` property to **yes** to enable the grouping with local document consumer:

- `INGWLocalRegistry` - Takes the value of registry URL.

- `INGWLocalRepository` - Takes the value of repository URL.
- `INGWGroupedWithDocumentConsumer=`no

For example,

- `INGWLocalRegistry=`
- `INGWLocalRepository=`

5.4 Configuring Responding Gateway Using Home Community ID

Prerequisite: Responding Gateway (RG) Query and retrieve endpoints.

The following is the syntax for configuring the initiating gateway for a specific home community ID. You can configure multiple responding gateways.

Configuration for query transaction:

- Syntax: `CrossGatewayQuery_homecommunityid=RespondingGatewayQueryURL`
- Syntax: `CrossGatewayRetrieve_ homecommunityid=RespondingGatewayRetrieveURL`

5.5 Configuring Multiple Responding Gateways for Broadcasting Mode

Prerequisite: All the responding gateways query URLs and home community IDs that need to be configured.

You can configure multiple responding gateways for the Cross Gateway Query queries by patient ID.

- `XCARespondingGateway_<count>` - This parameter takes the value of the responding gateway query URL.

  `<count>` is the variable which starts from one and can go to any number of responding gateways that you would like to configure.
- `XCARespondingGateway_<count>_HomeCommunityId` - Takes the value of the home community ID of the responding gateway.

For example, *when <count> value is 1,*

```
XCARespondingGateway_1=
```

```
XCARespondingGateway_1_HomeCommunityId=
```

When <count> value is 2,

```
XCARespondingGateway_1=
```

```
XCARespondingGateway_1_HomeCommunityId=
```

```
XCARespondingGateway_2=
```

```
XCARespondingGateway_2_HomeCommunityId=
```

As mentioned, `<count>` is the number of responding gateways that you plan to configure.

5.6 Configuring Local MPI to Initiating Gateway

Prerequisite: Local MPI PDQ Supplier endpoint.

`XCA_Local_PDQSupplier` - Takes the value of the PDQ supplier endpoint URL.

For example,

```
XCA_Local_PDQSupplier=
```

5.7 ATNA Audit Configuration

Prerequisites: Audit repository host name or IP and audit repository UDP or TLS port.

- `ATNASyslogProtocol` - Set this value to UDP or TLS.
- `auditMessageType` - Represents the audit message type (DICOM XML schema compliant or RFC3881 XML schema compliant) that system generates. Set this value to either RFC3881 or DICOM.

Ensure to configure the following properties when you use TLS for ATNAsyslogProtocol:

- `keyStore`: Enter the file path of the keystore. For example, `/home/common/cert/keystore.jks`.
- `keyStoreType`: Specify the type of the keystore. By default, the value is set to JKS.
- `trustStore`: Enter the file path of the truststore. For example, `/home/common/cert/keystore.jks`.
- `trustStoreType`: Specify the type of the truststore. By default, the value is set to JKS.
- `credentialStore`: Enter the directory where Oracle wallet is created. For example, `/home/common`.

To enable auditing, set **Audit** to `Yes`.

For example, Audit Configuration:

```
auditRepositoryServer=

auditRepositoryPort=

ATNASyslogProtocol=

auditMessageType=

keyStore=

keyStoreType=JKS

trustStore=

trustStoreType=JKS

credentialStore=

Audit=no
```

For storing keyStore and trustStore password in credentialStore, see Section 9.

5.8 Enabling MTOM Option

You can configure this property to enable or disable the MTOM option on the Cross Gateway Document Retrieve Web Service Client Request.

`enableMTOM` - Set this value to true or false.

5.9 Configuring Number of Threads and Timeout for Initiating Gateway

You can configure one initiating gateway for multiple responding gateways. Multiple threads ensure better performance.

- `maximumThreadCount` - Takes the value of max number of threads that you want to create.

  For example, number of threads required to send the cross gateway requests:

  `maximumThreadCount=`

Time out configurations for the requests:

- `default_timeout_sync` - Takes the value of the time out for synchronous transactions.
- `default_timeout_async` - Takes the value of the time out for asynchronous transactions.

For example,

- `default_timeout_sync=`
- `default_timeout_async=`

6 Configuring XCPD Initiating Gateway

6.1 Configuring XCPD Responding Gateway

Prerequisite: XCPD URL and Homecommunityid of the responding gateway.

