Oracle® Health Sciences Information Manager

Health Record Locator User Guide

Release 2.0.1

E37030-02

October 2013

This guide provides information on Oracle® Health Sciences Information Manager (OHIM) Health Record Locator (HRL). It describes features and functionalities of Document Registry, Integrating the Healthcare Enterprise (IHE) standards, and Web Services with their configuration options.

This document is intended for Oracle Health Record Locator users.

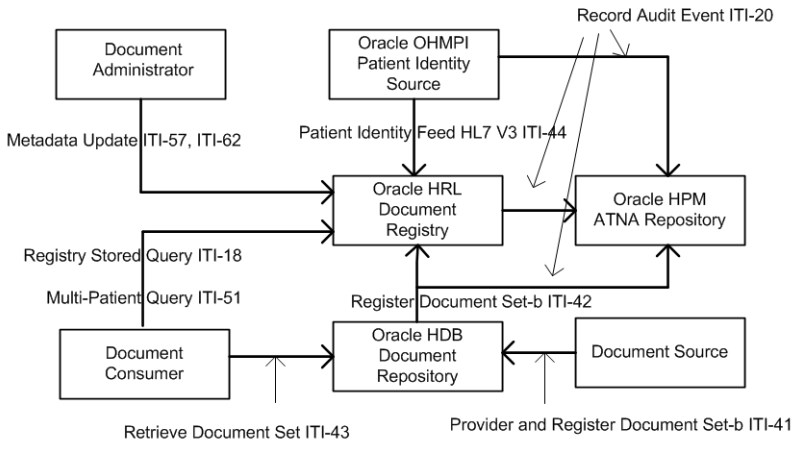
Overview

HRL keeps track of patients' documents by indexing them using the Document Metadata. HRL is IHE and Cross-Enterprise Document Sharing (XDS) standards compliant and implements the XDS Document Registry Actor.

Cross-Enterprise Document Sharing Actors and Transactions

Figure 1 shows the XDS actors and transactions among them. It does not contain actors and transaction related to Document Metadata Subscription (DSUB).

Figure 1 XDS Actors and Transactions



Actors and Transactions Supported by Health Record Locator

HRL supports the following IHE profiles and transactions:

Table 1 Actors and Transactions Supported by HRL

Profile	Actor	Option	ITI TXN Number[1]
MPQ[2]	Document Registry	None	ITI-51
MPQ	Document Registry	Asynchronous Web Services Exchange	ITI-51
XDS.b[3]	Document Registry	Patient Identity Feed (HL7 V3)	ITI-44
XDS.b	Document Registry	None	ITI-18 ITI-42
XDS.b	Document Registry	Asynchronous Web Services Exchange	ITI-18 ITI-42
XDS.b	Document Registry	Document Metadata Update	ITI-57 ITI-62
XPID[4]	Document Registry	None	ITI-64
XDS.b	Document Registry	Patient Identity Feed (HL7 V2)	ITI-8
DSUB[5]	Document Metadata Notification Broker Document Metadata Publisher	None	ITI-52 ITI-53 ITI-54

[1] IT Infrastructure Transaction Number
[2] MPQ - Multi-patient Queries
[3] XDS.b - Cross-Enterprise Document Sharing
[4] XPID - XAD-PID Change Management Profile
[5] DSUB - Document Metadata Subscription

Services Provided

Most of the IHE ITI transactions supported by HRL are supported through SOAP 1.2 based Web Services. The following are the SOAP 1.2 Web Services supported by HRL:

- Core Registry Service (Patient Feed, Register Document Set, and Registry Stored Query) (see Core Registry Service)
- Multi-patient Query Service (see Multi-patient Query Service)
- Metadata Update Service (see Metadata Update Service)

Web Services

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

Core Registry Service

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

- ITI-44 Patient Identity Feed

- ITI-42 Register Document Set
- ITI-18 Registry Stored Query

  The Registry Stored Query is classified into the following types:

  - FindDocuments
  - FindSubmissionSets
  - FindFolders
  - GetDocuments
  - GetFolders
  - GetAssociations
  - GetDocumentsAndAssociations
  - GetSubmissionSets
  - GetSubmissionSetAndContents
  - GetFolderAndContents
  - GetFoldersForDocument
  - GetRelatedDocuments
  - GetAll

