ICW Professional Exchange Server 3.2

Administration Manual

Document version: 1.0 | Status: Approved

Security level: sensitive

Imprint

InterComponentWare AG
Altrottstr. 31
69190 Walldorf, Germany
Tel.: +49 (6227) 385 – 0
Fax: +49 (6227) 385 – 199
E-Mail: info@icw.de

Document ID: 102394e2-6404-2e10-5bac-f2bafca1cc35
Document version: 1.0
Document language: en-US
Security level: sensitive
Product name: PXS - Professional Exchange Server
Product release: ICW Professional Exchange Server 3.2

Last change: January 2011

Table of Contents

1 Preface

This document describes Professional Exchange Server (PXS), a product of InterComponentWare AG.

This software offers a consolidated view of electronic medical records across the boundaries between medical institutions and between departments of the same institution whose data originates from disparate source systems (in hospitals, medical practices) or from the LifeSensor personal health record.

PXS links between patient identifiers in dissimilar systems to consolidate patient data from hospitals, rehabilitation and convalescent centers and other medical care facilities. It provides all involved parties with patient information that is current and up to date.

The product offers manual and automatic functions to provide safe access controls to patient data. Other functions working across the different components include management for system administration and security settings.

1.1 Document overview

1.2 Document Conventions

Mark up	Explanation
italic	Emphasis
bold	Important information
bold and italic	Very important information
Underlined and colored	Hyperlinks, i.e. http://www.icw.com.
`Non-proportional font`	Section of code or other low-level labels, commands and outputs.
File paths and/or file names	File paths and/or a file names, i.e. *C:/temp*, *C:/temp/readme.txt* or *../readme.txt*
Menu path	Format for a menu path, i.e. File | New | **New document**
<<wildcard>>	Wildcards, i.e. *C:/Documents and settings/ <<Username>>*
[Shortcut]	Keyboard shortcuts, e.g. [STRG+O]
⚠	Warnings are highlighted, accompanied by the label **Warning**

Mark up	Explanation
ℹ	Notices are highlighted, accompanied by the label **Note**
⚙	Examples are highlighted, accompanied by the label **Example**

2 System Administration Tools

The following sections describe the most important tools that can be used to perform system administration tasks for the Professional Exchange Server.

2.1 Java Management Extensions (JMX)

The Professional Exchange Server uses Java Management Extensions (JMX) to offer a standardized interface for monitoring the application, performing maintenance tasks and for applying configuration changes during runtime. The JMX capabilities can be used remotely through any JMX client that supports RMI connections via SSL with username and password. An example is Oracle's JConsole, which is part of the Java 2 Platform, Standard Edition (J2SE) 6.0. This document focuses on the JConsole but the application can be managed with any compatible JMX client. For further information on how to configure another JMX client, please refer to its documentation.

2.1.1 Opening the JConsole

The Professional Exchange Server secures all remote JMX connections via SSL. Therefore the JMX client has to trust the server certificate. The server certificates issued by most of the important commercial certificate authorities (CA) are automatically trusted. If the issuer of the application's server certificate is trusted by the JVM by default, then the JConsole can be opened without any additional command line parameters:

```
jconsole
```

If the server certificate's CA is not represented in the default JVM truststore, then a truststore that contains the CA's certificate must be passed in via a command line parameter:

```
jconsole -J-Djavax.net.ssl.trustStore=/path/to/ca.keystore
-J-Djavax.net.ssl.trustStorePassword=<password>
```

2.1.2 Connecting to the JMX interface through JConsole

The format of the connection URL for the Professional Exchange Server is as follows:

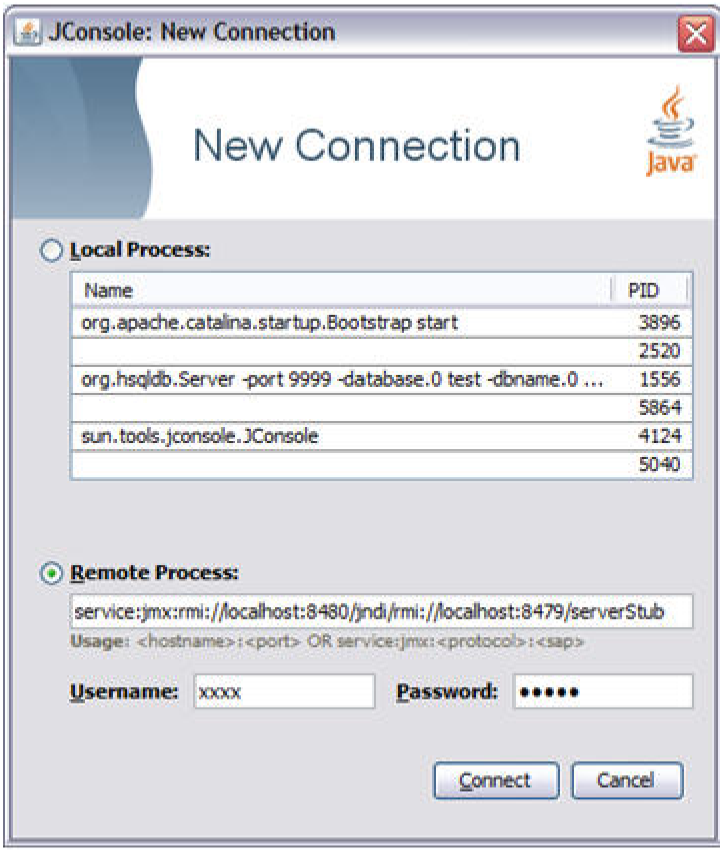
```
service:jmx:rmi://<host>:<port1>/jndi/rmi://<host>:<port2>/server-
Stub
```

<host> is the host name of the machine where the application's Tomcat server is running. <port1> and <port2> are the "JMX port for remote communication" and the "JNDI

Port to obtain JMX Stub”, respectively, that were configured during the installation of Professional Exchange Server. <port1> defaults to 8480 and <port2> defaults to 8479.

Example: The connection URL using localhost and default ports

```
service:jmx:rmi://localhost:8480/jndi/rmi://localhost:8479/server-
Stub
```



○ Local Process:

Name	PID
org.apache.catalina.startup.Bootstrap start	3896
	2520
org.hsqldb.Server -port 9999 -database.0 test -dbname.0 ...	1556
	5864
sun.tools.jconsole.JConsole	4124
	5040

● Remote Process: service:jmx:rmi://localhost:8480/jndi/rmi://localhost:8479/serverStub

Usage: <hostname>:<port> OR service:jmx:<protocol>:<sap>

Username: xxxx Password: •••••

Figure 1: JConsole “New Connection” dialog box

The application requires user authentication using a username and password. The username and password must belong to an active user account. The user account must have the role “JMX Administrator”. For further information on creating user accounts and assigning roles please refer to the User Administration [page 28] section.

2.1.3 Changing runtime configuration settings in a clustered environment

When Professional Exchange Server is running in clustered mode, there is no automatic propagation of runtime configuration changes made via JMX. There are two ways to ensure that all cluster nodes use the same configuration.

1. Make the changes on one node and then repeat the same changes on all other nodes. This is discouraged, because such repetitive manual tasks are error prone.

The upside is that this should not have a negative effect on the application's availability.

2. Make the changes on one node and then restart the other nodes. This is the recommended approach, since the changes have to be made only once and the other nodes read the changed configuration items from the database when they are restarted. It does have the downside that there is only one cluster node available while the other restarts the application. But such changes can often be scheduled during low-traffic hours and the restart time of the application typically only takes a few minutes, so that the effects are manageable.

2.1.4 Disabling SSL for JMX

Disabling the SSL transport encryption of the JMX connector is discouraged. However, there are situations where this might be necessary, for example, when the JMX client you need to use does not support SSL.

To disable SSL, it is necessary to modify the file *ehf-jmx-context.xml*, which is located under `<tomcat>/webapps/<webapp_name>/WEB-INF/classes/META-INF`. In the `<bean>` element with id=jmxRmiConnectorServer, the following two elements must be removed (including their attributes and child elements) or at least commented out.

```
<entry key="jmx.remote.rmi.server.socket.factory">

<ref bean="serverSocketFactory"/>

</entry>

<entry key="jmx.remote.rmi.client.socket.factory">

<ref bean="clientSocketFactory"/>

</entry>
```

After the change a restart is necessary, before JMX without SSL is available. Please refer to the section on making changes in the Tomcat folder [page 27] for details on how to safely change this file.

2.2 The application's organization registry

The application contains an organization registry that allows all Professional Exchange Server modules and potentially other applications to query what organizations and systems are participating in the exchange. It also allows administrators to remotely read and change the list of organizations and systems connected to the exchange and their properties.

Administrators or other systems that want to access the data in the organization registry can do so using simple HTTP commands to retrieve the data in an XML format or to upload modified XML.

The URL to export and import the organization registry's data in XML format is:

```
https://<host>[:<port>]/<webapp_name>/resource/organizationData
```

Issuing an HTTP GET request using this URL will return the data in XML format. Issuing an HTTP POST request using this URL with an XML file as the message body will change the organization registry's data to fit the XML. The organization registry requires authentication using the basic authentication mechanism defined by RFC 2617.

2.2.1 Tools to access the organization registry's external interface

Any tool that can form the HTTP requests described above and that supports basic authentication can be used to access this interface. Two tools that can do this and that are freely available under Linux and Windows are cURL and wget.

2.2.1.1 To access the organization registry using cURL

The following command triggers an export of the organization registry data to a local file called *exported.xml*. It uses a file called *server.crt* that contains the server certificate's CA certificate (this is unnecessary if the server certificate was issued by a trusted CA). The string `user1` has to be replaced by the actual username and the string `pass34` by the actual password. The URL has to be changed as defined above.

```
Example:

>>log.txt 2>&1 curl --insecure --cacer server.crt --basic
-u user1:pass34 -o exported.xml
-v https://localhost:8443/pxs/resource/organizationData
```

The following command triggers an import of the organization registry data from a local file called *to_import.xml*. It uses a file called *server.crt* that contains the server certificate's CA certificate (and which is unnecessary if the server certificate was issued by a trusted CA). The string `user1` has to be replaced by the actual username and the string `pass34` by the actual password. The URL has to be changed as defined above.

```
Example:

>>log.txt 2>&1 curl --insecure --cacer server.crt --basic
-u  user1:pass34  -X  POST  -H  "Content-Type:  text/xml"  -d  @to_im-
port.xml
-v https://localhost:8443/pxs/resource/organizationData
```

For further information on cURL see http://curl.haxx.se.

2.2.1.2 To access the organization registry using wget

The following command triggers an export of the organization registry data to a local file called *exported.xml*. It does not check the server's certificate because of the switch `–no-check-certificate` (which is unnecessary if the server certificate was issued by a trusted CA). The string `user1` has to be replaced by the actual username and the string `pass34` by the actual password. The URL has to be changed as defined above.

```
Example:

wget --no-check-certificate --auth-no-challenge --http-user=user1
--http-password=pass34 -O exported.xml -o log.txt --no-cache
--no-cookies https://localhost:8443/pxs/resource/organizationData
```

The following command triggers an import of the organization registry data from a local file called *to_import.xml*. It does not check the server's certificate because of the switch `–no-check-certificate` (which is unnecessary if the server certificate was issued by a trusted CA). The string `user1` has to be replaced by the actual username and the string `pass34` by the actual password. The URL has to be changed as defined above.

```
Example:

wget --no-check-certificate --auth-no-challenge --http-user=username
--http-password=password --post-file=test.xml -o log.txt --no-cache
--no-cookies https://localhost:8443/pxs/resource/organizationData
```

For further information on wget see http://www.gnu.org/software/wget.

2.2.1.3 Best Practices for accessing the organization registry

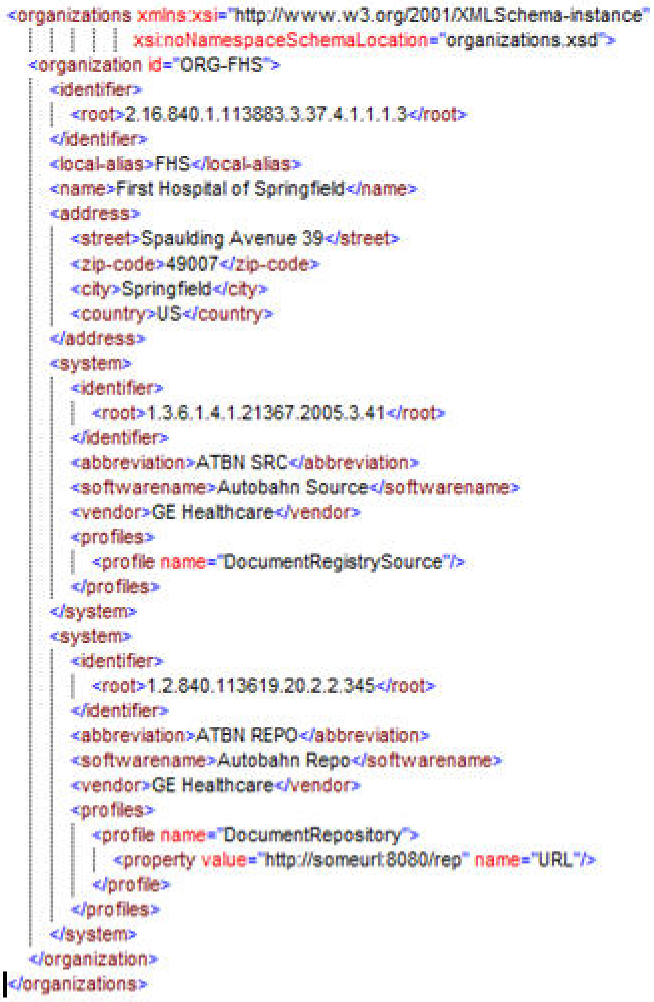
Before making changes to the organization registry, you should trigger an export to make sure you make the changes on the basis of the most recent organization data. If you use an outdated file you might accidentally overwrite more recent changes.

After you change the contents of the organization registry by importing a new XML file, you should verify that the changes were successful. First check the response code you received (in the wget example above you would need to check the log.txt file). Then issue another export and check that the newly exported XML reflects your changes.

2.2.2 How to use the organization data XML

The XML structure of the organization data is defined by an XML schema file called organizations.xsd that comes with the application. All exported organization data will adhere to this schema. Similarly, all organization data that the user wants to import must adhere to the schema.

The basic structure of the organization.xml can be seen in the following simple example:



```
<organizations xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
               xsi:noNamespaceSchemaLocation="organizations.xsd">
  <organization id="ORG-FHS">
    <identifier>
      <root>2.16.840.1.113883.3.37.4.1.1.1.3</root>
    </identifier>
    <local-alias>FHS</local-alias>
    <name>First Hospital of Springfield</name>
    <address>
      <street>Spaulding Avenue 39</street>
      <zip-code>49007</zip-code>
      <city>Springfield</city>
      <country>US</country>
    </address>
    <system>
      <identifier>
        <root>1.3.6.1.4.1.21367.2005.3.41</root>
      </identifier>
      <abbreviation>ATBN SRC</abbreviation>
      <softwarename>Autobahn Source</softwarename>
      <vendor>GE Healthcare</vendor>
      <profiles>
        <profile name="DocumentRegistrySource"/>
      </profiles>
    </system>
    <system>
      <identifier>
        <root>1.2.840.113619.20.2.2.345</root>
      </identifier>
      <abbreviation>ATBN REPO</abbreviation>
      <softwarename>Autobahn Repo</softwarename>
      <vendor>GE Healthcare</vendor>
      <profiles>
        <profile name="DocumentRepository">
          <property value="http://someurl:8080/rep" name="URL"/>
        </profile>
      </profiles>
    </system>
  </organization>
</organizations>
```

Figure 2: Example organization registry data

The current version of the Professional Exchange Server only focuses on systems, their namespaces and profiles. Please note that the organization registry must have at least one organization root that represents the affinity domain. An affinity domain defines a group of healthcare organizations that have agreed to work together using a common method for sharing patient healthcare information.

The following sections explain common changes to the organization data and how to accomplish them. Before changing the XML file, ensure that you are working with the latest version by downloading it from the server using the HTTP GET request described above.

2.2.2.1 Adding an organization

To add an organization to the organization registry, add a new `<organization>` element under the `<organizations>` root element. An `<organization>` element must have a unique `id` attribute. This is a transient attribute and it is not stored in the organization registry. It is only used for internal processing and to link child organizations to their parent organizations. The `<local-alias>` element is a string that identifies an organization and can be used to represent the ***Sending Facility*** in HL7v2 messages. The `<local-alias>` does not need to be unique in the affinity domain.

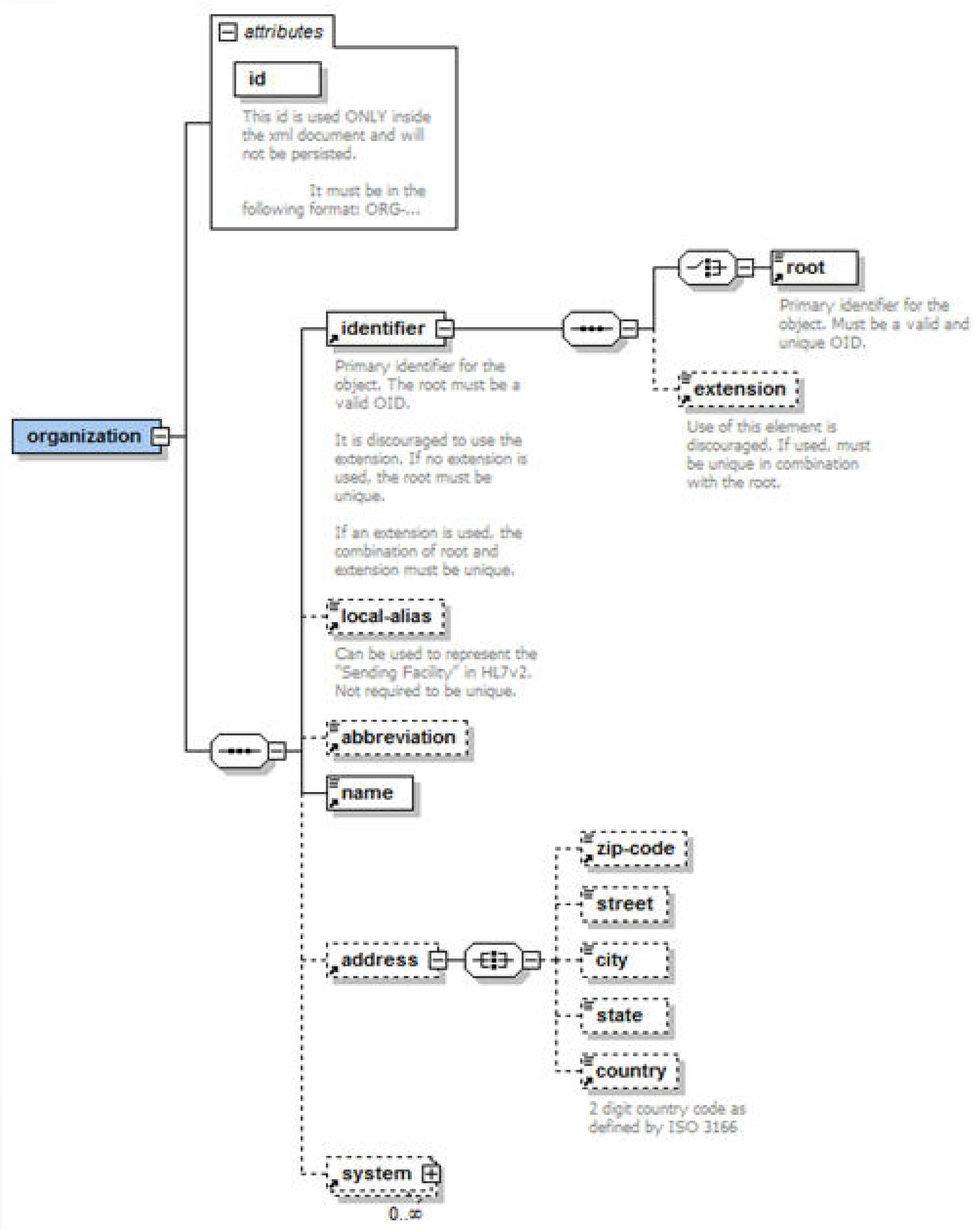

attributes
id
This id is used ONLY inside the xml document and will not be persisted.
It must be in the following format: ORG-...
organization
identifier
Primary identifier for the object. The root must be a valid OID.
It is discouraged to use the extension. If no extension is used, the root must be unique.
If an extension is used, the combination of root and extension must be unique.
root
Primary identifier for the object. Must be a valid and unique OID.
extension
Use of this element is discouraged. If used, must be unique in combination with the root.
local-alias
Can be used to represent the "Sending Facility" in HL7v2. Not required to be unique.
abbreviation
name
address
zip-code
street
city
state
country
2 digit country code as defined by ISO 3166
system
0..∞

Figure 3: Schema definition <organization> elements in the organization registry

An organization must have a unique identifier that consists of a root , an object identifier (OID), and an optional extension. We recommend using only the root attribute to identify organizations and systems, as the extension is only included to support legacy systems. Organizations also require a (potentially non-unique) name for display purposes.

If there is more than one organization, it is strongly recommended to build up an organization hierarchy using the `<organization-hierarchy>` element. To make a two-level hierarchy, simply add one `<parent-organization>` element with an `organization-id-ref` attribute that contains the parent organization's `id` attribute. Then add a `<child-organization>` element with an `organization-id-ref` attribute that contains the child organization's `id` attribute.

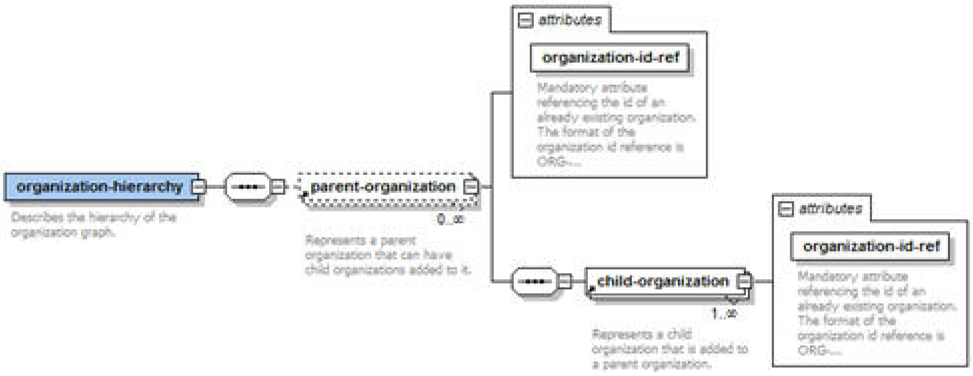

attributes
organization-id-ref
Mandatory attribute referencing the id of an already existing organization. The format of the organization id reference is ORG-...
organization-hierarchy
Describes the hierarchy of the organization graph.
parent-organization
0..∞
Represents a parent organization that can have child organizations added to it.
attributes
organization-id-ref
Mandatory attribute referencing the id of an already existing organization. The format of the organization id reference is ORG-...
child-organization
1..∞
Represents a child organization that is added to a parent organization.

Figure 4: Schema definition for the <organization-hierarchy> element in the organization registry

To establish a multi-level hierarchy, an organization that was used as a child can be referenced again as a parent organization, to define its child organizations.

Example:

```
<organization-hierarchy>
<parent-organization organization-id-ref="ORG-SHG">
<child-organization organization-id-ref="ORG-FHS" />
<child-organization organization-id-ref="ORG-SCH" />
</parent-organization>
<parent-organization organization-id-ref="ORG-FHS">
<child-organization organization-id-ref="ORG-FHS-CARDIO" />
<child-organization organization-id-ref="ORG-FHS-SRGERY" />
</parent-organization>
<parent-organization organization-id-ref="ORG-FHS-CARDIO">
<child-organization organization-id-ref="ORG-FHS-B1" />
```

```
<child-organization organization-id-ref="ORG-FHS-B2" />
</parent-organization>
<parent-organization organization-id-ref="ORG-SCH">
<child-organization organization-id-ref="ORG-SCH-B1" />
</parent-organization>
</organization-hierarchy>
```

NOTE

The Professional Exchange Server organization registry supports multiple parent organizations for each organization. The internal representation of this organization hierarchy is a directed-graph without cycles. The organization registry verifies on each import that the organization graph does not contain any cycles.

2.2.2.2 Moving an organization

To move an organization, the administrator needs to move the organization's `<child-organization>` element underneath a different `<parent-organization>` element.

Example:

```
<organization-hierarchy>
<parent-organization organization-id-ref="ORG-SHG">
<child-organization organization-id-ref="ORG-FHS" />
<child-organization organization-id-ref="ORG-SCH" />
</parent-organization>
<parent-organization organization-id-ref="ORG-FHS">
<child-organization organization-id-ref="ORG-FHS-SRGERY" />
</parent-organization>
<parent-organization organization-id-ref="ORG-FHS-CARDIO">
<child-organization organization-id-ref="ORG-FHS-B1" />
<child-organization organization-id-ref="ORG-FHS-B2" />
</parent-organization>
<parent-organization organization-id-ref="ORG-SCH">
<child-organization organization-id-ref="ORG-FHS-CARDIO" />
<child-organization organization-id-ref="ORG-SCH-B1" />
```

```
</parent-organization>
</organization-hierarchy>
```

In this example the ORG-FHS-CARDIO has been moved from ORG-FHS to ORG-SCH.

2.2.2.3 Deleting an organization

To ensure data consistency and availability, deleting an organization is not supported by the organization registry. It is recommended to establish a naming convention to be able to easily identify organizations that are no longer needed.

2.2.2.4 Modifying an organization

The administrator can modify an organization's metadata by changing any of the child elements and their values except for the `id` attribute and the `<identifier>` element. The organization registry interprets changing the identifier as a deletion of the original organization and the addition of a new organization. Deletion of organizations is not supported.

2.2.2.5 Adding a system

A `<system>` element must be a child element of an `<organization>`. When adding a system, the only mandatory information is the `<identifier>` child element. As with organizations, the root must be a unique OID and it is recommended to only use the root as the identifier. The `<system-alias>` element is a string that uniquely identifies a system and can be used to represent the Sending Application in HL7v2 messages.

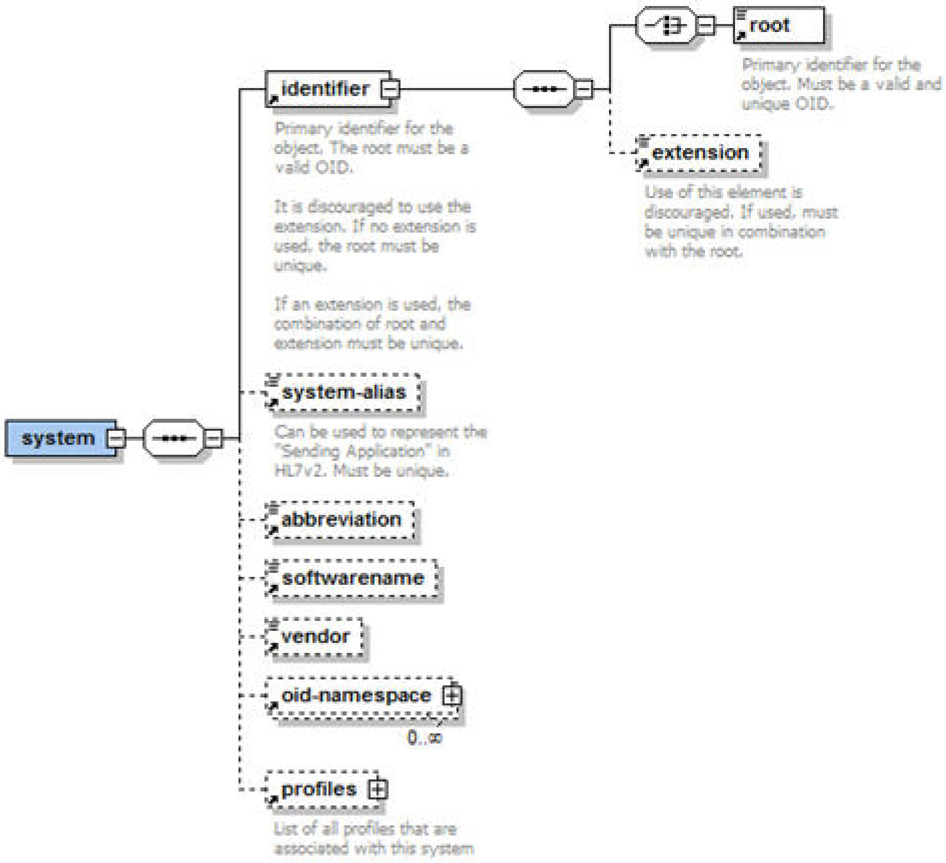

root
Primary identifier for the object. Must be a valid and unique OID.
identifier
Primary identifier for the object. The root must be a valid OID.
It is discouraged to use the extension. If no extension is used, the root must be unique.
If an extension is used, the combination of root and extension must be unique.
extension
Use of this element is discouraged. If used, must be unique in combination with the root.
system
system-alias
Can be used to represent the "Sending Application" in HL7v2. Must be unique.
abbreviation
softwarename
vendor
oid-namespace
0..∞
profiles
List of all profiles that are associated with this system

Figure 5: Schema definition for the <system> element in the organization registry

2.2.2.6 Moving a system

A system can be moved to a different organization by cutting the `<system>` element from its current position and pasting it into position as a child element of the target organization.

2.2.2.7 Deleting a system

To ensure data consistency and availability, system deletion is not supported by the organization registry. It is recommended to establish a naming convention to be able to easily identify systems that are no longer needed.

2.2.2.8 Modifying a system

The administrator can modify a system's metadata by changing any of the child elements and their values except for the `<identifier>` element. The organization registry interprets changing the identifier as a deletion of the original system and the addition of a new system. Deletion of systems is not supported.

2.2.2.9 Adding a namespace

A namespace belongs to a system. The root element must be a globally unique OID. Clients of the organization registry use this information in their processing, for example, to prefix a system's local identifiers with the namespace to make them globally unique. The type element is used to identify what types of objects are identified by IDs from this namespace. The options are:

- **P** for patient
- **D** for documents
- **MV** for movements

The `<namespace-alias>` is a string that uniquely identifies a namespace and can be used to represent the **Namespace ID** in HL7v2 messages.

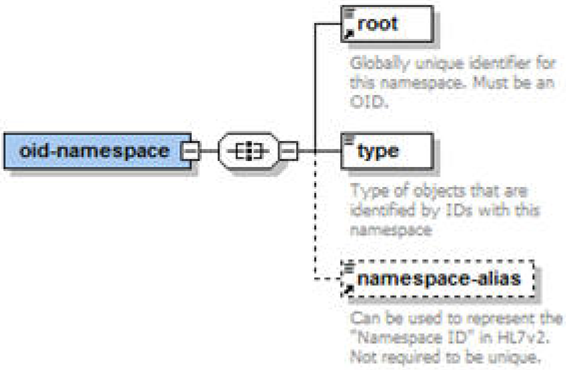

root
Globally unique identifier for this namespace. Must be an OID.
oid-namespace
type
Type of objects that are identified by IDs with this namespace
namespace-alias
Can be used to represent the "Namespace ID" in HL7v2. Not required to be unique.

Figure 6: Schema definition for the <oid-namespace> element in the organization registry

2.2.2.10 Moving a namespace

To assign a namespace to a different system, move the `<oid-namespace>` element to another parent `<system>` element.

2.2.2.11 Deleting a namespace

To ensure data consistency and availability, namespace deletion is not supported by the organization registry. It is recommended to establish a convention to be able to easily identify namespaces that are no longer needed, for example, by moving them to a dummy system created for this purpose.

2.2.2.12 Modifying a namespace

The administrator can modify a namespace's metadata by changing any of the child elements and their values except for the `<root>` element. The organization registry interprets changing the root as a deletion of the original namespace and the addition of a new namespace. Deletion of namespaces is not supported.

2.2.2.13 Adding a profile to a system

Profiles are used to reliably label systems and to associate them with additional metadata. By default the Professional Exchange Server organization registry supports the following profiles:

- DocumentRegistrySource
- DocumentRepository
- XdsPatientIdentitySourceProfile

Each of these profiles labels an organization as a specific IHE XDS actor. A system may have more than one profile, but only one profile of a kind. For example, a system may have a DocumentRegistrySource profile and a DocumentRepository profile, but it may not have two DocumentRepository profiles. The XdsPatientIdentitySourceProfile must be assigned to exactly one system in the registry, because the IHE XDS profile does not support multiple Patient Identity Sources. In case there is more than one Patient Identity Source, they have to be aggregated, for example, by using the Professional Exchange Server Master Patient Index.

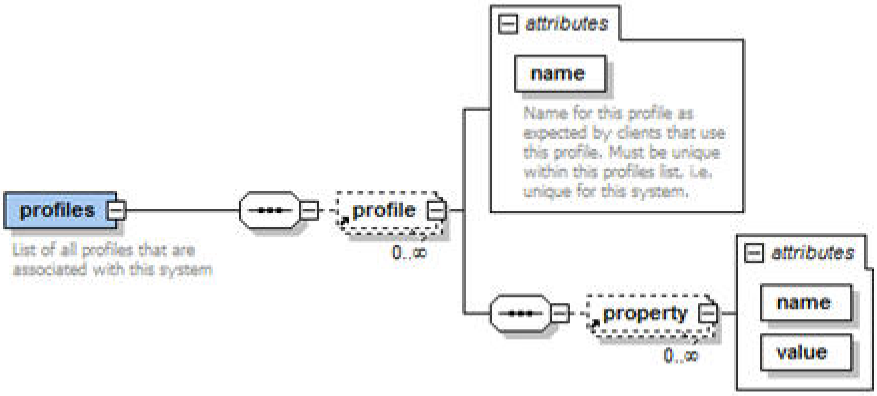

attributes
name
Name for this profile as expected by clients that use this profile. Must be unique within this profiles list, i.e. unique for this system.
profiles
List of all profiles that are associated with this system
profile
0..∞
attributes
property
0..∞
name
value

Figure 7: Schema definition for the <profiles> element in the organization registry

A profile has a name and potentially a set of properties, which are key-value pairs. The organization registry accepts other strings than the three listed above as valid profiles. This allows other systems and users to store additional metadata for systems in the organization registry without interfering with the operation of the Professional Exchange Server. When a custom profile is used, any key-value pair is accepted as a property.

2.2.2.14 Modifying a system's profile

The administrator can modify a profile’s metadata by changing any of the property elements and their values. Please note that changing the name will hinder the organization registry clients from using the profile information in the future, as they normally query by the profile’s name.

2.2.2.15 Removing a system's profile

To remove a profile, remove the `<profile>` element from the system.

2.3 Making changes to the Tomcat folder

Some administration tasks require you to make changes in the Tomcat folder, mostly in the *webapps* subfolder, but sometimes also in the *conf* or *bin* subfolders. Before you make any changes, please ensure that you have a current backup of the whole Tomcat folder. This way all changes are reversible. For complete and efficient migrations, it is strongly recommended to also backup the files after the changes are made.

It is also recommended to automate changes to any files in the Tomcat folder as much as possible. This ensures that the changes can be repeated, even if the Tomcat folder had to be restored from a backup or was overwritten during a migration.

Certain administration tasks described in the sections below require changes to the webapps folder. It is strongly recommended to shut down the Tomcat before making any changes to the webapps folder. It is also strongly recommended to make changes to the webapps folder in a safe and repeatable manner by updating the webapp’s WAR file through a script.

We suggest the following approach:

1. Create a new folder (*diff* folder) that contains only the files and the directory structure that are to be changed in the *webapps* folder.
2. If you want to modify a file, take the most recent original version from the WAR file, make your changes and then add it to the *diff* folder in the appropriate subfolder. For example, if you need to change the *web.xml* file and add an additional stylesheet, first extract the original *web.xml* file from the WAR file’s WEB-INF subfolder and make your changes, then save it in the *diff* folder.
3. Copy the stylesheet to the correct subfolder in the *diff* folder. The *diff* folder would then contain the following files and folders:

```
WEB-INF/web.xml
WEB-INF/classes/xsltTemplates/text_xml-custom_format.xsl
```

To update the *webapps* folder, you need to shut down Tomcat and then run the following script:

```
find -type f | xargs -i zip <install_target_path>/apache-tomcat-6.0.29/webapps/<war_file_name> {}
```

Example:

```
find -type f | xargs -i zip /opt/pxs3-install/apache-tomcat-6.0.29/webapps/pxs-vmr-assembly.war {}
```

4. Restart Tomcat.

NOTE ***diff* folder**

Please note that the *diff* folder must contain all changes to the webapp folder, as any changes that were made directly in the *<tomcat>/webapps/<webapp_name>* folder and not in the *diff* folder will be lost.