- `XCPD_RespondingGW_<TargetHomeCommunityID>` - Takes the value of the responding gateway XCPD URL.

  `<TargetHomeCommunityID>` should be replaced with the homecommunity id of the responding gateway.

```
XCPD_RespondingGW_TargetHomeCommunityID = XCPD Responding Gateway URL
```

For example, `XCPD_RespondingGW_1.0 = http://localhost:8080/RespondingGateway_Service/XCPDRespondingGateway`

6.2 Configuring Sender and Receiver OIDs

The following properties take sender and receiver OID values appropriately:

- `XCPD_IG_SenderOID=`
- `XCPD_IG_RecieverOID=`

6.3 Patient ID Mapping Workflow

The property `PatientID_Mapping_Workflow` takes two values:

- `xca` - When the value is xca, initiating gateway does not send any XCPD request to find patient id in remote community. IG uses the same patient ID that is sent by the document consumer.

- `xcpd`: When the value is xcpd, the initiating gateway will send XCPD request to each configured responding gateway, fetch the patient ID, and uses that patient ID for the respective Cross Gateway Query Transactions.

  For example,

  `PatientID_Mapping_Workflow=`

7 Configuring Responding Gateway

7.1 Configuring Responding Gateway Local Home Community

Enter the following IDs for configuring responding gateway local home community:

- `localHomeCommunityId_RG=`
- `localHomeCommunityId_XCPD=`

7.2 Configuring Responding Gateway’s Local Registry Repository

Prerequisite: Responding Gateway's local registry, repository URLs with repository unique ID.

- `RespondingGatewayRegistryURL=`
- `RespondingGatewayRepositoryID=`

Prerequisite: Get repository unique and repository URL for retrieving document transactions.

Update the configuration file as follows:

Syntax: `RepositoryUniqueId=RepositoryURL`

For example,

```
1.3.6.1.4.1.21367.13.40.39=http://<hostname>:<port>/services/xdsrepository
b
```

7.3 ATNA Audit Configuration

Prerequisites: Audit repository host name/IP and audit repository UDP port.

- `ATNASyslogProtocol` - This value should be set to UDP or TLS.
- `auditMessageType` - Represents the audit message type (DICOM XML schema compliant or RFC3881 XML schema compliant) that system generates. Set this value to either RFC3881 or DICOM.

Ensure to configure the following properties when you use TLS for ATNAsyslogProtocol:

- `keyStore`: Enter the file path of the keystore. For example, `/home/common/cert/keystore.jks`.
- `keyStoreType`: Specify the type of the keystore. By default, the value is set to JKS.
- `trustStore`: Enter the file path of the truststore. For example, `/home/common/cert/keystore.jks`.

- `trustStoreType`: Specify the type of the truststore. By default, the value is set to JKS.
- `credentialStore`: Enter the directory where Oracle wallet is created. For example, `/home/common`.

To enable auditing, set **Audit** to `Yes`.

For example, Audit Configuration:

```
auditRepositoryServer=

auditRepositoryPort=

ATNASyslogProtocol=

auditMessageType=

keyStore=

keyStoreType=JKS

trustStore=

trustStoreType=JKS

credentialStore=

Audit=no
```

For storing keyStore and trustStore password in credentialStore, see Section 9.

7.4 Configuring Local MPI to Responding Gateway

Prerequisite: Local MPI PDQ Supplier endpoint.

- `XCPD_RG_PDQSupplier<count>` - Takes the value of the PDQ endpoint of the MPI.
- `XCPD_RG_PDQSupplier<count>_domainID` - Takes the value of the domain ID.

For example, IHERED, IHEBLUE, and so on.

XCPD Responding Gateway settings:

You can have multiple PDQ Suppliers to talk with.

- `XCPD_RG_PDQSupplier<count>=`
- `XCPD_RG_PDQSupplier<count>_domainID=`

`<count>` can be replaced with any number of PDQ suppliers that are planned to configure. Responding gateway can look through multiple MPI systems to search for a patient.

For example, when <count> is 1,

```
XCPD_RG_PDQSupplier1=

XCPD_RG_PDQSupplier1_domainID=
```

When <count> is 2,

```
XCPD_RG_PDQSupplier1=

XCPD_RG_PDQSupplier1_domainID=

XCPD_RG_PDQSupplier2=

XCPD_RG_PDQSupplier2_domainID=
```

7.5 Configuring Health Data Locator

To enable Health Data Locator, set the value of `SupportsHealthDataLocator` property in the RG.properties file to `yes`.

