Oracle® Health Sciences Information Manager

Cross Community Access Installation and Configuration Guide

4.0
F50772-01
January 2022

ORACLE

Oracle Health Sciences Information Manager Cross Community Access Installation and Configuration Guide, 4.0

F50772-01

Contents

Preface

This preface contains the following sections:

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.

Related resources

All documentation and other supporting materials are available on the Oracle Help Center.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Access to Oracle Support

Oracle customers that have purchased support 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.

1
Get started

This section describes how to download Oracle Health Sciences Information Manager Cross Community Access (XCA) Gateway. Also, it includes minimum hardware and software requirements for installing XCA Gateway.

- Hardware requirements
  This section describes the minimum hardware requirements for installing XCA Gateway.
- Software requirements
  This section describes the software requirements for installing XCA Gateway.
- Configuration requirements
  This section describes the configuration requirements for installing XCA Gateway.
- Acronyms
  This section provides a list of commonly used acronyms.
- Download Health Sciences Information Manager XCA gateway
  This section describes how to download Oracle Health Sciences Information Manager XCA Gateway.

Hardware requirements

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

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

Software requirements

This section describes the software requirements for installing XCA Gateway.

The software requirements for installing XCA Gateway include:

- Java 1.8 executable in path (for installer)
- Oracle JDK 1.8.0_311+ and WebLogic Server 12c (12.2.1.4)
- Oracle Database 12cR1 (12.1.0.2.0), Oracle Database 12cR2 (12.2.0.1) and Oracle Database 19c (19.3.0.0.0)
- Oracle Enterprise Linux 7.x or higher
- Apache Ant 1.10.11 or later

Configuration requirements

This section describes the configuration requirements for installing XCA Gateway.

The configuration requirements include:

- Apache Ant 1.10.11 executable in path
- PATH=$PATH:<install_dir>/apache-ant-1.10.11/bin

Acronyms

This section provides a list of commonly used acronyms.

Table 1-1 Acronyms

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

Download Health Sciences Information Manager XCA gateway

This section describes how to download Oracle Health Sciences Information Manager XCA Gateway.

To download Oracle Health Sciences Information Manager XCA Gateway:

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 All Categories drop-down menu, select **Release** OR **Download Package**.
4. In the Search text area, type Oracle Health Sciences Information Manager, then click **Search**.
5. In the results list, select and click **Oracle Health Sciences Information Manager 4.0.0.0.0**, then the selected item will be added to View Items.
6. Click **Continue**.
7. From the Platforms/Languages drop-down menu, select Linux x86 or x86-64.
8. Click **Continue**
9. Review and accept the Oracle License Agreement by selecting the check box, then click **Continue**
10. Click Download for the following zip file and save the file to your system:

    Oracle Health Sciences Information Manager 4.0.0
11. Extract the files to get the corresponding Oracle Health Sciences Information Manager XCA Gateway compressed tar file (ohim_xca_installer.tgz).

2
Database schemas

This section describes how to prepare database schemas in Linux.

- Prepare database schemas in Linux
  Database schemas in Linux are used in XCA.

Prepare database schemas in Linux

Database schemas in Linux are used in XCA.

To prepare the database schemas in Linux for the XCA gateway:

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

   Execute the following commands:

   ```
   cd <install_dir>/ohim_xca_installer/addons/xcagateway/oracle_db/
   unzip gateway_oracle_db_scripts.zip
   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:

   ```
   cd /tmp
   unzip gateway_oracle_db_scripts.zip
   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 script:

   ```
   > bash ./create_tblspc_users.sh
   ```

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

Health Sciences Information Manager Gateway Installer

This section describes how to run the XCA Gateway installer and install the XCA Gateway.

- Run the XCA gateway installer
  This section describes how to run the XCA Gateway installer.
- Install the XCA gateway
  This section describes how to install the XCA Gateway.

Run the XCA gateway installer

This section describes how to run the XCA Gateway installer.

To run the XCA Gateway installer:

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/.

Install the XCA gateway

This section describes how to install the XCA Gateway.

1. 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
   ```

2. To follow prompts, refer to Run XCA Gateway installer.

4

Initiating gateway

This section describes how to configure the Initiating Gateway (IG), including repository and audit configuration.

- Provide local home community ID
  This section describes how to insert local home community IDs.
- Configure the repository
  This section describes how to configure the repository for Initiating Gateway (IG).
- Enable the grouping options with local document consumer
  This section describes how to enable the grouping option with Local Document Consumer for Initiating Gateway (IG).
- Configure Responding Gateway using home community ID
  This section describes how to configure responding gateway using home community ID.
- Configure multiple responding gateways for broadcasting mode
  This section describes how to configure multiple responding gateways for broadcasting mode.
- Configure local MPI to Initiating gateway
  This section describes how to configure local MPI to Initiating gateway.
- Configure ATNA Audit
  This section describes how to set up ATNA audit configuration.
- Enable MTOM option
  This section describes how to enable the MTOM option.
- Configure number of threads and timeout for Initiating gateway
  This section describes how to configure the number of threads and timeout for initiating gateway.

Provide local home community ID

This section describes how to insert local home community IDs.

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

- localHomeCommunityId_IG=
- localHomeCommunityId_XCPD=

Configure the repository

This section describes how to configure the repository for Initiating Gateway (IG).

> **Note:**
>
> 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
```

Enable the grouping options with local document consumer

This section describes how to enable the grouping option with Local Document Consumer for Initiating Gateway (IG).

