# Oracle® Health Sciences Information Manager

## Policy Monitor Installation and Configuration Guide

4.0
F50770-01
January 2022

ORACLE

Oracle Health Sciences Information Manager Policy Monitor Installation and Configuration Guide, 4.0

F50770-01

# Contents

## B Policy Monitor database



## C Audit Message XML schema reference



## D Password encoding

# 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 the hardware and software requirements for installing Oracle Health Sciences Information Manager Policy Monitor. Also included is supported IHE profiles, download information, and terminology. .

- Hardware requirements
  Hardware requirements for the Oracle Health Sciences Information Manager Policy Monitor include minimum RAM and disk space.
- Software requirements
  The Oracle Health Sciences Information Manager Policy Monitor has software requirements for installing and running the product.
- Supported IHE profiles
  Oracle Health Sciences Information Manager Policy Monitor supports IHE profiles. See the list below for supported profiles.
- Download Health Sciences Information Manager Health Policy Monitor
  Download the Oracle Health Sciences Information Manager Health Policy Monitor to your system that meets the hardware and software requirements.
- Terminology
  This section includes acronyms and definitions of commonly used terms.

## Hardware requirements

Hardware requirements for the Oracle Health Sciences Information Manager Policy Monitor include minimum RAM and disk space.

Minimum hardware requirements for installing the Oracle Health Sciences Information Manager Policy Monitor include:

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

## Software requirements

The Oracle Health Sciences Information Manager Policy Monitor has software requirements for installing and running the product.

Software requirements include:

- Java 1.8 executable in path (for installer)
- Oracle JDK 1.8.0_311+
- 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

Configuration requirements include:

- Apache Ant 1.10.11 executable in path

```
PATH=$PATH:<install_dir>/apache-ant-1.10.11/bin
```

# Supported IHE profiles

Oracle Health Sciences Information Manager Policy Monitor supports IHE profiles. See the list below for supported profiles.

Supported IHE profiles
Profile Name: **ATNA**

Version: `Revision 17.0 July 20, 2020`

Location:

https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Rev17-0_Vol2a_FT_2020-07-20.pdf

https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Rev17-0_Vol2b_FT_2020-07-20.pdf

http://wiki.ihe.net/index.php?title=ATNA

# Download Health Sciences Information Manager Health Policy Monitor

Download the Oracle Health Sciences Information Manager Health Policy Monitor to your system that meets the hardware and software requirements.

To download the Oracle Health Sciences Information Manager Health Policy Monitor:

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 Health Policy Monitor compressed tar file (ohim_hpm_installer.tgz).

.

# Terminology

This section includes acronyms and definitions of commonly used terms.

**Table 1-1 Acronyms**

| Acronym | Description |
|---|---|
| ARR | Audit Record Repository |
| CCD | Continuity of Care Document |
| CDA | Clinical Document Architecture |
| DER | Distinguished Encoding Rules |
| HIE | Health Information Exchange |
| HIO | Health Information Organization |
| HL7 | Health Level 7 |
| IHE | Integrating the Healthcare Enterprise |
| NAV | Notification Of Document Availability |
| NHIE | Nationwide Health Information Exchange |
| NHIO | Nationwide Health Information Organization |
| OHIM | Oracle Health Sciences Information Manager |
| SAML | Security Assertion Markup Language |
| WSDL | Web-Service Definition Language |
| XDM | Cross-Enterprise Document Media Interchange |

**Table 1-2 Terms**

| Term | Description |
|---|---|
| Health Information Exchange | Health Information Exchange is an entity that enables the movement of health-related data among entities within a state, a region, or a non-jurisdictional participant group, which might include "classic" regional health information organizations at regional and state levels, Health Information Organization integrated delivery systems and health plans, or health data banks that support health information exchange. |
| Health Information Organization | Health Information Organization is an organization that enables the movement of health-related data among entities, evolving as a replacement term for health information exchange or HIE. Healthcare Information Technology Standards Panel Or simply HITSP, a cooperative partnership between the public and private sectors formed and supported by ONC for the purpose of harmonizing and integrating standards that will meet clinical and business needs established by AHIC use cases for sharing information among organizations and systems. |

**Table 1-2 (Cont.) Terms**

| Term | Description |
|---|---|
| Integrating the Healthcare Enterprise | Integrating the Healthcare Enterprise is an initiative by healthcare professionals and industry to improve the way computer systems in healthcare share information, promoting and coordinating the use of established standards such as DICOM and HL7 to address specific clinical need in support of optimal patient care. The Nationwide Health Information Network is being developed by ONC to provide a secure, nationwide, interoperable health information infrastructure that will connect providers, consumers, and others involved in supporting health and healthcare. |
| Security Assertion Markup Language | Security Assertion Markup Language is an XML-based standard for exchanging authentication and authorization data between security domains. |
| Web Services Description Language | Web Services Description Language is an XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information. |
| XML Schema | XML Schema is a means for defining the structure, content, and semantics of XML documents. |

2

# Install and configure Health Sciences Information Manager Policy Monitor

The Oracle Health Sciences Information Manager Policy Monitor has components and templates that you can install and configure.

- Audit Record Repository (ARR)
  This section describes the Audit Record Repository (ARR) and provides links to Internet Official Protocol Standards (STD1).
- Install Health Sciences Information Manager
  This section shows the commands to install the Oracle Health Sciences Information Manager Policy Monitor and run the installer.
- Configure Health Sciences Information Manager Policy Monitor
  This section describes how to configure properties, set up the network, create certificates and start the Oracle Health Sciences Information Manager Policy Monitor.

## Audit Record Repository (ARR)

This section describes the Audit Record Repository (ARR) and provides links to Internet Official Protocol Standards (STD1).

The Policy Monitor implements an Audit Record Repository (ARR) as required by the ATNA profile. The following links provide context as to what ARR represents in this guide. Before setting up your OHIM Policy Monitor, Oracle recommends that you review these links.

Audit Trail and Node Authentication (ATNA) Integration Profile

http://wiki.ihe.net/index.php?title=ATNA

which is built on top of the following:

Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications

http://tools.ietf.org/html/rfc3881

Syslog Protocol

http://tools.ietf.org/html/rfc5424

Transmission of Syslog Messages over Transport Layer Security (TLS)

http://tools.ietf.org/search/rfc5425

Transmission of Syslog Messages over User Datagram Protocol (UDP)

https://tools.ietf.org/html/rfc5426

> **Note:**
>
> The above links open documents that describe the Internet Protocol suite, specifically Internet Official Protocol Standards (STD1) as related to ARR. They provide critical technical information about secure transmission of data over the Internet, including node authentication and audit trails. We recommend that you read them.

# Install Health Sciences Information Manager

This section shows the commands to install the Oracle Health Sciences Information Manager Policy Monitor and run the installer.

To install the Oracle Health Sciences Information Manager Policy Monitor:

1. Execute the following commands to install the Policy Monitor:

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

2. Run the Oracle Health Sciences Information Manager Policy Monitor installer.

```
$ cd <install_dir>
$ java -jar ohim_hpm_installer.jar
Oracle HIM HPM Installer 4.0.0.0
-- Command
Choose option install_command (usage, version, install)
> install
Starting init install
-- Policy monitor install directory
Enter policymonitor_install_dir [#null]
> arr
```

.

# Configure Health Sciences Information Manager Policy Monitor

This section describes how to configure properties, set up the network, create certificates and start the Oracle Health Sciences Information Manager Policy Monitor.

