Oracle® Health Sciences Information Manager

Cross Community Access User Guide

4.0
F50771-01
January 2022

Oracle Health Sciences Information Manager Cross Community Access User Guide, 4.0

F50771-01

Contents

3 Security configuration issues

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 guide provides information on Oracle Health Sciences Information Manager (OHIM) Cross-Community Access (XCA) Gateway.

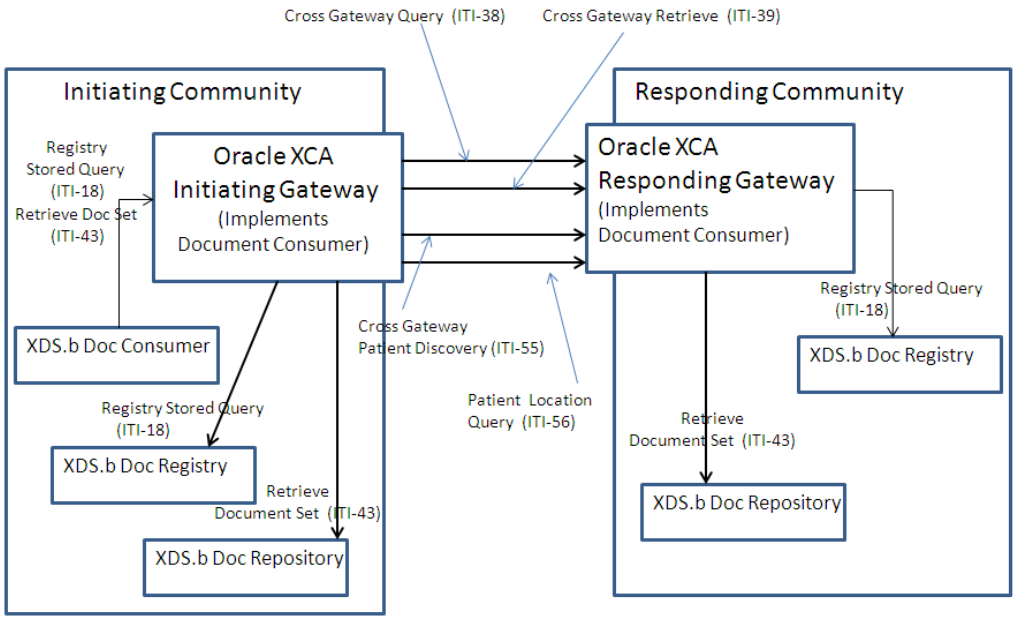
The guide describes the features and functions of the Gateway, Integrating the Healthcare Enterprise (IHE) standards, and the web services with their configuration options. This document is intended for Oracle Health Information XCA Gateway users.

The XCA Profile supports the means to query and retrieve patient relevant medical data held by other communities. The Cross-Community Patient Discovery (XCPD) Profile supports the means to locate communities that hold patient relevant health data and the translation of patient identifiers across communities holding the same patient's data.

- Cross-enterprise document sharing actors and transactions
  This section depicts the XDS actors and transactions in a diagram.
- Services provided
  This section describes the web services provided by XCA.
- Hardware requirements
  This section lists the minimum hardware requirements for installing XCA:
- Software requirements
  This section lists the minimum software requirements for installing XCA.
- Supported IHE profiles
  This section lists the IHE profiles supported by XCA.
- Related documents
  This section lists reference documents and the URLs where you can access them.
- Acronyms
  This section provides a list of commonly used acronyms.

Cross-enterprise document sharing actors and transactions

This section depicts the XDS actors and transactions in a diagram.