> **Note:**
>
> Prerequisite: Get the local community registry URL for Stored Query and Repository URL for retrieving document.

To enable grouping with local document consumer, set the following `INGWGroupedWithDocumentConsumer` property to yes:

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

For example:

```
INGWLocalRegistry=
INGWLocalRepository=
```

Configure Responding Gateway using home community ID

This section describes how to configure responding gateway using home community ID.

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

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

```
localHomeCommunityId_RG=
localHomeCommunityId_XCPD=
```

> **Note:**
>
> You can configure multiple responding gateways.

Configure multiple responding gateways for broadcasting mode

This section describes how to configure multiple responding gateways for broadcasting mode.

> **Note:**
>
> 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.

The parameter `XCARespondingGateway_<count>` takes the value of the responding gateway query URL, where <count> is the variable that starts from one and can go to any number of responding gateways that you would like to configure.

The following parameter takes the value of the home community ID of the responding gateway:

```
XCARespondingGateway_<count>_HomeCommunityId
```

For example, when <count> value is 1:

```
XCARespondingGateway_1=
XCARespondingGateway_1_HomeCommunityId=
```

For example, when <count> value is 2:

```
XCARespondingGateway_1=
XCARespondingGateway_1_HomeCommunityId=
XCARespondingGateway_2=
XCARespondingGateway_2_HomeCommunityId=
```

> **Note:**
>
> <count> is the number of responding gateways that you plan to configure.

Configure local MPI to Initiating gateway

This section describes how to configure local MPI to Initiating gateway.

> **Note:**
>
> Prerequisite: Local MPI PDQ Supplier endpoint.

To configure local MPI to Initiating gateway, use syntax:

```
XCA_Local_PDQSupplier
```

which takes the value of the PDQ supplier endpoint URL.

For example:

```
XCA_Local_PDQSupplier=
```

Configure ATNA Audit

This section describes how to set up ATNA audit configuration.

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

To set up ATNA audit configuration, use syntax:

```
ATNASyslogProtocol
```

where you set the value to UDP or TLS.

```
auditMessageType
```

Represents the audit message type (DICOM XML schema compliant or RFC3881 XML schema compliant) that the system generates. Set this value to either RFC3881 or DICOM.

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

Table 4-1 TLS Properties for ATNAsyslogProtocol

Property	Description
keyStore	File path of the keystore. For example: /home/common/ cert/keystore.jks
keyStoreType	Specify the type of keystore. By default, value set to JKS.
trustStore	File path of the truststore. For example: /home/common/ cert/keystore.jks
trustStoreType	Specify the type of truststore. By default, value 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 more information on storing keyStore and trustStore password in credentialStore, see Send audit messages using TLS protocol.

Enable MTOM option

This section describes how to enable the 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.

Configure number of threads and timeout for Initiating gateway

This section describes how to configure the 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 timeout for synchronous transactions.

```
default_timeout_async
```

takes the value of the timeout for asynchronous transactions.

For example:

```
default_timeout_sync=
default_timeout_async=
```

5

XCPD responding ateway

This section describes how to configure the XCPD responding gateway.

- Configure XCPD Responding gateway
  This section describes how to configure the XCPD responding gateway.
- Configure Sender and Receiver OID values
  This section describes how to configure sender and receiver OID values for the XCPD responding gateway.
- Configure Patient ID Mapping Workflow value
  This section describes how to configure patient ID mapping workflow value for the XCPD responding gateway.

Configure XCPD Responding gateway

This section describes how to configure the XCPD responding gateway.

> **Note:**
>
> Prerequisite: XCPD URL and Homecommunityid of the responding gateway.

Update the configuration file as follows:

Syntax:

```
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
```

Configure Sender and Receiver OID values

This section describes how to configure sender and receiver OID values for the XCPD responding gateway.

The following properties take sender and receiver OID values appropriately:

```
XCPD_IG_SenderOID=
XCPD_IG_RecieverOID=
```

Configure Patient ID Mapping Workflow value

This section describes how to configure patient ID mapping workflow value for the XCPD responding gateway.

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.

6

Responding gateway

This section describes how to configure the responding gateway.