- Configure properties
  From this release of OHIM Policy Monitor, you are not required to manually edit the file. You will be prompted through the script. Execute the following code to configure the OHIM Health Policy Monitor properties:
- Set up network
  Setting up the network involves opening ports to connect to UDP and TLS.

- Create and import self-signed certificates
  Before creating and importing self-signed certificates, you must perform prerequisite steps to ensure that the host name does not return a fully qualified name.
- Start Health Sciences Information Manager Policy Monitor
  This section describes how to start the Oracle Health Sciences Information Manager Policy Monitor, including commands for the following modes: UDP, TLS and TCP.

## Configure properties

From this release of OHIM Policy Monitor, you are not required to manually edit the file. You will be prompted through the script. Execute the following code to configure the OHIM Health Policy Monitor properties:

1. cd <arr_install_dir>/bin
2. ant -f arr.xml create-arr-properties-file

```
[input] Choose target database
[input] Enter oracle_host
[input] Enter oracle_port
[input] Enter oracle_sid
[input] Enter oracle_username
[input] Enter oracle_password
[input] Enter arr_port
[input] Enter property_file_name
```

To edit a password in a properties file:

- `ant -f arr.xml update-config-properties-file-password`

To edit a property in a properties file:

- `ant -f arr.xml update-config-properties-file-property`

For more information, see Password encoding.

## Set up network

Setting up the network involves opening ports to connect to UDP and TLS.

> **Note:**
>
> To open ports below 1024 requires root permissions.

To set up the network:

1. Open incoming ports to allow external connections to UDP and TLS port.

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

2. Add the following lines:

```
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport
514 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport
6514 -j ACCEPT
```

3. Restart the service.

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

## Create and import self-signed certificates

Before creating and importing self-signed certificates, you must perform prerequisite steps to ensure that the host name does not return a fully qualified name.

To create and import self-signed certificates:

1. Before creating and importing self-signed certificates, perform prerequisite steps. You must ensure that the host name does not return a fully qualified name for the machine. Check the following commands before proceeding:
   a. Check that the command returns a non-fully qualified name:

      ```
      > hostname
      ```

   b. Check that the command returns a fully qualified name:

      ```
      > hostname -f
      ```

   c. Check that the command returns the domain:

      ```
      > hostname -d
      ```

2. Change to install directory:

   ```
   > cd <arr_install_dir>/bin
   ```

3. Execute `create-and-import-selfsigned-certs.sh` to install the self-signed certificate.

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

   This performs the following:

   - creates the keystore for the private internal key
   - exports the certificate that authenticates the internal key
   - imports the trusted certificates into the truststore
   - provides these certificates to the server to use for authentication purposes

> **Note:**
>
> Before proceeding to the next step, copy the certificate of the host computer <HOSTNAME.cer> to <arr_install_dir>/bin/keystore folder.

4. To install a host machine's certificate, run the script:

```
> sh import-hostname-cert.sh
```

   Enter the host name of the machine whose certificate is being imported into the truststore: <HOSTNAME>.

- Avoid a Java security certificate exception

## Avoid a Java security certificate exception

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

To Make the Host Name Not Fully Qualified:

1. Set the OHIM host names to be not fully qualified.
2. Add aliases for all hosts.
3. Regenerate and reimport the certificates.
4. Restart all the servers.
5. Test that you do not have a Java security certificate exception.

# Start Health Sciences Information Manager Policy Monitor

This section describes how to start the Oracle Health Sciences Information Manager Policy Monitor, including commands for the following modes: UDP, TLS and TCP.

To start the Health Sciences Information Manager Policy Monitor:

1. Change directory:

```
cd <arr_install_dir>/bin
```

2. Select the mode and use the appropriate start command for the server.

   To start in UDP mode:

```
> arr.sh -propertyfile <ARR_PROPERTIES_FILE> -command start-udp-server
```

   To start in TLS mode:

```
> arr.sh -propertyfile <ARR_PROPERTIES_FILE> -command start-tls-server
```

   To start in TCP mode:

```
> arr.sh -propertyfile <ARR_PROPERTIES_FILE> -command start-tcp-server
```

.

A

# Policy Monitor script

This section provides a description of Policy Monitor scripts and includes examples of commands.

- Policy Monitor script commands
  Policy Monitor scripts include commands for various tasks such as: start, send, parse and table.

## Policy Monitor script commands

Policy Monitor scripts include commands for various tasks such as: start, send, parse and table.

Use the following script to start and test an instance of Policy Monitor (use CTRL-C to stop the server):

```
arr -propertyfile <propertyfile> -command <command> <...args>
```

JDBC Password - ensure the following property is available and encrypted in the input property file:

```
arr.jdbc_password
```

See the tables below for various commands.

**Table A-1 Start Commands**

| Command | Description | Options | Option Description |
|---|---|---|---|
| start-tls-server | Starts a TLS Policy Monitor running on a given port. Note: Ensure the following properties are available and encrypted in the input property file:<br>• arr.keystore_password<br>• arr.truststore_password<br>• arr.keymanager_keystore_password | -arr.port | The port to listen on (6514 is the standard port for syslog over TLS). |
| - | - | -arr.persistence_unit_name | The name of the javax persistence unit defined in persistence.xml. |

**Table A-1 (Cont.) Start Commands**

| Command | Description | Options | Option Description |
|---|---|---|---|
| - | - | -arr.jdbc_driver | The JDBC database driver type. For example: Oracle: oracle.jdbc.OracleDriver |
| - | - | -arr.jdbc_url | The JDBC database URL. |
| - | - | arr.jdbc_username | The JDBC database user name. |
| - | - | -arr.keystore | The server keystore. |
| - | - | -arr.truststore | The server truststore. |
| start-udp-server | Starts an UDP Policy Monitor running on a given port. | -arr.port | The port to listen on (514 is the standard port for syslog over UDP). |
| - | - | -arr.persistence_unit_name | The name of the javax persistence unit defined in persistence.xml. |
| - | - | -arr.jdbc_driver | The JDBC database driver type. For example: Oracle: oracle.jdbc.OracleDriver |
| - | - | -arr.jdbc_url | The JDBC database URL. |
| - | - | -arr.jdbc_username | The JDBC database user name. |
| start-tcp-server | Starts a TCP Policy Monitor running on a given port. Note: This command is not recommended for production use. | -arr.port | The port to listen on. |
| - | - | -arr.persistence_unit_name | The name of the javax persistence unit defined in persistence.xml. |
| - | - | -arr.jdbc_driver | The JDBC database driver type. For example: Oracle: oracle.jdbc.OracleDriver |
| - | - | -arr.jdbc_url | The JDBC database URL. |
| - | - | -arr.jdbc_username | The JDBC database user name. |

**Table A-2 Parse Commands**

| Command | Description | Options | Option Description |
|---|---|---|---|
| parse-audit-msg | Tests the validity of an audit message. | -arr.input_file | A file containing an audit message. |
| parse-syslog-msg | Tests the validity of a syslog message. | -arr.input_file | A file containing a syslog message. |

**Table A-3 Table Commands**

| Command | Description | Options | Option Description |
|---|---|---|---|
| create-tables | Creates the required Policy Monitor database tables and sequences. | -arr.persistence_unit_name | The name of the javax persistence unit defined in persistence.xml. |
| - | - | -arr.jdbc_driver | The JDBC database driver type. For example: Oracle: oracle.jdbc.OracleDriver |
| - | - | -arr.jdbc_url | The JDBC database user name. |
| checks-tables | Checks the required audit server database tables and sequences. | -arr.persistence_unit_name | The name of the javax persistence unit defined in persistence.xml. |
| - | - | -arr.jdbc_driver | The JDBC database driver type. For example: Oracle: oracle.jdbc.OracleDriver |
| - | - | -arr.jdbc_url | The JDBC database URL. |
| - | - | -arr.jdbc_username | The JDBC database user name. |
| drop-and-create-tables | Drops and recreates the Policy Monitor database tables and sequences. | -arr.persistence_unit_name | The name of the javax persistence unit defined in persistence.xml. |
| - | - | -arr.jdbc_driver | The JDBC database driver type. For example: Oracle: oracle.jdbc.OracleDriver |
| - | - | -arr.jdbc_url | The JDBC database URL. |
| - | - | -arr.jdbc_username | The JDBC database user name. |

### Send Commands

**`send-tls-msg`**

Sends a syslog message to a Policy Monitor supporting TLS. Note: Ensure the following properties are available and encrypted in the input property file:

```
arr.keystore_password
arr.truststore_password
arr.keymanager_keystore_password
```

Options:

`-arr.input_file` - A file containing a syslog message.