If the value is set to `yes`, RG responds to the XCPD request indicating that it supports patient location query.

If the value is set to `no`, RG does not support Health Data Locator.

8 Setting up the Keystore and Truststore for TLS Communication

XCA Gateway requires certificates to be loaded into the Keystore and Truststore of WebLogic Sever or Managed WebLogic Server for TLS communication with Web Service client.

1. For configuring the Identity and Trust for WebLogic Server or Managed WebLogic Server, follow the steps provided in `http://docs.oracle.com/middleware/1212/wls/SECMG/identity_trust.htm#i1196575`.
2. Enable SSL to secure communication between client and XCA Gateway application. For configuring the SSL, follow the steps provided in `http://docs.oracle.com/middleware/1212/wls/SECMG/ssl.htm#i1194343`.
3. Under **Advanced** section of SSL configuration:
   a. Set Hostname Verification to **None**
   b. Enable **Use Server Certs**
   c. Set the Two Way Client Cert Behavior option to **Client Certs Requested and Enforced**
4. Restart the WebLogic Server or Managed WebLogic Server after configuring the Keystore and Truststore values.

9 Sending Audit Messages Using TLS Protocol

To send audit messages using TLS protocol, perform the following steps:

1. Navigate to the audit-oss directory using the following steps:
   a. Execute the following command:
   ```
   cd <install_dir>/ohim_xca_installer/addons/xcagateway
   ```
   b. Extract the contents of audit-oss-bin.tar.gz file using the following command:
   ```
   > tar -zxvf audit-oss-bin.tar.gz
   ```
   c. Execute the following command:
   ```
   > cd audit-oss
   ```
2. Execute the following command. When prompted, enter the values for the wallet output directory, wallet password, keystore password, and truststore password. Ensure that you provide the correct passwords. fields.
   ```
   > sh setupCredentialStoreForATNA.sh
   ```
3. Configure the following properties:

For Initiating Gateway - <WebLogic_Home>/user_projects/domains/<domain_name>/config/xca/config/IG.properties file

or

For Responding Gateway - <WebLogic_Home>/user_projects/domains/<domain_name>/config/xca/config/RG.properties file

keyStore=/home/common/cert/keystore.jks

keyStoreType=JKS

trustStore=/home/common/cert/keystore.jks

trustStoreType=JKS

credentialStore=/home/common

4. Restart the WebLogic Server or Managed WebLogic Server after configuring the above properties.

10 Appendix A: Running Oracle Health Sciences Information XCA Gateway Installer

The XCA Gateway application can be deployed to either WebLogic Admin Server or Managed WebLogic Server. Provide the appropriate server name when the installer prompts you to enter the value for WebLogic server name. If you are deploying the application to Managed WebLogic Server, provide its corresponding http port value when prompted.

This appendix describes how to run the XCA Gateway installer. It contains the following topic:

10.1 XCA Gateway Installation with Start WebLogic=no

```
$ cd <install_dir>
$ java -jar ohim_xca_installer.jar
Oracle HIM XCA Installer 3.0.0.0
-- Feature
Choose option install_feature (xcagateway, xcagateway_ig, xcagateway_rg)
> xcagateway
-- Command
Choose option install_command (usage, version, install)
> install
Starting init install
-- Start weblogic
Choose option start_weblogic ([yes], no)
>
-- Xca gateway database host
Enter xcagateway_db_host [localhost]
>
-- Xca gateway database port
Enter xcagateway_db_port [1521]
-- Xca gateway database sid or service name
Enter xcagateway_db_sid [orcl]
> orcl
-- Xca gateway database gateway username
Enter xcagateway_db_gateway_username [gateway]
-- Xca gateway database gateway password
Enter xcagateway_db_gateway_password [<password>]
```

```
>
-- Weblogic install directory
Enter weblogic_install_dir [#null]
> /home/hiauser/Oracle/Middleware
-- Weblogic jdk directory
Enter weblogic_jdk_dir [/home/common/java/jdk1.6.0] 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 [<password>]
>
-- Weblogic admin protocol
Enter weblogic_admin_protocol [t3]
>
-- Weblogic host
Enter weblogic_host [localhost]
>
-- Weblogic admin port
Enter weblogic_admin_port [7001]
>
-- Weblogic http_port
Enter weblogic_http_port [7001]
-- Stop weblogic
Choose option stop_weblogic ([yes], no)
>
```