- Actors and transactions supported by the gateway
  This section lists the IHE profiles and transactions supported by XCA and XCPD:

Actors and transactions supported by the gateway

This section lists the IHE profiles and transactions supported by XCA and XCPD:

Table 1-1 Actors and transactions supported by XCA

Actors	Transactions
Initiating Gateway (IG)	Cross Gateway Query (ITI-38)
Initiating Gateway	Cross Gateway Retrieve (ITI-39)
Initiating Gateway	Registry Stored Query (ITI-18)
Initiating Gateway	Retrieve Document Set (ITI-43)
Responding Gateway (RG)	Cross Gateway Query (ITI-38)
Responding Gateway	Cross Gateway Retrieve (ITI-39)

Table 1-2 Actors and transactions supported by XCPD

Actors	Transactions
Initiating Gateway	Cross Gateway Patient Discovery (ITI-55)
Responding Gateway	Patient Location Query (ITI-56)
Responding Gateway	Cross Gateway Patient Discovery (ITI-55)
Responding Gateway	Patient Location Query (ITI-56)

Services provided

This section describes the web services provided by XCA.

All of the IHE ITI transactions supported by XCA and XCPD are supported through SOAP 1.2 based Web Services. The following are the SOAP 1.2 Web Services supported by XCA and XCPD:

- **Initiating Gateway Service**: Registry Stored Query, Retrieve Document set, Patient Discovery, Cross Gateway Query, Cross Gateway Retrieve.
- **Responding Gateway Service**: Patient Discovery, Cross Gateway Query, Cross Gateway Retrieve.

Web Services are implemented using JAX-WS Web Services API and stack on Oracle WebLogic server. For more information on Web Service definitions and related IHE XDS, XCA, and XCPD transactions, see IHE IT Infrastructure XDS, XCA, and XCPD Profile specifications.

- Core Gateway Service
  This section lists all the supported IHE transactions.

Core Gateway Service

This section lists all the supported IHE transactions.

The following Web Services operations and IHE transactions are supported for Core Gateway Services:

- ITI-18 Registry Stored Query The Registry Stored Query is classified into the following types:
  - FindDocuments
  - FindSubmissionSets
  - FindFolders
  - GetFolders
  - GetAssociations
  - GetDocumentsAndAssociations
  - GetSubmissionSets
  - GetSubmissionSetAndContents
  - GetFolderAndContents
  - GetFoldersForDocument
  - GetRelatedDocuments
- ITI-38 Cross Gateway Query
- ITI-39 Cross Gateway Retrieve
- ITI-55 XCPD Patient Discovery
- ITI-56 XCPD Patient Location Query

For details on these Web Services operations and IHE transactions, see http://www.ihe.net/Technical_Frameworks.

Hardware requirements

This section lists the minimum hardware requirements for installing XCA:

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

Software requirements

This section lists the minimum software requirements for installing XCA.

- Java 1.8 executable in path (for installer)
- Apache Ant 1.10.11 or later. The executable must be in the path
  `PATH=$PATH:<install_dir>/apache-ant-1.10.11/bin`
- 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), or Oracle Database 19c (19.3.0.0.0)
- Oracle Enterprise Linux 7.x or higher

Supported IHE profiles

This section lists the IHE profiles supported by XCA.

Table 1-3 Supported IHE profiles

Profile name	Version	Location
Cross-Community Access	Revision 11.0 Sept 23, 2014	http://ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2a.pdf http://ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2b.pdf http://ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2x.pdf http://ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol3.pdf

Table 1-3 (Cont.) Supported IHE profiles

Profile name	Version	Location
Cross-Community Patient Discovery (XCPD) Health Data Locator and Revoke Option	Trial Implementation October 13, 2014	http://ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_XCPD_HDL_Revoke_Option.pdf

Related documents

This section lists reference documents and the URLs where you can access them.

Refer to the following links for standard definitions of:

- **Integrating the Healthcare Enterprise (IHE) Actors**: http://wiki.ihe.net/index.php?title=Actors
- **IHE Profiles and Standards**: http://www.ihe.net/profiles/index.cfm IT
- **Infrastructure Domain**: http://wiki.ihe.net/index.php?title=IT_Infrastructure
- **Cross-Enterprise Document Sharing (XDS)**: http://wiki.ihe.net/index.php?title=Cross-Enterprise_Document_Sharing
- **Cross-Community Access (XCA)**: http://wiki.ihe.net/index.php?title=Cross-Community_Access

Acronyms

This section provides a list of commonly used acronyms.