`-arr.hostname` - The host name of the syslog server.

`-arr.port` - The port of the syslog server.

`-arr.keystore` - The client keystore.

`-arr.truststore` - The client truststore.

**`send-udp-msg`**

Sends a syslog message to Policy Monitor supporting UDP.

Options:

`-arr.input_file` - A file containing a syslog message.

`-arr.port` - The port of the syslog server.

`-arr.hostname` - The host name of the syslog server.

**`send-tcp-msg`**

Sends a syslog message to a Policy Monitor supporting TCP.

Options:

`-arr.input_file` - A file containing a syslog message.

`-arr.port` - The port of the syslog server.

`-arr.hostname` - The host name of the syslog server.

Here are some Policy Monitor commands and examples

**Table A-4 Policy Monitor script command examples**

| Command | Example |
|---|---|
| create-tables | > arr -propertyfile arr.properties -command create-tables |
| check-tables | > arr -propertyfile arr.properties -command check-tables |
| drop-and-create-tables | > arr -propertyfile arr.properties -command drop-and-create-tables |
| parse-audit-msg | > arr -propertyfile arr.properties -command parse-audit-msg -arr.input_file test_audit_msg.txt |
| parse-syslog-msg | > arr -propertyfile arr.properties -command parse-syslog-msg -arr.input_file test_syslog_msg.txt |
| send-tcp-msg | > arr -propertyfile arr.properties -command send-tls-msg -arr.hostname localhost -arr.input_file test_syslog_msg.txt |
| send-tls-msg | > arr -propertyfile arr.properties -command send-tls-msg -arr.hostname localhost -arr.input_file test_syslog_msg.txt |
| send-udp-msg | > arr -propertyfile arr.properties -command send-udp-msg -arr.hostname localhost -arr.input_file test_syslog_msg.txt |
| start-tcp-server | > arr -propertyfile arr.properties -command start-tcp-server |
| start-tls-server | > arr -propertyfile arr.properties -command start-tls-server |
| start-udp-server | > arr -propertyfile arr.properties -command start-udp-server |

B

# Policy Monitor database

This appendix describes the Policy Monitor database.

- Policy Monitor database overview
  This section provides information about the Policy Monitor database. The Policy Monitor is called the Audit Record Repository Server in Oracle Healthcare Master Person Index Working With IHE Profiles (Part Number E18591-01).

## Policy Monitor database overview

This section provides information about the Policy Monitor database. The Policy Monitor is called the Audit Record Repository Server in Oracle Healthcare Master Person Index Working With IHE Profiles (Part Number E18591-01).

The Policy Monitor's audit syslog messages are inserted into the database table ARR_SYS_MSG (see table below) or ARR_SYS_MSG_DI (see table below) based on the message structure in the received syslog message (RFC-3881 XML Schema compliant or DICOM XML Schema complaint). The columns in the table are parallel to the structure of a rfc5424 syslog message (see https://datatracker.ietf.org/doc/html/rfc5424). The tables whose name do not end with the string _DI, map the rfc3881 audit message structure (see https://tools.ietf.org/html/rfc3881) into database tables. The tables whose name end with the string _DI, map the dicom audit message structure (http://dicom.nema.org/medical/dicom/current/output/html/part15.html#sect_A.5.1) into database tables. These tables enable the data querying using JavaPersistence Query Language (JPQL) features.

**Table B-1 ARR_SYS_MSG database table**

| Column | Type |
|---|---|
| ID | NUMBER |
| TRANSPORT | VARCHAR |
| LOCALADDR | VARCHAR |
| LOCALHOST | VARCHAR |
| LOCALPORT | NUMBER |
| REMOTEADDR | VARCHAR |
| REMOTEHOST | VARCHAR |
| REMOTEPORT | NUMBER |
| FACILITY | NUMBER |
| SEVERITY | NUMBER |
| PRIORITY | NUMBER |
| VERSION | NUMBER |
| TIMESTAMP | DATE |
| HOSTNAME | VARCHAR |
| APPLICATIONNAME | VARCHAR |
| PROCESSID | VARCHAR |

**Table B-1 (Cont.) ARR_SYS_MSG database table**

| Column | Type |
|---|---|
| MESSAGEID | VARCHAR |
| STRUCTUREDDATA | VARCHAR |
| MESSAGEENCODING | VARCHAR |
| MESSAGERAWBYTES | BLOB |
| ADT_MSG_ID | NUMBER |

**Table B-2 ARR_SYS_MSG_DI**

| Column | Type |
|---|---|
| ID | NUMBER |
| TRANSPORT | VARCHAR |
| LOCALADDR | VARCHAR |
| LOCALHOST | VARCHAR |
| LOCALPORT | NUMBER |
| REMOTEADDR | VARCHAR |
| REMOTEHOST | VARCHAR |
| REMOTEPORT | NUMBER |
| FACILITY | NUMBER |
| SEVERITY | NUMBER |
| PRIORITY | NUMBER |
| VERSION | NUMBER |
| TIMESTAMP | DATE |
| HOSTNAME | VARCHAR |
| APPLICATIONNAME | VARCHAR |
| PROCESSID | VARCHAR |
| MESSAGEID | VARCHAR |
| STRUCTUREDDATA | VARCHAR |
| MESSAGEENCODING | VARCHAR |
| MESSAGERAWBYTES | BLOB |
| ADT_MSG_DICOM_ID | NUMBER |

**Note:**

If parsing of audit message fails, the Policy Monitor stores the messageRawBytes and other data elements of received messages in:

- ARR_SYS_MSG database table if the messageID value is IHE+RFC-3881
- ARR_SYS_MSG_DI database table if the messageID value is IHE+DICOM or some arbitrary string

C

# Audit Message XML schema reference

This appendix provides a reference for the RFC 3881 Audit Message compliant XML schema, DICOM Audit Message compliant XML schema, and examples for the types of Audit Message.

- RFC 3881 Compliant XML schema reference
  The following section contains the RFC 3881 Compliant XML schema reference:
- DICOM Audit Message XML schema reference
  The following section contains the DICOM Audit Message XML schema reference.