Multi-patient Query Service

The following Web Services operations and IHE transactions are supported for Multi-patient Query Service:

- ITI-51 Multi-patient Query

  The Multi-patient Query is classified into the following type:

  - FindDocumentsForMultiplePatients
  - FindFoldersForMultiplePatients

Metadata Update Service

The following Web Services operations and IHE transactions are supported for Metadata Update Service:

- ITI-57 Update Document Set
- ITI-62 Delete Document Set

DSUB Service

The following Web Services operations and IHE transactions are supported for DSUB Service:

- ITI-54 Document Metadata Publish
- ITI-52 Document Metadata Subscribe

HL7v2 Services

The following IHE transactions are supported in HL7v2 Server:

- ITI-8 Patient Identity Feed

- ITI-64 Notify XAD-PID Link Change

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

Deployment Environment

Core Registry, Multi-patient Query, and Metadata Update Services are implemented as Java Enterprise Edition (EE) components.

HL7v2 Services are implemented as an optional Application server components called XPID. You must deploy the XPID component on the same Application server instance as that of the core Registry Services component.

DSUB Document Metadata Notification Broker service is implemented in an optional Java EE component. You may choose to deploy it on the same Application Server instance as that of core Registry Services or on a separate instance.

DSUB Document Metadata Publisher is part of core Registry Services component. This is enabled through the configuration parameter.

System Requirements

- Oracle Enterprise Linux 5.5 or higher, Microsoft Windows 2003, Microsoft Windows 2008, Microsoft Windows XP, and Microsoft Windows 7

Hardware Requirement

Following are the hardware requirements for installing HRL:

- 2 GB (2048 MB) of RAM for GlassFish
- 4 GB (4096 MB) of RAM for WebLogic
- 12 GB of disk space
- 16 GB of disk space for 64-bit

Software Requirement

The following are the software requirements for installing OHIM Health Record Locator:

- Java 1.6 executable in path
- Oracle Database 10+ (11g Release 2)
- 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
- Oracle JDBC Driver 11.2.0.1.0 in the application server

Configuration Requirements

Apache Ant 1.8.2 executable in path

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

Configuration

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

- GlassFish: `<GlassFish Home>/domains/<domain name>/config/hrl/config/xconfig.xml`
- WebLogic: `<Weblogic Middleware Home>/user_projects/domains/<domain name>/config/hrl/config/xconfig.xml`

Restart the Application server for xconfig.xml changes to take effect.

The following is the structure of xconfig.xml file in which some configuration properties are specified under **HomeCommunity** and **Registry** elements.

```
<?xml version="1.0" encoding="utf-8"?>
<Config>
    <HomeCommunity name="home">
        <Property name="propName1">propVal1</Property>
          ...
    </HomeCommunity>

    <Registry name="localregistry">
        <Property name="propName2">propVal2</Property>
          ...
    </Registry>
</Config>
```

Enabling Sending ATNA UDP or TLS Messages

To enable sending ATNA UDP or TLS messages, edit the value of the following properties under **HomeCommunity** element and specify ATNA UDP or TLS server details:

- ATNAPerformAudit: Set this value to `true` to enable sending ATNA audit messages. By default, this value is set to `false`.
- ATNAsyslogProtocol: Set this value to `udp` or `tls`.
- ATNAsyslogHost: Specify the ATNA UDP or TLS server host name or IP address.
- ATNAsyslogPort: Specify the ATNA UDP or TLS server port number.

> **Note:** For TLS auditing in WebLogic, ensure to start the WebLogic with the following JVM options for the keystore and truststore file:
>
> `-Djavax.net.ssl.keyStore=<keystore file>`
>
> `-Djavax.net.ssl.keyStorePassword=<keystore pass>`
>
> `-Djavax.net.ssl.keyStoreType=<keystore type>`
>
> `-Djavax.net.ssl.trustStore=<truststore file>`
>
> `-Djavax.net.ssl.trustStorePassword=<truststore pass>`

Other HomeCommunity Level Properties

- ValidatePatientId: Set this value to `true` (default value) to validate known patients ID before registering document entry.