IG: Initiating Gateway

IHE: Integrating the Healthcare Enterprise

RG: Responding Gateway

XCA: Cross-Community Access

XCPD: Cross-Community Patient Discovery

XDS: Cross-Enterprise Document Sharing

2

Configure Health Sciences Information Manager Cross Community Access

This chapter provides information on all the configurations needed to set up XCA and XXPD.

The configuration file is located under the `config/xca/config` directory of the Application Server domain directory.

WebLogic:

- `<Weblogic Middleware Home>/user_projects/domains/<domain name>/config/xca/IG.properties`
- `<Weblogic Middleware Home>/user_projects/domains/<domain name>/config/xca/RG.properties`

- Initiating gateway configuration
  This section describes how to configure the local home community and repository of the Initiating Gateway.
- Enable the grouping option with the local document consumer
  This section describes how to enable grouping.
- Configure the responding gateway using the home community ID
  This section describes how to configure a responding gateway with the home community ID.
- Configure multiple responding gateways for broadcasting mode
  This section describes how to set up multiple responding gateways ofr broadcasting.
- Configure the local MPI to the initiating gateway
- ATNA audit configuration
  This section lists the parameters for ATNA audit configuration.
- Enable the MTOM option
  This section describes how to configure the MTOM option.
- Configure the number of threads and timeout for the initiating gateway
  This section describes how to configure the thread count and timeout value for the initiating gateway.
- XCPD Initiating Gateway configuration
  This section describes the configuration of the initiating XCPD Initiating Gateway.
- Responding gateway configuration
  This section describes how to configure the responding gateway.
- Transactions and web service URLs
  This section lists the web services supported by XCA.
- Oracle extensions
  This section describes how Oracle implemented the IHE specification on XCA and XCPD gateways.

Initiating gateway configuration

This section describes how to configure the local home community and repository of the Initiating Gateway.

- Provide the local home community ID for the initiating gateway
  This section describes how to configure the local home community ID for the initiating gateway.
- Configure the repository for the initiating gateway
  This section describes how to configure the repository for the initiating gateway.

Provide the local home community ID for the initiating gateway

This section describes how to configure the local home community ID for the initiating gateway.

Enter the following community IDs for configuring the initiating gateway:

- `localHomeCommunityId_IG=`
- `localHomeCommunityId_XCPD=`

Configure the repository for the initiating gateway

This section describes how to configure the repository for the initiating gateway.

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

Update the configuration file using this syntax: `RepositoryUniqueId=RepositoryURL`

For example: `#1.3.6.1.4.1.21367.13.40.39=https://<hostname>:<port>/hd/services/xdsrepositoryb`

Enable the grouping option with the local document consumer

This section describes how to enable grouping.

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=
INGWGroupedWithDocumentConsumer=no
```

Configure the responding gateway using the home community ID

This section describes how to configure a responding gateway with the home community ID.

Prerequisite: Responding Gateway 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 syntaxes:

```
CrossGatewayQuery_homecommunityid=RespondingGatewayQueryURL

CrossGatewayRetrieve_homecommunityid=RespondingGatewayRetrieveURL
```

Configure multiple responding gateways for broadcasting mode

This section describes how to set up multiple responding gateways ofr broadcasting.

Prerequisite: Get 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 ranges from one to the maximum number of Responding gateways that you want to configure.
- `XCARespondingGateway_<count>_HomeCommunityId`: Takes the value of the home community ID of the responding gateway.

For example, when the `<count>` value is `1`:

```
XCARespondingGateway_1=
XCARespondingGateway_1_HomeCommunityId=
```

When the `<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 want to configure.

Configure the local MPI to the initiating gateway

Prerequisite: Get the local MPI PDQ Supplier endpoint.

`XCA_Local_PDQSupplier` takes the value of the PDQ supplier endpoint URL.

For example: `XCA_Local_PDQSupplier=`

ATNA audit configuration

This section lists the parameters for ATNA audit configuration.

ATNA Audit configuration prerequisites: Get the audit repository host name or IP and audit repository UDP or TLS port.

- `ATNASyslogProtocol`: Set this value to UDP or TLS port.
- `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.

You must 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. An audit configuration example:

```
auditRepositoryServer=
auditRepositoryPort=
ATNASyslogProtocol=
auditMessageType=
keyStore=
keyStoreType=JKS
trustStore=
trustStoreType=JKS
credentialStore=
Audit=no
```

Enable the MTOM option

This section describes how to configure 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 the number of threads and timeout for the initiating gateway

This section describes how to configure the thread count and timeout value for the initiating gateway.

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

`maximumThreadCount`: Takes the value of the maximum number of threads you want to create. For example, the number of threads required to send the XCA Gateway requests:

```
maximumThreadCount=
```

Time out configurations for the requests:

`default_timeout_sync`: Takes the value of the time out for synchronous transactions:

```
default_timeout_sync=
```

`default_timeout_async`: Takes the value of the time out for asynchronous transactions:

```
default_timeout_async=
```

XCPD Initiating Gateway configuration

This section describes the configuration of the initiating XCPD Initiating Gateway.

- Configure the XCPD Responding Gateway
  This section describes the configuration of the responding gateway.
- Configure sender and receiver OIDs
  This section lists the settings for sending and receiving OIDs.
- Patient ID mapping workflow
  This section describes how to configure the patient ID workflow.

Configure the XCPD Responding Gateway

This section describes the configuration of the responding gateway.

Prerequisite: Get the XCPD URL and the HomeCommunity ID of the responding gateway.

- `XCPD_RespondingGW_<TargetHomeCommunityID>` : Takes the value of the responding gateway XCPD URL. `<TargetHomeCommunityID>` must be replaced with the `HomeCommunityID` of the responding gateway.
- `XCPD_RespondingGW_TargetHomeCommunityID=` the XCPD Responding Gateway URL For example,

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

Configure sender and receiver OIDs

This section lists the settings for sending and receiving OIDs.

The following properties take sender and receiver OID values appropriately:

- `XCPD_IG_SenderOID=`
- `XCPD_IG_RecieverOID=`

Patient ID mapping workflow

This section describes how to configure the patient ID workflow.

The property `PatientID_Mapping_Workflow` takes the following values:

- **xca**:When the value is `xca`, initiating gateway does not send any XCPD request to find patient ID in remote community. The initiating gateway uses the same patient ID sent by the document consumer.
- **xcpd**: When the value is `xcpd`, the initiating gateway sends the XCPD request to each configured responding gateway, fetches the patient ID, and uses that patient ID for the respective Cross Gateway Query Transactions. For example, `PatientID_Mapping_Workflow=`

Responding gateway configuration

This section describes how to configure the responding gateway.

- Configure the responding gateway local home community
  This section lists the configuration parameters for local home community configuration.
- Configure the responding gateway local registry repository
- ATNA audit configuration
  This section lists the parameters for ATNA audit configuration.
- Configure the local MPI to the responding gateway
  This section describes how to configure the XCPD Responding Gateway settings for local MPI.
- Configure Health Data Locator
  This section describes how to enable Health Record Locator.

Configure the responding gateway local home community

This section lists the configuration parameters for local home community configuration.

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

```
localHomeCommunityId_RG=
localHomeCommunityId_XCPD=
```

Configure the responding gateway local registry repository

Prerequisite: Get the responding gateway local registry, the repository URLs with the repository unique ID:

- `RespondingGatewayRegistryURL=`
- `RespondingGatewayRepositoryID=`

Prerequisite: Get the repository unique ID and the repository URL for retrieving document transactions. Update the configuration file as follows: The syntax is: `RepositoryUniqueId=RepositoryURL`. For example:

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

ATNA audit configuration

This section lists the parameters for ATNA audit configuration.

ATNA Audit configuration prerequisites: Get the audit repository host name or IP and audit repository UDP or TLS port.

- `ATNASyslogProtocol`: Set this value to UDP or TLS port.
- `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.

You must 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. An audit configuration example:

```
auditRepositoryServer=
auditRepositoryPort=
ATNASyslogProtocol=
```

```
auditMessageType=
keyStore=
keyStoreType=JKS
trustStore=
trustStoreType=JKS
credentialStore=
Audit=no
```

Configure the local MPI to the responding gateway

This section describes how to configure the XCPD Responding Gateway settings for local MPI.

Prerequisite: Get the 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.

You can have multiple PDQ suppliers to talk with:

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

Where `<count>` is the number of PDQ suppliers to configure. The 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=
```

Configure Health Data Locator

This section describes how to enable Health Record Locator.

To enable Health Data Locator, set the value of the `SupportsHealthDataLocator` property in the `RG.properties` file to yes. If the value is set to yes, the responding gateway responds to the XCPD request indicating that it supports patient location query. If the value is set to no, the responding gateway does not support Health Data Locator.

Transactions and web service URLs

This section lists the web services supported by XCA.

> **Note:**
>
> You can find the web service WSDL by adding the following to the URL: `?wsdl`.

Table 2-1 Transactions and web service URLs

Transaction	Synch	Asynch	Endpoint URL
Cross Patient Discovery (ITI-55)	Yes	Yes	`http(s)://<XCA_HOST>:<PORT>/RespondingGateway_Service/XCPDRespondingGateway`
Registry Stored Query (ITI-18)	Yes	No	`http(s)://<XCA_HOST>:<PORT>/InitiatingGatewayQuery_Service/XCAInitiatingGatewayQuery`
Retrieve Document Set (ITI-43)	Yes	No	`http(s)://<XCA_HOST>:<PORT>/InitiatingGatewayRetrieve_Service/XCAInitiatingGatewayRetrieve`
Cross Document Query (ITI-38)	Yes	Yes	`http(s)://<XCA_HOST>:<PORT>/RespondingGatewayQuery_Service/XCARespondingGatewayQuery`
Cross Document Retrieve (ITI-39)	Yes	Yes	`http(s)://<XCA_HOST>:<PORT>/RespondingGatewayRetrieve_Service/XCARespondingGatewayRetrieve`
Patient Location Query (ITI-56)	Yes	Yes	`http(s)://<XCA_HOST>:<PORT>/RespondingGateway_Service/XCPDRespondingGateway`

Table 2-1 (Cont.) Transactions and web service URLs

Transaction	Synch	Asynch	Endpoint URL
Asynchronous Registry Stored Query	No	Yes	`http(s)://<XCA_HOST>:<PORT>/IGAsyncServices/XCAInitiatingGatewayQuery`
Asynchronous Retrieve Document Set	No	Yes	`http(s)://<XCA_HOST>:<PORT>/IGAsyncServices/XCAInitiatingGatewayRetrieve`

Oracle extensions

This section describes how Oracle implemented the IHE specification on XCA and XCPD gateways.

As per the IHE specification, XCA and XCPD are two different profiles. The Oracle implementation is merged together. The Initiating Gateway first sends the XCPD request, finds out the patient identifiers in the remote community, and then uses this patient identifier for the next cross gateway query call to the responding gateway.

3

Security configuration issues

This section describes security configuration issues you must consider when implementing XCA.

- General security principles
  This section describes fundamental security principles for using any application securely.
- Configure strong database passwords
  This section discusses configuring strong passwords on the database.
- Follow the principle of least privilege
  This section describes the principle of least privilege.
- Disable Telnet service
  This section describes why you should not use the Telnet service.
- Disable other services
  This section explains why you should disable other unused services.
- Design multiple layers of protection
  This section describes the need for multiple layers of protection.
- Use SSL
  This section describes why SSL is a good choice for XCA.