## RFC 3881 Compliant XML schema reference

The following section contains the RFC 3881 Compliant XML schema reference:

```
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
    elementFormDefault="qualified" attributeFormDefault="unqualified">
    <xs:element name="AuditMessage">
        <xs:complexType>
            <xs:sequence>
                <xs:element name="EventIdentification"
                    type="EventIdentificationType" />
                <xs:element name="ActiveParticipant"
                    maxOccurs="unbounded">
                    <xs:complexType>
                        <xs:complexContent>
                            <xs:extension base="ActiveParticipantType" />
                        </xs:complexContent>
                    </xs:complexType>
                </xs:element>
                <xs:element name="AuditSourceIdentification"
                    type="AuditSourceIdentificationType"
maxOccurs="unbounded" />
                <xs:element name="ParticipantObjectIdentification"
                    type="ParticipantObjectIdentificationType" minOccurs="0"
                    maxOccurs="unbounded" />
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <xs:complexType name="EventIdentificationType">
        <xs:sequence>
            <xs:element name="EventID" type="CodedValueType" />
            <xs:element name="EventTypeCode" type="CodedValueType"
                minOccurs="0" maxOccurs="unbounded" />
        </xs:sequence>
        <xs:attribute name="EventActionCode" use="optional">
            <xs:simpleType>
                <xs:restriction base="xs:string">
```

```
                        <xs:enumeration value="C">
                            <xs:annotation>
                                <xs:appinfo>Create</xs:appinfo>
                            </xs:annotation>
                        </xs:enumeration>
                        <xs:enumeration value="R">
                            <xs:annotation>
                                <xs:appinfo>Read</xs:appinfo>
                            </xs:annotation>
                        </xs:enumeration>
                        <xs:enumeration value="U">
                            <xs:annotation>
                                <xs:appinfo>Update</xs:appinfo>
                            </xs:annotation>
                        </xs:enumeration>
                        <xs:enumeration value="D">
                            <xs:annotation>
                                <xs:appinfo>Delete</xs:appinfo>
                            </xs:annotation>
                        </xs:enumeration>
                        <xs:enumeration value="E">
                            <xs:annotation>
                                <xs:documentation>Execute</
xs:documentation>
                            </xs:annotation>
                        </xs:enumeration>
                    </xs:restriction>
                </xs:simpleType>
            </xs:attribute>
            <xs:attribute name="EventDateTime" type="xs:dateTime"
                use="required" />
            <xs:attribute name="EventOutcomeIndicator" use="required">
                <xs:simpleType>
                    <xs:restriction base="xs:integer">
                        <xs:enumeration value="0">
                            <xs:annotation>
                                <xs:appinfo>Success</xs:appinfo>
                            </xs:annotation>
                        </xs:enumeration>
                        <xs:enumeration value="4">
                            <xs:annotation>
                                <xs:appinfo>Minor failure</xs:appinfo>
                            </xs:annotation>
                        </xs:enumeration>
                        <xs:enumeration value="8">
                            <xs:annotation>
                                <xs:appinfo>Serious failure</xs:appinfo>
                            </xs:annotation>
                        </xs:enumeration>
                        <xs:enumeration value="12">
                            <xs:annotation>
                                <xs:appinfo>
                                    Major failure; action made unavailable
                                </xs:appinfo>
                            </xs:annotation>
```

```
                </xs:enumeration>
            </xs:restriction>
        </xs:simpleType>
    </xs:attribute>
</xs:complexType>
<xs:complexType name="AuditSourceIdentificationType">
    <xs:sequence>
        <xs:element name="AuditSourceTypeCode" type="CodedValueType"
            minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
    <xs:attribute name="AuditEnterpriseSiteID" type="xs:string"
        use="optional" />
    <xs:attribute name="AuditSourceID" type="xs:string"
        use="required" />
</xs:complexType>
<xs:complexType name="ActiveParticipantType">
    <xs:sequence minOccurs="0">
        <xs:element name="RoleIDCode" type="CodedValueType"
            minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
    <xs:attribute name="UserID" type="xs:string" use="required" />
    <xs:attribute name="AlternativeUserID" type="xs:string"
        use="optional" />
    <xs:attribute name="UserName" type="xs:string" use="optional" />
    <xs:attribute name="UserIsRequestor" type="xs:boolean"
        use="optional" default="true" />
    <xs:attribute name="NetworkAccessPointID" type="xs:string"
        use="optional" />
    <xs:attribute name="NetworkAccessPointTypeCode"
        use="optional">
        <xs:simpleType>
            <xs:restriction base="xs:unsignedByte">
                <xs:enumeration value="1">
                    <xs:annotation>
                        <xs:appinfo>
                            Machine Name, including DNS name
                        </xs:appinfo>
                    </xs:annotation>
                </xs:enumeration>
                <xs:enumeration value="2">
                    <xs:annotation>
                        <xs:appinfo>IP Address</xs:appinfo>
                    </xs:annotation>
                </xs:enumeration>
                <xs:enumeration value="3">
                    <xs:annotation>
                        <xs:appinfo>Telephone Number</xs:appinfo>
                    </xs:annotation>
                </xs:enumeration>
            </xs:restriction>
        </xs:simpleType>
    </xs:attribute>
</xs:complexType>
<xs:complexType name="ParticipantObjectIdentificationType">
    <xs:sequence>
```

```
                <xs:element name="ParticipantObjectIDTypeCode"
                    type="CodedValueType" />
                <xs:choice minOccurs="0">
                    <xs:element name="ParticipantObjectName"
                        type="xs:string" minOccurs="0" />
                    <xs:element name="ParticipantObjectQuery"
                        type="xs:base64Binary" minOccurs="0" />
                </xs:choice>
                <xs:element name="ParticipantObjectDetail"
                    type="TypeValuePairType" minOccurs="0"
maxOccurs="unbounded" />
            </xs:sequence>
            <xs:attribute name="ParticipantObjectID" type="xs:string"
                use="required" />
            <xs:attribute name="ParticipantObjectTypeCode" use="optional">
                <xs:simpleType>
                    <xs:restriction base="xs:unsignedByte">
                        <xs:enumeration value="1">
                            <xs:annotation>
                                <xs:appinfo>Person</xs:appinfo>
                            </xs:annotation>
                        </xs:enumeration>
                        <xs:enumeration value="2">
                            <xs:annotation>
                                <xs:appinfo>System object</xs:appinfo>
                            </xs:annotation>
                        </xs:enumeration>
                        <xs:enumeration value="3">
                            <xs:annotation>
                                <xs:appinfo>Organization</xs:appinfo>
                            </xs:annotation>
                        </xs:enumeration>
                        <xs:enumeration value="4">
                            <xs:annotation>
                                <xs:appinfo>Other</xs:appinfo>
                            </xs:annotation>
                        </xs:enumeration>
                    </xs:restriction>
                </xs:simpleType>
            </xs:attribute>
            <xs:attribute name="ParticipantObjectTypeCodeRole"
                use="optional">
                <xs:simpleType>
                    <xs:restriction base="xs:unsignedByte">