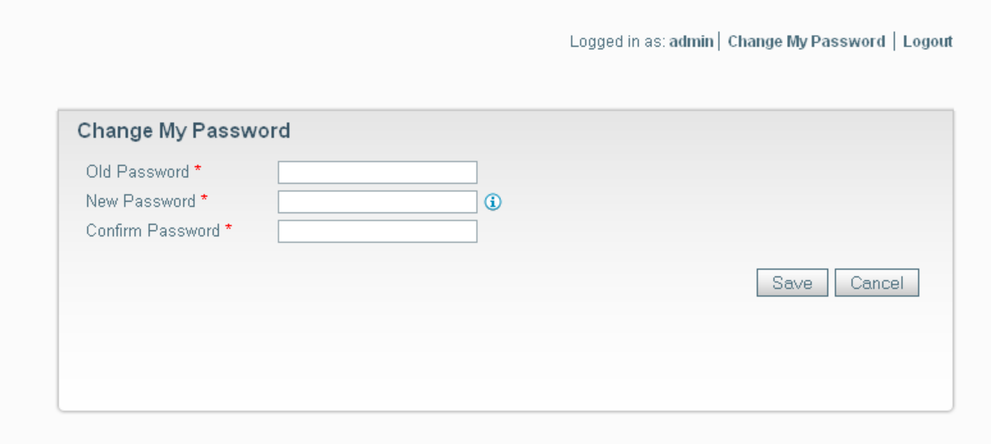
NOTE **Clustered deployment**

In a clustered deployment these changes will need to be applied to each node's Tomcat, which is another good reason to automate all changes.

2.4 User Administration GUI

2.4.1 Change password

1. Click **Change password** on the the navigation bar.
   ⇨ The *Change My Password* page opens.



Logged in as: admin | Change My Password | Logout

Change My Password

Old Password *

New Password *

Confirm Password *

Figure 8: The Change My Password page

2. Enter your current password into the **Old Password** field.
3. Enter your new password into the respective field.
4. Enter your new password for a second time into the **Confirm Password** field.

CAUTION **Password format**

The password has to consist of at least eight to 50 characters including a number and one of the following special characters: **_-#)(§!**. You cannot re-use any of your five latest passwords.

5. Click the **Save.** button.

   ⇨ Your password has been changed. The *Welcome page* opens.

2.4.2 Accessing the User Administration Interface

1. Enter the URL of Professional Exchange Server.

   ⇨ The Login page opens

2. Log in to the application.

   ⇨ The *Select Application* page opens.

3. Click **User Administration**.

   ⇨ The *User Administration* opens.

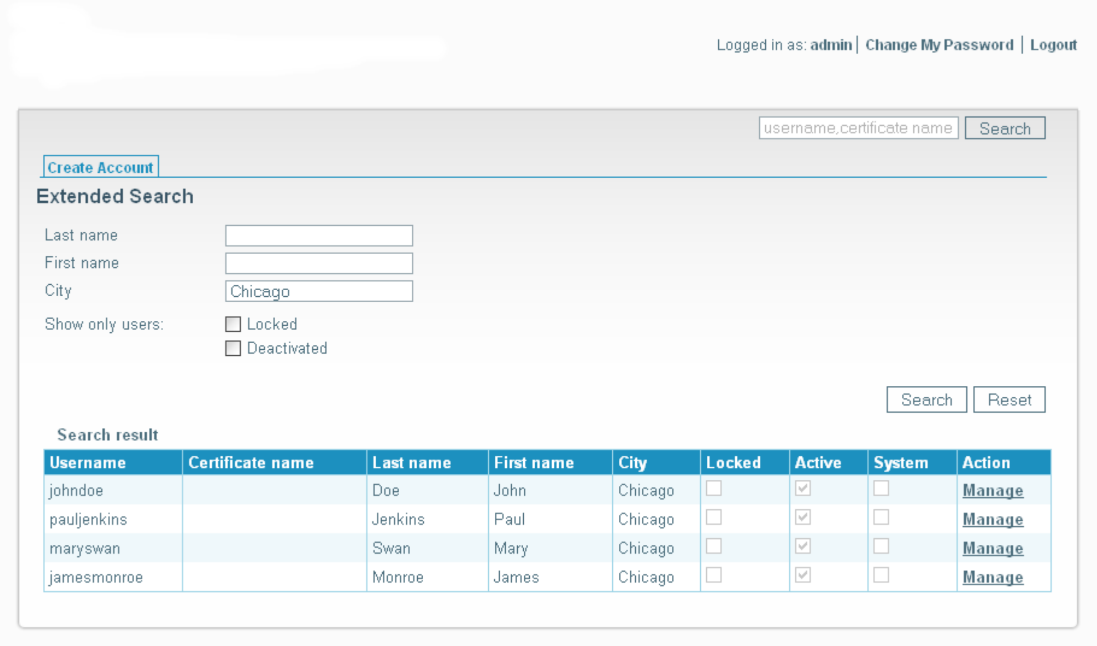
2.4.3 Search functions

2.4.3.1 User Administration Tasks

After accessing the *User Administration* of Professional Exchange Server the *Extended Search* page opens.

There are three functions you can use on this page:

- The *Quick search* function, to search for an existing user by entering one criterium. See the section The Quick Search Function [page 31].
- The *Extended search* function, to search for an existing user by entering more than one criteria. See the section Extended Search [page 32].
- The *Create Account* function, to create new user accounts. See the section Creating an Acount [page 33].



Logged in as: admin | Change My Password | Logout

Extended Search

Last name	
First name	
City	Chicago
Show only users:	□ Locked □ Deactivated

Search result

Username	Certificate name	Last name	First name	City	Locked	Active	System	Action
johndoe		Doe	John	Chicago	□	☑	□	Manage
pauljenkins		Jenkins	Paul	Chicago	□	☑	□	Manage
maryswan		Swan	Mary	Chicago	□	☑	□	Manage
jamesmonroe		Monroe	James	Chicago	□	☑	□	Manage

Figure 9: The Extended Search page offers three functions

The *Navigation* bar at the top of the page shows the *user name* you are logged in with. It also allows you to change your *password* and to *log out* from the system. The Navigation bar is available from every page in the *User Administration*.

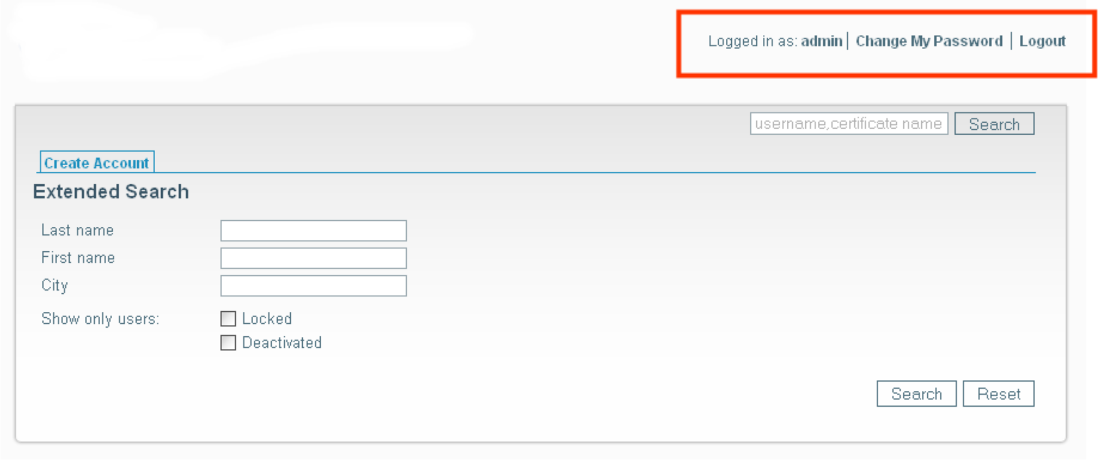


Figure 10: The navigation bar

2.4.3.2 Search for a User

In the *User Administration* you find two search functions. You can either use the *Quick search* to perform an exact search or the *Extended Search* to perform a more differentiated search.

2.4.3.2.1 The Quick Search Function

The *Search* field below the *Navigation* bar offers you the quick search function. It allows you to search for either a username or a certificate name.

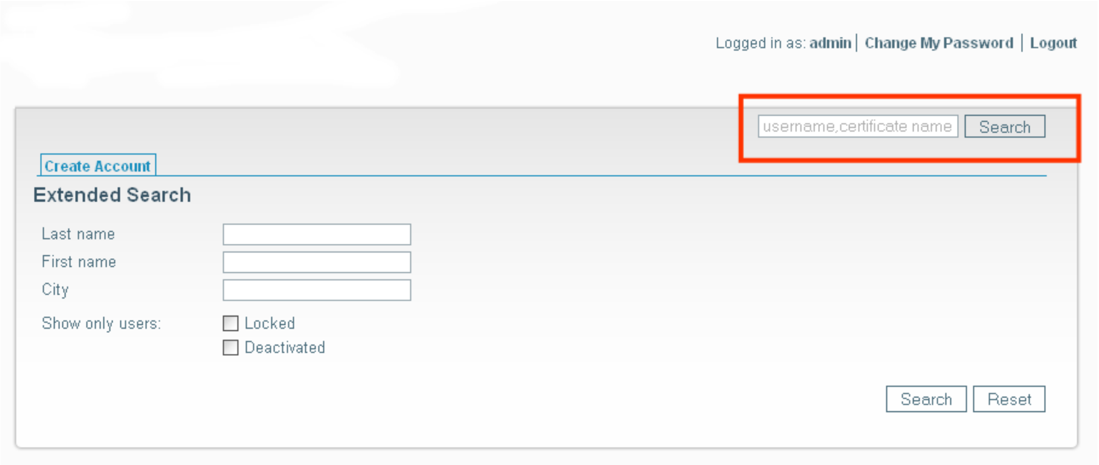


Figure 11: The Quick Search Field

1. Enter a <<username>> or a <<certificate name>> into the **Search** field
2. Click the **Search** button.

⇨ If a result is found the respective account page is opened. If there is no result a message is displayed.

NOTE **Wildcards**

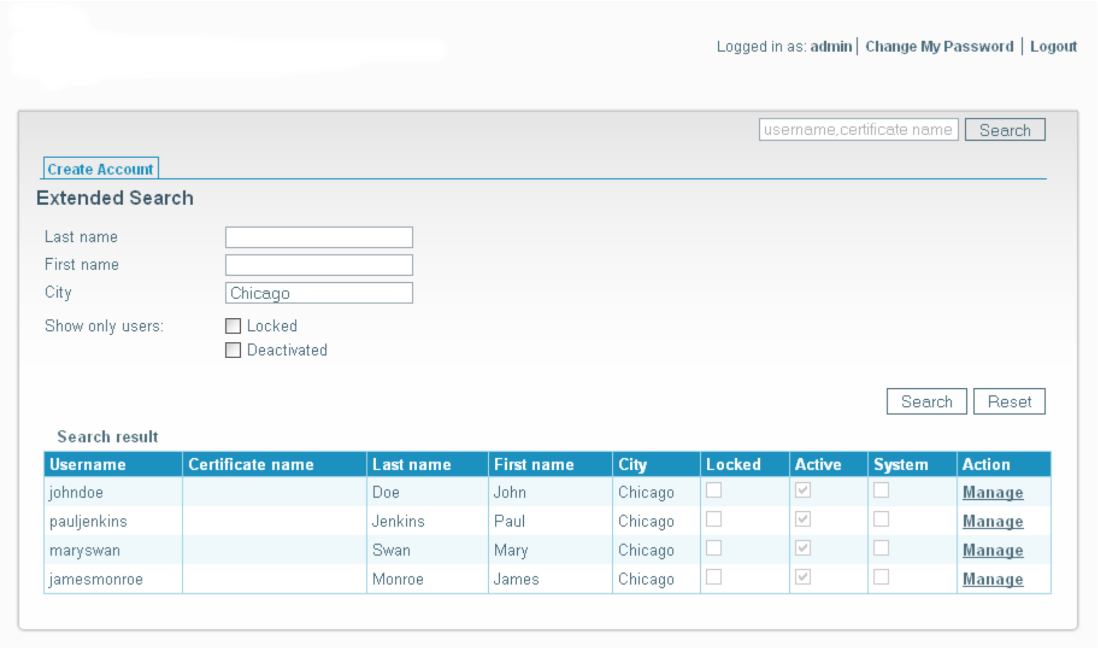
Wildcards like “*” are not allowed when searching by username or certificate name.

2.4.3.2.2 Extended Search

In the *Extended Search* page, which is available immediately after accessing the *User Administration* of Professional Exchange Server you can use several criteria to search for a user

The page offers you the following fields and checkboxes:

- *Last name*: Last name of the person you are looking for.
- *First name*: First name of the person you are looking for.
- *City*: Hometown of the person you are looking for.
- *Locked*: When this checkbox is active, only users, whose account is locked will be displayed.
- *Deactivated*: When this checkbox is active only deactivated users will be displayed.
- *Search*: This button starts your search
- *Reset*: This button clears the search results list displayed after your search.



Logged in as: admin | Change My Password | Logout
username,certificate name
Search
Create Account

Extended Search

Last name
First name
City: Chicago
Show only users: □ Locked
□ Deactivated

Search result

Username	Certificate name	Last name	First name	City	Locked	Active	System	Action
johndoe		Doe	John	Chicago	□	☑	□	Manage
pauljenkins		Jenkins	Paul	Chicago	□	☑	□	Manage
maryswan		Swan	Mary	Chicago	□	☑	□	Manage
jamesmonroe		Monroe	James	Chicago	□	☑	□	Manage

Figure 12: Example results of an extended search

NOTE **Wildcards**

The *Extended Search* offers the possibility to search with wildcards. For example, by entering "*" in any of the fields *Last name*, *First name* and *City*.

The results of the *Extended Search* are displayed in a table.

2.4.3.3 Search for a User with Extended Search

1. Open the *User Adminitration*.
   ⇨ The initial page with the *Extended Search* opens.
2. Enter your **search criteria** or a wildcard (*).
   ⇨ The *search results* list is displayed.
3. To open the user account click on **Manage** in the *Action* column.
   ⇨ The user account page opens.

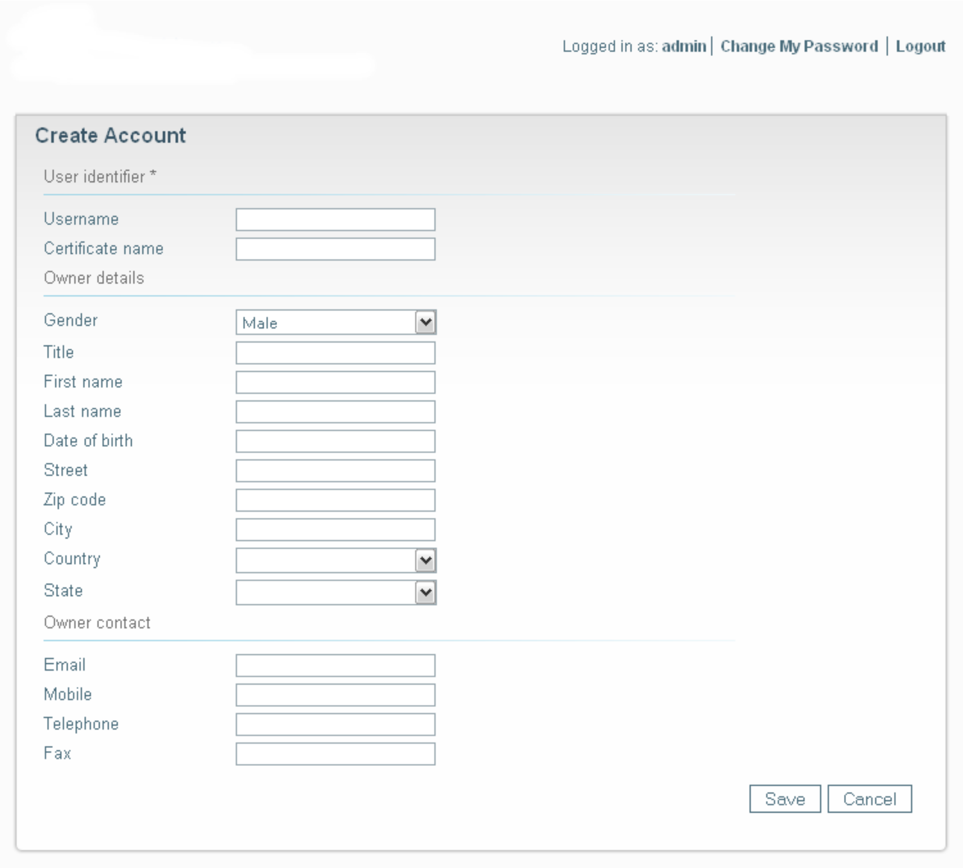
NOTE **Clearing the results list**

To clear the search results list click on the **Reset** button.

2.4.4 Accounts

2.4.4.1 Creating an account

1. Open the **User Administration**.
   ⇨ The initial page with the *Extended Search* opens.
2. Click the **Create Account** tab.
   ⇨ The *Create Account* page opens.



Logged in as: admin | Change My Password | Logout

Create Account

User identifier *

Username

Certificate name

Owner details

Gender: Male

Title

First name

Last name

Date of birth

Street

Zip code

City

Country

State

Owner contact

Email

Mobile

Telephone

Fax

Figure 13: The Create Account page

3. Fill out the following fields:
   - *Username*: The user name of the account. The field is required in case Certificate name is not filled out. A user name has to consist of at least 5 characters and a maximum of 30 characters. Special characters are not allowed.
   - *Certificate name*: The certificate name of the account. The field is required in case username is not filled out. You will find certificate names in the keystore of the application.

NOTE **Mandatory Information**

Only the user name or the certificate name field is required. But at least one of them is mandatory.

   - *Gender*: User’s gender
   - *Title*: The title of user.
   - *First name*: User’s first name.
   - *Last name*: User's family name.
   - *Date of birth*: User’s birth date. A validation check is carried out on the entered string. Please follow the pattern: MM/DD/YY.

- *Street*: User address information.
- *Zip code*: Postal code of user's address.
- *City*: User address information.
- *Country*: User address information.
- *State*: User address information.
- *Email*: User's email address. A validation check is carried out on this field. Follow the pattern xxx@yyy.zz.
- *Mobile*: User's cell phone number. A validation check is carried out on this field.
- *Telephone*: User's landline number. A validation check is carried out on this field.
- *Fax*: User's fax number. A validation check is carried out on this field.

4. Click the **Save** button to create the account.

   ⇨ The new account ist displayed. In the password field you find a newly generated one-time password.

5. Send the one-time password to the user asking him to change it after the first login.

NOTE **Password**

When you save a new account with user name, a one-time password is generated and displayed in the password field. If the account is saved without user name, but with a certificate name, an asterisk will be displayed in *Password* field.

2.4.4.2 Manage an account

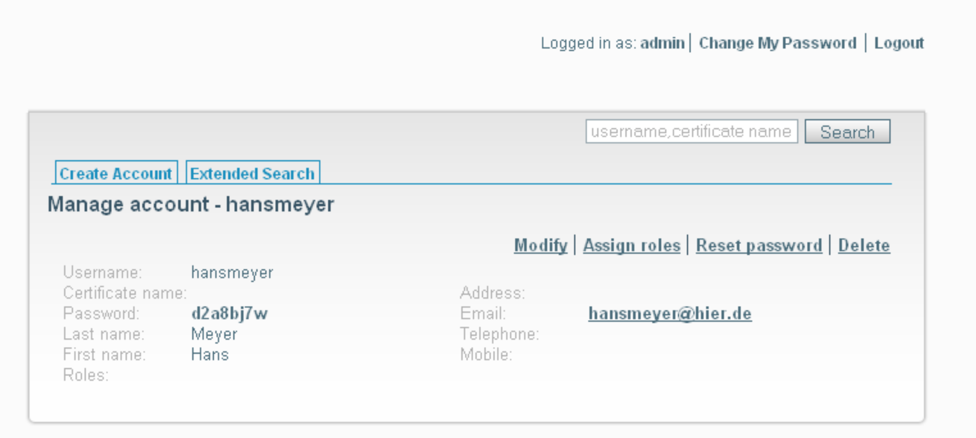
PATH

Search | Manage account

or

Extended Search | Search result | Action: Manage

The *Manage account* page displays basic information about a user account and allows you to modify user data by clicking on the actions in the action bar.


Logged in as: admin | Change My Password | Logout
username,certificate name
Search
Create Account
Extended Search
Modify | Assign roles | Reset password | Delete

Manage account - hansmeyer

Username:	hansmeyer		
Certificate name:		Address:	
Password:	d2a8bj7w	Email:	hansmeyer@hier.de
Last name:	Meyer	Telephone:	
First name:	Hans	Mobile:	
Roles:			

Figure 14: The Manage account page

You find the following actions:

- *Modify*: This action opens the *Modify account* page [page 37].
- *Assign roles*: This action opens the *Assign roles* page [page 39].
- *Reset password*: This action opens a dialog that allows you to reset the password [page 43].

NOTE **Password**

When you reset the password , a one-time password is generated and displayed in the password field of the manage account field. Send the password to the user asking him to change it after the first login.

If the account is saved without user name, but with a certificate name, an asterisk will be displayed in *Password* field.

- *Delete*: This action deletes [page 39] the user account that is currently open.

If you have entered an *Email* address the link allows you to open your Email program and send a message to the user.

There are two ways to open the page:

- Perform a **Quick Search** for a username, if known. See Quick Search [page 31]
- Perform an **Extended Search** and in the results table click the **Manage** link in the **Action** column. SeeExtended Search [page 33]

NOTE **Create Account**

From the Manage Account page you can access the Create Account tab and the Extended Search tab.

2.4.4.3 Overview of the Modify account page

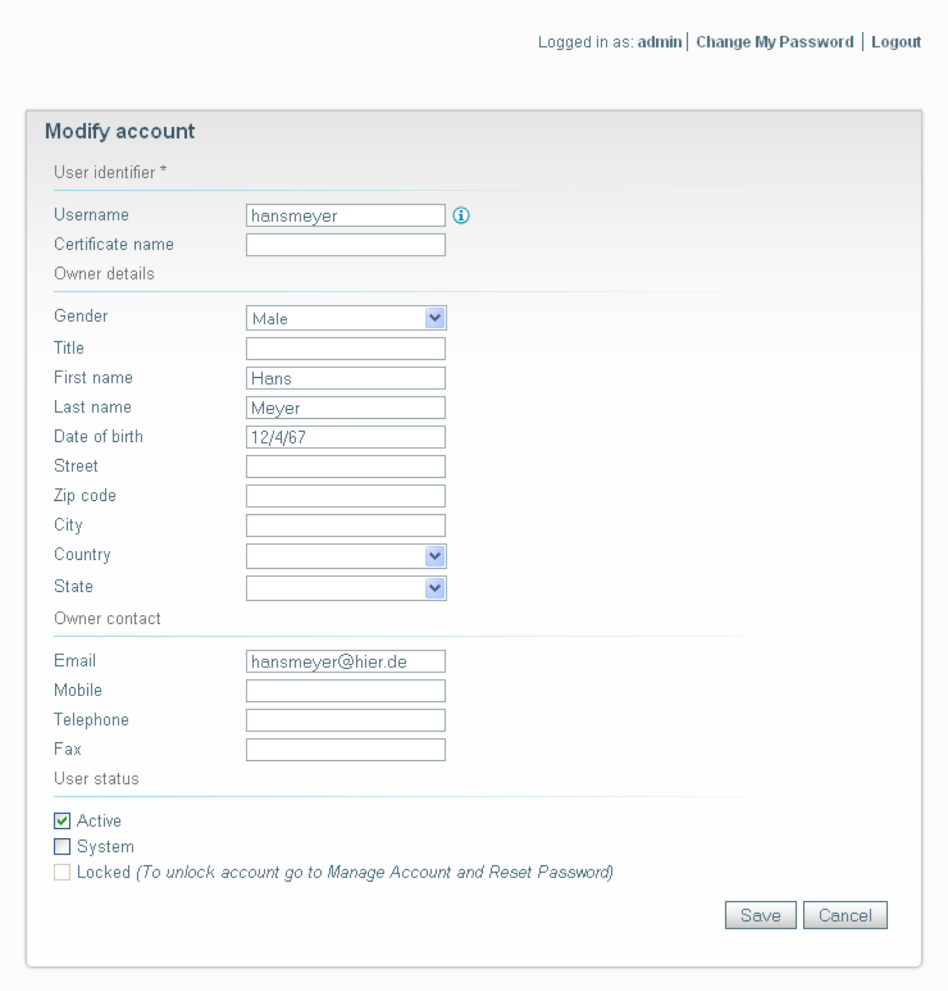
PATH

Search <<user name or certificate name>>| Manage account | Modify

or

Extended Search | Search result | Action: Manage | Modify

On the *Modify account* page you change user data such as name, address or phone number. You can also activate or deactivate the account.



Modify account

User identifier *

Username	hansmeyer
Certificate name	

Owner details

Gender	Male
Title	
First name	Hans
Last name	Meyer
Date of birth	12/4/67
Street	
Zip code	
City	
Country	
State	

Owner contact

Email	hansmeyer@hier.de
Mobile	
Telephone	
Fax	

User status

☑ Active
☐ System
☐ Locked *(To unlock account go to Manage Account and Reset Password)*

Figure 15: The Modify account page

You will find the following fields and check boxes:

- *Username*: The user name of the account. The field is required in case Certificate name is not filled out. A user name has to consist of at least 5 characters and a maximum of 30 characters. Special characters are not allowed.
- *Certificate name*: The Certificate name of the account. The field is required in case username is not filled out.

> **NOTE** **Mandatory Information**
>
> Only the user name or the certificate name field is required. But at least one of them is mandatory.

- *Gender*: user’s gender
- *Title*: The title of user.
- *First name*: user’s first name.
- *Last name*: user's family name.
- *Date of birth*: User’s birth date. A validation check is carried out on the entered string. Please follow the pattern: MM/DD/YY.
- *Street*: User address information.
- *Zip code*: Postal code of user’s address.
- *City*: User address information.
- *Country*: User address information.
- *Email*: User's email address. A validation check is carried out on this field.Please, follow the pattern xxx@yyy.zz.
- *Mobile*: User's cell phone number. A validation check is carried out on this field.
- *Telephone*: User's landline number. A validation check is carried out on this field.
- *Fax*: User's fax number. A validation check is carried out on this field.
- *Active*: This check box allows you to acivate or deactivate a user.
- *System*: This check box marks the user as a system user. If this check box is active the user cannot log in via the UI.
- *Locked*: This check box allows you to check on a user's status. To unlock an account you have to reset the password. See Reset Password [page 43]

See also

- Reset a password [page 43]

2.4.4.3.1 Modifying an account

1. Follow either of these paths:
   - Search <<user name or certificate name>>| Manage account | Modify

- Extended Search | Search result | Action: Manage | Modify

2. Click on **Modify**

   ⇨ The *Modify account* page opens.

3. Edit the desired fields.
4. Click on the **Save** button.

   ⇨ Your changes are saved.

2.4.4.4 Delete an account

⚠ **CAUTION**

Deleting a user account is an irreversible action. Once deleted, the account cannot be restored.

PATH

Search <<user name or certificate name>>| Manage account | Delete

or

Extended Search | Search result | Action: Manage | Delete

1. Follow either of these paths:
   - Search <<user name or certificate name>>| Manage account | Delete
   - Extended Search | Search result | Action: Manage | Delete

   ⇨ A dialog opens asking you to confirm the deletion.

2. Click **OK** to delete the account

   ⇨ The user's account will be deleted and is no longer available.

2.4.4.5 Assign Roles

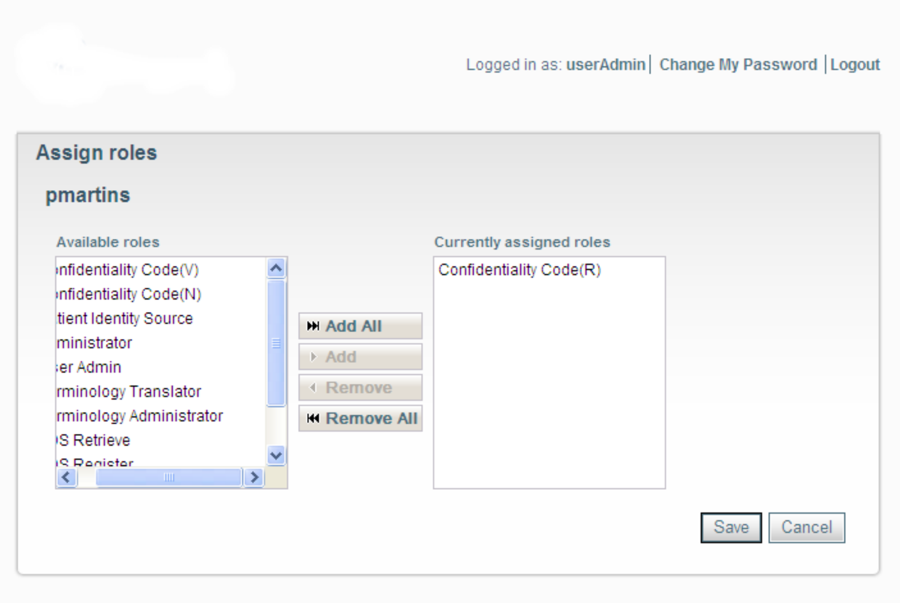
PATH

Search <<user name or certificate name>>| Manage account | Assign role

or

Extended Search | Search result | Action: Manage | Assign role

A role has to be defined for each user that allows him access to certain data in the system.



Assign roles

pmartins

Available roles

ɩnfidentiality Code(V)
ɩnfidentiality Code(N)
tient Identity Source
ministrator
ɩer Admin
rminology Translator
rminology Administrator
ɩS Retrieve
ɩS Register

Currently assigned roles

Confidentiality Code(R)

Figure 16: The Assign roles page

The *Assign roles* page displays all *Available roles* and a user accounts *Currently assigned roles*. A switch board allows you to add or remove roles for a user.

The following buttons add or remove roles:

- *Add all*: This button adds all available roles to a user.
- *Add*: This button moves one or more selected roles into the *Currently assigned roles* field.
- *Remove:* This button removes one or more selected roles from the *Currently assigned roles* field.
- *Remove all*: This button removes all currently assigned roles from the respective field.

The following default roles are available:

Role	Permissions
View Normal Medical Data	This role has access to medical data classified according to HL7 security standard ***Normal***. This includes: non-administrative login, change Password, search patients, view patient details, view document metadata of normal documents, view detailed metadata of normal documents from registry, view content of normal documents
View Restricted Medical Data	This role has access to medical data classified according to HL7 security standard ***Restricted***. This includes all permissions of the role ***View Normal Medical Data*** and the following additional permissions: view document metadata of restricted documents, view detailed metadata of resricted documents from registry, view content of restricted documents
View Very Restricted Medical Data	This role has access to medical data classified according to HL7 security standard ***Very Restricted***.This includes all permissions of the role ***View Restricted Medical Data*** and the following additional permissions: view document metadata of very restricted documents, view detailed metadata of very resricted documents from registry, view content of very restricted documents
JMX Administrator	Remote access to JMX Bean server via JConsole
Organization Adminstrator	Import and export of organisation and systems hierarchy
User Administrator	Manage user accounts
Terminology Administrator	Change translation for code, add codes to code systems, edit code sets, edit code categories
Terminology Translator	Change translation for code
Patient Identity Source	Send IHE ITI-8 PIX feeds to Professional Exchange Server, process feeds in the VMR.
XDS Query Registry	Execute ***Query Registry*** or ***Registry Stored Query*** transactions
XDS Retrieve Documents	Execute ***Retrieve Document Set*** transaction

Role	Permissions
XDS Register Documents	Execute ***Provide and Register*** and ***Register*** transactions.
DSUB Subscriber	Execute transaction ***Document Metadata Subscribe***
DSUB Publisher	Execute transaction ***Document Metadata Publish***
Security Override	Execute patient-based security override function

NOTE **Default Administrator roles**

After the installation the application contains a default Administrator who has the following roles: JMX Administrator, Organization Administrator, User Administrator and Terminology Administrator. The Administrator gets a password which was entered during the installation process. After the first log in this needs to be changed. For further information please refer to the *Installation Manual*.

2.4.4.5.1 Assigning Roles

1. Follow either of these paths:
   - Search <<user name or certificate name>>| Manage account | Assign role
   - Extended Search | Search result | Action: Manage | Assign role

   ⇨ The *Assign roles* page opens
2. Click a role from the **Available roles** field to select it.
3. Use the **Add** button to move the selected role or roles into the *Currently assigned roles* field. If you want to assign all roles to a user click the **Add all** button.

   ⇨ The selected roles are moved into the *Currently assigned roles* field and assigned to the current user.

   NOTE **Unassign roles**

   If you want to remove roles click on the respective role in the*Currently assigned roles* field and then click the **Remove** button. If you want to remove all roles for this user click on the **Remove all** button.
4. Click **Save**.

2.4.4.6 Reset a password

PATH

Search <<user name or certificate>>| Manage account | Reset password

or

Extended Search | Search result | Action: Manage | Reset password

1. Follow either of these paths:
   - Search <<user name or certificate name>>| Manage account | Reset password
   - Extended Search | Search result | Action: Manage | Reset password

   ⇨ The *Reset password* dialog opens
2. Click the **OK** button to confrm the password reset.

   ⇨ In the *Password* field of the *Manage account* page you will find a new one-time password.
3. Send this one-time password to the respective user and ask him to change this password after the first login. The one-time password is valid only for a limited amount of time.

NOTE **Password reset for certificate users**

The *Password reset* is disabled for certificate users

2.4.5 Assign a Role to an LDAP Group

The User Administration interface contains a Groups tab. Using this tab, LDAP groups can be assigned to Professional Exchange Server roles.

There are some things to keep in mind about LDAP. LDAP is always an extension to the existing user-managment. Professional Exchange Server only has read access to the LDAP user-managment system. This means for example that it is not possible to change an LDAP password from within Professional Exchange Server. LDAP users cannot be found and managed in the Professional Exchange Server User Administration interface. You do this using the LDAP administration.

2.5 Terminology Tools GUI

2.5.1 Accessing Terminology Tools

1. Enter the URL of Professional Exchange Server.
   ⇨ The *Login page* opens
2. Log in to the application.
   ⇨ The *Select Application* page opens.
3. Click **User Administration**.
   ⇨ The *User Administration* page opens.

2.5.2 Initial page of Terminology Tools

When you open the Terminology Tools page three tabs appear, which you can use for your configuration tasks.

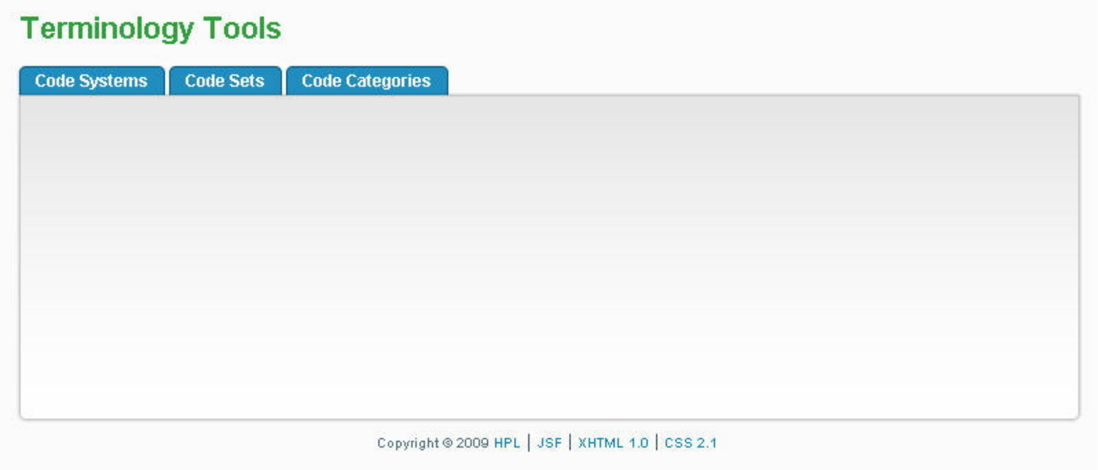


Figure 17: Terminology Tools initial page

.