- Configure Responding Gateway using home community ID
  This section describes how to configure responding gateway using home community ID.
- Configure local registry repository for the Responding gateway
  This section describes how to configure local registry repository for the responding gateway.
- Configure ATNA Audit
  This section describes how to set up ATNA audit configuration.
- Configure local MPI to Responding gateway
  This section describes how to configure local MPI to responding gateway.
- Configure Health Data Locator
  This section describes how to configure the Health Data Locator.

Configure Responding Gateway using home community ID

This section describes how to configure responding gateway using home community ID.

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

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

```
localHomeCommunityId_RG=
localHomeCommunityId_XCPD=
```

> **Note:**
>
> You can configure multiple responding gateways.

Configure local registry repository for the Responding gateway

This section describes how to configure local registry repository for the responding gateway.

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

```
RespondingGatewayRegistryURL=
RespondingGatewayRepositoryID=
```

> **Note:**
>
> 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/
xdsrepositoryb
```

Configure ATNA Audit

This section describes how to set up ATNA audit configuration.

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

To set up ATNA audit configuration, use syntax:

```
ATNASyslogProtocol
```

where you set the value to UDP or TLS.

```
auditMessageType
```

Represents the audit message type (DICOM XML schema compliant or RFC3881 XML schema compliant) that the system generates. Set this value to either RFC3881 or DICOM.

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

Table 6-1 TLS Properties for ATNAsyslogProtocol

Property	Description
keyStore	File path of the keystore. For example: /home/ common/ cert/keystore.jks
keyStoreType	Specify the type of keystore. By default, value set to JKS.
trustStore	File path of the truststore. For example: /home/ common/ cert/keystore.jks
trustStoreType	Specify the type of truststore. By default, value 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 more information on storing keyStore and trustStore password in credentialStore, see Send audit messages using TLS protocol.

Configure local MPI to Responding gateway

This section describes how to configure local MPI to responding gateway.

> **Note:**
>
> 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=
```

For example, when <count> is 2:

```
XCPD_RG_PDQSupplier1=
XCPD_RG_PDQSupplier1_domainID=
XCPD_RG_PDQSupplier2=
XCPD_RG_PDQSupplier2_domainID=
```

Configure Health Data Locator

This section describes how to configure the Health Data Locator.

To enable Health Data Locator, set the value of the following property in the RG.properties file to **yes**:

```
SupportsHealthDataLocator
```

SupportsHealthDataLocator

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.

7

Keystore and Truststore for TLS communication

This section describes how to set up the Keystore and Truststore for TLS communication.

Set up the Keystore and Truststore

This section describes how to set 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.

To set up the Keystore and Truststore for TLS communication:

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:
   - Set Hostname Verification to None
   - Enable Use Server Certs
   - 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.

8
Audit messages

This section describes how to send audit messages using TLS Protocol.

- Send audit messages using TLS protocol
  Set up sending audit messages using TLS Protocol.

Send audit messages using TLS protocol

Set up sending audit messages using TLS Protocol.

To send audit messages using TLS Protocol.

1. Navigate to the audit-oss directory:
   - Execute the following command:

     ```
     cd <install_dir>/ohim_xca_installer/addons/xcagateway
     ```

   - Extract the contents of audit-oss-bin.tar.gz file using the command:

     ```
     > tar -zxvf audit-oss-bin.tar.gz
     ```

   - 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 properties:
   - For Initiating Gateway:

     ```
     <WebLogic_Home>/user_projects/domains/<domain_name>/config/xca/config/
     IG.properties file
     ```

   - 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.

A

Run 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.

- Run XCA gateway installation with Start WebLogic=no
  This section describes how to run the XCA Gateway installer with Start WebLogic=no.
- Run XCA gateway installation with Start WebLogic=yes
  This section describes how to run the XCA Gateway installer with Start WebLogic=yes.

Run XCA gateway installation with Start WebLogic=no

This section describes how to run the XCA Gateway installer with Start WebLogic=no.

To run the XCA Gateway installer with Start WebLogic=no:

```
$ cd <install_dir>
$ java -jar ohim_xca_installer.jar
Oracle HIM XCA Installer 4.0.0.0
-- 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/jdk1.8.0] 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)
>
```

Run XCA gateway installation with Start WebLogic=yes

This section describes how to run the XCA Gateway installer with Start WebLogic=yes.

To run the XCA Gateway installer with Start WebLogic=yes:

```
$ cd <install_dir>
$ java -jar ohim_xca_installer.jar
Oracle HIM XCA Installer 4.0.0.0
-- 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/jdk1.8.0] 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)
>
```

B

Configure XCA endpoints

Use the endpoints in this section to configure XCA clients as needed.

- XCA transactions and endpoints
  This section lists XCA transactions and endpoint URLs.

XCA transactions and endpoints

This section lists XCA transactions and endpoint URLs.

Table B-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