                        <xs:enumeration value="1">
                            <xs:annotation>
                                <xs:appinfo>Patient</xs:appinfo>
                            </xs:annotation>
                        </xs:enumeration>
                        <xs:enumeration value="2">
                            <xs:annotation>
                                <xs:appinfo>Location</xs:appinfo>
                            </xs:annotation>
                        </xs:enumeration>
                        <xs:enumeration value="3">
```

```
        <xs:annotation>
            <xs:appinfo>Report</xs:appinfo>
        </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="4">
        <xs:annotation>
            <xs:appinfo>Resource</xs:appinfo>
        </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="5">
        <xs:annotation>
            <xs:appinfo>Master file</xs:appinfo>
        </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="6">
        <xs:annotation>
            <xs:appinfo>User</xs:appinfo>
        </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="7">
        <xs:annotation>
            <xs:appinfo>List</xs:appinfo>
        </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="8">
        <xs:annotation>
            <xs:appinfo>Doctor</xs:appinfo>
        </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="9">
        <xs:annotation>
            <xs:appinfo>Subscriber</xs:appinfo>
        </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="10">
        <xs:annotation>
            <xs:appinfo>Guarantor</xs:appinfo>
        </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="11">
        <xs:annotation>
            <xs:appinfo>
                Security User Entity
            </xs:appinfo>
        </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="12">
        <xs:annotation>
            <xs:appinfo>Security User Group</xs:appinfo>
        </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="13">
        <xs:annotation>
            <xs:appinfo>Security Resource</xs:appinfo>
        </xs:annotation>
```

```
</xs:enumeration>
<xs:enumeration value="14">
    <xs:annotation>
        <xs:appinfo>
            Security Granualarity Definition
        </xs:appinfo>
    </xs:annotation>
</xs:enumeration>
<xs:enumeration value="15">
    <xs:annotation>
        <xs:appinfo>Provider</xs:appinfo>
    </xs:annotation>
</xs:enumeration>
<xs:enumeration value="16">
    <xs:annotation>
        <xs:appinfo>Report Destination</xs:appinfo>
    </xs:annotation>
</xs:enumeration>
<xs:enumeration value="17">
    <xs:annotation>
        <xs:appinfo>Report Library</xs:appinfo>
    </xs:annotation>
</xs:enumeration>
<xs:enumeration value="18">
    <xs:annotation>
        <xs:appinfo>Schedule</xs:appinfo>
    </xs:annotation>
</xs:enumeration>
<xs:enumeration value="19">
    <xs:annotation>
        <xs:appinfo>Customer</xs:appinfo>
    </xs:annotation>
</xs:enumeration>
<xs:enumeration value="20">
    <xs:annotation>
        <xs:appinfo>Job</xs:appinfo>
    </xs:annotation>
</xs:enumeration>
<xs:enumeration value="21">
    <xs:annotation>
        <xs:appinfo>Job Stream</xs:appinfo>
    </xs:annotation>
</xs:enumeration>
<xs:enumeration value="22">
    <xs:annotation>
        <xs:appinfo>Table</xs:appinfo>
    </xs:annotation>
</xs:enumeration>
<xs:enumeration value="23">
    <xs:annotation>
        <xs:appinfo>Routing Criteria</xs:appinfo>
    </xs:annotation>
</xs:enumeration>
<xs:enumeration value="24">
    <xs:annotation>
```

```
                    <xs:appinfo>Query</xs:appinfo>
                </xs:annotation>
            </xs:enumeration>
        </xs:restriction>
    </xs:simpleType>
</xs:attribute>
<xs:attribute name="ParticipantObjectDataLifeCycle"
    use="optional">
    <xs:simpleType>
        <xs:restriction base="xs:unsignedByte">
            <xs:enumeration value="1">
                <xs:annotation>
                    <xs:appinfo>
                        Origination / Creation
                    </xs:appinfo>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="2">
                <xs:annotation>
                    <xs:appinfo>
                        Import / Copy from original
                    </xs:appinfo>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="3">
                <xs:annotation>
                    <xs:appinfo>Amendment</xs:appinfo>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="4">
                <xs:annotation>
                    <xs:appinfo>Verification</xs:appinfo>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="5">
                <xs:annotation>
                    <xs:appinfo>Translation</xs:appinfo>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="6">
                <xs:annotation>
                    <xs:appinfo>Access / Use</xs:appinfo>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="7">
                <xs:annotation>
                    <xs:appinfo>De-identification</xs:appinfo>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="8">
                <xs:annotation>
                    <xs:appinfo>
                        Aggregation, summarization, derivation
                    </xs:appinfo>
                </xs:annotation>
```

```
                        </xs:enumeration>
                        <xs:enumeration value="9">
                            <xs:annotation>
                                <xs:appinfo>Report</xs:appinfo>
                            </xs:annotation>
                        </xs:enumeration>
                        <xs:enumeration value="10">
                            <xs:annotation>
                                <xs:appinfo>
                                    Export / Copy to target
                                </xs:appinfo>
                            </xs:annotation>
                        </xs:enumeration>
                        <xs:enumeration value="11">
                            <xs:annotation>
                                <xs:appinfo>Disclosure</xs:appinfo>
                            </xs:annotation>
                        </xs:enumeration>
                        <xs:enumeration value="12">
                            <xs:annotation>
                                <xs:appinfo>
                                    Receipt of disclosure
                                </xs:appinfo>
                            </xs:annotation>
                        </xs:enumeration>
                        <xs:enumeration value="13">
                            <xs:annotation>
                                <xs:appinfo>Archiving</xs:appinfo>
                            </xs:annotation>
                        </xs:enumeration>
                        <xs:enumeration value="14">
                            <xs:annotation>
                                <xs:appinfo>Logical deletion</xs:appinfo>
                            </xs:annotation>
                        </xs:enumeration>
                        <xs:enumeration value="15">
                            <xs:annotation>
                                <xs:appinfo>
                                    Permanent erasure / Physical
destruction
                                </xs:appinfo>
                            </xs:annotation>
                        </xs:enumeration>
                    </xs:restriction>
                </xs:simpleType>
            </xs:attribute>
            <xs:attribute name="ParticipantObjectSensitivity"
                type="xs:string" use="optional" />
        </xs:complexType>
        <xs:complexType name="CodedValueType">
            <xs:attribute name="code" type="xs:string" use="required" />
            <xs:attributeGroup ref="CodeSystem" />
            <xs:attribute name="displayName" type="xs:string"
                use="optional" />
            <xs:attribute name="originalText" type="xs:string"
```

```
            use="optional" />
    </xs:complexType>
    <xs:complexType name="TypeValuePairType">
        <xs:attribute name="type" type="xs:string" use="required" />
        <xs:attribute name="value" type="xs:base64Binary"
            use="required" />
    </xs:complexType>
    <xs:attributeGroup name="CodeSystem">
        <xs:attribute name="codeSystem" type="OID" use="optional" />
        <xs:attribute name="codeSystemName" type="xs:string"
            use="optional" />
    </xs:attributeGroup>
    <xs:simpleType name="OID">
        <xs:restriction base="xs:string">
            <xs:whiteSpace value="collapse" />
        </xs:restriction>
    </xs:simpleType>
</xs:schema>
```