10.2 XCA Gateway Installation with Start WebLogic=yes

```
$ cd <install_dir>
$ java -jar ohim_xca_installer.jar
Oracle HIM XCA Installer 3.0.0.0
-- Feature
Choose option install_feature (xcagateway, xcagateway_ig, xcagateway_rg)
> xcagateway
-- Command
Choose option install_command (usage, version, install)
> install
Starting init install
-- Start weblogic
Choose option start_weblogic ([yes], no)
>
-- Weblogic install directory
Enter weblogic_install_dir [#null]
> /home/hiauser/Oracle/Middleware
-- Weblogic jdk directory
```

```
Enter weblogic_jdk_dir [/home/common/java/jdk1.6.0] based on [${install_java_
home}]
>
-- Weblogic domain name
Enter weblogic_domain_name [domain1]
>
-- Weblogic domain directory
Enter weblogic_domain_dir [/home/hiauser/Oracle/Middleware/user_
projects/domains/domain1] based on [${weblogic_install_dir}${/}user_
projects${/}domains${/}${weblogic_domain_name}]
>
-- Weblogic admin username
Enter weblogic_admin_username [weblogic]
>
-- Weblogic admin password
Enter weblogic_admin_password [<password>]
>
-- Weblogic admin protocol
Enter weblogic_admin_protocol [t3]
>
-- Weblogic host
Enter weblogic_host [localhost]
>
-- Weblogic admin port
Enter weblogic_admin_port [7001]
>
-- Weblogic server name
Enter weblogic_server_name [AdminServer]
>
-- Weblogic http_port
Enter weblogic_http_port [7001]
>
-- Xca gateway database host
Enter xcagateway_db_host [localhost]
>
-- Xca gateway database port
Enter xcagateway_db_port [1521]
-- Xca gateway database sid or service name
Enter xcagateway_db_sid [orcl]
> orcl
-- Xca gateway database gateway username
Enter xcagateway_db_gateway_username [gateway]
-- Xca gateway database gateway password
Enter xcagateway_db_gateway_password [<password>]
>
-- Stop weblogic
Choose option stop_weblogic ([yes], no)
>
```

11 Appendix B: XCA Endpoints

Use the endpoints in Table 1 to configure XCA clients as needed.

Table 1 XCA Transactions and Endpoint URLs

Transaction	Endpoint URL
Initiating Gateway Cross Gateway Query (ITI-18)	`http(s)://<XCA_HOST>:<PORT>/InitiatingGatewayQuery_Service/XCAInitiatingGatewayQuery`
Initiating Gateway Cross Gateway Retrieve (ITI-43)	`http(s)://<XCA_HOST>:<PORT>/InitiatingGatewayRetrieve_Service/XCAInitiatingGatewayRetrieve`
Responding Gateway Cross Gateway Query (ITI-38)	`http(s)://<XCA_HOST>:<PORT>/RespondingGatewayQuery_Service/XCARespondingGatewayQuery`
Responding Gateway Cross Gateway Retrieve (ITI-39)	`http(s)://<XCA_HOST>:<PORT>/RespondingGatewayRetrieve_Service/XCARespondingGatewayRetrieve`
XCPD Responding Gateway (ITI-55)	`http(s)://<XCA_HOST>:<PORT>/RespondingGateway_Service/XCPDRespondingGateway`
Patient Location Query (ITI-56)	`http(s)://<XCA_HOST>:<PORT>/RespondingGateway_Service/XCPDRespondingGateway`
Asynchronous Registry Stored Query (ITI-18)	`http(s)://<XCA HOST>:<PORT>/IGAsyncServices/XCAInitiatingGatewayQuery`
Asynchronous Retrieve Document Set (ITI -43)	`http(s)://<XCA HOST>:<PORT>/IGAsyncServices/XCAInitiatingGatewayRetrieve`

12 Appendix C: Acronyms

This section provides a list of commonly used acronyms.

- IG - Initiating Gateway
- OHIM - Oracle Health Sciences Information Manager
- RG - Responding Gateway
- XCA - Cross Community Access
- XCPD - Cross-Community Patient Discovery

13 Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Oracle® Health Sciences Information Manager Cross Community Access Installation and Configuration Guide, Release 3.0
E61376-01

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.