- The *Code Systems* tab: Here you can add or edit Code Systems and Codes. You can determine the number of Code Systems and Codes that are displayed in the list by clicking **Show <<number>>** below the list. Use the **page navigation** if the list is displayed on more than one page.
- The *Code Sets* tab: Here you can add or edit Code Sets. You can determine the number of Code Sets and Codes that are displayed in the list by by clicking **Show <<number>>** below the list. Use the **page navigation** if the list is displayed on more than one page.
- The *Code Categories* tab: Here you can edit Code Categories. You can determine the number of Code Sets and Codes that are displayed on the list by by clicking **Show <<number>>** below the list. Use the **page navigation** if the list is displayed on more than one page.

Selecting a tab will load and display the currently available data elements, configured for that tab.

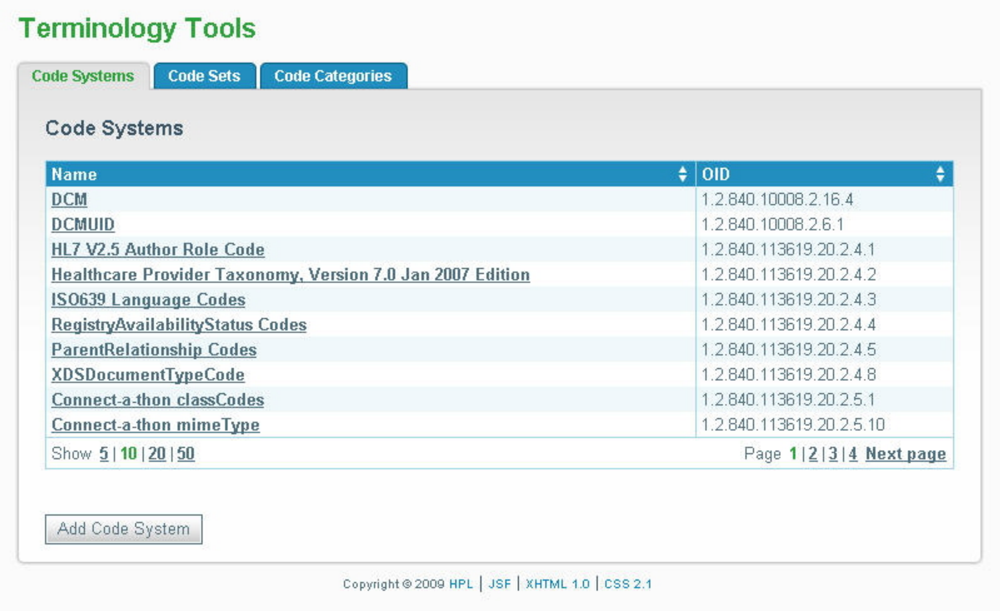
2.5.3 Code Systems

In this tab you can add or edit Code Systems and their Codes.

2.5.3.1 Add a Code System

1. Select the *Code System* tab.

   ⇨ A page with the available Code Systems opens.



Terminology Tools

Code Systems

Name	OID
DCM	1.2.840.10008.2.16.4
DCMUID	1.2.840.10008.2.6.1
HL7 V2.5 Author Role Code	1.2.840.113619.20.2.4.1
Healthcare Provider Taxonomy, Version 7.0 Jan 2007 Edition	1.2.840.113619.20.2.4.2
ISO639 Language Codes	1.2.840.113619.20.2.4.3
RegistryAvailabilityStatus Codes	1.2.840.113619.20.2.4.4
ParentRelationship Codes	1.2.840.113619.20.2.4.5
XDSDocumentTypeCode	1.2.840.113619.20.2.4.8
Connect-a-thon classCodes	1.2.840.113619.20.2.5.1
Connect-a-thon mimeType	1.2.840.113619.20.2.5.10
Show 5 | 10 | 20 | 50	Page 1 | 2 | 3 | 4 Next page

Copyright © 2009 HPL | JSF | XHTML 1.0 | CSS 2.1

Figure 18: Default Code Systems list

2. Click **Add Code System**.

   ⇨ The *Add New Code Systems* page opens.

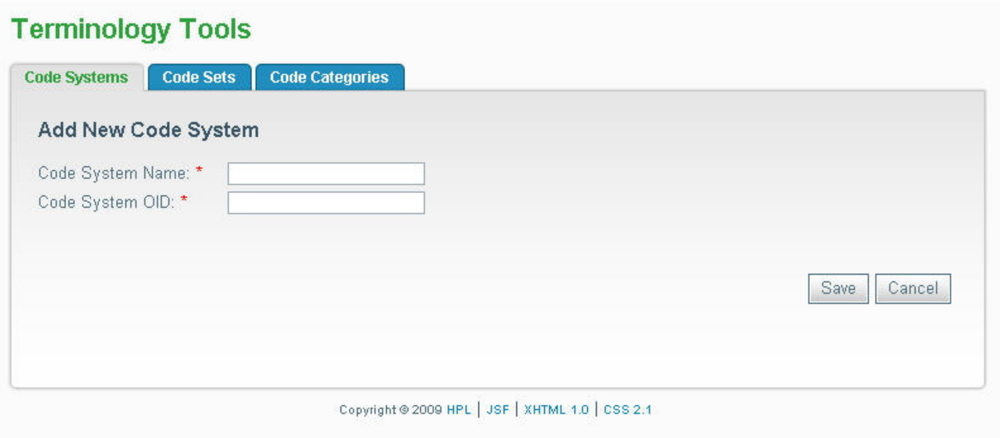


Figure 19: Add New Code System page

3. Enter a unique Code System name in the Code System Name field. This field is mandatory.
4. Enter a unique Code System OID in the Code System OID field. This field is mandatory.

NOTE **Validation Rules**

Code System Name is mandatory and must be unique across the system. Code System OID is mandatory and must be unique across the system.

5. Click **Save**.

   ⇨ The Code System is saved and the Code System list page will be redisplayed. You can navigate through the list to find the newly addedd Code System.

2.5.3.2 Add a Code

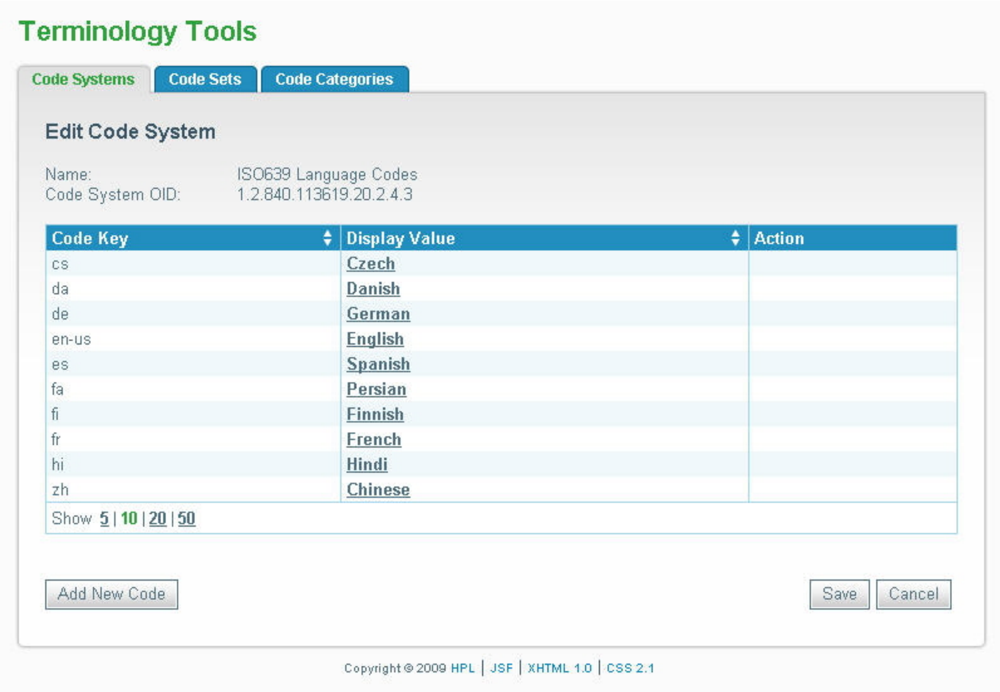
Existing Code Systems can be extended by adding a new Code.

1. Select the *Code System* tab.

   ⇨ The list of currently configured Code Systems is displayed.

2. Select the Code System <*Name*> to add a Code to the Code System.
   The Code System <*Name* > is a link that opens the *Edit Code System* page.

   ⇨ The Codes assigned to the Code System are displayed.



Edit Code System

Name: ISO639 Language Codes
Code System OID: 1.2.840.113619.20.2.4.3

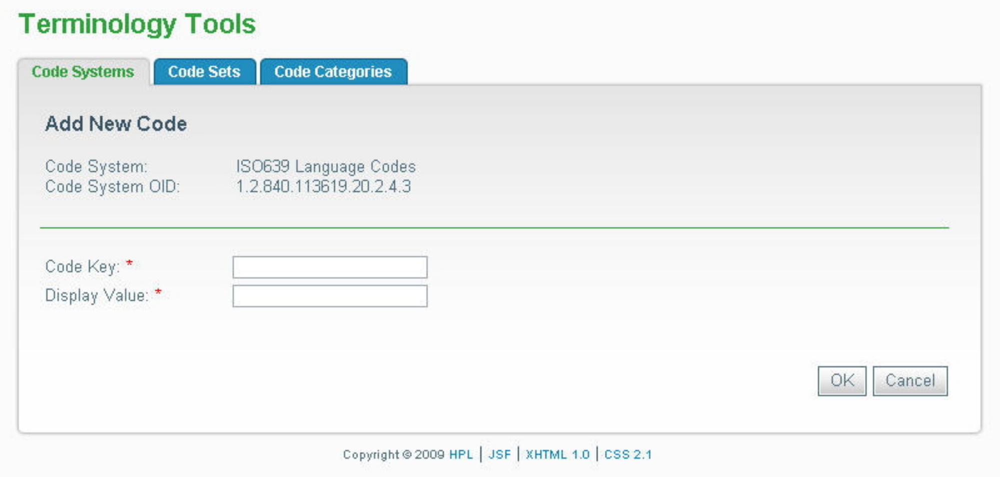
Code Key	Display Value	Action
cs	Czech	
da	Danish	
de	German	
en-us	English	
es	Spanish	
fa	Persian	
fi	Finnish	
fr	French	
hi	Hindi	
zh	Chinese	

Show 5 | 10 | 20 | 50

Figure 20: Edit Code System page

3. Click **Add New Code**.

⇨ The **Add New Code** page is displayed.



Add New Code

Code System: ISO639 Language Codes
Code System OID: 1.2.840.113619.20.2.4.3

Code Key: *
Display Value: *

Figure 21: Add New Code page

4. Enter a Code in the Code Key field that is unique for the Code System. This field is mandatory.
5. Enter a Display Value in the Display Value field. This field is mandatory.

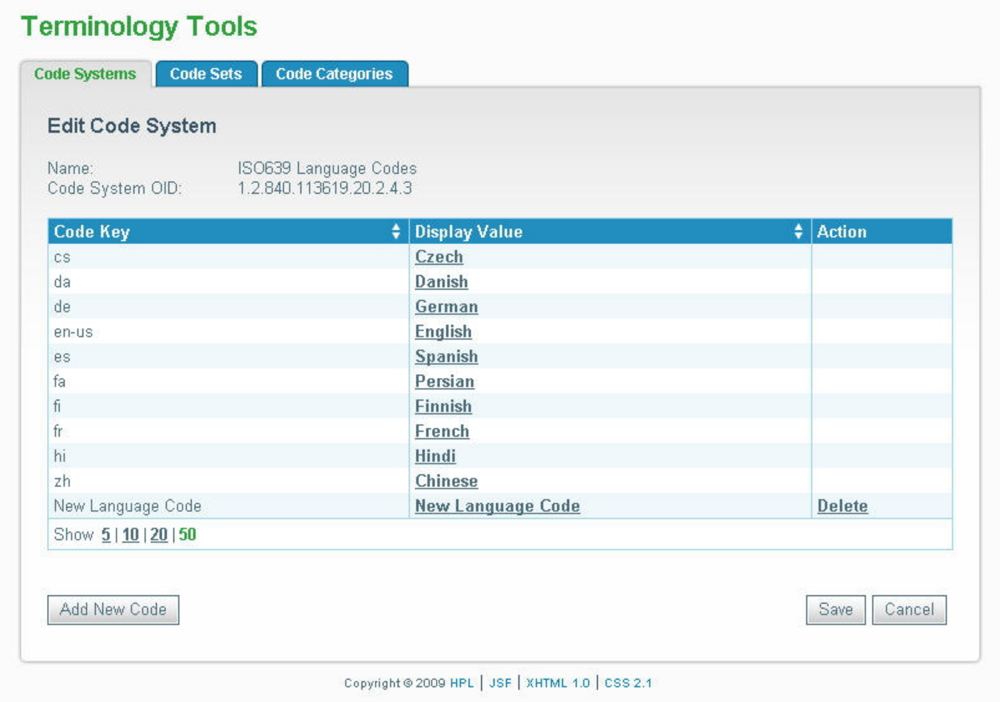
NOTE **Validation Rules**

The *Code Key* is mandatory and must be unique within the Code System. The following characters should not be used in the Code Key field: single quote (**'**), ampersand (**&**), angle brackets(**< >**), backslash (****) or forward slash (**/**). Using them leads to difficulties in the message exchange.

A *Display Value* is also mandatory

6. Click the **OK** button.

⇨ The Code will be temporarily added to the Code System and the *Edit Code System* page will be redisplayed, with the newly added Code. The new Code is displayed at the end of the list. In the **Action** column an action is displayed that can be performed on it.



Edit Code System

Name: ISO639 Language Codes
Code System OID: 1.2.840.113619.20.2.4.3

Code Key	Display Value	Action
cs	Czech	
da	Danish	
de	German	
en-us	English	
es	Spanish	
fa	Persian	
fi	Finnish	
fr	French	
hi	Hindi	
zh	Chinese	
New Language Code	New Language Code	Delete

Show 5 | 10 | 20 | 50

Figure 22: Code System with newly added Code

⇨ The Code has not yet been saved as part of the Code Set yet. Hence, it can be deleted by clicking **Delete** in the **Action** column.

7. To save the new Code permanently as part of the Code Set click **Save**.

⇨ The new Code will be saved as assigned to the Code System. The Code System list page will be displayed

2.5.3.3 Modify an Existing Code

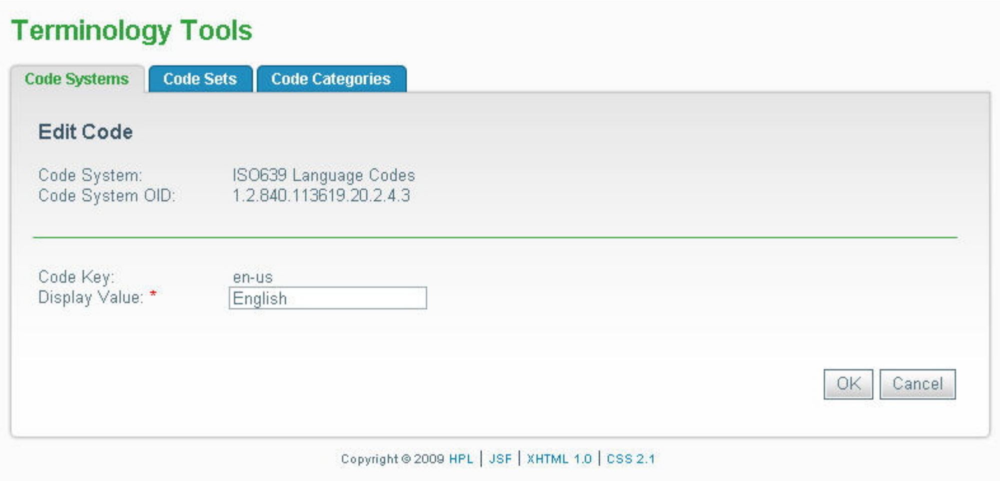
1. Select the *Code Systems* tab.

   ⇨ The list of currently configured Code Systems is displayed.

2. Select the Code System <*Name*>. The Code System <*Name*> is a link that will open the *Edit Code System* page and display all Codes assigned to the Code System.

3. Select the Code you want to modify by selecting the appropriate **Display Value** link from the list of Codes.

   ⇨ The **Edit Code** page is displayed.



Terminology Tools

Edit Code

Code System: ISO639 Language Codes
Code System OID: 1.2.840.113619.20.2.4.3

Code Key: en-us
Display Value: * English

Figure 23: The Edit Code page

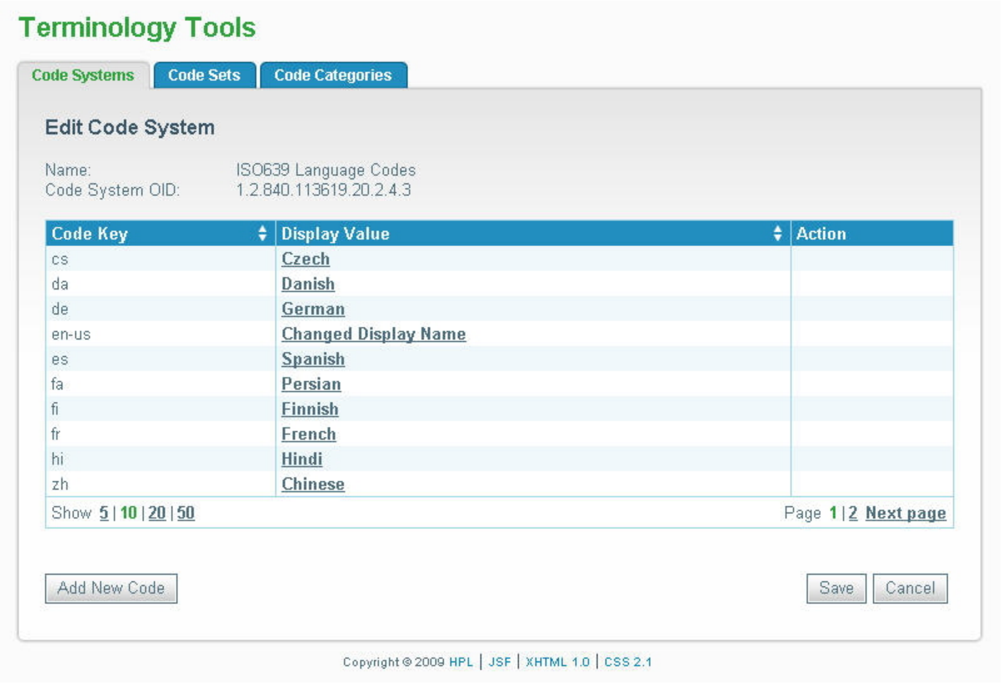
4. Enter a new value in the **Display Value** field. This field is mandatory.

   NOTE

   Only the *Display Value* field is editable. The *Code Key* field is static.

5. Click **OK**.

   ⇨ The Code Display Value will be temporarily changed for the Code System and the *Edit Code System* page will be redisplayed including the modification.



Edit Code System

Name: ISO639 Language Codes
Code System OID: 1.2.840.113619.20.2.4.3

Code Key	Display Value	Action
cs	Czech	
da	Danish	
de	German	
en-us	Changed Display Name	
es	Spanish	
fa	Persian	
fi	Finnish	
fr	French	
hi	Hindi	
zh	Chinese	

Figure 24: Edit Code System with Modified Code Display Name

⇨ The change of the *Code display name* has not yet been saved to the database. If you click on the *Cancel* button or navigate to one of the other tabs, your modification is not saved. The changes are lost.

6. Click the **Save** button change the Code permanently.

⇨ The Code System list page will be displayed.

2.5.3.4 Read-Only Code Systems

There can be a configured set of Code Systems, which are designated as **Read-Only**. In this case, the Code System may only be viewed and not edited. Additionally, any Codes, which are assigned to the Code System, are also designated as **Read-Only** and may only be viewed.

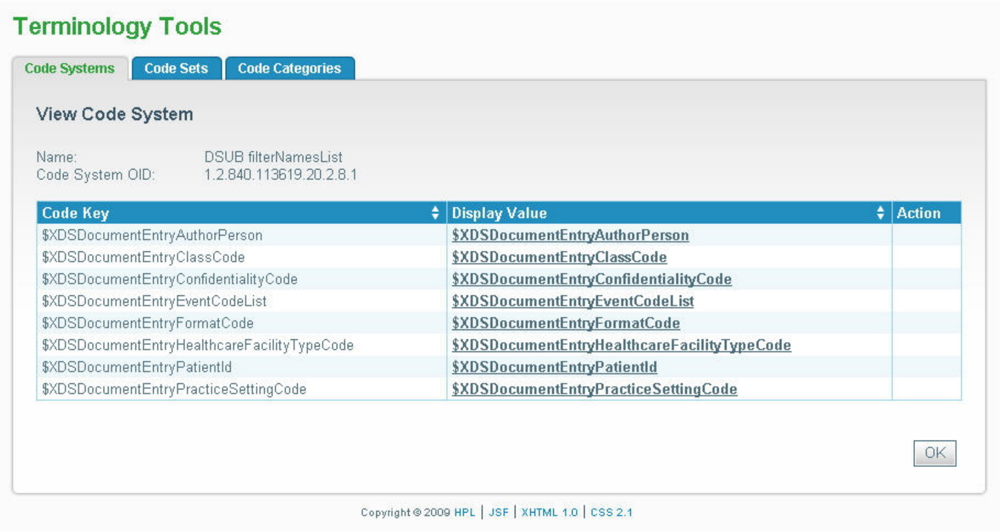
Here is an example flow of events for this particular case:

1. Select the **Code System** tab.

⇨ The list of currently configured Code Systems is displayed.

2. Select a Code System <*Name*> which belongs to an OID that is configured as Read-Only. The Code System <*Name*> is a link that will open the *Edit Code System* page and display all Codes assigned to the Code System.

⇨ The *View Code System* page is displayed. Note there is no button to allow a new Code to be created for the Code System.



Terminology Tools

View Code System

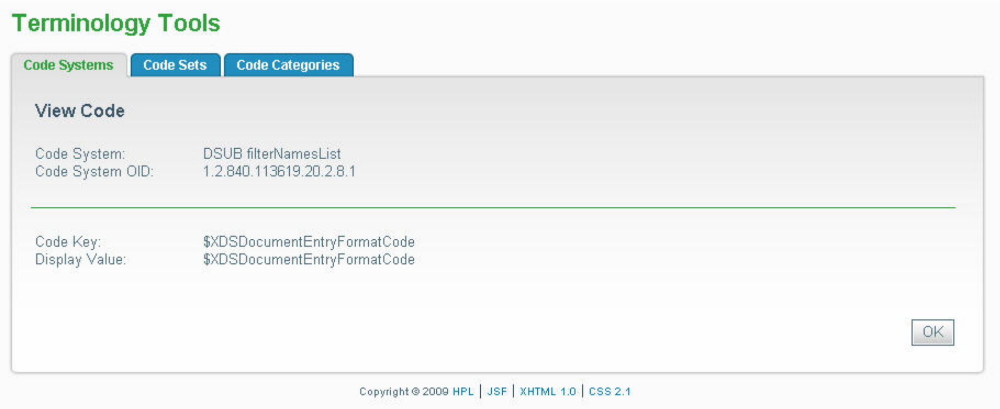
Name: DSUB filterNamesList
Code System OID: 1.2.840.113619.20.2.8.1

Code Key	Display Value	Action
$XDSDocumentEntryAuthorPerson	$XDSDocumentEntryAuthorPerson	
$XDSDocumentEntryClassCode	$XDSDocumentEntryClassCode	
$XDSDocumentEntryConfidentialityCode	$XDSDocumentEntryConfidentialityCode	
$XDSDocumentEntryEventCodeList	$XDSDocumentEntryEventCodeList	
$XDSDocumentEntryFormatCode	$XDSDocumentEntryFormatCode	
$XDSDocumentEntryHealthcareFacilityTypeCode	$XDSDocumentEntryHealthcareFacilityTypeCode	
$XDSDocumentEntryPatientId	$XDSDocumentEntryPatientId	
$XDSDocumentEntryPracticeSettingCode	$XDSDocumentEntryPracticeSettingCode	

Figure 25: Read-Only Code Systems View

3. Select a Code's **Display Value** from the list.

⇨ The *View Code* page is displayed, and the details of the selected Code Key are shown. Note the Code is treated as **Read-Only**.



Terminology Tools

View Code

Code System: DSUB filterNamesList
Code System OID: 1.2.840.113619.20.2.8.1

Code Key: $XDSDocumentEntryFormatCode
Display Value: $XDSDocumentEntryFormatCode

Figure 26: Read-Only Code in Code System View

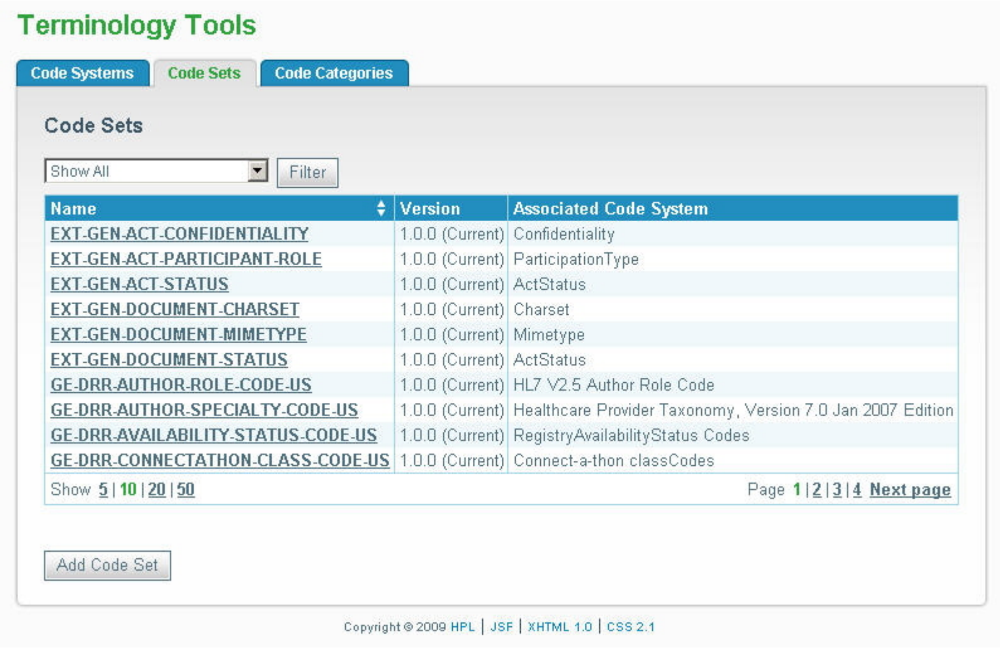
2.5.4 Code Sets

The *Code Sets* tab lets you add and edit Code Sets. A Filter on the Code Sets page allows you show all Code Sets or to only have current Code Sets displayed.

2.5.4.1 Add a Code Set

1. Select the **Code Set** tab.

⇨ The list of currently configured Code Sets is displayed



Terminology Tools

Code Sets

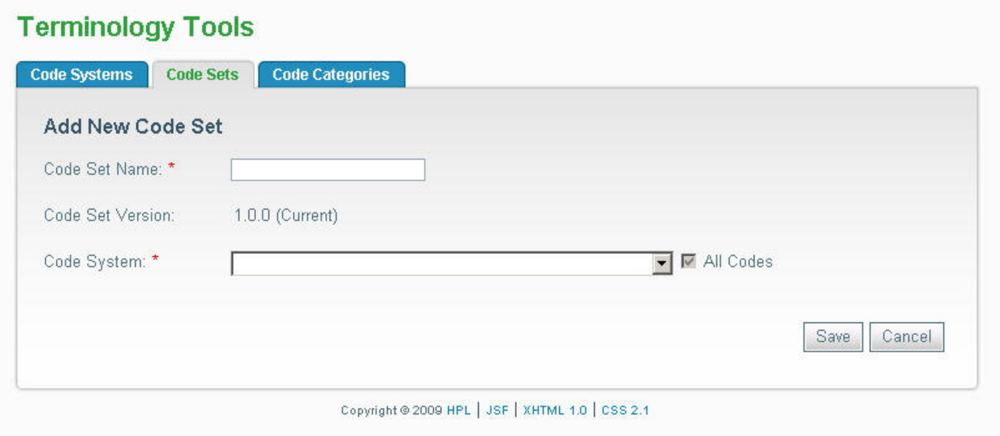
Name	Version	Associated Code System
EXT-GEN-ACT-CONFIDENTIALITY	1.0.0 (Current)	Confidentiality
EXT-GEN-ACT-PARTICIPANT-ROLE	1.0.0 (Current)	ParticipationType
EXT-GEN-ACT-STATUS	1.0.0 (Current)	ActStatus
EXT-GEN-DOCUMENT-CHARSET	1.0.0 (Current)	Charset
EXT-GEN-DOCUMENT-MIMETYPE	1.0.0 (Current)	Mimetype
EXT-GEN-DOCUMENT-STATUS	1.0.0 (Current)	ActStatus
GE-DRR-AUTHOR-ROLE-CODE-US	1.0.0 (Current)	HL7 V2.5 Author Role Code
GE-DRR-AUTHOR-SPECIALTY-CODE-US	1.0.0 (Current)	Healthcare Provider Taxonomy, Version 7.0 Jan 2007 Edition
GE-DRR-AVAILABILITY-STATUS-CODE-US	1.0.0 (Current)	RegistryAvailabilityStatus Codes
GE-DRR-CONNECTATHON-CLASS-CODE-US	1.0.0 (Current)	Connect-a-thon classCodes

Show 5 | 10 | 20 | 50
Page 1 | 2 | 3 | 4 Next page
Add Code Set
Copyright © 2009 HPL | JSF | XHTML 1.0 | CSS 2.1

Figure 27: Code Sets List

2. Click **Add Code Set**.

⇨ The **Add New Code Set** page is displayed



Terminology Tools

Add New Code Set

Code Set Name: *

Code Set Version: 1.0.0 (Current)

Code System: * ☑ All Codes

Figure 28: Add New Code Set

3. Enter a unique Code Set name in the **Code Set Name** field. This field is mandatory.
4. Select a **Code System** from the list. This field is mandatory.

NOTE **Validation Rules**

A *Code Set Name* is necessary and must be unique.

A Code System must be selected.

By default, the *All Codes* checkbox is selected and disabled. This indicates that the *Code Set* will contain all Codes from the Code System.

NOTE

This behavior conforms to the constraint imposed by the Terminology authoring API which requires at least one Code to be selected. Thus, by default all Codes in the Code System will be included in the Code Set when a Code Set is added. To deselect a Code (indicating it will not be included in the Code Set) edit the *Code Set* from the *Code Set list* view page. See Add/Remove Codes in a Code Set [page 53].

5. Click **Save**.

   ⇨ The *Code Set* will be saved and the *Code Set list page* will be redisplayed. You can navigate through the list to find the newly created Code Set.

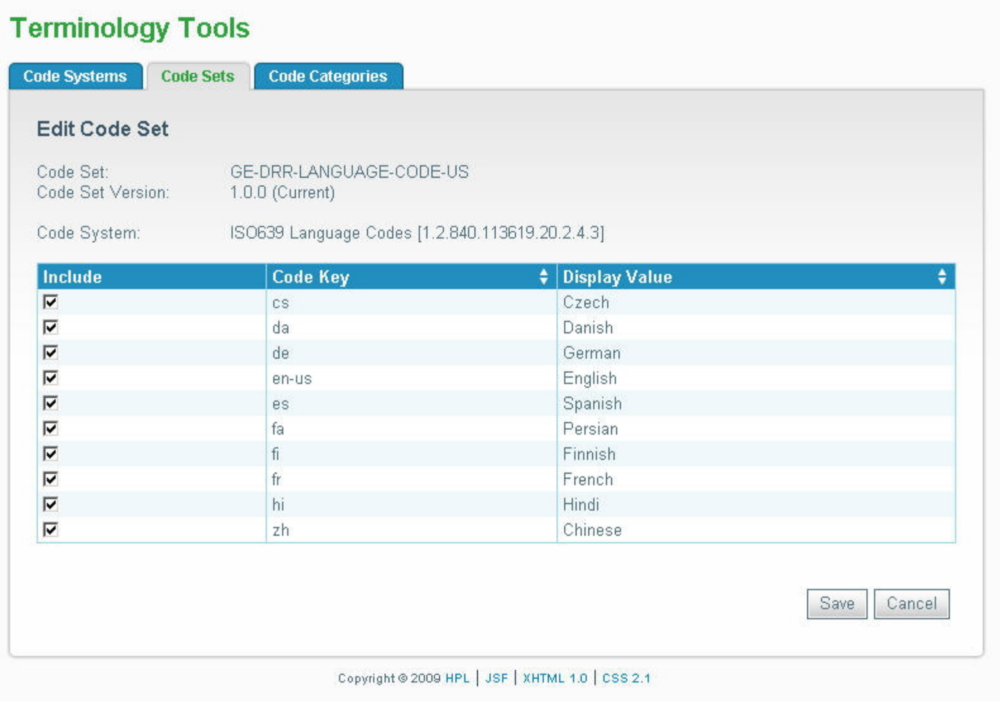
2.5.4.2 Add/Remove Codes in a Code Set

1. Select the *Code Sets* tab.

   ⇨ The list of currently configured Code Sets is displayed.

2. Select the Code Set to modify by clicking the appropriate **<<Name>>** link. Note that only Codes Sets marked as the **Current** version can be modified. A Code Set, which is not current, can only be viewed.

   ⇨ The *Edit Code Set* page is displayed.



Edit Code Set

Code Set: GE-DRR-LANGUAGE-CODE-US
Code Set Version: 1.0.0 (Current)

Code System: ISO639 Language Codes [1.2.840.113619.20.2.4.3]

Include	Code Key	Display Value
☑	cs	Czech
☑	da	Danish
☑	de	German
☑	en-us	English
☑	es	Spanish
☑	fa	Persian
☑	fi	Finnish
☑	fr	French
☑	hi	Hindi
☑	zh	Chinese

Copyright © 2009 HPL | JSF | XHTML 1.0 | CSS 2.1

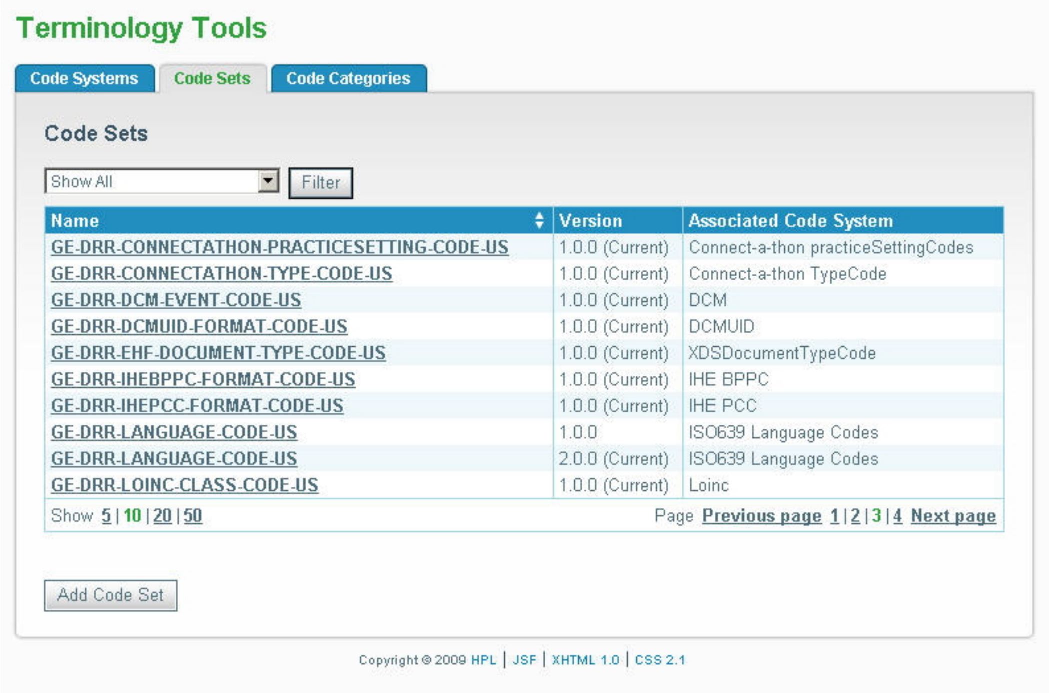
Figure 29: Edit Code Set

3. Select the appropriate **Include** checkbox to add a Code to the Code Set.

- To remove a Code from the Code set deselect the appropriate **Include** check-box.