Example of RFC 3881 Schema Compliant Audit Message:

```
<AuditMessage>
    <EventIdentification EventActionCode="E"
EventDateTime="2012-08-16T05:30:00.450-07:00" EventOutcomeIndicator="0">
        <EventID code="110100" codeSystemName="DCM" displayName="Application
Activity"></EventID>
        <EventTypeCode code="110120" codeSystemName="DCM"
displayName="Application Start"></EventTypeCode>
    </EventIdentification>
    <ActiveParticipant AlternativeUserID="19041@hiadev001"
NetworkAccessPointID="10.145.240.60" NetworkAccessPointTypeCode="2"
UserID="root" UserIsRequestor="false">
        <RoleIDCode code="110150" codeSystemName="DCM"
displayName="Application"></RoleIDCode>
    </ActiveParticipant>
    <AuditSourceIdentification
AuditSourceID="10.145.240.60@REGISTRY_ORACLE_HIM"></
AuditSourceIdentification>
</AuditMessage>
```

# DICOM Audit Message XML schema reference

The following section contains the DICOM Audit Message XML schema reference.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
elementFormDefault="qualified">
<!--
  This defines the coded value type. The comment shows a pattern that can be
used to further
  constrain the token to limit it to the format of an OID. Not all schema
software
```

```
  implementations support the pattern option for tokens.
   -->
<xs:attributeGroup name="other-csd-attributes">
      <xs:attribute name="codeSystemName" use="required"
type="xs:token"/>
      <xs:attribute name="displayName" type="xs:token"/>
      <xs:attribute name="originalText" use="required"
type="xs:token"/>
</xs:attributeGroup>
  <!-- Note: this also corresponds to DICOM "Code Meaning" -->
  <xs:attributeGroup name="CodedValueType">
      <xs:attribute name="csd-code" use="required" type="xs:token"/>
      <xs:attributeGroup ref="other-csd-attributes"/>
  </xs:attributeGroup>
    <!-- Define the event identification, used later -->
   <xs:complexType name="EventIdentificationContents">
       <xs:sequence>
          <xs:element ref="EventID"/>
          <xs:element minOccurs="0" maxOccurs="unbounded"
ref="EventTypeCode"/>
          <xs:element minOccurs="0" ref="EventOutcomeDescription"/>
          <!-- Added per ITI Supplement XUA++ Revision 1.3 section
3.20.7.8 -->
          <xs:element name="PurposeOfUse" minOccurs="0"
maxOccurs="unbounded">
               <xs:complexType>
                   <xs:attributeGroup ref="CodedValueType"/>
               </xs:complexType>
           </xs:element>
       </xs:sequence>
       <xs:attribute name="EventActionCode">
           <xs:simpleType>
               <xs:restriction base="xs:token">
                   <xs:enumeration value="C">
                      <xs:annotation>
                          <xs:documentation>Create</xs:documentation>
                      </xs:annotation>
                   </xs:enumeration>
                   <xs:enumeration value="R">
                       <xs:annotation>
                           <xs:documentation>Read</xs:documentation>
                       </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="U">
                        <xs:annotation>
                            <xs:documentation>Update</xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="D">
                        <xs:annotation>
                            <xs:documentation>Delete</xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="E">
                        <xs:annotation>
```

```
                            <xs:documentation>Execute</xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                </xs:restriction>
            </xs:simpleType>
        </xs:attribute>
        <xs:attribute name="EventDateTime" use="required"
type="xs:dateTime"/>
        <xs:attribute name="EventOutcomeIndicator" use="required">
            <xs:simpleType>
                <xs:restriction base="xs:token">
                    <xs:enumeration value="0">
                        <xs:annotation>
                            <xs:documentation>Nominal Success (use if status
otherwise unknown or ambiguous)</xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="4">
                        <xs:annotation>
                            <xs:documentation>Minor failure (per reporting
application definition)</xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="8">
                       <xs:annotation>
                          <xs:documentation>Serious failure (per reporting
application definition)</xs:documentation>
                       </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="12">
                      <xs:annotation>
                         <xs:documentation>Major failure, (reporting
application now unavailable)</xs:documentation>
                       </xs:annotation>
                    </xs:enumeration>
                </xs:restriction>
            </xs:simpleType>
        </xs:attribute>
    </xs:complexType>
    <xs:element name="EventID">
        <xs:complexType>
            <xs:attributeGroup ref="CodedValueType"/>
        </xs:complexType>
    </xs:element>
    <xs:element name="EventTypeCode">
        <xs:complexType>
            <xs:attributeGroup ref="CodedValueType"/>
        </xs:complexType>
    </xs:element>
    <xs:element name="EventOutcomeDescription" type="xs:string"/>
    <!-- Define AuditSourceIdentification, used later -->
    <xs:complexType name="AuditSourceIdentificationContents">
        <xs:sequence>
            <xs:element minOccurs="0" maxOccurs="unbounded"
ref="AuditSourceTypeCode"/>
```

```
        </xs:sequence>
        <xs:attribute name="AuditEnterpriseSiteID" type="xs:token"/>
        <xs:attribute name="AuditSourceID" use="required"
type="xs:token"/>
    </xs:complexType>
    <xs:element name="AuditSourceTypeCode">
        <xs:complexType>
            <xs:attributeGroup ref="AuditSourceTypeCodeContent"/>
        </xs:complexType>
    </xs:element>
    <!--
      Define AuditSourceTypeCodeContent so that an isolated single
digit
      value is acceptable, or a token with other csd attributes so that
      any controlled terminology can also be used.
    -->
    <xs:attributeGroup name="AuditSourceTypeCodeContent">
        <xs:attribute name="csd-code" use="required">
            <xs:simpleType>
                <xs:union>
                    <xs:simpleType>
                        <xs:restriction base="xs:token">
                            <xs:enumeration value="1">
                               <xs:annotation>
                                  <xs:documentation>End-user display
device, diagnostic device</xs:documentation>
                               </xs:annotation>
                            </xs:enumeration>
                        </xs:restriction>
                    </xs:simpleType>
                    <xs:simpleType>
                        <xs:restriction base="xs:token">
                            <xs:enumeration value="2">
                               <xs:annotation>
                                  <xs:documentation>Data acquisition
device or instrument</xs:documentation>
                               </xs:annotation>
                            </xs:enumeration>
                        </xs:restriction>
                    </xs:simpleType>
                    <xs:simpleType>
                        <xs:restriction base="xs:token">
                            <xs:enumeration value="3">
                               <xs:annotation>
                                   <xs:documentation>Web Server
process or thread</xs:documentation>
                               </xs:annotation>
                            </xs:enumeration>
                        </xs:restriction>
                    </xs:simpleType>
                    <xs:simpleType>
                        <xs:restriction base="xs:token">
                            <xs:enumeration value="4">
                               <xs:annotation>
                                  <xs:documentation>Application Server
```

```
process or thread</xs:documentation>
                                </xs:annotation>
                            </xs:enumeration>
                        </xs:restriction>
                    </xs:simpleType>
                    <xs:simpleType>
                        <xs:restriction base="xs:token">
                            <xs:enumeration value="5">
                               <xs:annotation>
                                  <xs:documentation>Database Server process
or thread</xs:documentation>
                               </xs:annotation>
                            </xs:enumeration>
                        </xs:restriction>
                    </xs:simpleType>
                    <xs:simpleType>
                        <xs:restriction base="xs:token">
                            <xs:enumeration value="6">
                               <xs:annotation>
                                  <xs:documentation>Security server, e.g., a
domain controller</xs:documentation>
                               </xs:annotation>
                            </xs:enumeration>
                        </xs:restriction>
                    </xs:simpleType>
                    <xs:simpleType>
                        <xs:restriction base="xs:token">
                            <xs:enumeration value="7">
                                <xs:annotation>
                                    <xs:documentation>ISO level 1-3 network
component</xs:documentation>
                                </xs:annotation>
                            </xs:enumeration>
                        </xs:restriction>
                    </xs:simpleType>
                    <xs:simpleType>
                        <xs:restriction base="xs:token">
                            <xs:enumeration value="8">
                                <xs:annotation>
                                    <xs:documentation>ISO level 4-6
operating software</xs:documentation>
                                </xs:annotation>
                            </xs:enumeration>
                        </xs:restriction>
                    </xs:simpleType>
                    <xs:simpleType>
                        <xs:restriction base="xs:token">
                            <xs:enumeration value="9">
                                <xs:annotation>
                                    <xs:documentation>other</
xs:documentation>
                                </xs:annotation>
                            </xs:enumeration>
                        </xs:restriction>
                    </xs:simpleType>
```