- XMLSchemaValidationEnabled: Set this value to `true` (default value) to schema validate incoming messages.
- LogEnabled: Set this value to `true` (default value) to enable logging of registry request and response messages in Log schema tables.

> **Note:** This parameter is different from enabling ATNA audit log messages.

Registry Level Properties

- ReceiverDeviceId: Set this value to construct response messages in HL7v2 Services.
- ReceiverDeviceName: Set this value to construct response messages in HL7v2 Services. By default, this value is set to `ORACLE_HIA_RLS_XDSbRegistry`.
- AcceptPIDOnlyFrom: Set this property to let registry accept patient feed only from the specified domain.

  Comment or delete this property to let registry accept patient feed from all domain.
- MaxLeafObjectsAllowedFromQuery: Specify an integer value that determine the maximum number of document entries returned with Registry Stored Query response messages. By default, this value is set to `25`.

> **Note:** This property is applicable only when query request contains return type value `LeafClass`.

- TrimLogQueueMessages: Set this value to `true` (default value) to trim the messages logged in Log schema tables.
- MaxLeafObjectsPerLogQueueMsg: Specify the maximum number of Leaf objects to be logged per message. By default, this value is set to `5`.
- MaxObjectRefsPerLogQueueMsg: Specify the maximum value of Object references to be logged per message. By default, this value is set to `5`.

DSUB Properties

- NotificationEnabled: Set this value to `true` to enable publishing registry events to the DSUB Notification Broker. By default, this value is set to `false`.
- PublishEndPoint: Specify the endpoint URL of the DSUB Notification Broker.
- DsubValidateCodeAndCodingScheme: Set this value to `true` (default value) to validate code and coding scheme containing DSUB subscription message against codes file of the registry.
- DefaultDaysBeforeExpiryOfSubscription: Enter an integer value, which indicates the number of days before which the subscription will expire. By default, this value is set to `30`.
- NotificationBrokerSubscribeEndPoint: Specify the endpoint URL of the DSUB Notification Broker.
- DeleteExpiredSubscriptionsIntervalDuration: Enter an integer value specifying milliseconds interval.

- DeleteExpiredSubscriptionsTimerStartInterval: Enter an integer value specifying milliseconds interval.

XPID

- xpid.classification.scheme: Content type classification coding scheme. This scheme should be present in the codes file.
- xpid.classification.code: Content type code for the coding scheme. This code should be present in the codes file.

Updating Codes

The codes file is located under the `config/hrl/codes` directory of the Application Server domain directory.

- GlassFish: `<GlassFish Home>/domains/<domain name>/config/hrl/codes/codes.xml`
- WebLogic: `<Weblogic Middleware Home>/user_projects/domains/<domain name>/config/hrl/codes/codes.xml`

You can update these files with new codes as applicable. Restart the Application server for new codes to take effect.

Transactions and Web Service Uniform Resource Locator

Table 2 lists the Web Services supported by HRL. You can find the Web Service WSDL by suffixing endpoint Uniform Resource Locator (URL) with `?wsdl`.

Table 2 Transactions and Web Service URL

Transaction	Synch	Asynch	Endpoint URL
Register Document Set-b (ITI-42)	Yes	Yes	http(s)://<HRL_ HOST>:<PORT>/hrl/regsvc
Registry Stored Query (ITI-18)	Yes	Yes	http(s)://<HRL_ HOST>:<PORT>/hrl/regsvc
Patient Identity Feed (HL7 V3) (ITI-44)	Yes	Yes	http(s)://<HRL_ HOST>:<PORT>/hrl/regsvc
Multi Patient Query (ITI-51)	Yes	Yes	http(s)://<HRL_ HOST>:<PORT>/hrl/regmpqsvc
Metadata Update - Update (ITI-57)	Yes	Yes	http(s)://<HRL_ HOST>:<PORT>/hrl/regupdsvc
Metadata Update - Delete (ITI-62)	Yes	Yes	http(s)://<HRL_ HOST>:<PORT>/hrl/regupdsvc

Oracle Extensions

Getting the Latest Deprecated Version of Document Entry

When you execute **FindDocument Registry Stored Query (ITI-18)** with status parameter value of **deprecated** (`urn:oasis:names:tc:ebxml-regrep:StatusType:Deprecated`), registry returns all document versions with the status **deprecated** as per the IHE specification.