4. Click the **Save** button.

⇨ The *Code Sets* page is redisplayed. It includes the new version of the Code Set (Current).



Terminology Tools

Code Sets

Name	Version	Associated Code System
GE-DRR-CONNECTATHON-PRACTICESETTING-CODE-US	1.0.0 (Current)	Connect-a-thon practiceSettingCodes
GE-DRR-CONNECTATHON-TYPE-CODE-US	1.0.0 (Current)	Connect-a-thon TypeCode
GE-DRR-DCM-EVENT-CODE-US	1.0.0 (Current)	DCM
GE-DRR-DCMUID-FORMAT-CODE-US	1.0.0 (Current)	DCMUID
GE-DRR-EHF-DOCUMENT-TYPE-CODE-US	1.0.0 (Current)	XDSDocumentTypeCode
GE-DRR-IHEBPPC-FORMAT-CODE-US	1.0.0 (Current)	IHE BPPC
GE-DRR-IHEPCC-FORMAT-CODE-US	1.0.0 (Current)	IHE PCC
GE-DRR-LANGUAGE-CODE-US	1.0.0	ISO639 Language Codes
GE-DRR-LANGUAGE-CODE-US	2.0.0 (Current)	ISO639 Language Codes
GE-DRR-LOINC-CLASS-CODE-US	1.0.0 (Current)	Loinc

Show 5 | 10 | 20 | 50 Page Previous page 1 | 2 | 3 | 4 Next page

Copyright © 2009 HPL | JSF | XHTML 1.0 | CSS 2.1

Figure 30: Edit Code Set - Code Set with multiple versions

NOTE **Validation Rules**

At least one Code Key must be selected, from the **Include** column, before the Code Set changes can be saved.

Only the current version of a specific Code Set can be edited. All other versions of a Code Set can only be viewed.

2.5.4.3 Code Set Versioning

When a Code Set is first created, it is versioned as 1.0.0 and marked as the *Current* Code Set. A new version of the Code Set is created when saving changes.

1. Select the **Code Sets** tab.

   ⇨ The list of currently configured Code Sets is displayed.

2. Edit the Code Set that needs to be modified.

   ⇨ The new version will be marked as the Current version of the Code Set. The previous version will also be updated so it no longer is marked as Current.

The versioning of Code Sets follows these guidelines:

- Update the major version if a code is removed from the Code Set (for example, from 1.0.0 to 2.0.0)
- Update the minor version if codes are only added to the Code Set (for example, from 1.0.0 to 1.1.0)
- The last digit is unused and should always be zero – it is reserved for future functionality.

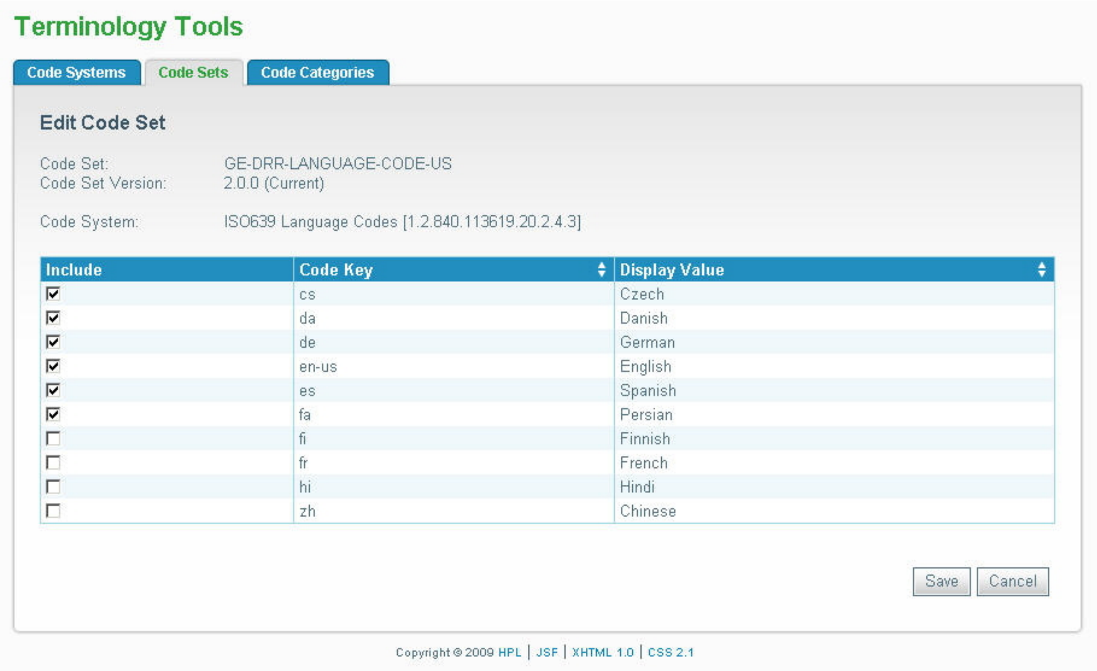
NOTE **Codes removed and added during the same transaction**

If codes are removed and added during the same transaction, then two new versions will be created. This is because the Terminology authoring APIs are not able to handle a single request with both removal and addition of Codes. Thus, Two separate Terminology authorization requests must be made, and two versions will be created.

Codes removed and added during the same transaction

The behavior is as follows:

Starting with a Code Set as identified in the screen shot below. See Figure: Edit Code Set Example (Starting point). There is a combination of assigned and unassigned Codes. Version 2.0.0. is the Current version.



Edit Code Set

Code Set: GE-DRR-LANGUAGE-CODE-US
Code Set Version: 2.0.0 (Current)

Code System: ISO639 Language Codes [1.2.840.113619.20.2.4.3]

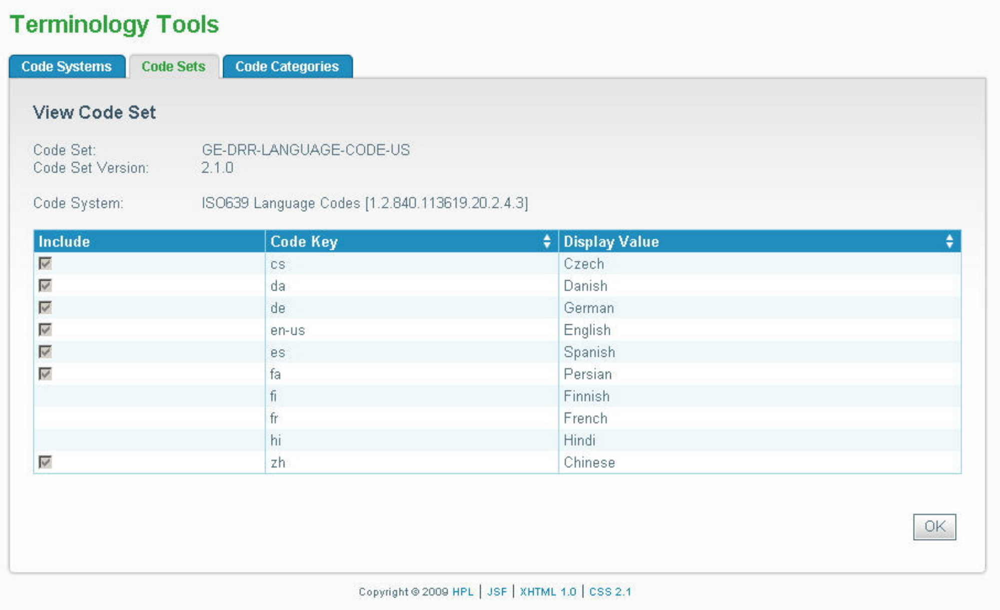
Include	Code Key	Display Value
☑	cs	Czech
☑	da	Danish
☑	de	German
☑	en-us	English
☑	es	Spanish
☑	fa	Persian
☐	fi	Finnish
☐	fr	French
☐	hi	Hindi
☐	zh	Chinese

Figure 31: Edit Code Set Example (Starting point)

On the *Edit Code Set* page perform the following:

1. Deselect Code Key **cs**
2. Select Code Key **zh**
3. Click **Save**.

⇨ Two new versions of the Code Set are created:
Version 2.1.0 for the added Code *zh*



Terminology Tools

View Code Set

Code Set: GE-DRR-LANGUAGE-CODE-US
Code Set Version: 2.1.0

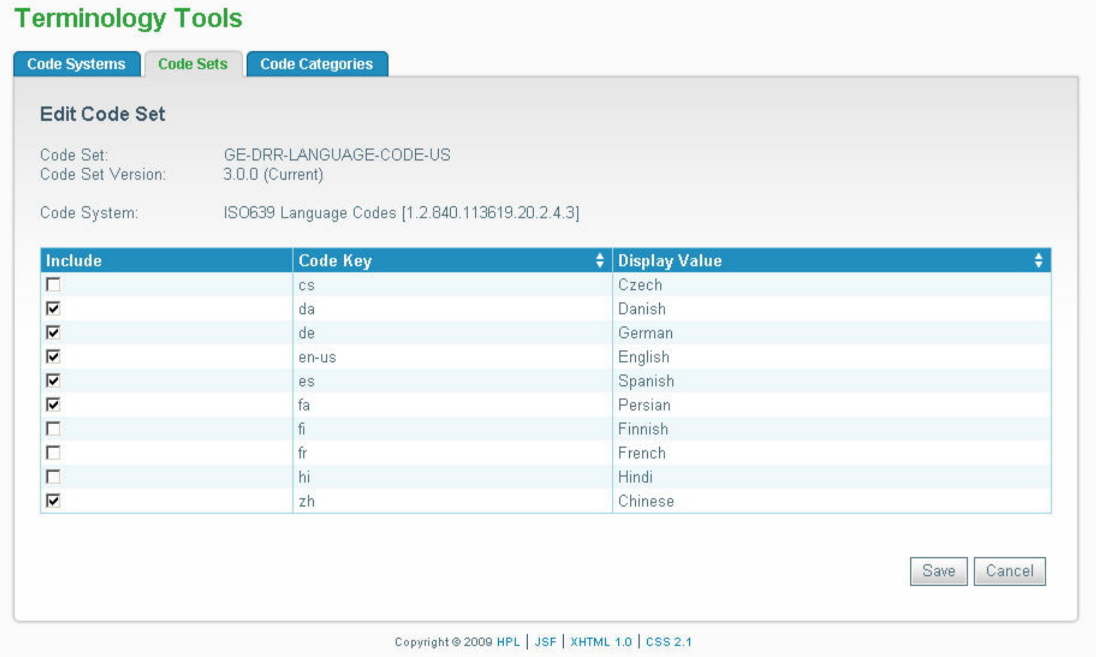
Code System: ISO639 Language Codes [1.2.840.113619.20.2.4.3]

Include	Code Key	Display Value
☑	cs	Czech
☑	da	Danish
☑	de	German
☑	en-us	English
☑	es	Spanish
☑	fa	Persian
	fi	Finnish
	fr	French
	hi	Hindi
☑	zh	Chinese

Copyright © 2009 HPL | JSF | XHTML 1.0 | CSS 2.1

Figure 32: Edit Code Set Example (Version 2.1.0 created)

Version 3.0.0 for the removed Code *cs*. This version is marked as the *Current* Code Set.



Edit Code Set

Code Set: GE-DRR-LANGUAGE-CODE-US
Code Set Version: 3.0.0 (Current)

Code System: ISO639 Language Codes [1.2.840.113619.20.2.4.3]

Include	Code Key	Display Value
□	cs	Czech
☑	da	Danish
☑	de	German
☑	en-us	English
☑	es	Spanish
☑	fa	Persian
□	fi	Finnish
□	fr	French
□	hi	Hindi
☑	zh	Chinese

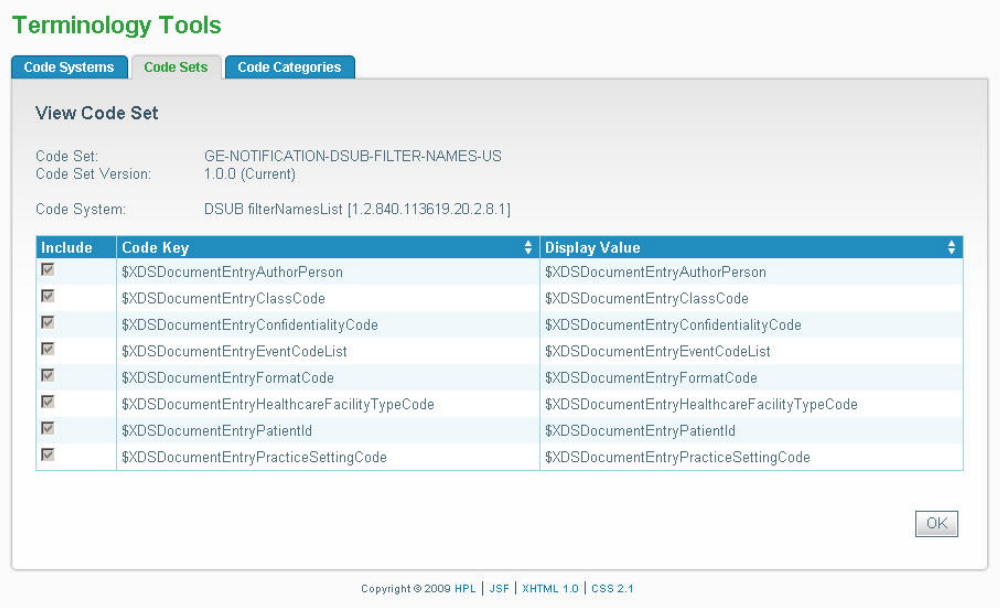
Figure 33: Edit Code Set Example: Version 3.0.0 created

2.5.4.4 Read-Only Code Sets

There can be a configured set of Code Systems, which are designated as **Read-Only**. See [page 50] A Code Set that contains one of these Code Systems is also treated as **Read-Only**. The Code Set version will be marked **Current** as version 1.0.0 but can not be edited.

A Read-Only Code set is diplayed as follows:

1. Select the *Code Sets* tab.
   - ⇨ The list of currently configured Code Sets is displayed
2. Select a Code Set **<<Name>>** hyperlink from the list, whose associated Code System OID is configured as **Read-Only**.
   - ⇨ The *View Code Set* page is displayed.



View Code Set

Code Set: GE-NOTIFICATION-DSUB-FILTER-NAMES-US
Code Set Version: 1.0.0 (Current)

Code System: DSUB filterNamesList [1.2.840.113619.20.2.8.1]

Include	Code Key	Display Value
☑	$XDSDocumentEntryAuthorPerson	$XDSDocumentEntryAuthorPerson
☑	$XDSDocumentEntryClassCode	$XDSDocumentEntryClassCode
☑	$XDSDocumentEntryConfidentialityCode	$XDSDocumentEntryConfidentialityCode
☑	$XDSDocumentEntryEventCodeList	$XDSDocumentEntryEventCodeList
☑	$XDSDocumentEntryFormatCode	$XDSDocumentEntryFormatCode
☑	$XDSDocumentEntryHealthcareFacilityTypeCode	$XDSDocumentEntryHealthcareFacilityTypeCode
☑	$XDSDocumentEntryPatientId	$XDSDocumentEntryPatientId
☑	$XDSDocumentEntryPracticeSettingCode	$XDSDocumentEntryPracticeSettingCode

Copyright © 2009 HPL | JSF | XHTML 1.0 | CSS 2.1

Figure 34: Read Only Code Set View

Note the Codes cannot be selected or deselected from the *Include* column.

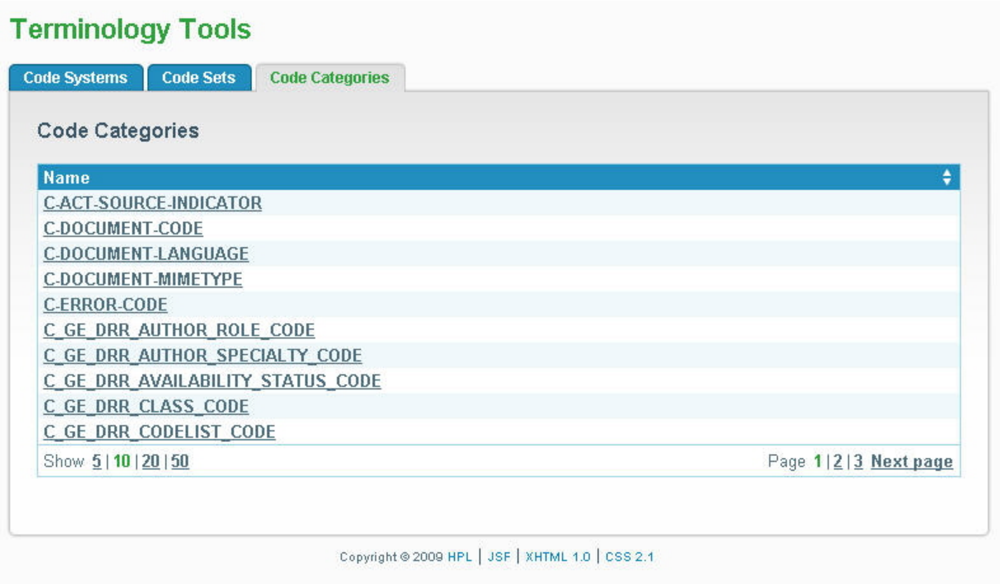
2.5.5 Code Category

The *Code Catgories* tab lets you edit Code Categories.

2.5.5.1 Assign a Code Set to a Code Category

1. Select the **Code Categories** tab.

   ⇨ The list of Code Categories is displayed.



Terminology Tools

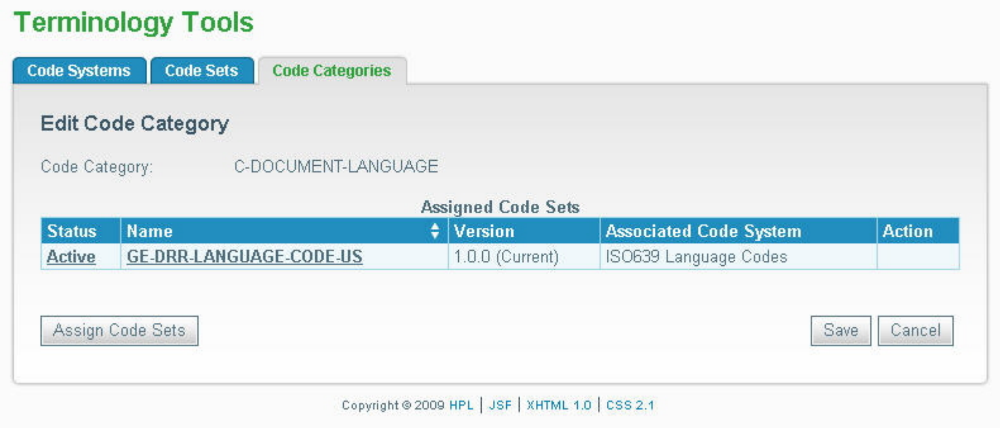
Code Categories

Name
C-ACT-SOURCE-INDICATOR
C-DOCUMENT-CODE
C-DOCUMENT-LANGUAGE
C-DOCUMENT-MIMETYPE
C-ERROR-CODE
C_GE_DRR_AUTHOR_ROLE_CODE
C_GE_DRR_AUTHOR_SPECIALTY_CODE
C_GE_DRR_AVAILABILITY_STATUS_CODE
C_GE_DRR_CLASS_CODE
C_GE_DRR_CODELIST_CODE

Figure 35: Code Categories list

2. Select the Code Category to add a Code to by selecting the appropriate <<**Name.**>>

   ⇨ The *Edit Code Category* page for the selected Code Category opens.



Terminology Tools

Edit Code Category

Code Category: C-DOCUMENT-LANGUAGE

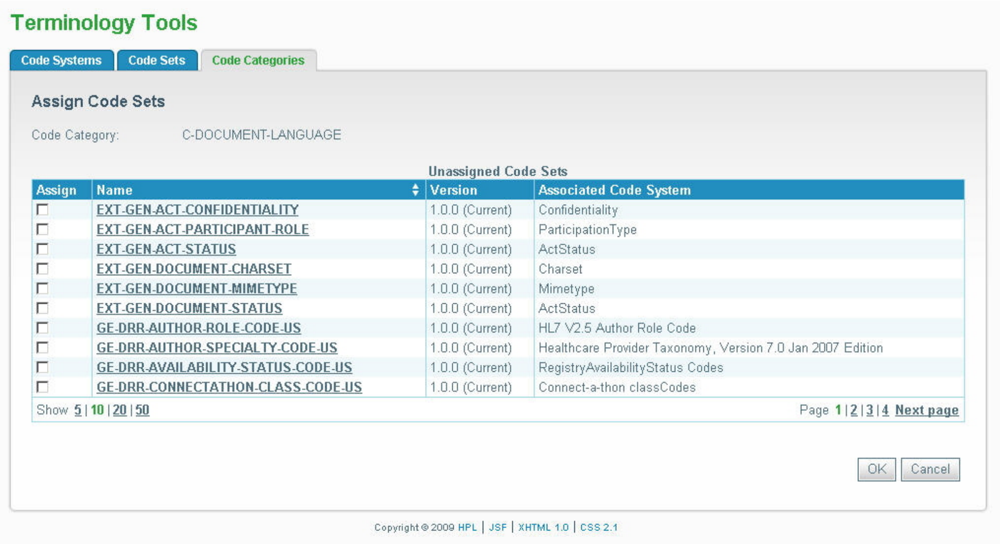
Assigned Code Sets

Status	Name	Version	Associated Code System	Action
Active	GE-DRR-LANGUAGE-CODE-US	1.0.0 (Current)	ISO639 Language Codes	

Figure 36: Edit Code Category

3. Click **Assign Code Sets**.
   Only current versions of a Code Set can be assigned to a Code Category.

   ⇨ The *Assign Code Sets* page opens.



Terminology Tools

Assign Code Sets

Code Category: C-DOCUMENT-LANGUAGE

Unassigned Code Sets

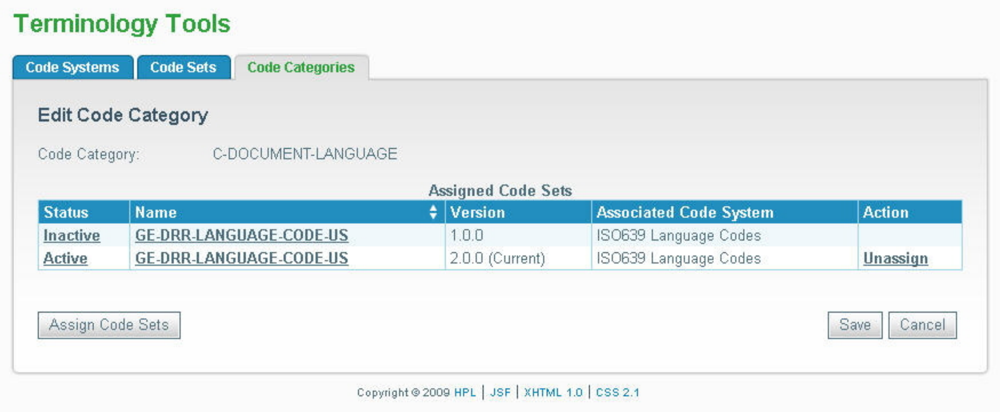
Assign	Name	Version	Associated Code System
□	EXT-GEN-ACT-CONFIDENTIALITY	1.0.0 (Current)	Confidentiality
□	EXT-GEN-ACT-PARTICIPANT-ROLE	1.0.0 (Current)	ParticipationType
□	EXT-GEN-ACT-STATUS	1.0.0 (Current)	ActStatus
□	EXT-GEN-DOCUMENT-CHARSET	1.0.0 (Current)	Charset
□	EXT-GEN-DOCUMENT-MIMETYPE	1.0.0 (Current)	Mimetype
□	EXT-GEN-DOCUMENT-STATUS	1.0.0 (Current)	ActStatus
□	GE-DRR-AUTHOR-ROLE-CODE-US	1.0.0 (Current)	HL7 V2.5 Author Role Code
□	GE-DRR-AUTHOR-SPECIALTY-CODE-US	1.0.0 (Current)	Healthcare Provider Taxonomy, Version 7.0 Jan 2007 Edition
□	GE-DRR-AVAILABILITY-STATUS-CODE-US	1.0.0 (Current)	RegistryAvailabilityStatus Codes
□	GE-DRR-CONNECTATHON-CLASS-CODE-US	1.0.0 (Current)	Connect-a-thon classCodes

Show 5 | 10 | 20 | 50
Page 1 | 2 | 3 | 4 Next page
OK
Cancel
Copyright © 2009 HPL | JSF | XHTML 1.0 | CSS 2.1

Figure 37: Assign Code Sets

4. Select all Code Sets that are to be assigned by selecting the checkbox in the **Assign** column.
5. Click **OK**.

⇨ The *Edit Code Category* page reopens and displays the newly assigned Code Sets.



Terminology Tools

Edit Code Category

Code Category: C-DOCUMENT-LANGUAGE

Assigned Code Sets

Status	Name	Version	Associated Code System	Action
Inactive	GE-DRR-LANGUAGE-CODE-US	1.0.0	ISO639 Language Codes	
Active	GE-DRR-LANGUAGE-CODE-US	2.0.0 (Current)	ISO639 Language Codes	Unassign

Figure 38: Newly Assigned Code Set to Code Category

NOTE **Change modes**

At this point the changes are only temporary. The newly assigned Code Sets will not be permanently assigned until you click **Save**.

6. Click the **Save** button to make the changes permanent .

⇨ The *Code Categories* list page is displayed.

7. Browse to the Code Category to verify the Code Set has been added.

If a more recent version of a Code Set is being added to the Code Category where an older version is already assigned, the older version of that Code Set will be marked as*Inactive*. Notice the newly added Code Set version is marked as *Active.*

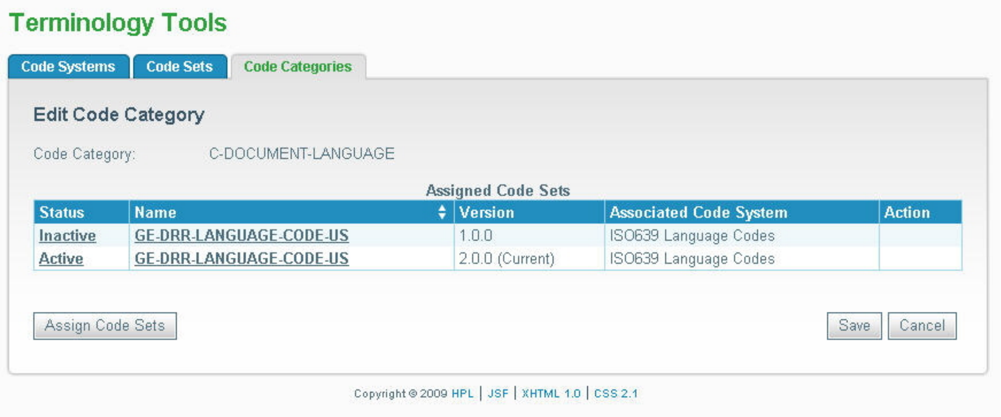
To un-assign a newly assigned Code Set, select the **Unassign** action for that Code Set. Once the *Save* button is clicked, the Code Set is permanently assigned to the Code Category.

NOTE **Validation Rules**

Only one version of a specific Code Set can be *Active* at any given time.
All other versions for that specific Code Set will be set to *Inactive* once a new current version is assigned.

2.5.5.2 Activate/Deactivate Code Sets in a Code Category

1. Select the *Code Categories* tab.
   ⇨ The list of Code Categories is displayed.
2. Select a Code Category by selecting the appropriate **<<Name>>** link.
   ⇨ The *Edit Code Category* page for the selected Code Category opens.



Edit Code Category

Code Category: C-DOCUMENT-LANGUAGE

Assigned Code Sets

Status	Name	Version	Associated Code System	Action
Inactive	GE-DRR-LANGUAGE-CODE-US	1.0.0	ISO639 Language Codes	
Active	GE-DRR-LANGUAGE-CODE-US	2.0.0 (Current)	ISO639 Language Codes	

Figure 39: Edit Code Category with multiple Code Sets

3. You have two options:
   - To deactivate a Code Set that is currently marked as Active, select the **Active link** for that Code Set.
     This will switch the status to Inactive
   - To activate a Code Set that is currently marked as Inactive, select the **Inactive link** for that Code Set.
     This will switch the status to Active. Also, any current Active status for other Code Sets will be toggled to Inactive.

NOTE **Change modes**

These changes are temporary until the *Save* button is clicked

4. Click the **Save** button to make your modification permanent.

   ⇨ The Code Categories list page is displayed.

5. Browse to the Code Category to verify the proper Code Set statuses have been saved.

NOTE **Validation Rules**

Only one version of a specific Code Set can be *Active* at any given time.

All other versions for that specific Code Set will be set to *Inactive* once a new current version is made *Active.*

3 Managing connected systems

This section describes the necessary steps to add and remove systems or change their integration with the Professional Exchange Server. It is based on the IHE actors that are relevant to the application. A system may group two or more actors, in which case the steps in the User Administration interface will be simpler.

3.1 Managing XDS Document Source systems

3.1.1 Connect a new XDS Document Source system to the application

3.1.1.1 Add user account for XDS Document Source

This step is only required for Document Sources that use the application's Document Repository. Other Document Sources will only communicate directly with their Document Repository and do not make connections to the Professional Exchange Server, unless they are grouped with other actors. If they are grouped with other actors, please see the appropriate sections of this document for instructions on how to add those actors.

Unless unauthenticated XDS access is supported in your Professional Exchange Server installation, the Document Source must identify itself to the application using either a certificate or a username and password. If the XDS Document Source supports certificates, it is strongly recommended to use certificate-based authentication.

3.1.1.1.1 Certificate-based authentication

When using the certificate-based authentication, you need to have a certificate for the XDS Document Source and the issuer’s CA certificate.

1. Go to the User Administration and create a new account. Use the certificate’s common name (CN) as the “certificate name” in the User Administration GUI.
2. Make sure to check the **system** checkbox.

After creating the account, you need to assign roles to the account. To act as an XDS Document Source, the system needs the role *XDS Register Documents*. If the actor is grouped with other actors, more roles may be appropriate. See the sections on the other actors for the role names.

If the client certificate’s issuer is not already represented in the CA truststore that the application uses, you need to retrieve the CA’s certificate and add it to the truststore. Please refer to the documentation of Sun’s keytool to learn more about how to add a certificate to a truststore. The application's truststore is located in the Tomcat folder under `webapps/<webapp_name>/WEB-INF/classes/META-INF/ca.keystore`. Please refer to the section on Making changes to the Tomcat folder [page 27] for instructions on how to modify this file safely.

3.1.1.1.2 Password-based authentication

If it is not possible to use certificate-based authentication, you will have to determine a password that is known in the XDS Document Source and in the Professional Exchange Server User Administration. The User Administration interface is only able to generate one-time passwords. Therefore a new permanent password will have to be added at a later time using the *change password* functionality.

1. Go to the User Administration interface and create a new account.
2. Do not yet check the *system* checkbox.
   ⇨ The system displays the generated one-time password.
3. Note the password and log out.
4. Log in again using the new user account with the one-time password.
5. Change the one time password to the new permanent password.
6. Log out again.
7. Log in as the administrator, search for and open the newly created user account.
8. Click **Modify** and then select the **System** checkbox.
9. Save the account and exit.
10. Go to the **Document Source system** and ensure that it uses the permanent password.

NOTE

The password expires after 90 days. At that point in time it is necessary to change the password in the User Administration interface (see the section on changing passwords for systems [page 104] for details) and in the XDS Document Source system.

3.1.1.1.3 No authentication

If the Document Source does not support client certificate authentication or password-based authentication, verify that the application was installed with support for unauthenticated XDS access. If the Professional Exchange Server was not installed with support for unauthenticated XDS access, please refer to the section on how to enable unauthenticated XDS access after the installation.

For Document Sources that use unauthenticated XDS access, you need to use a URL containing the `unsecured_webservices` string. For more information on the appropriate URL to use, see the section below.

3.1.1.2 Decide between enhanced and standard services

The enhanced services support Basic Patient Privacy Proof (BPPC) enforcement by default and can be configured to allow Metadata Injection (for details refer to the section on Metadata Injection [page 100]). The enhanced services should be selected for a Document Source if it is not grouped with a Document Consumer which supports the BPPC option. If the Document Source is grouped with such a consumer, it should verify that the patient agreed to publication of his documents (that is, Policies 1,3,4,5 in the section on Content Creators below) before executing a “Provide and Register Document Set-b” using the standard service.

The enhanced services use the same interface and messages as the standard services. They differ only in their processing.

3.1.1.3 Select the appropriate URL

There are four URLs that an XDS *Document* Source connected directly to the Professional Exchange Server may use:

Standard and authenticated *Provide and Register Document Set-b*:

`https://<host>[:<port>]/<webapp_name>/webservices/xdsb-provideandregister`

Standard and unauthenticated *Provide and Register Document Set-b*:

`https://<host>[:<port>]/<webapp_name>/unsecured_webservices/xdsb-provideandregister`

Enhanced and authenticated *Provide and Register Document Set-b*:

`https://<host>[:<port>]/<webapp_name>/webservices/security-xdsb-provideandregister`

Enhanced and unauthenticated *Provide and Register Document Set-b*:

`https://<host>[:<port>]/<webapp_name>/unsecured_webservices/security-xdsb-provideandregister`

3.1.1.4 Custom web service for withdrawing documents

Beyond these IHE-specified web services, there is also a custom web service that may be utilized by a Document Source to mark documents as "deprecated” without registering a replacement document. This web service can be reached under the following two URLs.

Authenticated *Withdraw Documents*:

```
https://<host>[:<port>]/<webapp_name>/webservices/WithdrawDocuments
```

Unauthenticated *Withdraw Documents*:

```
https://<host>[:<port>]/<webapp_name>/unsecured_webservices/WithdrawDocuments
```

An example message that uses the *Withdraw Documents* web service is shown below.