```
                    <xs:simpleType>
                        <xs:restriction base="xs:token"/>
                    </xs:simpleType>
                </xs:union>
            </xs:simpleType>
        </xs:attribute>
        <xs:attribute name="codeSystemName" type="xs:token"/>
        <xs:attribute name="displayName" type="xs:token"/>
        <xs:attribute name="originalText" type="xs:token"/>
    </xs:attributeGroup>
    <!-- Define ActiveParticipantType, used later -->
    <xs:complexType name="ActiveParticipantContents">
        <xs:annotation>
            <xs:documentation>If these are present, they define the
meaning of code</xs:documentation>
        </xs:annotation>
        <xs:sequence>
            <xs:element minOccurs="0" maxOccurs="unbounded"
ref="RoleIDCode"/>
            <xs:element minOccurs="0" ref="MediaIdentifier"/>
        </xs:sequence>
        <xs:attribute name="UserID" use="required"/>
        <xs:attribute name="AlternativeUserID"/>
        <xs:attribute name="UserName"/>
        <xs:attribute name="UserIsRequestor" use="required"
type="xs:boolean"/>
        <xs:attribute name="NetworkAccessPointID" type="xs:token"/>
        <xs:attribute name="NetworkAccessPointTypeCode">
            <xs:simpleType>
                <xs:restriction base="xs:token">
                    <xs:enumeration value="1">
                        <xs:annotation>
                            <xs:documentation>Machine Name, including
DNS name</xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="2">
                        <xs:annotation>
                            <xs:documentation>IP Address</
xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="3">
                        <xs:annotation>
                            <xs:documentation>Telephone Number</
xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="4">
                        <xs:annotation>
                            <xs:documentation>Email address</
xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="5">
```

```
                        <xs:annotation>
                            <xs:documentation>URI (user directory, HTTP-PUT,
ftp, etc.)</xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                </xs:restriction>
            </xs:simpleType>
        </xs:attribute>
    </xs:complexType>
    <xs:element name="RoleIDCode">
        <xs:complexType>
            <xs:attributeGroup ref="CodedValueType"/>
        </xs:complexType>
    </xs:element>
    <xs:element name="MediaIdentifier">
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="MediaType"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <xs:element name="MediaType">
        <xs:complexType>
            <xs:attributeGroup ref="CodedValueType"/>
        </xs:complexType>
    </xs:element>
    <!--
      The BinaryValuePair is used in ParticipantObject descriptions to
capture parameters.
      All values (even those that are normally plain text) are encoded as
xsd:base64Binary.
      This is to preserve details of encoding (e.g., nulls) and to protect
against text
      contents that contain XML fragments. These are known attack points
against applications,
      so security logs can be expected to need to capture them without
modification by the
      audit encoding process.
    -->
    <xs:attributeGroup name="ValuePair">
        <xs:attribute name="type" use="required" type="xs:token"/>
        <xs:attribute name="value" use="required" type="xs:base64Binary"/>
    </xs:attributeGroup>
    <!-- used to encode potentially binary, malformed XML text, etc. -->
    <!-- Define ParticipantObjectIdentification, used later -->
    <!-- Participant Object Description, used later -->
    <xs:complexType name="DICOMObjectDescriptionContents">
        <xs:sequence>
            <xs:element minOccurs="0" maxOccurs="unbounded" ref="MPPS"/>
            <xs:element minOccurs="0" maxOccurs="unbounded" ref="Accession"/>
            <xs:element minOccurs="0" maxOccurs="unbounded" ref="SOPClass"/>
            <xs:element minOccurs="0" ref="ParticipantObjectContainsStudy"/>
            <xs:element minOccurs="0" ref="Encrypted"/>
            <xs:element minOccurs="0" ref="Anonymized"/>
        </xs:sequence>
```

```
    </xs:complexType>
    <xs:element name="MPPS">
        <xs:complexType>
            <xs:attribute name="UID" use="required" type="xs:token"/>
        </xs:complexType>
    </xs:element>
    <xs:element name="Accession">
        <xs:complexType>
            <xs:attribute name="Number" use="required"
type="xs:token"/>
        </xs:complexType>
    </xs:element>
    <xs:element name="SOPClass">
        <xs:complexType>
            <xs:sequence>
                <xs:element minOccurs="0" maxOccurs="unbounded"
ref="Instance"/>
            </xs:sequence>
            <xs:attribute name="UID" type="xs:token"/>
            <xs:attribute name="NumberOfInstances" use="required"
type="xs:integer"/>
        </xs:complexType>
    </xs:element>
    <xs:element name="Instance">
        <xs:complexType>
            <xs:attribute name="UID" use="required" type="xs:token"/>
        </xs:complexType>
    </xs:element>
    <xs:element name="ParticipantObjectContainsStudy">
        <xs:complexType>
            <xs:sequence>
                <xs:element minOccurs="0" maxOccurs="unbounded"
ref="StudyIDs"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <xs:element name="StudyIDs">
        <xs:complexType>
            <xs:attribute name="UID" use="required" type="xs:token"/>
        </xs:complexType>
    </xs:element>
    <xs:element name="Encrypted" type="xs:boolean"/>
    <xs:element name="Anonymized" type="xs:boolean"/>
    <xs:complexType name="ParticipantObjectIdentificationContents">
        <xs:sequence>
            <xs:element ref="ParticipantObjectIDTypeCode"/>
            <!-- IHE: The minOccurs entry on the following choice
element was
                 added because DICOM does not actually follow the
requirement to
                 have one of these two elements -->
            <xs:choice minOccurs="0">
                <xs:element ref="ParticipantObjectName"/>
                <xs:element ref="ParticipantObjectQuery"/>
            </xs:choice>
```

```
            <xs:element minOccurs="0" maxOccurs="unbounded"
ref="ParticipantObjectDetail"/>
            <xs:element minOccurs="0" maxOccurs="unbounded"
ref="ParticipantObjectDescription"/>
        </xs:sequence>
        <!-- ParticipantObjectID is not always mandatory for IHE -->
        <xs:attribute name="ParticipantObjectID" use="optional"
type="xs:token"/>
        <xs:attribute name="ParticipantObjectTypeCode">
            <xs:simpleType>
                <xs:restriction base="xs:token">
                    <xs:enumeration value="1">
                        <xs:annotation>
                            <xs:documentation>Person</xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="2">
                        <xs:annotation>
                            <xs:documentation>System object</
xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="3">
                        <xs:annotation>
                            <xs:documentation>Organization</xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="4">
                        <xs:annotation>
                            <xs:documentation>Other</xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                </xs:restriction>
            </xs:simpleType>
        </xs:attribute>
        <xs:attribute name="ParticipantObjectTypeCodeRole">
            <xs:simpleType>
                <xs:restriction base="xs:token">
                    <xs:enumeration value="1">
                        <xs:annotation>
                            <xs:documentation>Patient</xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="2">
                        <xs:annotation>
                            <xs:documentation>Location</xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="3">
                        <xs:annotation>
                            <xs:documentation>Report</xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="4">
                        <xs:annotation>
```