General security principles

This section describes fundamental security principles for using any application securely.

General security principals include:

- **Keep software up-to-date**: Keep all software versions and patches up-to-date.
- **Keep up-to-date on the latest security information and critical patches:** Oracle continually improves its software and documentation. Critical patch updates are the primary means of releasing security fixes for Oracle products to customers with valid support contracts. Oracle recommends you to apply these patches as soon as they are released.
- **Managing default user accounts**: Lock and expire default user accounts.
- **Closing all open ports when not in use**: Keep only the minimum number of ports open. You should close all ports when not in use.

Configure strong database passwords

This section discusses configuring strong passwords on the database.

Repeat the following basic rule of security management:

Ensure all passwords are strong. You can strengthen passwords by creating and using password policies for your organization. For guidelines on securing passwords and for

additional ways to protect passwords, refer to the *Oracle® Database Security Guide* specific to the database release you are using.

You should modify the following passwords to use your policy-compliant strings:

- Passwords for the database default accounts, such as SYS and SYSTEM.
- Passwords for the database application-specific schema accounts, such as Gateway.
- Password for the database listener. Oracle recommends that you do not configure a password for the database listener as this enables remote administration. For more information, refer to the section *Removing the Listener Password of Oracle® Database Net Services Reference 11g Release 2 (11.2)*.

Follow the principle of least privilege

This section describes the principle of least privilege.

The principle of least privilege states that users should be given the least amount of privilege to perform their jobs. Overly ambitious granting of responsibilities, roles, grants - especially early on in an organization's life cycle when people are few and work needs to be done quickly - often leaves a system wide open for abuse. User privileges should be reviewed periodically to determine relevance to current job responsibilities.

To restrict access, use the following default file permissions in a Unix environment:

- 740 for executable files
- 640 for regular files

Disable Telnet service

This section describes why you should not use the Telnet service.

The Oracle XCA standard configuration does not use the Telnet service. By default, Telnet listens on port 23. Telnet, which sends clear-text passwords and user names through a log in, is a security risk to your servers. If the Telnet service is available on any system, disable Telnet in favor of Secure Shell (SSH). Disabling Telnet protects your system security.

Disable other services

This section explains why you should disable other unused services.

In addition to not using Telnet, the Oracle XCA Gateway standard configuration does not use the following services or information for any functionality:

- **Simple Mail Transfer Protocol (SMTP)**: This protocol is an Internet standard for e-mail transmission across Internet Protocol (IP) networks.
- **Identification Protocol (identd):** This protocol is generally used to identify the owner of a TCP connection on UNIX.
- **Simple Network Management Protocol (SNMP):** This protocol is a method for managing and reporting information about different systems.

Restricting these services or information does not affect the use of the Oracle XCA Gateway standard configuration. If you are not using these services for other applications, disable these services to minimize your security exposure. If you need SMTP, identd, or SNMP for other applications, ensure to upgrade to the latest version of the protocol to provide the most up-to-date security for your system.

Design multiple layers of protection

This section describes the need for multiple layers of protection.

When designing a secure deployment, design multiple layers of protection. If a hacker gains access to one layer, such as Application server, that should not automatically give them easy access to other layers, such as the database server. Providing multiple layers of protection may include:

- Enabling only those ports required for communication between different tiers. For example, only allow communication to the database tier on the port used for SQL*NET communications (by default, 1521).
- Placing firewalls between servers so that only expected traffic can move between servers.

Use SSL

This section describes why SSL is a good choice for XCA.

Consider using the Application Server SSL service for the XCA application. The XCA application is a standard Java EE application and can utilize an industry standard security infrastructure and framework. There is no configuration required on the XCA application. The application Server (WebLogic) provides SSL service. For more information about configuring SSL to achieve SSL security for XCA, see the Application Server documentation.

When SSL or TLS is configured, use TLS_RSA_WITH_AES_128_CBC_SHA cipher instead of SSL_RSA_WITH_3DES_EDE_CBC_SHA for TLS authentication.