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:typ="http://gehcit.com/platform/cws/DocumentDirectory/types"
xmlns:cor="http://gehcit.com/platform/cws/types/coreMessageTypes">
<soapenv:Header/>
<soapenv:Body>
<typ:WithdrawDocumentsRequest>
<typ:patientId>
<cor:domainId>1.2.840.113619.20.2.1.2</cor:domainId>
<cor:idValue>9876</cor:idValue>
</typ:patientId>
<typ:sourceId>1.3.6.1.4.1.21367.2005.3.41</typ:sourceId>
<typ:reasonComment>Withdraw</typ:reasonComment>
<!--1 or more repetitions, contains the XDSDocumentEntry.uniqueId-->
<typ:documentId>4.1.2.4.1.3.19087.2008.5034.8821</typ:documentId>
</typ:WithdrawDocumentsRequest>
</soapenv:Body>
</soapenv:Envelope>
```

3.1.1.5 Adjust the Affinity Domain's XDS metadata restriction

Compare the Document Source's metadata settings with the Affinity Domain's and adjust either one or both as necessary. For more information on how to change the Affinity Domain's XDS metadata restrictions, please refer to the section on the Affinity Domain Metadata [page 105].

The Document Source must use the confidentiality codes that the Professional Exchange Server defines. There are three codes:

- N (normal)
- R (restricted)
- V (very restricted).

3.1.1.6 Connect CWEB viewer as a source system

The GE Centricity Enterprise Web DICOM viewer, is integrated by default in the Professional Exchange Server application. The CWEB DICOM Viewer is used to Show DICOM documents with the MIME-Type *application/dicom*, these are digital images, which include, for example, digital X-rays, magnetic resonance imaging and so on.

- The Professional Exchange Server application includes the CWEB DICOM Viewer as part of the standard installation, but it must be configured.
- The CWEB DICOM viewer can be configured using JConsole. First change to the directory `pxs-cweb-web/cWebHandlerJMX/Attributes`. There you'll find three attributes, which are filled with placeholders. These attributes can be configured as follows:
  - **CwebPage**: the URL used to call the CWEB DICOM Viewer, (for example, `http://<HOSTNAME.DOMAIN|IP>/ami`)
  - **User Name**: Name of the user.
  - **Password**: the user's password.

Note that, without this configuration, you cannot use the CWEB DICOM Viewer and therefore DICOM documents cannot be displayed.

If you have trouble viewing DICOM documents or if you would like to learn more about the configuring the CWEB DICOM Viewer you are referred to the Centricity Enterprise Web DICOM Viewer documentation.

3.1.2 Disconnect a XDS Document Source from the application

When an XDS Document Source is no longer a participant in the exchange, the following changes may be made.

You may want to disable the Document Source actor or completely remove the system. The correct approach depends on whether the system is a grouped actor with other functionality that is still required. For example, a system might have the capability to act as a Document Source and as a Document Repository. If you want to only use it as a Document Repository in the future, follow the instructions for disabling a Document Source actor. If you want to use neither the Document Source nor the Document Repository functionality of that system you can completely remove it.

3.1.2.1 Disabling a Document Source actor

Unless your installation uses unauthenticated XDS access, find the system's user account in the User Administration interface and remove the *XDS Register Documents* role. Skip this step if the other grouped actors still require this role (for example, Document Repositories use the same role).

Delete the *DocumentRegistrySource profile* of the corresponding system element in the organization registry.

3.1.2.2 Removing a Document Source system

Unless your installation uses unauthenticated XDS access, delete the system's user account or deactivate it. Please see the section Delete an account [page 39] for details on how to do this.

Delete the *DocumentRegistrySource profile* of the corresponding system element in the organization registry. Change the system's name according to your convention for labeling systems that are no longer needed.

3.2 Managing XDS Document Repository systems

3.2.1 Managing the application's internal XDS Document Repository

3.2.1.1 Activating the application's internal XDS Document Repository

To use the internal Professional Exchange Server repository in your affinity domain, you need to add a new system to the organization registry. The system's OID must be the identifier entered during Professional Exchange Server installation as the document repository OID. If you have entered an incorrect OID during installation or if you have used the default document repository OID, you must change the OID as described below.

Add a profile with the name *DocumentRepository* to the system. Add a property to this profile with the name *URL* and the value pointing to the internal Professional Exchange Server repository's web service:

```
<property name=”URL” value=”xds-
```

```
iti43://<pxs_host>[:<pxs_port>]/<webapp_name>/webservices/xdsb-
retrievedocuments?secure=true&amp;soap11=true” />
```

Example:

```
<property name=”URL” value=”xds-
iti43://somehost:8456/pxs/webservices/xdsb-
retrievedocuments?secure=true&amp;soap11=true” />
```

NOTE **Protocol handler**

Please note that the protocol handler must be “xds-iti43”, not http or https. When accessing documents that are stored in the internal repository through the Professional Exchange Server GUI, the URL property is disregarded in favor of direct access. Therefore, the URL property is currently not actively used in Professional Exchange Server in the standard product, but it might be used by custom developed modules/applications with access to the organization registry.

3.2.1.2 Deactivating the application's internal XDS Document Repository

The internal Professional Exchange Server document repository must not be deactivated after it has received documents through the “Provide and Register Document Set-b” transaction. If this was the case, you may only prohibit Document Sources from providing new documents by deactivating the direct connection from Document Sources to the Professional Exchange Server, as described in the section on deactivating XDS Document Sources above.

If the internal Professional Exchange Server Document Repository has not received any documents yet, you can deactivate it by removing the *DocumentRepository* profile from the corresponding system element in the organization registry.

3.2.1.3 Changing the OID of the application’s internal XDS Document Repository

The internal Professional Exchange Server Document Repository’s OID must not be changed after the repository has received documents. As specified by the IHE XDS profile, the document repository’s unique ID (OID) must not be changed: “The Document Repository id is considered immutable throughout the lifetime of the Document Repository to which it is associated.” (IHE ITI Technical Framework, Volume 3: 4.1.7.3)

If the internal Professional Exchange Server Document Repository has not received any documents, you may change its OID by changing the value for the property with the key “drr.repository.id” in the file `ehealth.properties` in the Tomcat `webapps\<webapp_name>\WEB-INF\classes\META-INF` folder. After changing this file, Tomcat must be restarted. How to change this value in a safe way is described in the sectionMaking changes to the Tomcat folder [page 27].

3.2.2 Connect a new XDS Document Repository system to the application

3.2.2.1 Adding an XDS Document Repository to the organization registry

1. Add a new system to the organization registry, unless the system already exists because it is a grouped actor. The system’s OID must be the OID used in the XDS messages in the `XDSDocumentEntry.repositoryUniqueId` field.
2. Add a profile with the name **DocumentRepository** to the system.
3. Add a property to this profile with the name **URL** and the value pointing to the Document Repository’s web service:

   ```
   <property value=” xds-iti43://<host>[:<port>]/<path to repository’s soap endpoint>?secure=true&amp;soap11=true” name=”URL” />
   ```

   Example:

   ```
   <property value=
   "xds-iti43://somehost:8543/repository/services/retrievedocumentset-b?secure=true&amp;soap11=true" name="URL" />
   ```

   NOTE

   The protocol handler must be “xds-iti43”, not http or https.

   The URL is used when a user attempts to access a document through the Professional Exchange Server GUI that is stored in the newly added Document Repository. In this case the Professional Exchange Server acts as a Document Consumer and initiates the *Retrieve Document Set* transaction.
   For details on adding a system to the organization registry, see the sections above.

3.2.2.2 Adding a user account for the XDS Document Repository

Unless unauthenticated XDS access is supported in your Professional Exchange Server installation, the Document Repository must identify itself towards the application using either a certificate or a username and password. If the XDS Document Repository supports certificates, it is strongly recommended to use certificate-based authentication.

3.2.2.2.1 Certificate-based authentication

▹ When using the certificate-based authentication, you need to have a certificate for the XDS Document Repository and the issuer's CA certificate.

1. Go to the User Administration interface and create a new account. Use the certificate's CN (common name) as the *Certificate name*in the Create Account page.
2. Make sure to check the *system* checkbox.
3. Assign roles to the account.
   To act as an XDS Document Repository, the system needs the role *XDS Register Documents*. If the actor is grouped with other actors, more roles may be appropriate. See the sections for the other actors for the role names.

If the client certificate's issuer is not already represented in the CA truststore that the application uses, you need to retrieve the CA's certificate and add it to the truststore.

Please refer to the documentation of Sun's keytool to learn more about how to add a certificate to a truststore.

The application's truststore is located in the Tomcat folder under `webapps/<webapp_name>/WEB-INF/classes/META-INF/ca.keystore`.

Please refer to the chapter on Making changes to the Tomcat folder [page 27] for instructions on how to modify this file safely.

3.2.2.2.2 Password-based authentication

If it is not possible to use certificate-based authentication, you will have to determine a password that is known in the XDS Document Repository and in the Professional Exchange Server User Administration. The User Administration GUI can only generate one-time passwords. Therefore the permanent password will have to be added at a later time using the *change password* functionality.

1. Go to the User Administration interface and create a new account.
2. Do not yet check the *system* checkbox.
   ⇨ The system displays the generated one-time password.
3. Note the password and log out.
4. Log in again using the new user account with the one-time password.
5. Change the one time password to the new permanent password. Log out again.
6. Log in as the administrator, search for and open the newly created user account.
7. Click **Modify** and then check the **System** checkbox.
8. Save the account and exit.
9. Go to the Document Repository system and ensure that it uses the permanent password.

NOTE

The password expires after 90 days. At that point in time it is necessary to change the password in the user administration GUI (see the section on changing passwords for systems [page 104] for details) and in the XDS Document Repository.

See also

- User Administration GUI [page 28]

3.2.2.2.3 No authentication

If the Document Repository does not support client certificate authentication or password-based authentication, verify that the Professional Exchange Server was installed with support for unauthenticated XDS access. If the Professional Exchange Server was not installed with support for unauthenticated XDS access, please refer to the section below on how to enable this after the installation.

For Document Repositories that use unauthenticated XDS access, you need to use a URL containing the `unsecured_webservices` string. For more information on the appropriate URL to use, see the section Select the appropriate URL [page 72].

3.2.2.3 Select the appropriate URL

There are two URLs that a XDS Document Repository connected to the Professional Exchange Server may use:

Authenticated *Register Document Set-b*:

```
https://<host>[:<port>]/<webapp_name>/webservices/xdsb-registerdocuments
```

Unauthenticated *Register Document Set-b*:

```
https://<host>[:<port>]/<webapp_name>/unsecured_webservices/xdsb-registerdocuments
```

There is no BPPC Enforcement support for the *Register Document Set-b* transaction.

3.2.2.4 Preparing the Document Repository for document retrieval

As explained above, the Professional Exchange Server acts as a Document Consumer and starts the *Retrieve Document Set* transaction when a user clicks on a document in the GUI that is stored in this repository. Please ensure that the Document Repository allows the Professional Exchange Server to establish the connection. The Professional Exchange Server uses the client certificate that was selected during installation for this purpose. You may need to add the client certificate's CA certificate to the target Document Repository's truststore. Please refer to the Document Repository's documentation for details on how to do this. If you need to change the client certificate, please refer to the chapter on changing certificate stores below.

NOTE

If unauthenticated access is possible and desired, the Document Repository's URL property in the organization registry can be changed to contain "`secure=false`" instead of "`secure=true`".

To change the client certificate that the Professional Exchange Server should use to make the connection, refer to the chapter on changing the client certificate store after installation.

3.2.2.5 Connect CWEB viewer as a repository system

The GE Centricity Enterprise Web DICOM viewer, is integrated by default in the Professional Exchange Server application. The CWEB DICOM Viewer is used to Show DICOM documents with the MIME-Type *application/dicom*, these are digital images, which include, for example, digital X-rays, magnetic resonance imaging and so on.

- The Professional Exchange Server application includes the CWEB DICOM Viewer as part of the standard installation, but it must be configured.
- The CWEB DICOM viewer can be configured using JConsole. First change to the directory `pxs-cweb-web/cWebHandlerJMX/Attributes`. There you'll find three attributes, which are filled with placeholders. These attributes can be configured as follows:
  - **CwebPage**: the URL used to call the CWEB DICOM Viewer, (for example, `http://<HOSTNAME.DOMAIN|IP>/ami`)
  - **User Name**: Name of the user.
  - **Password**: the user's password.

Note that, without this configuration, you cannot use the CWEB DICOM Viewer and therefore DICOM documents cannot be displayed.

If you have trouble viewing DICOM documents or if you would like to learn more about the configuring the CWEB DICOM Viewer you are referred to the Centricity Enterprise Web DICOM Viewer documentation.

3.2.3 Disconnect an XDS Document Repository from the application

When an XDS Document Repository is no longer a participant in the exchange, the following changes may be made.

You may want to disable the Document Repository actor or completely remove the system. The correct approach to take depends on whether the system is a grouped actor with other functionality that is still required. For example, a system might have the capability to act as a Document Source and as a Document Repository. If you want to use it only as a Document Source in the future, follow the instructions for disabling a Document Repository actor. If you do not want to use the Document Source or the Document Repository functionality of that system you can completely remove it.

3.2.3.1 Disabling a Document Repository actor

1. Unless your installation uses unauthenticated XDS access, find the system’s user account in the User Administration interface and remove the *XDS Register Documents* role. Skip this step if the other grouped actors still require this role (for example, document sources use the same role).

   ⇨ This will stop the Document Repository from registering new document meta data in the Professional Exchange Server Document Registry.

2. Delete the *DocumentRepository* profile of the corresponding system element in the organization registry.

   ⇨ All documents stored in this document repository are now inaccessible from the application's UI.

3.2.3.2 Removing a Document Repository system

1. Unless your installation uses unauthenticated XDS access, delete [page 39] the system’s user account or deactivate [page 38] it.

   ⇨ This will stop the Document Repository from registering new document metadata in the Professional Exchange Server Document Registry.

2. Delete the *DocumentRepository* profile of the corresponding system element in the organization registry.

3. Change the system’s name according to your convention for labeling systems as no longer needed.

   ⇨ All documents stored in this document repository will now be inaccessible from the application's UI.

3.3 Managing PIX Patient Identity Source systems

3.3.1 Adding PIX Patient Identity Source to organization registry

1. Add a new system to the organization registry, unless the system already exists because it is a grouped actor.
   The system's system-alias should be the *Sending Application* used in the PIX ITI-8 MSH-3 field.
   The system's parent organization's `<local-alias>` should be the *Sending Facility* used in the PIX ITI-8 MSH-4 field.
2. Add a **namespace** to the system.
   The root identifies the XDS Patient Identifier domain and must be the universal ID used in the PIX ITI-8 PID-3-4-2 field.
   As defined by the IHE XDS specification, the namespace must also define the *namespace ID* used in the PIX ITI-8 PID-3-4-1 field.
   As this is a namespace for patient objects, the namespace type must be set to **P**.
3. Add a profile with the name *XdsPatientIdentitySourceProfile* to the system.

> **NOTE**
>
> There may only be one PIX Patient Identity Source connected to the Professional Exchange Server and accordingly only one system with this profile in the organization registry.
> For details on adding a system to the organization registry, please refer to the section on The application's organization registry. [page 16]

3.3.2 Adding a user account for PIX Patient Identity Source

Unless unauthenticated MLLP (Minimal Lower Layer Protocol) access is supported in your Professional Exchange Server installation, the Patient Identity Source must identify itself to the application using a certificate. If the PIX Patient Identity Source supports certificates, it is strongly recommended to use certificate-based authentication.

3.3.2.1 Certificate-based authentication

- When using certificate-based authentication, you need to have a certificate for the PIX Patient Identity Source and the issuer's CA certificate.

1. Go to the User Administration interface and create a new account. Use the certificate's CN (common name) as the *Certificate name* in the Create Account page.

2. Make sure to check the `system` checkbox, otherwise MLLP access attempts will be rejected.
3. After creating the account, you need to assign roles to the account. To act as a PIX Patient Identity Source, the system needs the role *Patient Identity Source*.
   If the actor is grouped with other actors, more roles may be appropriate. See the sections on the other actors for the role names.

⇨ If the client certificate's issuer is not already represented in the CA truststore that the application uses, you need to retrieve the CA's certificate and add it to the truststore.
Please refer to the documentation of Sun's keytool to learn more about how to add a certificate to a truststore. The application's truststore is located in the Tomcat folder under `webapps/<webapp_name>/WEB-INF/classes/META-INF/ca.keystore`.
Please refer to the chapter on Making changes to the Tomcat folder [page 27] for instructions on how to modify this file safely.

3.3.2.2 No authentication

If the Document Repository does not support client certificate authentication, verify that the Professional Exchange Server was installed with support for unauthenticated MLLP access. If the Professional Exchange Server was not installed with support for unauthenticated MLLP access, please see below for how to enable this after the installation.

For a PIX Patient Identity Source that uses unauthenticated MLLP access, you need to use the port for unauthenticated MLLP communication. For more information on configuring the MLLP ports, see the section Configuring the Patient Import Interface [page 76].

3.3.3 Configuring the Patient Import Interface

The configuration of the Patient Import Interface consists of the port selection for MLLP and MLLP with TLS (Transport Layer Security). Currently they can only be configured during installation. The default encoding is ISO-8859-1. After the installation, it is possible to change the encoding of patient feed messages with the property `patient.import.module.mllp.encoding`. This property is located in `webapps/<webapp_name>/WEB-INF/classes/META-INF/deploy.properties`. Changes are applied after a restart of the web container. Possible values are charsets that are supported by the JAVA platform that is in use.

3.3.4 Disconnect a PIX Patient Identity Source

When a PIX Patient Identity Source is no longer a participant in the exchange, the following changes may be made.

You may want to disable the PIX Patient Identity Source actor or completely remove the system. The correct approach to take depends on whether the system is a grouped actor with other functionality that is still required. For example, a system might have the capability to act as a Document Source and as a Patient Identity Source. If you want to only use it as a Document Source in the future, follow the instructions for disabling a Patient Identity Source actor. If you want to use neither the Document Consumer nor the Patient Identity Source functionality of that system you can completely remove it.

3.3.4.1 Disabling a PIX Patient Identity Source actor

1. Unless your installation uses unauthenticated MLLP access, find the system's user account in the User Administration interface and remove the *Patient Identity Source* role.
2. Delete the *XdsPatientIdentitySourceProfile* profile of the corresponding system element in the organization registry.
3. If you are using a different system as the new Patient Identity Source, move the namespace for the XDS Patient Identifier Domain to the new patient identity source's representation.

3.3.4.2 Removing a PIX Patient Identity Source system

1. Unless your installation uses unauthenticated MLLP access, delete [page 39] the system's user account or deactivate [page 38] it.
2. Delete the *XdsPatientIdentitySourceProfile* profile of the corresponding system element in the organization registry.
3. If you are using a different system as the new Patient Identity Source, move the profile to the new patient identity source's representation.
4. Change the system's name according to your convention for labeling systems as no longer needed.

3.4 Managing XDS Document Consumer systems

3.4.1 Connect a new XDS Document Consumer system to the application

3.4.1.1 Add a user account for XDS Document Consumer

Unless unauthenticated XDS access is supported in the Professional Exchange Server installation, the Document Consumer must identify itself to the application using either a certificate or a username and password. If the XDS Document Consumer supports certificates, it is strongly recommended to use certificate-based authentication.

3.4.1.1.1 Certificate-based authentication

▹ When using certificate-based authentication, you need to have a certificate for the XDS Document Consumer and the issuer's CA certificate.

1. Go to the User Administration interface and create a new account. Use the certificate's CN (common name) as the *Certificate name* in the Create Account page.
2. Make sure to check the `system` checkbox, otherwise MLLP access attempts will be rejected.
3. After creating the account, you need to assign roles to the account. To act as an XDS Document Consumer, the system needs the roles *XDS Query Documents* and *XDS Retrieve Documents*.
   If the actor is grouped with other actors, more roles may be appropriate. See the sections on the other actors for the role names.

⇨ If the client certificate's issuer is not already represented in the CA truststore that the application uses, you need to retrieve the CA's certificate and add it to the truststore.
Please refer to the documentation of Sun's keytool to learn more about how to add a certificate to a truststore. The application's truststore is located in the Tomcat folder under `webapps/<webapp_name>/WEB-INF/classes/META-INF/ca.keystore`.
Please refer to the chapter on Making changes to the Tomcat folder [page 27] for instructions on how to modify this file safely.

3.4.1.1.2 Password-based authentication

If it is not possible to use certificate-based authentication, you will have to determine a password that is known in the XDS Document Repository and in the Professional

Exchange Server User Administration. The User Administration interface can only generate one-time passwords. Therefore, the permanent password will have to be added at a later time using the *change password* functionality.

1. Open the User Administration interface and create a new account.
2. Do not check the **system** checkbox.
   ⇨ The system displays the generated one-time password.
3. Note the password and log out.
4. Log in again using the new user account with the one-time password.
5. Change the one time password to the new permanent password. Log out again.
6. Log in as an **administrator**, search for and open the newly created user account.
7. Click **Modify** and then select the **System** checkbox.
8. Save the account and exit.
9. Go to the XDS Document Repository system and ensure that it uses the permanent password.

NOTE

The password expires after 90 days. At that point in time it is necessary to change the password in the User Administration interface (see the section on changing passwords for systems [page 104] for details) and in the XDS Document Repository.

See also

- User Administration GUI [page 28]

3.4.1.1.3 No authentication

If the Document Consumer does not support client certificate authentication or password-based authentication, verify that the Professional Exchange Server was installed with support for unauthenticated XDS access. If the Professional Exchange Server was not installed with support for unauthenticated XDS access, please refer to the section on enabling unauthenticated XDS access after the installation.

For Document Consumer that use unauthenticated XDS access, you need to use a URL containing the `unsecured_webservices` string. For more information see the section Select the appropriate URL [page 82].

3.4.1.2 Decide between enhanced and standard services

The enhanced services support (limited) BPPC enforcement by default. They can also be configured to add user privilege checks on a system user level (that is, Role Based Access Control or RBAC). See the section Enabling or disabling the RBAC functionality of the enhanced services [page 81] for more information.

The enhanced services without RBAC only verify that the patient has agreed to share medical documents (that is, Policies 3, 4, and 5 in the section on Content Creators [page 91]).

The enhanced services with RBAC additionally limit the query by injecting constraints on the confidentiality levels of documents in accordance with the user privileges of the Document Consumer's system user account. For example, if the user account has the roles *XDS Query Documents* and *View Normal Medical Data* and the patient agreed to policy 5, the query response will contain only documents with a confidentiality code of normal. Please note that RBAC can only be enabled or disabled for all Document Consumers who use the enhanced services, but each Document Consumer can of course have different roles assigned to their system user.

It is always the Document Consumer's responsibility, no matter if standard or enhanced services are used or if RBAC is enabled, to further limit its query to local access control. This is done through confidentiality code constraints based on what privileges the querying consumer's user account has. The information about which user (of the consumer system, not of the Professional Exchange Server) triggered a query is not transmitted from the consumer system to the Professional Exchange Server and therefore even the enhanced service cannot take over this responsibility.

An example: A user of the Document Consumer system who has only limited privileges triggers a Registry Stored Query. Let us assume that the user's privileges are equivalent to the application's *View Normal Medical Data* role, which is authorized to view documents with a confidentiality level of normal. Then the consumer must automatically include the confidentiality code *normal* as a query constraint (or potentially filter out documents with a higher confidentiality level at a later time before displaying the result to the user). The mapping of the consumer systems privilege levels to the confidentiality codes used in Professional Exchange Server is the consumer systems responsibility.

The same limitation applies to privilege escalation. If the Document Consumer has a security override mechanism, the Document Consumer must check the patient consent and only allow the privilege escalation if the patient agreed to policy 3 or policy 5. The enhanced service cannot check this, because the information on whether a security override was triggered is not transmitted.

To summarize:

If the Document Consumer does not support the Basic Patient Privacy Proof option, it should use the enhanced services. It still has the responsibility to limit access according to local access control rules.

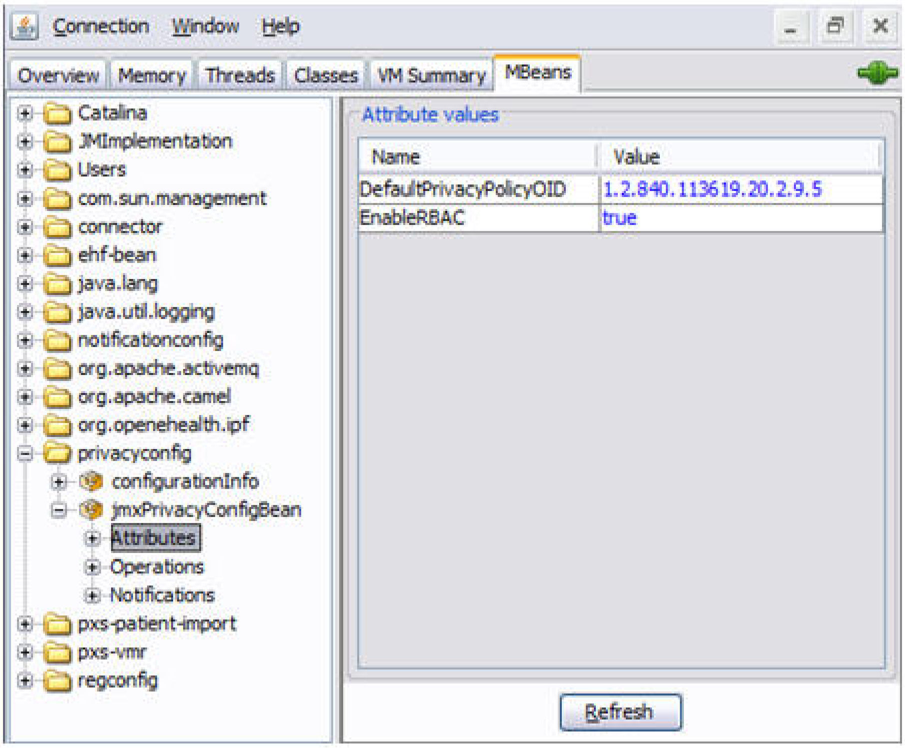
If the Document Consumer supports the Basic Patient Privacy Proof option and is able to ensure that the patient's privacy decisions are respected (for example, patients with policy 1 do not want their data to be shared with any user), then the Document Consumer should use the standard services. In this case all filtering responsibilities lie with the Document Consumer.

The RBAC option should only be enabled to automatically limit a Document Consumer's queries to a limited confidentiality level. For example, by giving the consumer's system user account in the Professional Exchange Server the *XDS Query Documents* and *View Normal Medical Data* roles it will generally be limited to documents with the confidentiality level *normal*. All other Document Consumers that should not be limited to *normal*-level documents, but still want to benefit from the enhanced services, would then need to additionally have the role *View Very Restricted Medical Data*.

The enhanced services use the same interface and messages as the standard service, they only differ in their processing.

3.4.1.2.1 Enabling or disabling the RBAC functionality of the enhanced services

RBAC for enhanced services is enabled by default. To disable it or to re-enable it if it has been disabled previously, connect to the Professional Exchange Server via JMX. Open the MBean `privacyconfig:name=jmxPrivacyConfigBean`. Set the `EnableRBAC` attribute to `true` to enable RBAC for the enhanced services (and all Document Consumers that use them) or to `false` if it should be disabled.



Name	Value
DefaultPrivacyPolicyOID	1.2.840.113619.20.2.9.5
EnableRBAC	true

Figure 40: Enabling or Disabling RBAC in the JConsole

3.4.1.3 Select the appropriate URL

There are five URLs that an XDS Document Consumer connected to the Professional Exchange Server can use:

Standard and authenticated *Registry Stored Query*:

```
https://<host>[:<port>]/<webapp_name>/webservices/xdsb-storedquery
```

Standard and unauthenticated *Registry Stored Query*:

```
https://<host>[:<port>]/<webapp_name>/unsecured_webservices/xdsb-storedquery
```

Enhanced and authenticated *Registry Stored Query*:

```
https://<host>[:<port>]/<webapp_name>/webservices/security-xdsb-storedquery
```

Enhanced and unauthenticated *Registry Stored Query*:

```
https://<host>[:<port>]/<webapp_name>/unsecured_webservices/security-xdsb-storedquery
```

Standard and authenticated *Retrieve Document Set*:

```
https://<host>[:<port>]/<webapp_name>/webservices/xdsb-retrievedocuments
```

3.4.2 Disconnect a XDS Document Consumer from the application

When an XDS Document Consumer is no longer a participant in the exchange, the following changes may be made.

You may want to disable the Document Consumer actor or completely remove the system. The correct approach to take depends on whether the system is a grouped actor with other functionality that is still required. For example, a system might have the capability to act as a Document Consumer and as a Document Repository. If you want to only use it as a Document Repository in the future, follow the instructions for disabling a Document Consumer actor. If you do not want to use either the Document Consumer or the Document Repository functionality of that system you can completely remove it.

3.4.2.1 Disabling a Document Consumer actor

Unless your installation uses unauthenticated XDS access, find the system's user account in the User Administration interface and remove the *XDS Query Documents* and *XDS Retrieve Documents* roles.

3.4.2.2 Removing a Document Consumer system

Unless your installation uses unauthenticated XDS access, delete [page 39] the system's user account or deactivate [page 38] it.

3.5 Managing DSUB Document Metadata Subscriber systems

3.5.1 Connect a new DSUB Document Metadata Subscriber system to the application

3.5.1.1 Add user account for DSUB Document Metadata Subscriber

Unless unauthenticated XDS access is supported in this Professional Exchange Server installation, the Document Metadata Subscriber must identify itself to the application using either a certificate or a username and password. If the DSUB Document Metadata Subscriber supports certificates, it is strongly recommended to use certificate-based authentication.

3.5.1.1.1 Certificate-based authentication

▹ When using the certificate-based authentication, you need to have a certificate for the DSUB Document Metadata Subscriber and the issuer's CA certificate.

1. Go to the User Administration interface and create a new account. Use the certificate's CN (common name) as the *certificate name* in the Create Account page.
2. Make sure to check the `system` checkbox, otherwise MLLP access attempts will be rejected.
3. After creating the account, you need to assign roles to the account. To act as a DSUB Document Metadata Subscriber, the system needs the role *DSUB Subscriber*.
   If the actor is grouped with other actors, more roles may be appropriate. See the sections on the other actors for the role names.

⇨ If the client certificate's issuer is not already represented in the CA truststore that the application uses, you need to retrieve the CA's certificate and add it to the truststore.
Please refer to the documentation of Sun's keytool to learn more about how to add a certificate to a truststore. The application's truststore is located in the Tomcat folder under `webapps/<webapp_name>/WEB-INF/classes/META-INF/ca.keystore`.
Please refer to the section on making changes to the Tomcat folder [page 27] for instructions on how to modify this file safely.

3.5.1.1.2 Password-based authentication

If it is not possible to use certificate-based authentication, you will have to determine a password that is known in the DSUB Document Metadata Subscriber and in the Professional Exchange Server User Administration. The User Administration interface is only able to generate one-time passwords. Therefore the permanent password will have to be added at a later time using the *change password* functionality.

1. Open the **User Administration** interface and create a new account.
2. Do not select the **System** checkbox yet.
   ⇨ The system displays the generated one-time password.
3. Note the password and log out.
4. Log in again using the new user account with the one-time password.
5. Change the one time password to the new permanent password. Log out again.
6. Log in as the administrator, search for and open the newly created user account.
7. Click **Modify** and then check the **System** checkbox.

8. Save the account and exit.
9. Go to the DSUB Document Metadata Subscriber and ensure that it uses the permanent password.

> **NOTE**
>
> The password expires after 90 days. At that point in time it is necessary to change the password in the User Administration interface (see the section on changing passwords for systems [page 104] for details) and in the DSUB Document Metadata Subscriber.

See also

- User Administration GUI [page 28]

3.5.1.1.3 No authentication

If the DSUB Document Metadata Subscriber does not support client certificate authentication or password-based authentication, verify that the Professional Exchange Server was installed with support for unauthenticated XDS access. If the Professional Exchange Server was not installed with support for unauthenticated XDS access, you need to use a URL containing the `unsecured_webservices` string. For more information on which URL to use, see the section Select the appropriate URL [page 85].

3.5.1.2 Select the appropriate URL

There are four URLs that a DSUB Document Metadata Subscriber connected to the Professional Exchange Server may use:

Authenticated “Document Metadata Subscribe”:

```
https://<host>[:<port>]/<webapp_name>/webservices/NotificationBroker/Subscribe
```

Unauthenticated “Document Metadata Subscribe”:

```
https://<host>[:<port>]/<webapp_name>/unsecured_webservices/NotificationBroker/Subscribe
```

The unsubscribe URL is contained in the subscription response. If necessary, it can also be hardcoded in the`DSUB Document Metadata Subscriber`

Authenticated “Document Metadata Unsubscribe”:

```
https://<host>[:<port>]/<webapp_name>/webservices/NotificationBroker/Unsubscribe
```

Unauthenticated “Document Metadata Unsubscribe”:

```
https://<host>[:<port>]/<webapp_name>/unsecured_webservices/NotificationBroker/Unsubscribe
```

3.5.2 Disconnect a DSUB Document Metadata Subscriber from the application

When a DSUB Document Metadata Subscriber is no longer a participant in the exchange, the following changes may be made.

You may want to disable the DSUB Document Metadata Subscriber actor or completely remove the system. The correct approach depends on whether the system is a grouped actor with other functionality that is still required. For example, a system might have the capability to act as a Document Consumer and as a Document Metadata Subscriber. If you want to only use it as a Document Consumer in the future, follow the instructions for disabling a Document Metadata Subscriber actor. If you want to use neither the Document Consumer nor the Document Metadata Subscriber functionality of that system you can completely remove it.

3.5.2.1 Disabling a DSUB Document Metadata Subscriber actor

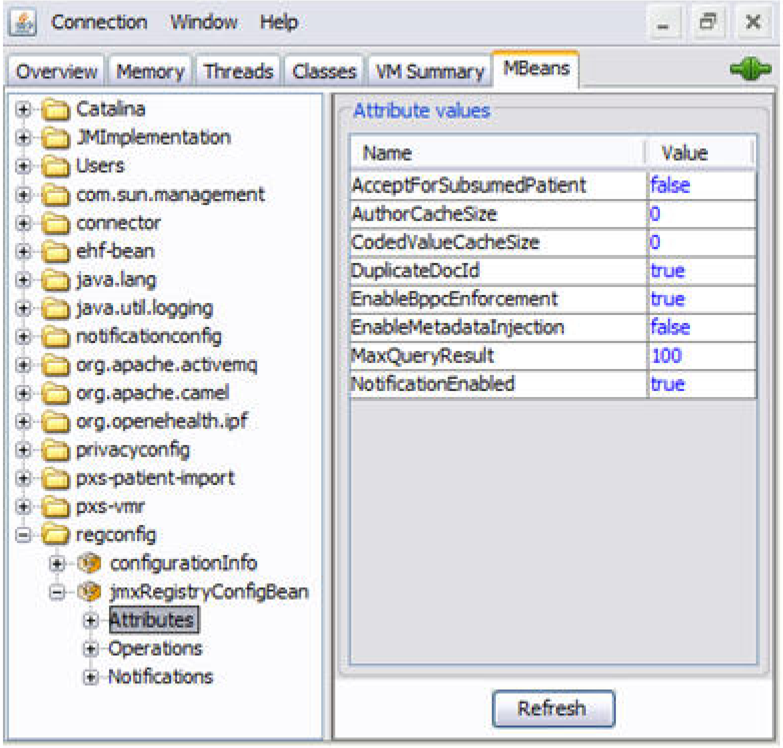
Unless your installation uses unauthenticated XDS access, find the system’s user account in the User Administration interface and remove the *DSUB Subscriber* role.

3.5.2.2 Removing a DSUB Document Metadata Subscriber system

Unless your installation uses unauthenticated XDS access, delete [page 39] the system’s user account or deactivate [page 38] it.

3.5.3 Enabling or disabling the notification feature

The DSUB-compatible notification feature of the Professional Exchange Server is activated by default. The feature can be disabled for performance reasons. This can be done at runtime through the JMX interface. To change the current settings, connect to the Professional Exchange Server using a JMX client and go to the MBean named *regconfig:name=jmxRegistryConfigBean*. Change the setting to *true* to enable notifications of Document Metadata Subscribers or to *false* to disable it.



Name	Value
AcceptForSubsumedPatient	false
AuthorCacheSize	0
CodedValueCacheSize	0
DuplicateDocId	true
EnableBppcEnforcement	true
EnableMetadataInjection	false
MaxQueryResult	100
NotificationEnabled	true

Figure 41: Enabling or Disabling Notifications in the JConsole

3.6 Managing DSUB Document Metadata Publisher systems

3.6.1 Connect a new DSUB Document Metadata Publisher system to the application

3.6.1.1 Add a user account for DSUB Document Metadata Publisher

Unless unauthenticated XDS access is supported in this Professional Exchange Server installation, the Document Metadata Publisher must identify itself to the application using either a certificate or a username and password. If the DSUB Document Metadata Publisher supports certificates, it is strongly recommended to use certificate-based authentication.

3.6.1.1.1 Certificate-based authentication

- ▹ When using the certificate-based authentication, you need to have a certificate for the DSUB Document Metadata Publisher and the issuer’s CA certificate.

1. Open the User Administration interface and create a new account. Use the certificate's CN (common name) as the *certificate name* in the Create Account page.
2. Make sure to check the **System** checkbox, otherwise MLLP access attempts will be rejected.
3. After creating the account, you need to assign roles to the account. To act as a DSUB Document Metadata Publisher, the system needs the role *DSUB Publisher*.
   If the actor is grouped with other actors, more roles may be appropriate. See the sections for the other actors for the role names.

⇨ If the client certificate's issuer is not already represented in the CA truststore that the application uses, you need to retrieve the CA's certificate and add it to the truststore.
Please refer to the documentation of Sun's keytool to learn more about how to add a certificate to a truststore. The application's truststore is located in the Tomcat folder under `webapps/<webapp_name>/WEB-INF/classes/META-INF/ca.keystore`.
Please refer to the chapter on making changes to the Tomcat folder [page 27] for instructions on how to modify this file safely.

3.6.1.1.2 Password-based authentication

If it is not possible to use certificate-based authentication, you will have to determine a password that is known in the DSUB Document Metadata Publisher and in the Professional Exchange Server User Administration. The User Administration interface is only able to generate one-time passwords. Therefore the permanent password will have to be added at a later time using the *change password* functionality.

1. Open the User Administration interface and create a new account.
2. Do not select the **System** checkbox yet.
   ⇨ The system displays the generated one-time password.
3. Note the password and log out.
4. Log in again using the new user account with the one-time password.
5. Change the one time password to the new permanent password. Log out again.
6. Log in as the administrator, search for and open the newly created user account.
7. Click **Modify** and then select the **System** checkbox.
8. Save the account and exit.
9. Go to the DSUB Document Metadata Publisher and ensure that it uses the permanent password.

NOTE

The password expires after 90 days. At that point in time it is necessary to change the password in the User Administration interface (see the section on changing passwords for systems [page 104] for details) and in the DSUB Document Metadata Publisher

See also

- User Administration GUI [page 28]

3.6.1.1.3 No authentication

If the DSUB Document Metadata Publisher does not support client certificate authentication or password-based authentication, verify that the Professional Exchange Server was installed with support for unauthenticated XDS access. If the Professional Exchange Server was not installed with support for unauthenticated XDS access, you need to use a URL containing the `unsecured_webservices` string. For more information on the appropriate URL to use, see the section Select the appropriate URL [page 85].

3.6.1.2 Select the appropriate URL

There are two URLs that a DSUB Document Metadata Subscriber connected to the Professional Exchange Server may use:

Authenticated *Document Metadata Publish*:

```
https://<host>[:<port>]/<webapp_name>/webservices/NotificationBroker/Publish
```

Unauthenticated *Document Metadata Publish*:

```
https://<host>[:<port>]/<webapp_name>/unsecured_webservices/NotificationBroker/Publish
```

3.6.2 Disconnect a DSUB Document Metadata Publisher from the application

When a DSUB Document Metadata Publisher is no longer a participant in the exchange, the following changes may be made.

You may want to disable the DSUB Document Metadata Publisher actor or completely remove the system. The correct approach depends on whether the system is a grouped actor with other functionality that is still required. For example, a system might have the capability to act as a Document Consumer and as a Document Metadata Publisher.

If you want to only use it as a Document Consumer in the future, follow the instructions for disabling a Document Metadata Publisher actor. If you want to use neither the Document Consumer nor the Document Metadata Publisher functionality of that system you can completely remove it.

3.6.2.1 Disabling a DSUB Document Metadata Publisher actor

Unless your installation uses unauthenticated XDS access, find the system's user account in the User Administration interface and remove the *DSUB Publisher* role.

3.6.2.2 Removing a DSUB Document Metadata Publisher system

Unless your installation uses unauthenticated XDS access, delete [page 39] the system's user account or deactivate [page 38] it.

3.7 Configuring the ATNA Audit Record Repository

The application must always be operated with a properly configured recipient for ATNA audit records. The recipient must support the BSD syslog protocol (RFC 3164). The ATNA audit repository host and port are set during installation. To change the audit repository settings that were selected during installation, you need to modify the file:

```
<tomcat_folder>/webapps/<webapp_name>/WEB-INF/classes/META-INF/ehf-
ipf-context.xml
```

In this file change the following bean definition:

```
<bean id="iheAuditorConfig"
factory-bean="iheAuditorContext"
factory-method="getConfig">
<property name="auditRepositoryHost" value="<audit_repo_host>" />
<property name="auditRepositoryPort" value="<audit_repo_port>" />
<property name="auditSourceId" value="<audit_source_id>" />
<property name="auditEnterpriseSiteId"
value="<audit_enterprise_id>" />
</bean>
```

Please refer to the chapter Making changes to the Tomcat folder [page 27] for instructions on how to modify this file safely.

The `<audit_repo_host>` parameter is the hostname of the target ATNA audit repository. The `<audit_repo_port>` parameter is the port that the ATNA audit repository listens on for BSD syslog protocol messages. The other two parameters (`<au-`

dit_source_id>, <audit_enterprise_id>) are used to uniquely identify messages from this Professional Exchange Server installation in the ATNA Audit Record Repository. For further details on the meaning of these settings, please refer to the IHE ATNA integration profile.

3.8 Managing Content Creator systems for BPPC policy acknowledgment

The Professional Exchange Server relies on Patient Privacy Consent Acknowledgment Documents, as described in the IHE BPPC profile, to control access to the patient's medical data. The actor that creates these documents is called a Content Creator with the Basic Patient Privacy Acknowledgement option. It is responsible for creating a Patient Privacy Consent Acknowledgment Document when the patient's preference for a privacy policy has been recorded. The document is a structured CDA document that is described in detail in the IHE profile. The profile also specifies the document metadata that has to be used with the document.

3.8.1 Configuring a Content Creator with the Basic Patient Privacy Acknowledgement option

As the Professional Exchange Server is based on the IHE XDS profile, the Content Creator has to be grouped with an XDS Document Source, so that the document can be registered in the application. Please refer to the documentation on how to manage systems that are XDS Document Source [page 63] actors.

The Content Creator needs to be configured to support the following patient privacy policies:

Policy	Policy OID / Event Code	Display Name	Description
1	1.2.840.113619.20.2.9.1	Publish	Patient **does not agree** to share their medical documents through the exchange and **does not allow** the user to override view restrictions in emergency situations. Patient **agrees** that their medical documents are published to the exchange.
2	1.2.840.113619.20.2.9.2	No Publish or Share	Patient **does not agree** to share their medical documents through the exchange and **does not allow** the user to override view restrictions in emergency situations. Patient **does not agree** that their medical documents are published to the exchange.
3	1.2.840.113619.20.2.9.3	Publish with Override	Patient **does not agree** to share their medical documents through the exchange, but **allows** the user to override view restrictions in emergency situations. Patient **agrees** that their medical documents are published to the exchange.
4	1.2.840.113619.20.2.9.4	Publish and Share	Patient **agrees** to share their medical documents through the exchange, but **does not allow** the user to override view restrictions in emergency situations. Patient agrees that their medical documents are published to the exchange.
5	1.2.840.113619.20.2.9.5	Publish and Share with Override	Patient **agrees** to share their medical documents through the exchange and **allows** the user to override view restrictions in emergency situations. Patient agrees that their medical documents are published to the exchange.

Table 1: Supported Privacy Policies

NOTE

The sharing of medical data as described in the privacy policies is conditional, that is it depends on the user’s privileges. There are three levels of confidentiality, normal, restricted and very restricted. A user may have privileges for documents with a normal confidentiality level, for documents with normal and restricted confidentiality levels, or for documents with normal, restricted and very restricted confidentiality levels. If the user overrides view restrictions in emergency situation (also known as security override), his privileges are automatically elevated to the highest level.

When the privacy policy is referenced in the `XDSDocumentEntry.eventCode` of the Patient Privacy Consent Acknowledgment Document’s XDS message, make sure that you use the appropriate event code and display name listed above and the coding scheme *Privacy Policies*.

Example:

```
<rim:Classification
 classificationScheme=
"urn:uuid:2c6b8cb7-8b2a-4051-b291-b1ae6a575ef4"
 classifiedObject="Document01"
nodeRepresentation="1.2.840.113619.20.2.9.5">
     <rim:Name>
        <rim:LocalizedString value="Publish and Share with Override"/
>
     </rim:Name>
     <rim:Slot name="codingScheme">
        <rim:ValueList>
             <rim:Value>Privacy Policies</rim:Value>
         </rim:ValueList>
     </rim:Slot>
</rim:Classification>
```

If the Document Source that the Content Creator is grouped with communicates directly with the Professional Exchange Server (that is, not through another XDS Document Repository), it should use the standard services for registering *Patient Privacy Consent Acknowledgment* Documents and not the enhanced services. Otherwise a patient who has agreed to Policy 2 will not be able to replace that consent acknowledgment document before the consent duration (that is, the `XDSDocumentEntry.serviceStopTime`) has been reached. This is necessary because the enhanced services do not accept a *Provide and Register Document Set-b* message for a patient who has “opted-out”, even though it contains a new consent acknowledgment document.

3.8.2 Configuring a Content Creator without the Basic Patient Privacy Acknowledgement option

You can use the Policyack Webservice as an alternative way to add patient consent documents, for example, if they are not standards conform. With this service it is easier to add or update consents for external services. This is an Apache Axis based webservice available under the following url:

```
https://<host>[:<port>]/<webapp_name>/axis-webservices/v1-0-0/
PolicyackwebserviceBppcAcknowledgmentWebService
```

If unsecure webservice (no authentication required) is selected during the installation process, there is an additional endpoint available for that service:

```
https://<host>[:<port>]/<webapp_name>/axis-unsecured_webservices/
v1-0-0/
PolicyackwebserviceBppcAcknowledgmentWebService
```

This endpoint provides a method `acknowledgePolicyForPatient` with 4 parameters:

parameter-name	parameter-type	description
consentValidForever	boolean	If set to true, this consent does not expire and the duration parameter is ignored.
duration	integer	The duration parameter is set in minutes. Describes the validity time of this consent.
patientIdentifier	instanceIdentifier (root+extension)	
policyOID	instanceIdentifier (root+extension)	Valid policy OIDs are described below.

Example request

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/
envelope/"
 xmlns:ser="/policyackwebservice/v1-0-0/service">
    <soapenv:Header/>
    <soapenv:Body>
        <ser:acknowledgePolicyForPatient>
            <ser:request>
                <ser:consentValidForever>false</
ser:consentValidForever>
                <ser:duration>200</ser:duration>
                <ser:patientIdentifier>
                    <ser:extension>${#Project#patientID}</
ser:extension>
                    <ser:root>2.16.840.1.113883.3.37.4.1.1.2.2.1</
ser:root>
                </ser:patientIdentifier>
                <ser:policyOID>
```

```
                    <ser:extension></ser:extension>
                    <ser:root>1.2.840.113619.20.2.9.1</ser:root>
                </ser:policyOID>
            </ser:request>
        </ser:acknowledgePolicyForPatient>
    </soapenv:Body>
</soapenv:Envelope>
```

3.8.2.1 Policy OIDs

The application accepts consent acknowledgment documents pointing to the OID of one of the five privacy policies (listed in Table 1: Supported Privacy Policies [page 91])

3.8.2.2 Policy Acknowledgement Module Configuration

The Policy Acknowledgement Module depends upon some configurations in order to process the request and return a response. Some of these configurations can be modified at runtime and some require a server restart.

Configurations

The CDA templates, which can be customized as needed, are in the following location:

`<tomcat_folder>/webapps/<webapp_name>\WEB-INF\classes\ConsentDocuments\`

These can be changed at runtime.

Consent Metadata Configuration

The metadata can be configured via properties in the following location:

`<tomcat_folder>/webapps/<webapp_name>\WEB-INF\classes\META-INF\ehealth.properties`

Please refer to the section on Making changes to the Tomcat folder [page 27] for instructions on how to modify this file safely.

Property	Description	Default value
policyack. esmrepository.typeCode	The typeCode for the consent document that is created.	`PolicyAckDocument`
policyack. esmrepository. typeCodeSystemOID	The TypeCodeSystem for the consent document that is created	`1.2.840.113619.20.2.4.8`
policyack. esmrepository. typeCodeVersion	The TypeCodeVersion for the consent document that is created.	`1.0.0`
policyack. authorOrgName	The organization that authored the consent document. This is an optional element, and no default value is provided.	-
policyack. authorRoleCode	The author role code value for the consent document. This is an optional element, and no default value is provided.	-
policyack. authorRoleCodeSystem	The author role code system for the consent document. This is an optional element, and no default value is provided.	-
policyack. authorSpecialityCode	The author specialty code value for the consent document. This is an optional element, and no default value is provided.	-
policyack. classCodeSystem	The class code system for the consent document. This code system should have a code value "Consent".	`IHE Class Codes`
policyack. confCodeSystem	The confidentiality code system for the consent document.	`HL7 Confidentiality Codes`

Property	Description	Default value
policyack. confCodeValue	The confidentiality code value for the consent document.	N
policyack. contentTypeCodeSystem	The content type code system for the consent document.	`LOINC`
policyack. contentTypeCodeValue	The content type code value for the consent document.	`11488-4`
policyack. documentUniqueIdBase	The base OID that can be used as a unique ID for the document. This is incremented for every publish transaction.	`4.1.2.345.1.3.16687`
policyack. eventCodeSystem	The event code system for the consent document. This code system should hold the Policy OID's.	`Privacy Policies`
policyack. formatCodeSystem	The format code system for the consent document. This code system should have one of its code values as `urn:ihe:iti:bppc:2007`.	`IHE Format Codes`
policyack. hcfCodeSystem	The healthcare facility code system for the consent document.	`Health Care Provider Taxonomy`
policyack. hcfCodeValue	The healthcare facility code value for the consent document.	`261Q00000X`
policyack. languageCode	The language code for the consent document.	`en-us`
policyack. pracSettingCodeSystem	The practice setting code system for the consent document.	`Health Care Provider Taxonomy`
policyack. pracSettingCodeValue	The practice setting code value for the consent document.	`103TH0004X`

Property	Description	Default value
policyack. sourceId	The source identifier for the consent document. This must be a properly configured document source as described in: Managing XDS Document Source systems [page 63]	`1.3.6.1.4.1.21367.2005.3.41`
policyack. submissionSetUniqueIdBase	The base OID that can be used as a unique ID for the submission set. This is incremented for every publish transaction.	`1.2.4.2.4.3.21345`
policyack. typeCodeSystem	The type code system for the consent document.	`LOINC`
policyack. typeCodeValue	The type code value for the consent document.	`44943-9`

Table 2: Consent metadata configuration

System Time Configuration

NOTE

To ensure proper operation the server time must be set correctly.

3.9 Managing OMI Document Source Systems

3.9.1 Connect a new OMI Document Source system to the application

In contrast to the other system connections of the application, the OMI message based communication is not based on IHE standards, but on underlying standards like HL7 v2. Important configuration settings are made during installation of the application. They includes port numbers and support for authenticated and/ or unauthenticated communication.

3.9.1.1 Certificate-based authentication

When using certificate-based authentication, you need to have a certificate for the PIX Patient Identity Source and the issuer's CA certificate.

1. Go to the User Administration interface and create a new account. Use the certificate's CN (common name) as the Certificate name in the Create Account page.
2. Make sure to check the system checkbox, otherwise MLLP access attempts will be rejected.
3. After creating the account, you need to assign roles to the account. To act as a OMI Document Source, the system needs the role *XDS Register Documents*. This is necessary,because the OMI messages transformed internally into XDS messages. If the actor is grouped with other actors, more roles may be appropriate. See the sections on the other actors for the role names.

⇨ If the client certificate's issuer is not already represented in the CA truststore that the application uses, you need to retrieve the CA's certificate and add it to the truststore. Please refer to the documentation of Oracle's keytool to learn more about how to add a certificate to a truststore. The application's truststore is located in the Tomcat folder under `webapps/<webapp_name>/WEB-INF/classes/META-INF/ca.keystore`. Please refer to the chapter on Making changes to the Tomcat folder [page 27] for instructions on how to modify this file safely.

3.9.1.2 No authentication

If the OMI Document Source Systems do not support client certificate authentication, verify that the Professional Exchange Server was installed with support for unauthenticated MLLP access for OMI messages. OMI Document Source Systems need to use the port for unauthenticated MLLP communication.

3.9.2 Disconnect an OMI Document Source System

When an OMI Document Source is no longer a participant in the exchange, the following changes may be made.

You may want to disable the OMI Document Source actor or completely remove the system. The correct approach depends on whether the system is a grouped actor with other functionality that is still required. For example, a system might have the capability to act as a Document Source and as a Document Repository. If you want to only use it as a Document Repository in the future, follow the instructions for disabling a Document Source actor. If you want to use neither the Document Source nor the Document Repository functionality of that system you can completely remove it.

3.9.2.1 Disabling an OMI Document Source System

Unless your installation uses unauthenticated access, find the system's user account in the User Administration interface and remove the *XDS Register Documents* role. Skip this step if the other grouped actors still require this role (for example, Document Repositories use the same role). Delete the *DocumentRegistrySource* profile of the corresponding system element in the organization registry.

3.9.2.2 Removing an OMI Document Source System

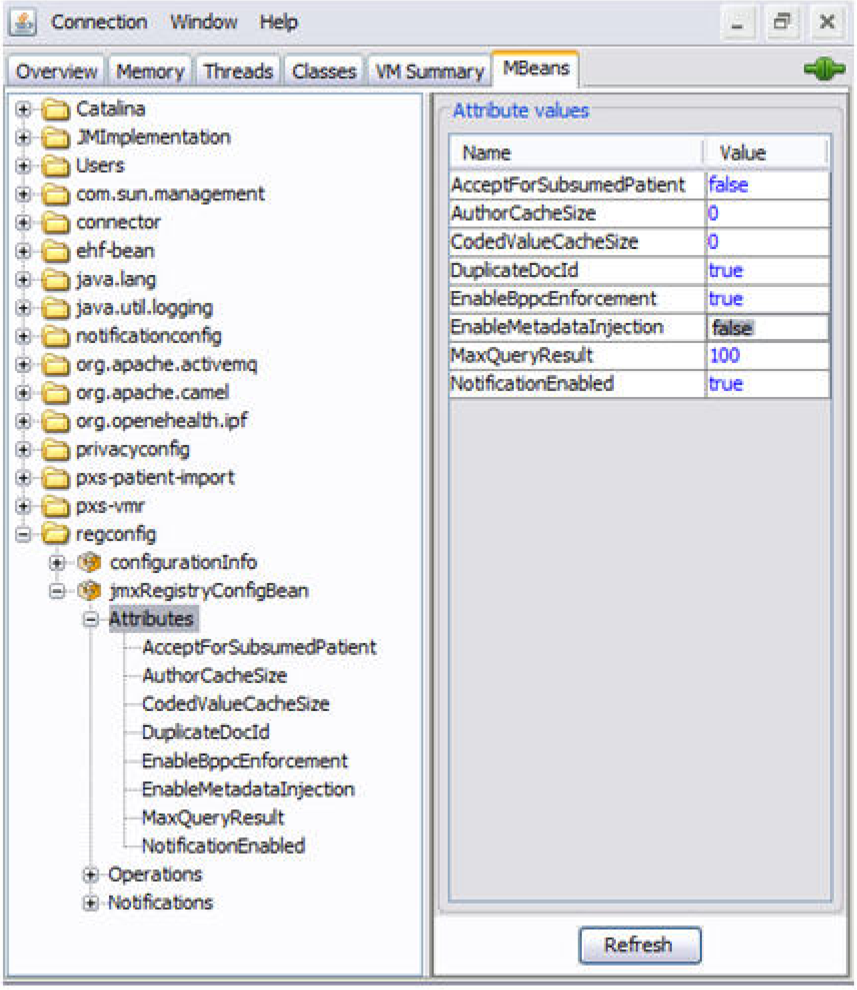
Unless your installation uses unauthenticated access, delete the system's user account or deactivate it. Please see the section Delete an account [page 39] for details on how to do this. Delete the *DocumentRegistrySource* profile of the corresponding system element in the organization registry. Change the system's name according to your convention for labeling systems that are no longer needed.

3.10 Configuring metadata injection

The metadata injection mechanism allows you to define rules, in the dynamic Groovy programming language, that are evaluated before a *Provide and Register Document Set-b* message is processed. One use case for this mechanism is to set the confidentiality code of a document to a predetermined value if it matches certain parameters.

3.10.1 Enabling or disabling metadata injection

The metadata injection rules are only executed for *Provide and Register Document Set-b* transactions that use the enhanced services. By default the metadata injection is disabled. The feature can be enabled and disabled at runtime via JMX. To do so, connect to the Professional Exchange Server via JMX. Open the MBean “regconfig:name=jmxRegistryConfigBean”. Set the `EnableMetadataInjection` attribute to `true` if metadata injection should be enabled for the enhanced services or to `false` if it should be disabled.



Name	Value
AcceptForSubsumedPatient	false
AuthorCacheSize	0
CodedValueCacheSize	0
DuplicateDocId	true
EnableBppcEnforcement	true
EnableMetadataInjection	false
MaxQueryResult	100
NotificationEnabled	true

Figure 42: Enabling or Disabling metadata injection in JConsole

3.10.2 Rationale for injecting metadata

Metadata injection relies on GroovyRules, a lightweight rule engine. It enables you to change the metadata that Document Sources use to register documents. A common use case is to set a document entry’s confidentiality code based on the document’s metadata. For example, you could set all documents from psychiatric hospitals to have a *very restricted* confidentiality code.

In most cases it is preferable to reconfigure the Document Source to use the correct metadata, instead of using metadata injection to override the original values. The problem with metadata injection is that the Document Source is not aware of the manipulation. Often such a Document Source is grouped with a Document Consumer. Such a system could make assumptions about certain metadata fields and might fail when it queries the document registry and does not find the documents it just registered. For example, if a script replaces a document’s practice setting code, the source might be unable to locate it later if it queries the registry using the document’s original practice setting code. In that case the document source might be unable to perform replacements, transformations and addendums might stop working.

However, there are many situations where the Document Source might not be sufficiently configurable, or such a configuration might be costly, unstable, or have other drawbacks. In these situations the metadata injection mechanism can be a very valuable tool.

3.10.3 Defining metadata injection rules

To define metadata injection rules, you need to create a file named sensitivityruleset.xml in the Tomcat webapps directory (`<tomcat_home>/webapps/<webapp_name>/WEB-INF/classes/sensitivityruleset.xml`).

Alternatively you can put the file into the Tomcat's `lib`, `bin` or `conf` folders. Please see the section on how to change files in the Tomcat directory [page 27] for instructions how to do this safely.

The file must contain the following structure:

```
<?xml version="1.0" encoding="UTF-8"?>

<ruleexecutionset>

<name>Metadata Injection Rule Set</name>

<description>Defines rules for document metadata</description>

<ruleroot>${path_to_rules}</ruleroot>

<rules>

<rule>${rule_1_filename}</rule>

<rule>${rule_2_filename}</rule>

...

<rule>${rule_n_filename}</rule>

</rules>

</ruleexecutionset>
```

Where `${path_to_rules}` must be replaced by the absolute path to the directory containing the groovyrule files and `${rule_1_filename}` to `${rule_n_filename}` must be replaced by the file names of the different GroovyRule files you want to use.

```
Example:

<?xml version="1.0" encoding="UTF-8"?>

<ruleexecutionset>

<name>Metadata Injection Rule Set</name>
```

```
<description>Defines rules for document metadata</description>
<ruleroot>
/home/pxs/bin/groovyrules
</ruleroot>
<rules>
<rule>sensitivity.groovyrule</rule>
<rule>facility.groovyrule</rule>
</rules>
</ruleexecutionset>
```

The GroovyRule files follow Groovy syntax. For a full description of the capabilities and limits of GroovyRules, see https://groovyrules.dev.java.net/.

Example:

```
documentEntry = data.getFirstObjectOfType(
com.gehcit.ehealth.cnf.drr.ehf.registry.transfer.DocumentEntryDto);
def confCode=new com.icw.ehf.core.transfer.AnnotatedCodeDto()
def conf=new com.gehcit.ehealth.cnf.drr.ehf.registry.transfer.DocumentConfidentialityCodeDto()
def set=new HashSet()

if(documentEntry.practiceSettingCode.key=="2471C3402X") {
confCode.key="V";
confCode.value="Very Restricted";
confCode.systemId="2.16.840.1.113883.5.25";
conf.setConfidentialityCode(confCode);
set.add(conf);
documentEntry.setConfidentialityCodes(set);
}
```

This GroovyRule example picks the first document entry in the submission set, checks if it has the practice setting code “`2471C3402X`” and if that is the case it replaces the existing confidentiality code with the code “V” for “Very Restricted”.

Please note that in a clustered environment the GroovyRule directory needs to be accessible from all nodes or it must be synced between the nodes.

3.11 Changing a system user account's password

In certain situations when the connected systems do not support certificate based authentication, it might be necessary to fallback to using passwords for system user accounts. One of the big disadvantages of this approach is that the passwords expire after 90 days, for security reasons. The administrator needs to take the following steps to change a system user’s account to a new password that is again valid for the next 90 days:

1. Log in to the User Administration interface with an admin account
2. Search for the system user in question and open the user account
3. Select **Modify Account** and then uncheck the **System** checkbox and save
4. Reset the password and note the newly generated password
5. Logout
6. Log in to the application using the system user's username and the newly generated password
7. Click **Change Password** and set the new password
8. Logout
9. Set the same new password as the connection password in the system in question (for example, in the Document Source)
10. Log in to the User Administration interface with an admin account
11. Search for the system user in question and open the user account
12. Select **Modify Account** and then check the **System** checkbox, save and logout

4 Managing the Affinity Domain

4.1 Changing the Affinity Domain's terminology

The following sections describe what Codes, Code Systems and Code Sets are accepted for the different fields in XDS and (to a lesser extent) PIX messages and how to change them.

4.1.1 Configuring the accepted XDS Document MIME types

4.1.1.1 Adding a new MIME type

To add a new MIME type that is not yet part of the Code System in use, follow these steps:

1. Log in to the Terminology Tools section of the Administration interface.
2. Open the Code System Mimetypes with the OID 2.16.840.1.113883.6.10
3. Click **Add New Code**
4. Add the new MIME type Code Key and Display Value (for example, *text/veryplain* and *Alternate type for plaintext*)
5. Click **OK** and then **Save**
6. Switch to the *Code Sets* tab.
7. Select the current version of the Code Set EXT-GEN-DOCUMENT-MIMETYPE
8. Select the checkbox beside the newly added Code (for example, next to "text/veryplain")
9. Click **Save**

   ⇨ A new (minor) version of the Code Set has been created (for example, version 1.1.0)

10. Switch to the *Code Categories* tab.
11. Select the Code Category C-DOCUMENT-MIMETYPE
12. Click **Assign Code Set**
13. Select the new minor version of the EXT-GEN-DOCUMENT-MIMETYPE Code Set (for example, version 1.1.0)
14. Click **OK**

    ⇨ The new version of the Code Set is now assigned and active. The old version is inactive.

15. Click **Save**

4.1.1.2 Deactivating a MIME type

To remove a MIME type you need to follow these steps:

1. Log in to the Terminology Tools section of the Administration interface.
2. Switch to the *Code Sets* tab.
3. Select the current version of the Code Set *XT-GEN-DOCUMENT-MIMETYPE*
4. Deselect the MIME type you want to deactivate
5. Click **Save**

   ⇨ A new major version of the Code Set is created (for example, version 2.0.0)
6. Switch to the *Code Categories* tab.
7. Select the Code Category C-DOCUMENT-MIMETYPE
8. Click **Assign Code Set**
9. Select the new major version of the EXT-GEN-DOCUMENT-MIMETYPE Code Set (for example, version 2.0.0)
10. Click **OK**

    ⇨ The new version of the Code Set is now assigned and active, the old version is inactive
11. Click **Save**

4.1.1.3 Reactivating an existing MIME type

To reactivate a MIME type that is already part of the Code System, but has been removed from the current Code Set, follow these steps:

1. Log in to the Terminology Tools section of the Administration interface.
2. Switch to the *Code Sets* tab.
3. Select the current version of the Code Set EXT-GEN-DOCUMENT-MIMETYPE
4. Select the checkbox beside the Code you want to reactivate
5. Click **Save**

   ⇨ A new minor version of the Code Set has been created (for example, version 2.1.0)
6. Switch to the *Code Categories* tab.
7. Select the Code Category C-DOCUMENT-MIMETYPE
8. Click **Assign Code Set**
9. Select the new minor version of the EXT-GEN-DOCUMENT-MIMETYPE Code Set (for example, version 2.1.0)
10. Click **OK**

- ⇨ The new version of the Code Set is now assigned and active. The old version is inactive.

11. Click **Save**

4.1.2 Configuring the accepted XDS Document class codes

4.1.2.1 Adding a LOINC-based class code

Follow these steps to allow a new LOINC Code to be used as a class Code:

1. Log in to the Terminology Tools section of the Administration interface.
2. Open the Code System LOINC with the OID 2.16.840.1.113883.6.1
   If the Code you want to add as a class Code is already part of the Code System, write down the Code. You can skip the next 3 steps and switch to *Code Sets* tab directly.
3. Click **Add New Code**
4. Add the new LOINC type's Code Key and Display Value (for example, *X-CON* and *Document*)
5. Click **OK** and then **Save**
6. Switch to the *Code Sets* tab.
7. Select the current version of the Code Set LOINC-CLASS-CODES-DEFAULT
8. Select the check box in front of the newly added Code (for example, in front of *X-CON*)
9. Click **Save**
   - ⇨ A new (minor) version of the Code Set has been created (for example, version 1.1.0)
10. Switch to the *Code Categories* tab.
11. Select the Code Category C_GE_DRR_CLASS_CODE
12. Click **Assign Code Set**
13. Select the new minor version of the LOINC-CLASS-CODES-DEFAULT Code Set (for example, version 1.1.0)
14. Click **OK**
    - ⇨ The new version of the Code Set is now assigned and active. The old version is inactive.
15. Click **Save**

4.1.2.2 Deactivating a class code

You can deactivate any class Code, except for the *Consent* in the IHE-CLASS-CODES-DEFAULT Code Set, which is needed for the Professional Exchange Server to function properly. The following instructions assume that you know the Code Set of the class Code you want to deactivate.

1. Log in to the Terminology Tools section of the Administration interface.
2. Switch to the *Code Sets* tab.
3. Select the current version of the Code Set LOINC-CLASS-CODES-DEFAULT
4. Deselect the class Code you want to deactivate
5. Click **Save**.
   - ⇨ A new major version of the Code Set has been created (for example, version 2.0.0)
6. Switch to the *Code Categories* tab.
7. Select the Code Category C_GE_DRR_CLASS_CODE
8. Click **Assign Code Set**
9. Select the new major version of the LOINC-CLASS-CODES-DEFAULT Code Set (for example, version 2.0.0)
10. Click **OK**
    - ⇨ The new version of the Code Set is now assigned and active. The old version is inactive.
11. Click **Save**.

4.1.2.3 Adding a new code system for class codes

Adding a new Code System for class Codes is necessary if LOINC does not meet your needs. If you want to use another Code System that already exists (for example, DCM), skip the first 10 steps and switch to the *Code Sets* tab directly.

1. Log in to the Terminology Tools section of the Administration interface.
2. Click **Add Code System**
3. Enter a Code System name (for example, Custom Class Codes) and a Code System OID (for example, 1.2.3.4.5.6.7)
4. Click **Save**
5. Select the newly created Code System
6. Click **Add New Code**.
7. Enter a Code Key (for example, A1) and a Display Value (for example, Notes).
8. Click **OK**.

9. Add the Codes you need.
10. Click **Save**.
11. Switch to the *Code Sets* tab.
12. Click **Add Code Set**.
13. Enter a Code Set name (for example, MY-CLASS-CODES).
14. Select the new Code System in the dropdown box (for example, Custom Class Codes).
15. Click **Save**.
16. Switch to the *Code Categories* tab.
17. Select the Code Category C_GE_DRR_CLASS_CODE.
18. Click **Assign Code Sets**.
19. Select the new Code Set (for example, MY-CLASS-CODES).
20. Click **OK**.
21. Click **Save**.

4.1.2.4 Deactivating a code system for class codes

You can deactivate Code Systems and replace them with a different terminology. Do not deactivate the IHE-CLASS-CODES-DEFAULT Code Set which is needed for the Professional Exchange Server to function properly. Follow these steps to stop supporting a specific Code System for class Codes (for example, Custom Class Codes):

1. Log in to the Terminology Tools section of the Administration interface.
2. Switch to the *Code Categories* tab.
3. Select the Code Category C_GE_DRR_CLASS_CODE.
4. In the Status column click the **Active** link in the Code Set row (for example, MY-CLASS-CODES) of the Code System you want to deactivate (for example, Custom Class Codes).
5. Click **Save**.

4.1.3 Configuring the accepted XDS Folder codes

4.1.3.1 Adding a HL7 encounter code

Follow these steps to allow a new HL7 Encounter Code to be used as a folder Code:

1. Log in to the Terminology Tools section of the Administration interface.

2. Open the EncounterCode Code System with the OID 2.16.840.1.113883.1.11.13955
   If the Code you want to add as a folder Code is already part of the Code System, write down the Code. You can skip the next 3 steps and switch to the *Code Sets* tab directly.
3. Click **Add new Code**.
4. Add the new encounter Code's Code Key and Display Value (for example, PHYRHB and Physical Rehab).
5. Click **OK** and **Save**.
6. Switch to the *Code Sets* tab.
7. Select the current version of the Code Set ENCOUNTER-CODES-DEFAULT.
8. Select the checkbox next to the new Code (for example, next to PHYRHB).
9. Click **Save**.
   ⇨ A new (minor) version of the Code Set has been created (for example, version 1.1.0).
10. Switch to the *Code Categories* tab.
11. Select the Code Category C_GE_DRR_CODELIST_CODE
    .
12. Click **Assign Code Set**.
13. Select the new minor version of the ENCOUNTER-CODES-DEFAULT Code Set (for example, version 1.1.0).
14. Click **OK**.
    ⇨ The new version of the Code Set is now assigned and active. The old version is inactive.
15. Click **Save**.

4.1.3.2 Deactivating a folder code

The following instructions assume that you know the Code Set of the folder Code you want to deactivate.

1. Log in to the Terminology Tools section of the Administration interface.
2. Switch to the *Code Sets* tab.
3. Select the current version of the Code Set of the folder Code you want to deactivate (for example, ENCOUNTER-CODES-DEFAULT).
4. Deselect the Code you want to deactivate.
5. Click **Save**.

⇨ A new major version of the Code Set is created (for example, version 2.0.0).

6. Switch to the *Code Categories* tab.
7. Select the Code Category C_GE_DRR_CODELIST_CODE.
8. Click **Assign Code Set**.
9. Select the new major version of the Code Set you just edited (for example, ENCOUNTER-CODES-DEFAULT version 2.0.0).
10. Click **OK**.

    ⇨ The new version of the Code Set is now assigned and active. The old version is inactive.

11. Click **Save**.

4.1.3.3 Adding a new code system for folder codes

Adding a new Code System for folder Codes is necessary if HL7 Encounter Codes do not meet your needs. If you want to use another Code System that already exists (for example, LOINC), you can skip the first 10 steps.

1. Log in to the Terminology Tools section of the Administration interface.
2. Click **Add Code System**.
3. Enter a Code System name (for example, Custom Folder Codes) and a Code System OID (for example, 1.2.3.4.5.6.8).
4. Click **Save**.
5. Select the newly created Code System.
6. Click **Add New Code**.
7. Enter a Code Key (for example, A1) and a Display Value (for example, Chronic).
8. Click **OK**.
9. Add the Codes you need.
10. Click **Save**.
11. Switch to the *Code Sets* tab.
12. Click **Add Code Set**.
13. Enter a Code Set name (for example, MY-FOLDER-CODES).
14. Select the new Code System in the dropdown box (for example, Custom Folder Codes).
15. Click **Save**.
16. Switch to the *Code Categories* tab.
17. Select the Code Category C_GE_DRR_CODELIST_CODE.

18. Click **Assign Code Sets**.
19. Select the new Code Set (for example, MY-FOLDER -CODES).
20. Click **OK**.
21. Click **Save**.

4.1.3.4 Deactivating a Code system for folder codes

You can deactivate Code Systems and replace them with a different terminology. Follow these steps to stop supporting a specific Code System for folder Codes (for example, Custom Folder Codes).

1. Log in to the Terminology Tools section of the Administration interface.
2. Switch to the *Code Categories* tab.
3. Select the Code Category C_GE_DRR_CODELIST_CODE.
4. Click on the **Active** link in the Status column of the respective Code Set row (for example, MY-FOLDER-CODES).
5. Click **Save**.

4.1.4 Configuring the accepted XDS SubmissionSet content types

4.1.4.1 Adding a LOINC or DCM-based content type Code

Follow these steps to allow a new LOINC or DCM Code to be used as a content type Code.

1. Log in to the Terminology Tools section of the Administration interface.
2. Open the Code System LOINC with the OID 2.16.840.1.113883.6.1 or DCM with the OID 1.2.840.10008.2.16.4.
   If the Code you want to add as a content type Code is already part of the Code System, write down the Code. You can skip the next 3 steps and switch to the *Code Sets* tab directly.
3. Click **Add New Code**.
4. Add the new content type's Code Key and Display Value (for example, X-CON and Contract Document).
5. Click **OK** and then on **Save**.
6. Switch to the *Code Sets* tab.
7. Select the current version of the Code Set LOINC-CONTENT-TYPE-DEFAULT or DCM-CONTENT-TYPE-DEFAULT.
8. Select the checkbox next to the new Code (for example, X-CON).