```
                        <xs:documentation>Resource</
xs:documentation>
                    </xs:annotation>
                </xs:enumeration>
                <xs:enumeration value="5">
                    <xs:annotation>
                        <xs:documentation>Master File</
xs:documentation>
                    </xs:annotation>
                </xs:enumeration>
                <xs:enumeration value="6">
                    <xs:annotation>
                        <xs:documentation>User</xs:documentation>
                    </xs:annotation>
                </xs:enumeration>
                <xs:enumeration value="7">
                    <xs:annotation>
                        <xs:documentation>List</xs:documentation>
                    </xs:annotation>
                </xs:enumeration>
                <xs:enumeration value="8">
                    <xs:annotation>
                        <xs:documentation>Doctor</xs:documentation>
                    </xs:annotation>
                </xs:enumeration>
                <xs:enumeration value="9">
                    <xs:annotation>
                        <xs:documentation>Subscriber</
xs:documentation>
                    </xs:annotation>
                </xs:enumeration>
                <xs:enumeration value="10">
                    <xs:annotation>
                        <xs:documentation>Guarantor</
xs:documentation>
                    </xs:annotation>
                </xs:enumeration>
                <xs:enumeration value="11">
                    <xs:annotation>
                        <xs:documentation>Security User Entity</
xs:documentation>
                    </xs:annotation>
                </xs:enumeration>
                <xs:enumeration value="12">
                    <xs:annotation>
                        <xs:documentation>Security User Group</
xs:documentation>
                    </xs:annotation>
                </xs:enumeration>
                <xs:enumeration value="13">
                    <xs:annotation>
                        <xs:documentation>Security Resource</
xs:documentation>
                    </xs:annotation>
                </xs:enumeration>
```

```
                    <xs:enumeration value="14">
                        <xs:annotation>
                            <xs:documentation>Security Granularity
Definition</xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="15">
                        <xs:annotation>
                            <xs:documentation>Provider</xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="16">
                        <xs:annotation>
                            <xs:documentation>Data Destination</
xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="17">
                        <xs:annotation>
                            <xs:documentation>Data Archive</xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="18">
                        <xs:annotation>
                            <xs:documentation>Schedule</xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="19">
                        <xs:annotation>
                            <xs:documentation>Customer</xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="20">
                        <xs:annotation>
                            <xs:documentation>Job</xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="21">
                        <xs:annotation>
                            <xs:documentation>Job Stream</xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="22">
                        <xs:annotation>
                            <xs:documentation>Table</xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="23">
                        <xs:annotation>
                            <xs:documentation>Routing Criteria</
xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="24">
                        <xs:annotation>
```

```
                            <xs:documentation>Query</xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="25">
                        <xs:annotation>
                            <xs:documentation>Data Source</
xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="26">
                        <xs:annotation>
                            <xs:documentation>Processing Element</
xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                </xs:restriction>
            </xs:simpleType>
        </xs:attribute>
        <xs:attribute name="ParticipantObjectDataLifeCycle">
            <xs:simpleType>
                <xs:restriction base="xs:token">
                    <xs:enumeration value="1">
                        <xs:annotation>
                            <xs:documentation>Origination, Creation</
xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="2">
                        <xs:annotation>
                            <xs:documentation>Import/ Copy</
xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="3">
                        <xs:annotation>
                            <xs:documentation>Amendment</
xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="4">
                        <xs:annotation>
                            <xs:documentation>Verification</
xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="5">
                        <xs:annotation>
                            <xs:documentation>Translation</
xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="6">
                        <xs:annotation>
                            <xs:documentation>Access/Use</
xs:documentation>
```

```
                        </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="7">
                        <xs:annotation>
                            <xs:documentation>De-identification</
xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="8">
                        <xs:annotation>
                            <xs:documentation>Aggregation, summarization,
derivation</xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="9">
                        <xs:annotation>
                            <xs:documentation>Report</xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="10">
                        <xs:annotation>
                            <xs:documentation>Export</xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="11">
                        <xs:annotation>
                            <xs:documentation>Disclosure</xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="12">
                        <xs:annotation>
                            <xs:documentation>Receipt of Disclosure</
xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="13">
                        <xs:annotation>
                            <xs:documentation>Archiving</xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="14">
                        <xs:annotation>
                            <xs:documentation>Logical deletion</
xs:documentation>
                        </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="15">
                       <xs:annotation>
                          <xs:documentation>Permanent erasure, physical
destruction</xs:documentation>
                       </xs:annotation>
                    </xs:enumeration>
                </xs:restriction>
            </xs:simpleType>
        </xs:attribute>
```

```
        <xs:attribute name="ParticipantObjectSensitivity"
type="xs:token"/>
    </xs:complexType>
    <xs:element name="ParticipantObjectIDTypeCode">
        <xs:complexType>
            <xs:attributeGroup ref="CodedValueType"/>
        </xs:complexType>
    </xs:element>
    <xs:element name="ParticipantObjectName" type="xs:token"/>
    <xs:element name="ParticipantObjectQuery" type="xs:base64Binary"/>
    <xs:element name="ParticipantObjectDetail">
        <xs:complexType>
            <xs:attributeGroup ref="ValuePair"/>
        </xs:complexType>
    </xs:element>
    <xs:element name="ParticipantObjectDescription"
type="DICOMObjectDescriptionContents"/>
    <!-- The basic message -->
    <xs:element name="AuditMessage">
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="EventIdentification"/>
                <xs:element maxOccurs="unbounded"
ref="ActiveParticipant"/>
                <xs:element ref="AuditSourceIdentification"/>
                <xs:element minOccurs="0" maxOccurs="unbounded"
ref="ParticipantObjectIdentification"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <xs:element name="EventIdentification"
type="EventIdentificationContents"/>
    <xs:element name="ActiveParticipant"
type="ActiveParticipantContents"/>
    <xs:element name="AuditSourceIdentification"
type="AuditSourceIdentificationContents"/>
    <xs:element name="ParticipantObjectIdentification"
type="ParticipantObjectIdentificationContents"/>
    <!-- And finally the magic statement that message is the root of
everything. -->
</xs:schema>
```

Example of DICOM Schema Compliant Audit Message:

```
<AuditMessage>
    <EventIdentification EventActionCode="E"
        EventDateTime="2021-03-02T08:16:57.992"
EventOutcomeIndicator="0">
        <EventID codeSystemName="DCM" csd-code="110100"
originalText="Application Activity"/>
        <EventTypeCode codeSystemName="DCM" csd-code="110120"
originalText="Application Start"/>
    </EventIdentification>
    <ActiveParticipant
```

```
        AlternativeUserID="14584@hiadev010"
        NetworkAccessPointID="10.0.0.29" NetworkAccessPointTypeCode="2"
        UserID="root" UserIsRequestor="false">
        <RoleIDCode codeSystemName="DCM" csd-code="110150"
originalText="Application"/>
    </ActiveParticipant>
    <AuditSourceIdentification
AuditSourceID="10.0.0.29@REGISTRY_ORACLE_HIM"/>
</AuditMessage>
```

D

# Password encoding

This section shows the password encoding cipher and config properties.

- Edit cipher.properties
  This section describes how to edit cipher.properties.
- Edit config.properties
  This section describes how to edit a password and a property in a properties file.

## Edit cipher.properties

This section describes how to edit cipher.properties.

For example, AES:

```
cipher_algorithm=aes
cipher_passphrase=hiapassphrase123
cipher_salthex=001020304050F0F
cipher_ivhex=0001020304050F0F08090A0B0C0D0E0F
cipher_iterations=19
```

For example, RSA:

```
cipher_algorithm=rsa
cipher_privatekeyfile=private.key
cipher_publickeyfile=public.key
```

## Edit config.properties

This section describes how to edit a password and a property in a properties file.

To edit a password in a properties file, execute the following command:

```
> ant update-config-properties-file-password
```

To edit a property in a properties file, execute the following command:

```
> ant update-config-properties-file-property
```