To query only the latest deprecated version of document entry, a new status parameter value **deleted** (`urn:orcl.reg:names:StatusType:Deleted`) is added to HRL. When this status parameter value **deleted** is specified in the query, registry returns the latest version of the document entry for a patient where all versions have deprecated status.

> **Note:** This parameter value is only applicable to FindDocument query type of Registry Stored Query (ITI-18).

Querying AuthorPerson

The `$XDSDocumentEntryAuthorPerson` query parameter value is used in *case-sensitive* manner in Registry Stored Query (ITI-18) to retrieve matching document entries.

To query for document entries with AuthorPerson value in *case-insensitive* manner, a new parameter `$orcl.caseInsensitive.DocumentEntryAuthorPerson` is added.

Handling Large Number of Document Entries

Registry queries executed without any filters retrieve all document entries of a patient.

Ensure to design client document consumer actor to query with filter conditions or parameters. However, using filter may still result in large document entries and hence Oracle recommends that you use the following queries instead of one large query retrieving all document entry metadata.

Execute large query with `returnType="ObjectRef"`, which returns all document entries Object References or Universally Unique Identifier (UUID)s. This query executes faster compared to one with `returnType="LeafClass"`, which returns all metadata (XML structure).

Subsequent queries can use limited number of UUIDs to query document entries metadata depending on the page size.

For example,

- Executing `FindDocuments` query type with `returnType="ObjectRef"` returns a large number of ObjectRefs (UUIDs).
- Executing subsequent `GetDocuments` query type with `returnType="LeafClass"` with limited number of UUIDs from the list returns document entries metadata (XML structure) to be processed and displayed on one page.

Security Configuration Issues

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

General Security Principles

The following are fundamental principles for using any application securely:

Keep software up-to-date

Keep all software versions and patches up-to-date.

Keep up-to-date on latest security information critical patch

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.

Configure 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 ADT, HRLCORE, and LOG.
- Password for the database listener.

  Oracle recommends that you do not configure a password for the database listener as it will enable remote administration. For more information, refer to the section *Removing the Listener Password* of *Oracle® Database Net Services Reference 11g Release 2 (11.2)*.

Follow the principle of least privilege

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

To restrict access, it is recommended to have the following default file permissions in Unix environment.

- 740 for executable
- 640 for regular files

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.

Disabling the Telnet service

Oracle HRL 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, it is recommended to disable Telnet in favor of Secure Shell (SSH). Disabling Telnet protects your system security.

Disabling Other Unused Services

In addition to not using Telnet, the HRL 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 Oracle HRL standard configuration. If you are not using these services for other applications, it is recommended to 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.

Designing 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.

Utilizing SSL

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

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

Performance Tuning

Oracle Database

Oracle recommends the following generic Oracle database optimizations for HRL and on the specific database behavior:

Parameter	Value
db_cache_size	1 GB
memory_target	8 GB
memory_max_target	8 GB
log_buffer	3 MB

Parameter	Value
LARGE_POOL_SIZE	100 MB
PGA_AGGREGATE_TARGET	2 GB
SGA_MAX_SIZE	4 GB
SGA_TARGET	4 GB
SHARED_POOL_SIZE	1 GB
processes	1200
session	1350
open_cursors	1200
java_pool_size	100 MB

GlassFish

Oracle recommends the following parameter if HRL is running on the Oracle GlassFish server:

- Minimum Java heap size 512 MB
- Maximum Java heap size 2048 MB

Related Documents

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

Appendix A: Acronyms

This section provides a list of commonly used acronyms.

- DSUB - Document Metadata Subscription
- HRL - Health Record Locator
- IHE - Integrating the Healthcare Enterprise
- MPQ - Multi-patient Queries
- OHIM - Oracle Health Sciences Information Manager
- XDS - Cross-Enterprise Document Sharing
- XPID - XAD-PID Change Management Profile

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 Health Record Locator User Guide, Release 2.0.1
E37030-02