9. Click **Save**.
   - ⇨ A new (minor) version of the Code Set has been created (for example, version 1.1.0).
10. Switch to the *Code Categories* tab.
11. Select the Code Category C_GE_DRR_CONTENTTYPE_CODE.
12. Click **Assign Code Set**.
13. Select the new minor version of the LOINC-CONTENT-TYPE-DEFAULT or DCM-CONTENT-TYPE-DEFAULT Code Set for example, version 1.1.0.
14. Click **OK**.
   - ⇨ The new version of the Code Set is now assigned and active. The old version is inactive.
15. Click **Save**.

4.1.4.2 Deactivating a content type code

The following instructions assume that you know the Code Set of the content type Code you want to deactivate.

1. Log in to the Terminology Tools section of the Administration interface.
2. Click **Code Sets**.
3. Select the current version of the Code Set of the content type Code you want to deactivate, for example, LOINC-CONTENT-TYPE-DEFAULT.
4. Deselect the Code you want to deactivate.
5. Click **Save**.
   - ⇨ A new major version of the Code Set has been created (for example, version 2.0.0).
6. Switch to the *Code Categories* tab.
7. Select the Code Category C_GE_DRR_CONTENTTYPE_CODE.
8. Click **Assign Code Set**.
9. Select the new major version of the Code Set you just edited, for example, LOINC-CONTENT-TYPE-DEFAULT version 2.0.0.
10. Click **OK**.
   - ⇨ The new version of the Code Set is now assigned and active. The old version is inactive.
11. Click **Save.**

4.1.4.3 Adding a new code system for content type codes

Adding a new Code System for class Codes is necessary if LOINC or DCM does not meet your needs. If you want to use another Code System that already exists (for example, Health Care Provider Taxonomy), you can skip the first 10 steps.

1. Log in to the Terminology Tools section of the Administration interface.
2. Click **Add Code System**.
3. Enter a Code System name (for example, Custom Content Type Codes) and a Code System OID (for example, 1.2.3.4.5.6.9).
4. Click **Save**.
5. Select the newly created Code System.
6. Click **Add New Code**
7. Enter a Code Key (for example, A1) and a Display Value (for example, Regular Examination).
8. Click **OK**.
9. Add the Codes you need.
10. Click **Save**.
11. Switch to the *Code Sets* tab.
12. Click **Add Code Set**.
13. Enter a Code Set name (for example, MY-CONTENT-TYPE-CODES).
14. Select the new Code System in the dropdown box (for example, Custom Content Type Codes).
15. Click **Save**.
16. Switch to the *Code Categories* tab.
17. Select the Code Category C_GE_DRR_CONTENTTYPE_CODE.
18. Click **Assign Code Sets**.
19. Select the new Code Set (for example, MY- CONTENT-TYPE-CODES).
20. Click **OK**.
21. Click **Save**.

4.1.4.4 Deactivating a code system for content type codes

You can deactivate Code Systems, for example, when replacing them with a different terminology. Follow these steps to stop supporting a specific Code System for content type Codes (for example, Custom Content Type Codes).

1. Log in to the Terminology Tools section of the Administration interface.

2. Switch to the *Code Categories* tab.
3. Select the Code Category C_GE_DRR_CONTENTTYPE_CODE.
4. Click the **Active** link in the Status column of the Code Set (for example, MY- CONTENT-TYPE-CODES) in the Code System you want to deactivate (for example, Custom Content Type Codes)
5. Click **Save**.

4.1.5 Configuring the accepted XDS Document event codes

4.1.5.1 Adding a LOINC or DCM-based event code

Follow these steps to allow a new LOINC or DCM Code to be used as an event Code.

1. Log in to the Terminology Tools section of the Administration interface.
2. Open the Code System LOINC with the OID 2.16.840.1.113883.6.1 or DCM with the OID 1.2.840.10008.2.16.4.
   If the Code you want to add as an event Code is already part of the Code System, write down the Code. You can skip the next 3 steps and switch to the *Code Sets* tab directly.
3. Click **Add New Code**.
4. Add the new event Code Key and Display Value (for example, X-CON and Contract Document).
5. Click**OK** and then **Save**.
6. Switch to the *Code Sets* tab.
7. Select the current version of the Code Set LOINC-EVENT-CODES-DEFAULT or DCM-EVENT-CODE-DEFAULT.
8. Select the checkbox beside the new Code (for example, X-CON).
9. Click **Save**.
   ⇨ A new (minor) version of the Code Set is created (for example, version 1.1.0).
10. Switch to the *Code Categories* tab.
11. Select the Code Category C_GE_DRR_EVENT_CODE.
12. Click **Assign Code Set**.
13. Select the new minor version of the LOINC-EVENT-CODES-DEFAULT (or DCM-EVENT-CODE-DEFAULT) Code Set (for example, version 1.1.0).
14. Click on **OK**.
    ⇨ The new version of the Code Set is now assigned and active, the old version is inactive.

15. Click **Save**.

4.1.5.2 Deactivating an event code

The following instructions assume that you know the Code Set of the event type Code you want to deactivate. Please note that you must not deactivate any event Codes from the PRIVACY-POLICIES-PROTECTED-DEFAULT Code Set.

1. Log in to the Terminology Tools section of the Administration interface.
2. Click **Code Sets**.
3. Select the current version of the Code Set of the event Code you want to deactivate (for example, LOINC-EVENT-CODES-DEFAULT).
4. Deselect the Code you want to deactivate.
5. Click on **Save**.

   ⇨ A new major version of the Code Set is created (for example, version 2.0.0).
6. Switch to the *Code Categories* tab.
7. Select the Code Category C_GE_DRR_EVENT_CODE.
8. Click **Assign Code Set**.
9. Select the new major version of the Code Set you just edited (for example, LOINC-EVENT-CODES-DEFAULT version 2.0.0).
10. Click **OK**.

    ⇨ The new version of the Code Set is now assigned and active. The old version is inactive.
11. Click **Save.**

4.1.5.3 Adding a new code system for event codes

Adding a new Code System for class Codes is necessary if LOINC or DCM does not meet your needs. If you want to use another Code System that already exists (for example, HL7 Encounter Codes) you can skip the first 10 steps.

1. Log in to the Terminology Tools section of the Administration interface.
2. Click **Add Code System**.
3. Enter a Code System name (for example, Custom Event Codes) and a Code System OID (for example, 1.2.3.4.5.6.10).
4. Click **Save**.
5. Select the newly created Code System.
6. Click **Add New Code**.

7. Enter a Code Key (for example, A1) and a Display Value (for example, Regular Examination).
8. Click **OK**.
9. Add as many Codes as you need.
10. Click **Save**.
11. Switch to the *Code Sets* tab.
12. Click **Add Code Set**.
13. Enter a Code Set name (for example, MY-EVENT-CODES).
14. Select the new Code System in the dropdown box (for example, Custom Event Codes).
15. Click **Save**.
16. Switch to the *Code Categories* tab.
17. Select the Code Category C_GE_DRR_EVENT_CODE.
18. Click **Assign Code Sets**.
19. Select the new Code Set (for example, MY-EVENT-CODES).
20. Click **OK** and then **Save**.

4.1.5.4 Deactivating a code system for event codes

You can deactivate Code Systems, for example, when replacing them with a different terminology. Do not deactivate the PRIVACY-POLICIES-PROTECTED-DEFAULT Code Set which is needed for the Professional Exchange Server to function properly. Follow these steps to stop supporting a specific Code System for content type Codes (for example, *Custom Event Codes*).

1. Log in to the Terminology Tools section of the Administration interface.
2. Switch to the *Code Categories* tab.
3. Select the Code Category C_GE_DRR_EVENT_CODE.
4. Click the **Active** link in the Status column of the Code Set row (for example, MY-EVENT-CODES).
5. Click **Save**.

4.1.6 Configuring the accepted XDS Document Format Codes

4.1.6.1 Adding an IHE format code

The IHE format Codes may be extended, but the other default Code Systems for format Codes (DCMUID [1.2.840.10008.2.6.1] and General Format Codes [2.16.840.1.113883.3.37.4.1.9.101]) should not be extended, to simplify upgrades to newer versions of the Professional Exchange Server. It is recommended to add a new Code System instead (for example, Custom Format Codes).

Follow these steps to allow a new IHE format Code to be used as a format Code.

1. Log in to the Terminology Tools section of the Administration interface.
2. Open the Code System IHE Format Codes with the OID 1.3.6.1.4.1.19376.1.2.3. If the Code you want to add as a format Code is already part of the Code System, write down the Code. You can skip the next 3 steps and switch to the Code Sets tabs directly.
3. Click **Add New Code**.
4. Add the new IHE format Code Key (for example, urn:ihe:iti:xds-sd:pdf:2011) and Display Value (for example, Scanned Documents with PDF (XDS-SD 2011)).
5. Click **OK** and then **Save**.
6. Switch to the *Code Sets* tab.
7. Select the current version of the Code Set IHE-FORMAT-CODES-DEFAULT.
8. Select the checkbox beside the new Code (for example, beside urn:ihe:iti:xds-sd:pdf:2011).
9. Click **Save**.
   - ⇨ A new (minor) version of the Code Set has been created (for example, version 1.1.0).
10. Switch to the *Code Categories* tab.
11. Select the Code Category C_GE_DRR_FORMAT_CODE.
12. Click **Assign Code Set**.
13. Select the new minor version of the IHE-FORMAT-CODES-DEFAULT Code Set (for example, version 1.1.0).
14. Click **OK**.
   - ⇨ The new version of the Code Set is now assigned and active. The old version is inactive.
15. Click **Save**.

4.1.6.2 Deactivating a format code

The following instructions assume that you know the Code Set of the format Code you want to deactivate.

1. Log in to the Terminology Tools section of the Administration interface.
2. Switch to the Code Sets tab.
3. Select the current version of the Code Set of the format Code you want to deactivate (for example, GENERAL-FORMAT-CODES-DEFAULT).
4. Deselect the Code you want to deactivate.
5. Click **Save**.
   - ⇨ A new major version of the Code Set has been created (for example, version 2.0.0).
6. Switch to the *Code Categories* tab.
7. Select the Code Category C_GE_DRR_FORMAT_CODE.
8. Click on **Assign Code Set**.
9. Select the new major version of the Code Set you just edited (for example, GENERAL-FORMAT-CODES-DEFAULT version 2.0.0).
10. Click **OK**.
    - ⇨ The new version of the Code Set is now assigned and active. The old version is inactive.
11. Click **Save**.

4.1.6.3 Adding a new code system for format codes

Adding a new Code System for format Codes is necessary if the standards-based IHE Codes and the default General Format Codes do not meet your needs.

1. Log in to the Terminology Tools section of the Administration interface.
2. Click **Add Code System**.
3. Enter a Code System name (for example, Custom Format Codes) and a Code System OID (for example, 1.2.3.4.5.6.11).
4. Click **Save.**
5. Select the newly created Code System.
6. Click **Add New Code**.
7. Enter a Code Key (for example, National CDA) and a Display Value (for example, National CDA Standard).
8. Click **OK**.

9. Add the Codes you need.
10. Click **Save**.
11. Switch to the *Code Sets* tab.
12. Click **Add Code Set**.
13. Enter a Code Set name, (for example, CUSTOM-FORMAT-CODES).
14. Select the new Code System in the dropdown box (for example, Custom Format Codes).
15. Click **Save**.
16. Switch to the *Code Categories* tab.
17. Select the Code Category C_GE_DRR_FORMAT_CODE.
18. Click **Assign Code Sets**.
19. Select the new Code Set (for example, CUSTOM-FORMAT-CODES).
20. Click **OK**.
21. Click Save.

4.1.6.4 Deactivating a code system for format codes

You can deactivate Code Systems, for example when replacing them with a different terminology. Follow these steps to stop supporting a specific Code System for folder Codes (for example, Custom Format Codes).

1. Log in to the Terminology Tools section of the Administration interface.
2. Switch to the *Code Categories* tab.
3. Select the Code Category C_GE_DRR_FORMAT_CODE.
4. Click the **Active** link in the Status column of the Code Set row (for example, CUSTOM-FORMAT-CODES) of the Code System you want to deactivate (for example, Custom Format Codes).
5. Click **Save**.

4.1.7 Configuring the accepted XDS Document Healthcare Facility Type Codes

4.1.7.1 Adding a Health Care Provider Taxonomy code

Follow these steps to allow a new Health Care Provider Taxonomy Code to be used as a healthcare facility type Code.

1. Log in to the Terminology Tools section of the Administration interface.

2. Open the Code System Health Care Provider Taxonomy with the OID 2.16.840.1.113883.6.101.
   If the Code you want to add as a healthcare facility type Code is already part of the Code System, write down the Code. You can skip the next 3 steps and switch to the *Code Sets* tab directly.
3. Click **Add New Code**.
4. Add the new Health Care Provider Taxonomy Code Key and Value Display (for example, 101YM0800X and Bionics Center).
5. Click **OK** and then **Save**.
6. Switch to the *Code Sets* tab.
7. Select the current version of the Code Set PROVIDER-TXNMY-HEALTHCARE-FACILITY-DEFAULT.
8. Select the checkbox to include the new Code (for example, next to 101YM0800X).
9. Click **Save**.
   ⇨ A new (minor) version of the Code Set has been created (for example, version 1.1.0).
10. Switch to the *Code Categories* tab.
11. Select the Code Category C_GE_DRR_HEALTHCAREFACILITY_CODE.
12. Click on **Assign Code Set**.
13. Select the new minor version of the PROVIDER-TXNMY-HEALTHCARE-FACILITY-DEFAULT Code Set (for example, version 1.1.0).
14. Click **OK**.
    ⇨ The new version of the Code Set is now assigned and active. The old version is inactive.
15. Click **Save**.

4.1.7.2 Deactivating a Healthcare facility type Code

The following instructions assume that you know the Code Set of the healthcare facility type Codes you want to deactivate.

1. Log in to the Terminology Tools section of the Administration interface.
2. Switch to the *Code Sets* tab.
3. Select the current version of the Code Set of the healthcare facility type Code you want to deactivate (for example, PROVIDER-TXNMY-HEALTHCARE-FACILITY-DEFAULT).
4. Deselect the Code you want to deactivate.

5. Click **Save**.
   - ⇨ A new major version of the Code Set has been created (for example, version 2.0.0).
6. Switch to the *Code Categories* tab.
7. Select the Code Category C_GE_DRR_HEALTHCAREFACILITY_CODE.
8. Click **Assign Code Set**.
9. Select the new major version of the Code Set you just edited, for example, PROVIDER-TXNMY-HEALTHCARE-FACILITY-DEFAULT version 2.0.0
10. Click **OK**.
    - ⇨ The new version of the Code Set is now assigned and active and the old version is inactive.
11. Click **Save**.

4.1.7.3 Adding a new Code system for healthcare facility type codes

Adding a new Code System for healthcare facility type Codes is necessary if the Health Care Provider Taxonomy Codes do not meet all your needs.

1. Log in to the Terminology Tools section of the Administration interface.
2. Click **Add Code System**.
3. Enter a Code System Name (for example, Custom Facility Type Codes) and a Code System OID (for example, 1.2.3.4.5.6.12)
4. Click **Save**.
5. Select the newly created Code System.
6. Click on **Add New Code**.
7. Enter a Code Key (for example, KB) and a Display Value (for example, Bionics Research Facility)
8. Click **OK**.
9. Add the Codes that you need.
10. Click **Save**.
11. Switch to the *Code Sets* tab.
12. Click **Add Code Set**.
13. Enter a Code Set Name (for example, CUSTOM-FACILITY-TYPE-CODES).
14. Select the new Code System in the dropdown box (for example, Custom Facility Type Codes).
15. Click **Save**.
16. Switch to the *Code Categories* tab.

17. Select the Code Category C_GE_DRR_HEALTHCAREFACILITY_CODE.
18. Click on **Assign Code Sets**.
19. Select the new Code Set (for example, CUSTOM-FACILITY-TYPE-CODES).
20. Click **OK**.
21. Click **Save**.

4.1.7.4 Deactivating a Code system for healthcare facility type codes

You can deactivate Code Systems, for example when replacing them with a different terminology. Follow these steps to stop supporting a specific Code System for healthcare facility type Codes (for example, Custom Facility Codes):

1. Log in to the Terminology Tools section of the Administration interface.
2. Switch to **Code Categories**.
3. Select the **Code Category** C_GE_DRR_HEALTHCAREFACILITY_CODE.
4. Click the **Active** link in the status column of Code Set row (for example, CUSTOM-FACILITY-CODES).
5. Click **Save**.

4.1.8 Configuring the accepted XDS Document Practice Setting Codes

4.1.8.1 Adding a Health Care Provider Taxonomy Code

Follow these steps to allow a new Health Care Provider Taxonomy Code to be used as a practice setting Code.

1. Log in to the Terminology Tools section of Administration interface.
2. Open the Code System Health Care Provider Taxonomy with the OID 2.16.840.1.113883.6.101
   - ⇨ If the Code you want to add as a practice setting Code is already part of the Code System, write down the Code. You can skip the next 3 steps and switch to the *Code Sets* tab directly.
3. Click **Add New Code**
4. Add the new Health Care Provider Taxonomy Code Key and Display Value (for example, 101YM0800X and Bionics Center).
5. Click **OK** and then **Save**
6. Switch to the *Code Sets* tab.

7. Select the current version of the Code Set PROVIDER-TXNMY-PRACTICE-SETTING-DEFAULT
8. Select the checkbox in front of the new Code (for example, in front of 101YM0800X).
9. Click **Save**.
   - ⇨ A new (minor) version of the Code Set has been created (for example, version 1.1.0)
10. Switch to the *Code Categories* tab.
11. Select the Code Category C_GE_DRR_PRACTICESETTING_CODE
12. Click **Assign Code Set**.
13. Select the new minor version of the PROVIDER-TXNMY-PRACTICE-SETTING-DEFAULT Code Set (for example, version 1.1.0)
14. Click on **OK**.
    - ⇨ The new version of the Code Set is now assigned and active, the old version is inactive.
15. Click **Save.**

4.1.8.2 Deactivating a practice setting code

The following instructions assume that you know the Code Set of the practice setting Codes you want to deactivate.

1. Log in to the Terminology Tools section of Administration interface.
2. Switch to the *Code Sets* tab.
3. Select the current version of the Code Set of the practice setting Code you want to deactivate, for example, PROVIDER-TXNMY-PRACTICE-SETTING-DEFAULT
4. Deselect the Code you want to deactivate.
5. Click **Save**.
   - ⇨ A new major version of the Code Set has been created (for example, version 2.0.0)
6. Switch to the *Code Categories* tab.
7. Select the Code Category C_GE_DRR_PRACTICESETTING_CODE
8. Click **Assign Code Set**.
9. Select the new major version of the Code Set you just edited, for example, PROVIDER-TXNMY-PRACTICE-SETTING-DEFAULT version 2.0.0
10. Click **OK**

⇨ The new version of the Code Set is now assigned and active, the old version is inactive.

11. Click **Save**.

4.1.8.3 Adding a new code system for practice setting codes

Adding a new Code System for practice setting Codes is necessary if the Health Care Provider Taxonomy Codes do not fulfill your needs.

1. Log in to the Terminology Tools section of Administration interface.
2. Click **Add Code System**.
3. Enter a Code System name (for example, Custom Speciality Codes) and a Code System OID (for example, 1.2.3.4.5.6.13).
4. Click **Save**.
5. Select the newly created Code System.
6. Click **Add New Code**.
7. Enter a Code Key and a Display Value (for example, bio and Bionics).
8. Click **OK**.
9. Add the Codes you need.
10. Click **Save**.
11. Switch to the *Code Sets* tab.
12. Click **Add Code Set**.
13. Enter a Code Set name (for example, CUSTOM-SPECIALITY-CODES).
14. Select the new Code System in the dropdown box (for example, Custom Speciality Codes).
15. Click **Save**.
16. Switch to the *Code Categories* tab.
17. Select the Code Category C_GE_DRR_PRACTICESETTING_CODE.
18. Click on **Assign Code Sets**.
19. Select the new Code Set (for example, CUSTOM-SPECIALITY-CODES).
20. Click **OK**.
21. Click **Save**.

4.1.8.4 Deactivating a code system for practice setting codes

You can deactivate Code Systems, for example when replacing them with a different terminology. Follow these steps to stop supporting a specific Code System for practice setting Codes (for example, Custom Speciality Codes).

1. Log in to the Terminology Tools section of the Administration interface.
2. Switch to the *Code Categories* tab.
3. Select the Code Category C_GE_DRR_PRACTICESETTING_CODE.
4. Click the **Active** link in the Status column of the Code Set row (for example, CUSTOM-SPECIALITY-CODES).
5. Click **Save**.

4.1.9 Configuring the accepted XDS Document type codes

4.1.9.1 Adding a LOINC-based type code

Follow these steps to allow a new LOINC Code to be used as a type Code:

1. Log in to the Terminology Tools section of the Administration interface.
2. Open the Code System LOINC with the OID 2.16.840.1.113883.6.1.
   If the Code you want to add as a type Code is already part of the Code System, write down the Code. You can skip the next 3 steps and switch to the *Code Sets* tab directly.
3. Click **Add new Code**.
4. Add the new LOINC type's Code Key and Display Value (for example, X-CON and Contract Document).
5. Click **OK** and then **Save**.
6. Switch to the *Code Sets* tab.
7. Select the current version of the Code Set LOINC-TYPE-CODE-DEFAULT.
8. Select the include checkbox for the new Code, (for example, in front of X-CON).
9. Click **Save**.
   ⇨ A new (minor) version of the Code Set has been created (for example, version 1.1.0).
10. Switch to the *Code Categories* tab.
11. Select the Code Category C_GE_DRR_TYPE_CODE.
12. Click **Assign Code Set**.

13. Select the new minor version of the LOINC-TYPE-CODE-DEFAULT Code Set (for example, version 1.1.0).
14. Click **OK**.
    - ⇨ The new version of the Code Set is now assigned and active. The old version is inactive.
15. Click **Save.**.

4.1.9.2 Deactivating a type code

You can deactivate any type Code. The following instructions assume that you know the Code Set of the type Code you want to deactivate.

1. Log in to the Terminology Tools section of the Administration interface.
2. Switch to the *Code Sets* tab.
3. Select the current version of the Code Set of the type Code you want to deactivate (for example, LOINC-TYPE-CODE-DEFAULT).
4. Deselect the Code you want to deactivate.
5. Click **Save**.
    - ⇨ A new major version of the Code Set has been created (for example, version 2.0.0).
6. Switch to the *Code Categories* tab.
7. Select the Code Category C_GE_DRR_TYPE_CODE.
8. Click **Assign Code Set**.
9. Select the new major version of the Code Set you just edited (for example, LOINC-TYPE-CODE-DEFAULT version 2.0.0).
10. Click **OK**.
    - ⇨ The new version of the Code Set is now assigned and active. The old version is inactive.
11. Click **Save**.

4.1.9.3 Adding a new code system for type codes

Adding a new Code System for type Codes is necessary if LOINC does not meet your needs. If you want to use another Code System that already existis (for example, DCM), you may skip the first 10 steps.

1. Log in to the Terminology Tools section of the Administration interface.
2. Click **Add Code System**.

3. Enter a Code System Name (for example, Custom Type Codes) and a Code System OID (for example, 1.2.3.4.5.6.15).
4. Click **Save**.
5. Select the newly created Code System.
6. Click **Add New Code**.
7. Enter a Code Key (for example, P1) and a Display Value (for example, Progress Note).
8. Click **OK**.
9. Add the Codes you need.
10. Click **Save**.
11. Switch to the *Code Sets* tab.
12. Click **Add Code Set**.
13. Enter a Code Set Name (for example, MY-TYPE-CODES).
14. Select the new Code System in the dropdown box (for example, Custom Type Codes).
15. Click **Save**.
16. Switch to the *Code Categories* tab.
17. Select the Code Category C_GE_DRR_TYPE_CODE.
18. Click **Assign Code Sets**.
19. Select the new Code Set (for example, MY-TYPE-CODES).
20. Click **OK**.
21. Click **Save**.

4.1.9.4 Deactivating a code system for type codes

You can deactivate Code Systems for example, when replacing them with a different terminology. Follow these steps to stop supporting a specific Code System for type Codes (for example, Custom Type Codes).

1. Log in to the Terminology Tools section of the Administration interface.
2. Switch to the *Code Categories* tab.
3. Select the Code Category C_GE_DRR_TYPE_CODE.
4. Click **Save**.

4.1.10 Configuring the accepted XDS Document language codes

4.1.10.1 Adding a new language code

The `XDSDocumentEntry.languageCode` is specified as an RFC 3066 language tag. The RFC suggests that the use of 2 letter ISO 639-1 Codes, possibly in combination with a 2 letter ISO 3166 country Code is preferred.

NOTE **Case sensitivity**

Note that Codes in the Professional Exchange Server are case-sensitive.

The RFC suggests, but does not require, using lower case language Codes and upper case country Codes. If you need to support both upper and lower case country Codes, you need to add two Codes (which can have the same display value) per supported language tag. For example: “en-us” vs. “en-US”. The application includes all of the ISO 639-1 Codes and a selection of “language code-country code” values with upper case country Codes.

NOTE **Language codes**

Note that the Professional Exchange Server can only support one Code System for all language Codes.

In the current version of the application, the Professional Exchange Server Document Repository enforces that only the configured language Codes are used. Therefore, there are no checks on the language Codes during **Register Document Set-b** transactions, checks occur only during **Provide and Register Document Set-b** transactions. This means that you do not need to add any language Codes in the Professional Exchange Server if you are not using the Professional Exchange Server Document Repository.

1. Log in to the Terminology Tools section of Administration interface.
2. Open the Code System ISO639-1 Language Codes with the OID 1.0.639.1
3. Click **Add New Code**.
4. Add the new language Code Key andDisplay Value (for example, ar-EG and Arabic (Egypt)).
5. Click **OK** and then **Save**.
6. Switch to the*Code Sets* tab.
7. Select the current version of the Code Set LANG-CODES-ALPHA2-DEFAULT.
8. Select the checkbox next to the newly added Code (for example, next to ar-EG).

9. Click **Save**.
   - ⇨ A new (minor) version of the Code Set has been created (for example, version 1.1.0).
10. Switch to the *Code Categories* tab.
11. Select the Code Category C-DOCUMENT-LANGUAGE.
12. Click **Assign Code Set**.
13. Select the new minor version of the LANG-CODES-ALPHA2-DEFAULT Code Set (for example, version 1.1.0).
14. Click **OK**.
    - ⇨ The new version of the Code Set is now assigned and active. The old version is inactive.
15. Click **Save**.
    If you need support for lower-case country Codes as well, repeat the steps using a lower case version of the country Code (for example, ar-eg and Arabic (Egypt)).

4.1.10.2 Deactivating a language code

In the current version of the application, the Professional Exchange Server Document Repository enforces that only the configured language Codes are used. Therefore there are no checks on the language Codes during **Register Document Set-b** transactions, only during **Provide and Register Document Set-b** transactions. This means that even after deactivating a language Code in the application the Professional Exchange Server Document Registry will accept document metadata with the newly deactivated language Code.

To deactivate a language Code you need to follow these steps:

1. Log in to the Terminology Tools section of the Administration interface.
2. Switch to the *Code Sets* tab.
3. Select the current version of the LANG-CODES-ALPHA2-DEFAULT Code Set.
4. Deselect the Language Code you want to deactivate.
5. Click **Save**.
   - ⇨ A new major version of the Code Set has been created (for example, version 2.0.0).
6. Switch to the *Code Categories* tab.
7. Select the Code Category C-DOCUMENT-LANGUAGE.
8. Click **Assign Code Set**.

9. Select the new major version of the LANG-CODES-ALPHA2-DEFAULT Code Set (for example, version 2.0.0).
10. Click **OK**.
    - ⇨ The new version of the Code Set is now assigned and active. The old version is inactive.
11. Click **Save**.

4.1.10.3 Reactivating an existing language code

To reactivate a language Code that is already part of the Code System, but has been removed from the current Code Set, follow these steps.

1. Log in to the Terminology Tools section of the Administration interface.
2. Switch to the *Code Sets* tab.
3. Select the current version of the Code Set LANG-CODES-ALPHA2-DEFAULT.
4. Select the checkbox next to the Code that you want to reactivate.
5. Click **Save**.
    - ⇨ A new (minor) version of the Code Set has been created (for example, version 2.1.0).
6. Switch to the *Code Categories* tab.
7. Select the Code Category C-DOCUMENT-LANGUAGE.
8. Click **Assign Code Set**.
9. Select the new minor version of the LANG-CODES-ALPHA2-DEFAULT Code Set (for example, version 2.1.0).
10. Click **OK**.
    - ⇨ The new version of the Code Set is now assigned and active. The old version is inactive.
11. Click **Save**.

4.2 Changing the display values of codes

Please see theTerminology Tools [page 43] section for general information on how to change the display value of a Code. This section focuses on special procedures.

4.2.1 Configuring the displayed patient marital status codes

4.2.1.1 Adding a new marital status code for display

NOTE

The Professional Exchange Server can only support one Code System for marital status codes!
Unlike XDS metadata, the Professional Exchange Server accepts most patient data even if it does not know all the Codes. The application will accept and store any marital status Code it can find in a PIX patient identity feed message. It will attempt to resolve the Code for display in the application's GUI, but if it fails because the Code is not configured, it simply leaves the marital status empty. Therefore, the effect of adding a new marital status Code is limited to what is displayed, not what is accepted as input as is the case with the Code Systems for XDS.

1. Log in to the Terminology Tools section of the Administration interface.
2. Open the Code System Personal Maritalstatus with the OID 2.16.840.1.113883.12.2.
3. Click on **Add New Code**.
4. Add the new marital status Code Key and Display Value (for example, P and Polygamy).
5. Click **OK** and then **Save**.
6. Switch to the *Code Sets* tab.
7. Select the current version of the Code Set *PXS-PERSON-MARITALSTATUS.*
8. Select the checkbox in front of the newly added Code (for example, in front of P).
9. Click **Save**.
   A new (minor) version of the Code Set has been created (for example, version 1.1.0).
10. Switch to the *Code Categories* tab.
11. Select the Code Category C-PERSON-MARITALSTATUS.
12. Click **Assign Code Set**.
13. Select the new minor version of the C-PERSON-MARITALSTATUS Code Set (for example, version 1.1.0).
14. Click **OK**.

- ⇨ The new version of the Code Set is now assigned and active. The old version is inactive.

15. Click on **Save**.

4.2.1.2 Deactivating a marital status Code to prohibit display

The marital status codes are used only for display purposes. If the Code stored for a patient is not part of the Code Category, the marital status is not displayed.

To deactivate a marital status Code you need to follow these steps:

1. Log in to the Terminology Tools section of the Administration interface.
2. Switch to the *Code Sets* tab.
3. Select the current version of the Code Set PXS-PERSON-MARITALSTATUS.
4. Deselect the marital status Code you want to deactivate.
5. Click on **Save**.
   - ⇨ A new major version of the Code Set has been created (for example, version 2.0.0).
6. Switch to the *Code Categories* tab.
7. Select the Code Category C-PERSON-MARITALSTATUS.
8. Click on **Assign Code Set**.
9. Select the new major version of the C-PERSON-MARITALSTATUS Code Set (for example, version 2.0.0).
10. Click **OK**.
    - ⇨ The new version of the Code Set is now assigned and active. The old version is inactive.
11. Click **Save**.

4.3 Tasks after changing the Affinity Domain’s terminology

4.3.1 Reviewing metadata injection rules

If you are using metadata injection rules to manipulate incoming data, please review the GroovyRule files after making changes to the Affinity Domain’s terminology. The rules normally rely on certain metadata attributes that are often keys from Code Systems. Changes to the Code Systems might render some or all of the rules incompatible.

4.3.2 Changing metadata for the consent document

You should also keep in mind that the configured metadata for the consent document (for example, document type, facility type, and so on) needs to be changed manually (see Policy Acknowledgement Module Configuration [page 95]) whenever the user changes the relevant Code Systems using the Terminology UI.

5 Changing the application's system behavior

5.1 Configuring stylesheets for XML display in the application GUI

The application uses server-side stylesheet transformation to make structured data stored in XML formats human-readable. The application determines which stylesheet to use based on the combination of the MIME type and the `XDSDocumentEntry.formatCode`. For example, if the document to be transformed has the MIME type *text/xml* and the format code is `CDA` then a stylesheet for CDA documents is used.

The stylesheets are stored in the Tomcat folder under `<tomcat>/webapps/<webapp_name>/WEB-INF/classes/xsltTemplates`. The stylesheets are selected based on their file name, which is matched to the MIME type and format code of the document to display. The following algorithm is used to derive the stylesheet's filename from a MIME type and format code:

1. Convert MIME type to lower case.
2. Replace each character of the MIME type with an underscore "_" except for lower case letters (ASCII characters with decimal numbers between 97 and 122) and numbers (ASCII characters with decimal numbers between 48 and 57)
3. Convert format code to lower case.
4. Replace each character of the format code with an underscore "_" except for lower case letters (ASCII characters with decimal numbers between 97 and 122) and numbers (ASCII characters with decimal numbers between 48 and 57)
5. Concatenate the edited MIME type, the minus character, and the edited format code.
6. Add the file extension *.xsl*.

Example 1:

text/xml and *CDA/IHE 1.0* produce the filename `text_xml-cda_ihe_1_0.xsl`

Example 2:

text/xml and *CDAR2/IHE 1.0* produce the filename `text_xml-cdar2_ihe_1_0.xsl`

Changes to the stylesheets or the addition of new stylesheets do not necessarily require a restart of Tomcat, but please refer to the section on making changes to the Tomcat folder [page 27] for a discussion of the suggested approach.

5.2 Enabling or disabling unauthenticated XDS access

Access to the web services for XDS transactions normally requires authentication. During the installation the administrator may choose to allow unauthenticated XDS access. This is discouraged, but possible. If you decide to forego authentication for XDS, it is your responsibility to ensure that only authorized users have access to the patients' personal health information that is accessible through these interfaces. Instructions on how to ensure this using networking tools (VPNs, tunneling, IP filtering and so on) is outside the scope of this document.

If the administrator did not allow unauthenticated XDS access during the installation but needs this capability at a later time, then the web.xml file in Tomcat must be modified. The application's web.xml is located under `<tomcat>/webapps/<webapp_name>/WEB-INF`. Remove the comment tags around the following elements in the *web.xml*:

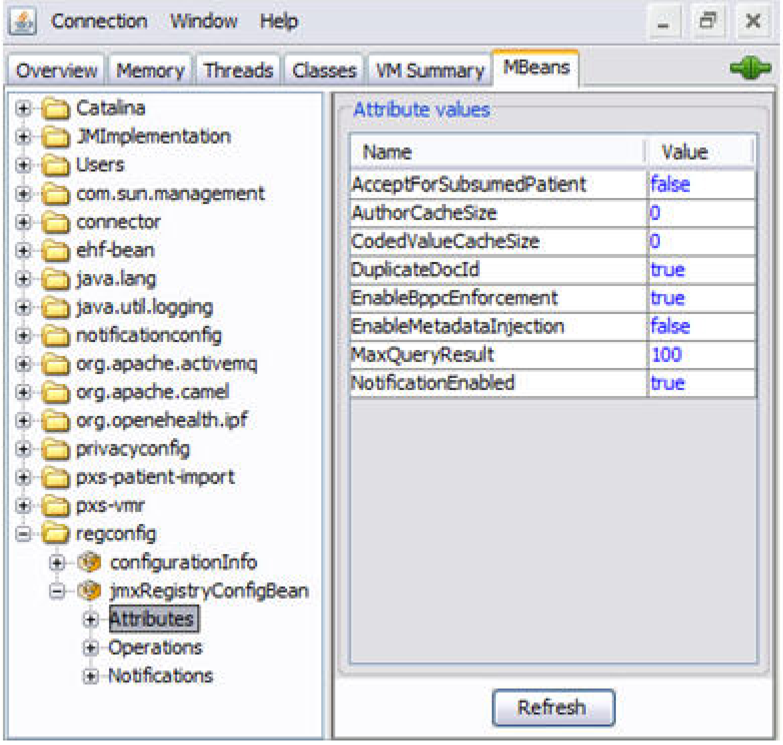
```
<filter-mapping>
<filter-name>anonymousAuthenticationFilter</filter-name>
<url-pattern>/unsecured_webservices/*</url-pattern>
</filter-mapping>

<servlet-mapping>
<servlet-name>CXFServlet</servlet-name>
<url-pattern>/unsecured_webservices/*</url-pattern>
</servlet-mapping>
```

You should shut down Tomcat before making any changes to the *web.xml*. Please see the section on making changes to the Tomcat folder [page 27] for instructions on how to safely perform this modification.

5.3 Changing the Document Registry configuration

The JMX runtime configuration interface allows changes of the registry's behavior. This section will give an overview of the different configuration options.



- Catalina
- JMImplementation
- Users
- com.sun.management
- connector
- ehf-bean
- java.lang
- java.util.logging
- notificationconfig
- org.apache.activemq
- org.apache.camel
- org.openehealth.ipf
- privacyconfig
- pxs-patient-import
- pxs-vmr
- regconfig
  - configurationInfo
  - jmxRegistryConfigBean
    - Attributes
    - Operations
    - Notifications

Attribute values

Name	Value
AcceptForSubsumedPatient	false
AuthorCacheSize	0
CodedValueCacheSize	0
DuplicateDocId	true
EnableBppcEnforcement	true
EnableMetadataInjection	false
MaxQueryResult	100
NotificationEnabled	true

Figure 43: Document Registry runtime configuration in JConsole

5.3.1 AcceptForSubsumedPatient

When set to *false* the registry will reject document registrations using patient IDs that have been the target of a PIX merge message (that is, the patient ID was communicated in the MRG segment of an ADT A40 PIX message). The default behavior is in line with the IHE XDS specification. Set this to `true` if you need more lenient behavior.

5.3.2 AuthorCacheSize

The author cache allows document registrations to be quickly processed by caching author data. When this parameter is set to `0`, caching is not used for authors. It is recommended to activate it. The suggested size is a direct function of the number of different author elements that can be expected in incoming messages. Given possible changes in author metadata and typos, it is recommended to use 1.5 * <number_of_authors> and rounding up to the next integer. *Number of authors* means the total number of providers in the exchange that will be referenced in the Document Source’s document registration messages.

5.3.3 CodedValueCacheSize

The *codedValueCache* also speeds up message processing by keeping coded values in memory. When this parameter is set to `0`, caching is not used for coded values. You are recommended to activate it. The suggested size is a function of the number of Code Keys in the application. The suggested value is 1.1 times the total number of code keys in the application (rounding up to the next integer). To calculate the total number of code keys, you may use the following SQL statement:

```
SELECT COUNT(DISTINCT(c.C_KEY))

FROM EHF_CODESYSTEM.T_CODECATEGORY ca, EHF_CODESYSTEM.T_CODESET cs, EHF_CODESYSTEM.J_CODESET jcs, EHF_CODESYSTEM.T_CODEVALUE cv, EHF_CODESYSTEM.T_CODE c

WHERE ca.C_CODESET_ID = cs.C_ID and cs.C_ID=jcs.T_CODESET_C_ID and jcs.CODES_C_ID=c.C_ID and c.C_OID = cv.C_OID and c.C_KEY=cv.C_KEY and ca.C_NAME like 'C_GE_DRR_%'
```

5.3.4 DuplicateDocId

This setting determines whether the Professional Exchange Server Registry accepts documents with duplicate IDs. This defaults to `true`, as specified by IHE XDS. Set this to `false` for stricter document handling.

5.3.5 EnableBPPCEnforcement, EnableMetadataInjection, and NotificationEnabled

These settings are discussed in a separate section.

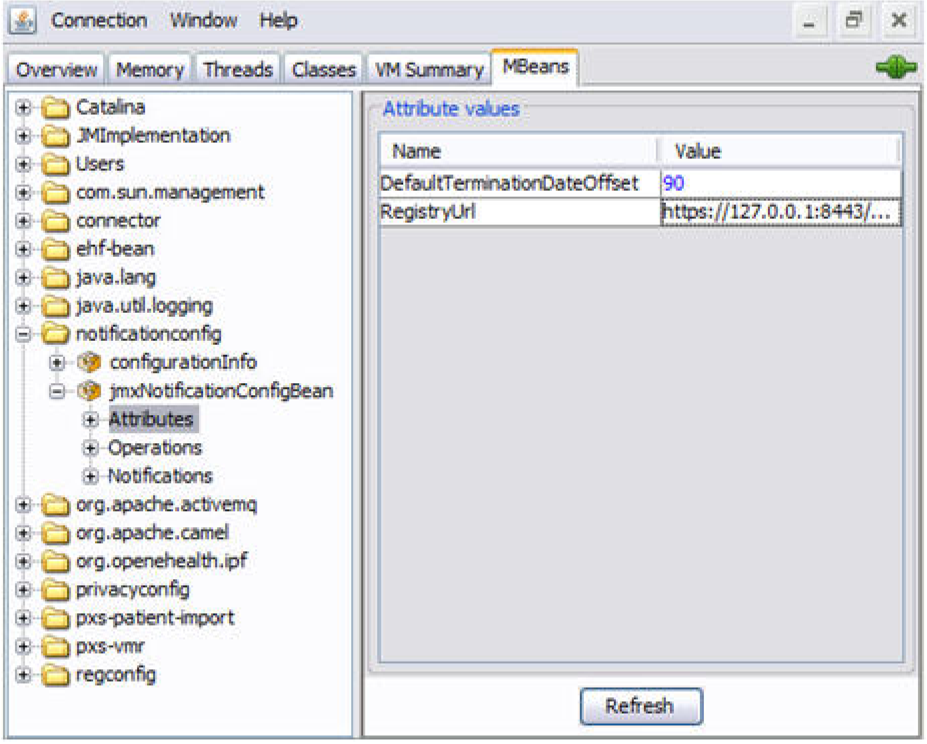
5.3.6 MaxQueryResult

To ensure fast responses the Document Registry does not answer *Registry Stored Query* requests if they cause too many results. This setting determines the maximum number of results, after which the registry will return an error message.

The default is 100 results.

5.4 Changing the Document Metadata Notification Broker configuration

The JMX runtime configuration interface allows changes to the DSUB notification broker's behavior. This section gives you an overview of the different configuration options.



Name	Value
DefaultTerminationDateOffset	90
RegistryUrl	https://127.0.0.1:8443/...

Figure 44: Notification Broker runtime configuration in JConsole

5.4.1 DefaultTerminationDateOffset

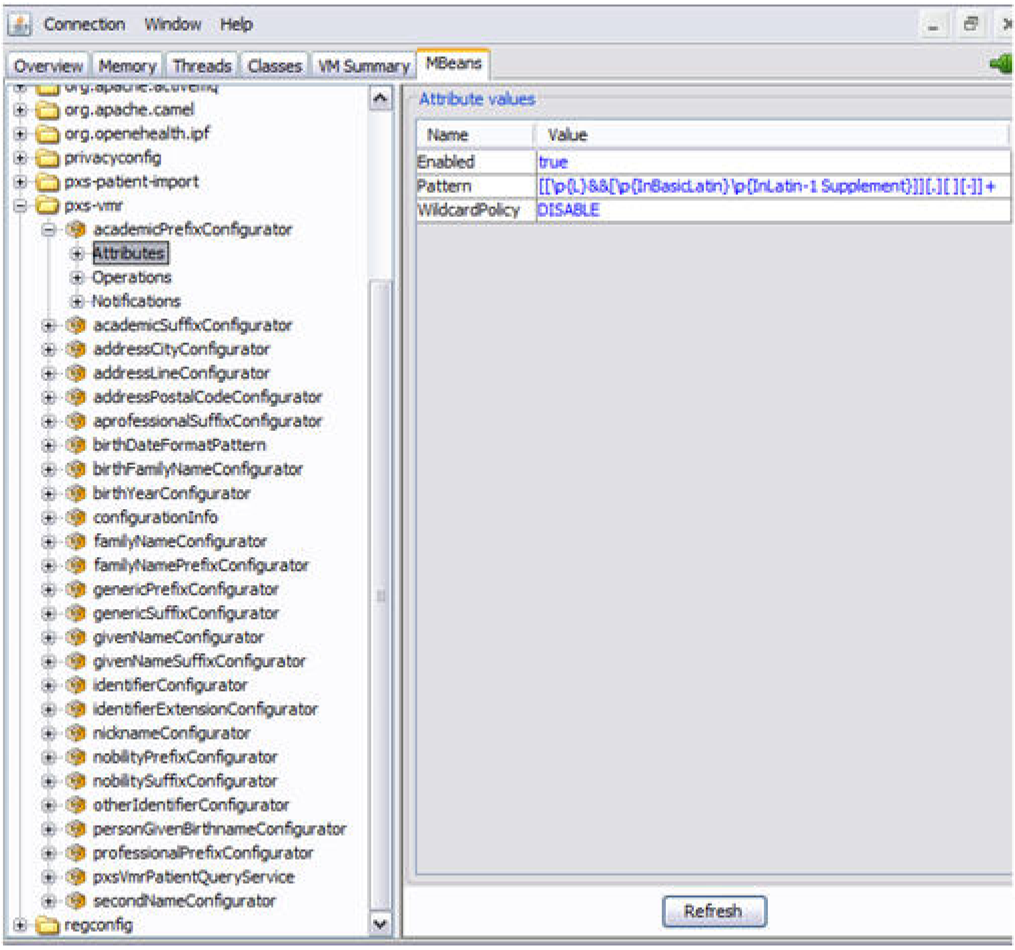
This offset determines how long a subscription is valid for, if no termination time was communicated by the subscriber. It is expressed as an offset in calendar days that is added to the current date when the subscription took place.

5.4.2 RegistryUrl

This is the URL that will be included as a producer reference in the outgoing notification in cases when the Professional Exchange Server Registry acts as the Document Metadata Publisher. It should point to one of the application's *Provide And Register Document Set-b* URLs, whichever URL is preferred.

5.5 Changing the application's GUI search behavior

The search in the GUI of Professional Exchange Server can be fine-tuned to achieve a balance between good performance and exhaustive searches. There are also two settings to limit each query’s resource usage.


Connection
Window
Help
Overview
Memory
Threads
Classes
VM Summary
MBeans
org.apache.activemq
org.apache.camel
org.openehealth.ipf
privacyconfig
pxs-patient-import
pxs-vmr
academicPrefixConfigurator
Attributes
Operations
Notifications
academicSuffixConfigurator
addressCityConfigurator
addressLineConfigurator
addressPostalCodeConfigurator
aprofessionalSuffixConfigurator
birthDateFormatPattern
birthFamilyNameConfigurator
birthYearConfigurator
configurationInfo
familyNameConfigurator
familyNamePrefixConfigurator
genericPrefixConfigurator
genericSuffixConfigurator
givenNameConfigurator
givenNameSuffixConfigurator
identifierConfigurator
identifierExtensionConfigurator
nicknameConfigurator
nobilityPrefixConfigurator
nobilitySuffixConfigurator
otherIdentifierConfigurator
personGivenBirthnameConfigurator
professionalPrefixConfigurator
pxsVmrPatientQueryService
secondNameConfigurator
regconfig
Attribute values
Refresh

Name	Value
Enabled	true
Pattern	[[\p{L}&&[\p{InBasicLatin}\p{InLatin-1 Supplement}]][.][ ][-]]+
WildcardPolicy	DISABLE

Figure 45: GUI runtime configuration in JConsole

5.5.1 MaxResultSize

This limits the resource usage of extensive queries by aborting searches that yield more than the configured number of patients (100 by default). In case a query returns more than the *MaxResultSize*, the user receives a message. It states that the query cannot be fulfilled because the result is too big and that the user needs to refine the search terms.

5.5.2 MaxSizeOfSearchTerms

The number of search terms that a user can use might also cause performance and stability issues. Therefore the number is limited to 10 by default. If the user enters more search terms than the default value, only the leftmost are considered.

5.5.3 *Configurator

There is a Configurator MBean for each patient demographics field that is stored in the application and which is searchable. This means the search can be fine tuned in three ways- by disabling the search for a field using the Enabled switch, by changing the wildcard policy and by modifying the regular expression.

Some background on how the search works:

Searching in the Professional Exchange Server GUI is done via one input field. For each separate search term, the application tries to interpret the input. It compares the search term to each enabled Configurator's regular expression to determine if the term could, for example, be a street name or a patient ID. For most search terms there will be many possibilities. All of the different possible interpretations of the search term are combined into a query using a logical OR. The same happens for the other search terms and for the complete query, the different search terms are combined using a logical AND.

The enabled flag for Configurators allows you to exclude patient data from the search that your users do not search for. For example, if nobody searches by address, you could deactivate all address-related Configurators and thereby improve the performance of the search.

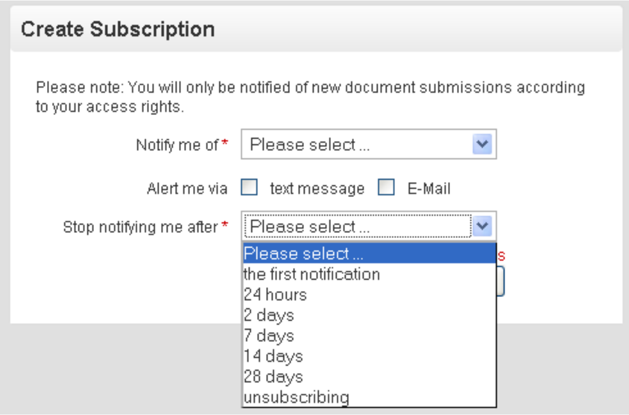
The wildcard policy can be set to "ENABLE", "DISABLE" or "AUTO". "ENABLE" means that the user may use the '*' as a wildcard character at the end of a search term (for example, "bosto*"). "DISABLE" means that the user cannot use a wildcard character for this patient data field (for example, for IDs it does not usually make sense). "AUTO" means that the algorithm always automatically appends a wildcard character to the term for this field.

The regular expression allows you to control how a search term is interpreted. For example, if all connected systems use only numerical patient IDs, you could ensure, through a regular expression, that only pure number strings lead to a query on the patient ID. The better you know the data in the system, the better you can fine tune the search to exclude searching in unnecessary columns.

5.6 Configuring Subscriptions

The *Create Subscription* dialog used to receive notifications about new patient data. It has three input fields that you can configure.

- The *Notify me of* field allows the user to select a subscription profile.
- *Alert me via* lets a user choose how they want to be notified.
- *Stop notifying me after* lets a user choose how long the notification period should last.



Create Subscription

Please note: You will only be notified of new document submissions according to your access rights.

Notify me of * Please select ...

Alert me via □ text message □ E-Mail

Stop notifying me after * Please select ...

Please select ...
the first notification
24 hours
2 days
7 days
14 days
28 days
unsubscribing

Figure 46: Create Subscription dialog

5.6.1 Subscription Profile Managment

Subscription profiles define the kinds of subscriptions that a user can subscribe to in the context of a patient. They are pre-defined filters that will match on one or more document criteria. Subscription profiles are managed as XML files on the file system, where one file represents one profile.

Subscription Profile configuration

Three default subscription profiles are delivered with the Professional Exchange Server application:

- Discharge Documents
- Emergency Care Documents
- Structured Documents

These profiles are defined in: `<tomcat>/webapps/<webapp_name>/WEB-INF/classes/subscriptionProfiles`

Configure custom profiles

You can switch to custom profiles while Professional Exchange Server is running. After switching to custom profiles, the default profiles are no longer available. No application restart is required.

1. Create a subscription directory on the Professional Exchange Server server and add your custom subscription profile XML file to that directory.
2. Open the JConsole configuration and open the MBeans tab.
3. Open the node `notificationprofileconfig - jmxNotification-Profile - Attributes` in the Mbeans tree.
4. Here you can configure the *ProfilesDirectory*. Always use a prefix `file:/` and an absolute, readable path to your subscription profile directory (for example, `file://home/pxs/subscriptionProfiles`).
5. After you configure the directory for your profiles, invoke `refreshProfiles` under `notificationprofileconfig - jmxNotification-Profile - Operations`
6. Check your application error log. If a file is unparseable or otherwise invalid during `refreshProfiles`, you will get error information there.

5.6.2 Alert option configuration

You can configure, which alert checkboxes should be available to users. Runtime configuration of the alerts can be done using JConsole.

To do this open the MBean called `pxs-vmr/notificationConfigurator`. The following attributes are relevant for alerting:

- *AlertViaTextMessageEnabled* - `true/false` - if set to `true`, the system will show a checkbox for getting text-messaging notifications, if the user has a mobile phone number. Default value is `false`.
- *AlertViaEmailEnabled* - `true/false` - if set to `true`, the system will show a checkbox to get email notifications. The user account musr have an associated e-mail address otherwise the checkbox will not be visible. Default value is `true`.

The email properties are located in the Tomcat webapps directory: `pxs-vmr-assembly\WEB-INF\classes\META-INF\ehealth.properties`

5.6.3 Subscription duration configuration

The options in the "Stop notifying me after" drop down menu can be configured at runtime. Runtime configuration of durations can be done using JConsole.

To do so open the MBean called *pxs-vmr/notificationConfigurator.* The following attributes are relevant for durations:

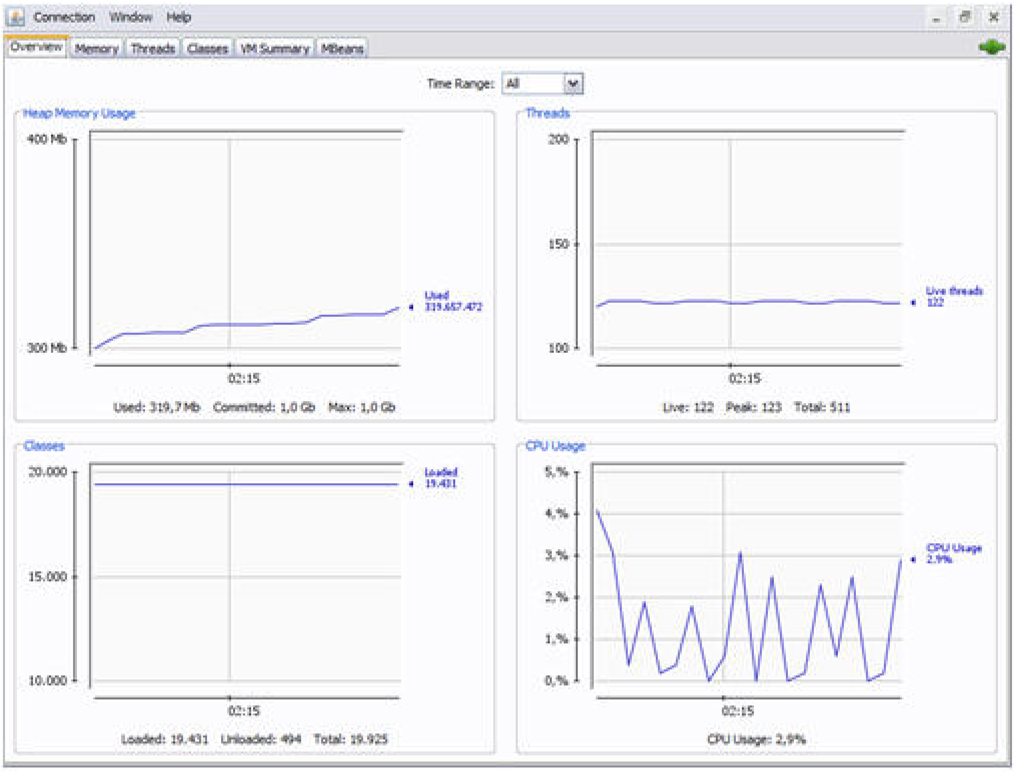
- *StopNotifyingAfterUnsubscribingEnabled* - `true/false` - if set to `true`, you will have an option to create a subscription that does not expire.
- *StopNotifyingAfterFirstNotificationEnabled* - `true/false` - if set to `true`, you will have an option to create a subscription that expires after the first document is matched.
- *SelectableCreateSubscriptionPeriodsInHours* - comma-seperated list of integers - defines duration periods. The values must be defined as hours. The system will automatically display this in a proper way (for example, 168 will be displayed as 7 days in the drop down menu).
- *SelectableNotificationViewPeriodsInHours* - comma-separated list of integers - defines values for notification view on dashboard. The values must be defined as hours. The system will automatically display them correctly.

6 Monitoring

There are several aspects of the application that can be monitored to ensure its continual operation. The JMX monitoring interface allows you to monitor the application's resource usage. Monitoring the application's log files allows you to stay informed about potential problems and failures during operation. Accessing the application monitoring page triggers a quick self-check. The IPF Manager client application allows you to oversee outgoing document notifications and to attempt resending them in case of failures. The ATNA audit record repository can be used to alert you of potential security breaches and enables audits of access to patient's health information. Files in Tomcat's `temp` folder should be removed regularly in order to avoid extensive disk usage and minimize data privacy issues.

6.1 JMX monitoring

See the section on the JMX interface for details about connecting to the application using a JMX client like the JConsole.



Time Range: All

Used: 319,7 Mb Committed: 1,0 Gb Max: 1,0 Gb

Live: 122 Peak: 123 Total: 511

Loaded: 19.431 Unloaded: 494 Total: 19.925

CPU Usage: 2,9%

Figure 47: Monitoring the application using the JConsole

See the documentation for JConsole for further information on the capabilities and usage of its monitoring features.

6.2 Log files

By default the application writes all log messages to the Tomcat log folder (<tomcat>/logs). The number, size and behavior of log files is determined by your installation settings. For further information you can refer to the Professional Exchange Server installation manual. If you want to change the application's log behavior, you can adjust the log4j.xml file that is located in the `<tomcat>/webapps/<webapp_name>/WEB-INF/classes/ folder`. The log4j web site contains documentation on possible configurations. Please refer to the section on changing files in the Tomcat folder [page 27] for information how to make changes safely.

NOTE

Changes made to the logging configuration will only be applied after an application restart.

Not all error and warning log messages are necessarily a cause for alarm. Some of them exist for purely technical reasons and do not hinder the successful operation of the application. See [page 155] for a list of known log messages that can be safely ignored.

6.3 Application Monitoring Page

The application monitoring page performs a simple self-test when an HTTP GET request is issued to its URL. It verifies that the database can be reached and written to and checks the status of the embedded ActiveMQ broker. The monitoring page is accessible via HTTP or HTTPS (as long as they were not disabled during the installation) and does not require authentication.

The URL for application monitoring is accessible using the following URLs:

`http://<host>[:<port>]/<webapp_name>/monitoring` (if available)

`https://<host>[:<port>]/<webapp_name>/monitoring` (if available)

The application monitoring page is intended to be used by monitoring tools that poll the application to verify that it is available and functioning properly. The description of suggested and compatible tooling for these tasks is outside of the scope of this document.

6.4 IPF Manager

The IPF Manager can be used to monitor outgoing document notifications and to trigger resending them. For further information on the IPF Manager and the underlying “Flow Manager” technology, please refer to `http://repo.openehealth.org/con-`

`fluence/display/ipftools/IPF+Manager`. If your version of the IPF Manager does not have the capability to communicate with the application's JMX connector via SSL, you have the option of disabling SSL for JMX. For details on how to disable JMX, refer to the chapter on using the JMX interface.

6.5 ATNA Audit Record Repository

Please refer to the documentation of your audit record repository for further information on how IHE ATNA can help you ensure the safety of patient's personal health information.

6.6 Temporary Tomcat Files

Tomcat stores temporary files in `<tomcat>/temp`. In seldom cases these temporary files are not deleted automatically but reside in this folder. This might happen if systems use the standard interfaces for XDS Document sources in an erroneous way. Then folders named `cxf-tmp-*` will be created in the temporary Tomcat folder. Such cxf folders can be and should be removed regularly in order to avoid extensive disk usage and minimize data privacy issues. Sending systems might not be aware that they unintentionally provide this data.

7 Backup

To ensure the safety of the application data and continued application availability it is important to have organizational and technical processes that ensure that regular backups are made. You should also verify that the backups can be restored.

During installation the runtime data folder and the installation data folder can be entered. The installation data folder must be backed up once after installation and potentially after upgrades to newer versions of the Professional Exchange Server. The proper backup procedures during upgrades will be detailed as part of the migration documentation. The runtime data folder should be backed up at regular intervals. It contains ActiveMQ data on (unsent) outgoing document notifications and Lucene index data that supports the operation of the IPF Manager.

NOTE

The installation data folder contains the master keys and the key packages generated from them. These keys enable access to the patient related documents stored in the Professional Exchange Server (if data encryption was activated during installation).

Depending on the log settings chosen during the installation, there is also a backup folder for old log files. These should also be part of the operator's backup strategy.

Some configuration changes have to be made in the Tomcat folder. To ensure continual operation of the application and the ability to recover quickly in case of disaster (for example, hard drive crashes and so on) it is vital to have backups of the complete Tomcat folder. Aside from backups before and after configuration changes, it is recommended to also perform scheduled backups of this folder.

The database is the major data store of the application and should therefore be the cornerstone of the operator's backup strategy. Please refer to the Oracle documentation for details on proper backup procedures for an Oracle database.

8 Connecting the MPI and VMR

This section describes how to use the Master Patient Index (MPI) as a patient identity source for the Professional Exchange Server VMR. The Master Patient Index synchronizes the registered index patients including their demographical data and corresponding data sets from the different organizations.

This setting includes the Medical Service Bus (MSB) that provides integration capabilities.

The configuration tasks concern the following processes:

- Master Patient Index sends a notification to the MSB
- MSB receives the notification
- MSB sends a patient feed to the Professional Exchange Server VMR
- Professional Exchange Server VMR receives the patient feed.

8.1 Configuration Items

When connecting the MPI with the Professional Exchange Server the applications involved (MPI, Professional Exchange Server VMR and the MSB) can be configured in different ways. It is possible to configure these applications in different ways by making changes to:

- Configuration settings during the installation of the Professional Exchange Server VMR.
- Property files: Changes within property files will only be activated after a restart of the application. This holds for the MSB as well.
- JMX configurations: JMX configuration changes are real-time changes. This also holds for the MPI and the Professional Exchange Server VMR.
  - MPI: JMX Management Console, see the MPI system administration manual.
  - Professional Exchange Server VMR: Java Management Extensions (JMX).
- Database settings : Database changes in this context will only be activated after a restart of the application. This also holds for the MPI.

NOTE

All configuration items correspond to MPI and MSB version 3.0. If you are using a different version, please refer to the relevant MPI and MSB manuals.

8.2 URL Configuration

8.2.1 MPI sends a notification to the MSB

The MPI creates a notification every time an index patient record is created or changed either manually or automatically. (See: Setting the MSB URL for IHE PIX Update Notifications in the MSB System Administration manual). This behavior can be activated or deactivated through a flag in the database. To connect the MPI to the Professional Exchange Server VMR the flag `mpi.pix.updateNotification.enabled` has to be set to `true`. The current setting is validated using the SQL command:

SELECT * FROM PROPERTY_CONFIGURATION WHERE
PROP_NAME='mpi.pix.updateNotification.enabled'

The MPI sends an update notification to one recipient. This recipient is defined in the MBean:

```
com.icw.epr/Context.MessageReceiver.RemoteProxy/prg-all/esb/
mpiUpdateNotificationMessageRecipient/ServiceUrl
```

Make sure that the following three attributes are set to `true` in the MBean `com.icw.epr/Context.Beans/eventRulesEnablement` for MPI :

- applicationAcceptAcknowledgeGenerator
- applicationErrorAcknowledgeGenerator
- commitErrorAcknowledgeGenerator

8.2.2 MSB receives a notification

The property file `<msb installation path>/conf/msb/context-common.properties` contains several properties that are combined into one URL. Together, `msb.http.port`, `mst.http.context.path`, `msb.http.request.path` and `pxs.update.uri` form the URL where the MSB receives notifications. (e.g. http://<server>:msb.http.port/msb.http.context.path/msb.http.request.path/pxs.update.uri)

Example:

http://<server>:8484/msb/plain/update; (in MSB version 2.8 or lower the default was http://0.0.0.0:8484/update)

This URL has to match the ServiceUrl as described in the section MPI sends a notification to the MSB [page 150]. For more Information refer to the section Receiving data over https from MPI in the MSB System Administration Manual.

8.2.3 MSB sends a patient feed

The MSB is able to send a patient feed (or update) to several recipients or subscribers. The configuration file `<msb installation path>/conf/msb/subscriber-pix.properties` defines them. Each subscriber has a set of different properties. For more information refer to the MSB System Administration Manual: sections: Sending data to subscribers over mllps and Subscriber for the transaction update notification. Here is a sample configuration for one subscriber:

```
s1.name=EMPI
s1.feedUrl=localhost:3800
s1.receivingApplication=VMR_TLS_APP
s1.receivingFacility=FEED_TLS_FAC
s1.matchingNamespaceIds=^.*$
s1.matchingUniversalIds=
```

Several subscribers can be defined this way. However, only the ones that are listed in the subscriber list at the beginning of this property file will receive patient feeds.

8.2.4 The application receives the patient feed

During the installation of the Professional Exchange Server VMR, the ports for secure and non-secure patient feeds are defined. These ports have to match the `feedUrl` configuration described in the section: MSB sends a patient feed [page 151]. For more information refer to Configuring the Patient Import Interface [page 76]

8.2.5 Encoding of incoming HL7 messages

The default encoding of HL7 messages for both, MSB and VMR is ISO-8859-1. This encoding is widely used, but not explicitly recommended by the IHE standard. If for example German umlauts are not properly displayed, check the encoding of both systems:

MSB

Property file location: `<msb installation path>/conf/msb/context-common.properties`

- property name : patient.import.module.mllp.encoding set to UTF-8 (hl7.charset=UTF-8)

VMR

Property file location: `<webapps-folder>/pxs-vmr-assembly/WEB-INF/classes/META-INF/deploy.properties`

- property name : patient.import.module.mllp.encoding

8.3 Patient Namespace Configuration

A proper patient namespace configuration is necessary because the Professional Exchange Server VMR accepts patient feeds only from one source system. The patient namespace is used to identify this source system.

8.3.1 MPI sends a notification to the MSB

The MPI uses the patient namespace from the ‘Enterprise Master Patient Index’ system. Administrators can check and alter the configuration within the application’s GUI:

Navigate to Administration/ Systems and choose a system of the type: Enterprise Master Patient Index (for example, ICW-MPI) or Patient namespace. The patient namespace ID is formatted as an object identifier and looks like this: 2.16.840.1.113883.3.37.4.1.1.2.1.1

8.3.2 MSB receives the notification and MSB sends a patient feed

The MSB provides a mapping functionality for patient namespaces. For further information see the section Translation of patient IDs in the MSB System Administration Manual . However, it is recommended to use the same patient namespace within MPI and Professional Exchange Server VMR. See sections MPI sends a notification to the MSB and The VMR receives the patient feed. By default this is set to 2.16.840.1.113883.3.37.4.1.1.2.1.1 in both MPI and MSB .

The optional mapping is defined within the property file `<msb installation path>/conf/msb/pixpdq-mappings.map`. The mappings `bdm-patientOid-serverside-PatientOid` and `bdm-patientNamespaceId-patientOid` can be used to compensate for configuration mismatches within MPI and Professional Exchange Server VMR.

8.3.3 The VMR receives the patient feed

The patient namespace is defined within the organizations configuration, see The Application's organization registry [page 16]. The system with an XdsPatientIdentitySourceProfile has an `oid-namespace` element. The value of the nested root tag has to match the namespace configuration as described in the section MSB receives the notification and MSB sends a patient feed. Here is an excerpt of a sample configuration:

```
<system>
<identifier>
<root>2.16.840.1.113883.3.37.4.1.1.2.2</root>
</identifier>
<system-alias>EMPI</system-alias>
<abbreviation>EMPI</abbreviation>
<softwarename>Master Patient Index</softwarename>
<vendor>InterComponentWare AG</vendor>
<oid-namespace>
<root>2.16.840.1.113883.3.37.4.1.1.2.1.1</root>
<type>P</type>
</oid-namespace>
<profiles>
<profile name="XdsPatientIdentitySourceProfile"/>
</profiles>
</system>
```

8.4 SSL Configuration

The communication between MSB and Professional Exchange Server VMR can be secure or non-secure. Please note, that the steps here are optional and can be omitted if the non-secure communication is used.

8.4.1 MPI sends a notification to the MSB and MSB receives the notification

No configuration is necessary.

8.4.2 MSB sends a patient feed to the application

The MSB uses the settings in the property file `<msb installation path>/conf/msb/context-common.properties`. It is important to define the client certificate and the truststore so that the Professional Exchange Server VMR server certificate is accepted. For further information refer to the section TLS settings in the MSB System Administration Manual.

Here is an excerpt from a sample configuration:

```
set.certificate.stores=true
keystore.path=/opt/tomcat-ehcp3/apache-tomcat-6.0.29/conf/client.keystore
keystore.password=initinit
truststore.path=/opt/tomcat-ehcp3/apache-tomcat-6.0.29/conf/ca.keystore
truststore.password=initinit
```

The `feedUrl` property in the subscriber configuration has to use the secure port configuration of the Professional Exchange Server VMR, see `<msb installation path>/conf/msb/subscriber-pix.properties`. In addition, some security parameters are attached like this:

```
s1.name=EHCP_VIA_TLS
s1.feedUrl=localhost:3805?secure=true&sslProtocols=TLSv1,SSLv3&sslCiphers=SSL_RSA_WITH_NULL_SHA,TLS_RSA_WITH_AES_128_CBC_SHA
s1.receivingApplication=VMR_TLS_APP s1.receivingFacility=FEED_TLS_FAC
s1.matchingNamespaceIds=^.*$
s1.matchingUniversalIds=
```

8.4.3 VMR receives the patient feed

The Professional Exchange Server VMR has two mechanisms for a successful and secure connection:

- The Professional Exchange Server VMR Tomcat has to trust the certificate authority of the client certificate (here MSB). The Tomcat configuration is defined in its *server.xml* configuration file.
- The CN of the client certificate has to be mapped to a Professional Exchange Server system user with the necessary permissions.

For further information refer to the section Add user account for PIX Patient Identity-Source [page 75]

9 Known and inconsequential log messages

```
1.
org.hibernate.cfg.AnnotationBinder#buildInheritanceStates WARN
[WrapperStartStopAppMain] - Mixing inheritance strategy in a entity
hierarchy is not allowed, ignoring sub strategy in:
com.gehcit.ehealth.cnf.drr.ehf.registry.domain.PersonAuthor
2.
org.hibernate.cfg.AnnotationBinder#buildInheritanceStates WARN
[WrapperStartStopAppMain] - Mixing inheritance strategy in a entity
hierarchy is not allowed, ignoring sub strategy in:
com.gehcit.ehealth.cnf.drr.ehf.registry.domain.DeviceAuthor
3.
org.apache.cxf.frontend.AbstractWSDLBasedEndpointFactory#createEndpo
int(140) - Could not find endpoint/port for {http://gehcit.com/
platform/cws/DocumentDirectory}DocumentDirectoryPort in wsdl. Using
{http://gehcit.com/platform/cws/
DocumentDirectory}DocumentDirectory_Port_Soap11.
4.
org.apache.cxf.frontend.AbstractWSDLBasedEndpointFactory#createEndpo
int(140) - Could not find endpoint/port for {urn:ihe:iti:xds-b:
2007}DocumentRepository_PortTypePort in wsdl. Using {urn:ihe:iti:xds-
b:2007}DocumentRepository_Port_Soap12.
5.
org.apache.cxf.frontend.AbstractWSDLBasedEndpointFactory#createEndpo
int(140) - Could not find endpoint/port for {urn:ihe:iti:xds-b:
2007}DocumentRegistry_PortTypePort in wsdl. Using {urn:ihe:iti:xds-b:
2007}DocumentRegistry_Port_Soap12.
6.
org.apache.cxf.frontend.AbstractWSDLBasedEndpointFactory#createEndpo
int(140) - Could not find endpoint/port for {urn:ihe:iti:xds-b:
2007}DocumentRepository_PortTypePort in wsdl. Using {urn:ihe:iti:xds-
b:2007}DocumentRepository_Port_Soap12.
7.
org.apache.cxf.frontend.AbstractWSDLBasedEndpointFactory#createEndpo
int(140) - Could not find endpoint/port for {urn:ihe:iti:xds-b:
2007}DocumentRepository_PortTypePort in wsdl. Using {urn:ihe:iti:xds-
b:2007}DocumentRepository_Port_Soap12.
8.
org.apache.cxf.frontend.AbstractWSDLBasedEndpointFactory#createEndpo
int(140) - Could not find endpoint/port for {urn:ihe:iti:xds-b:
2007}DocumentRegistry_PortTypePort in wsdl. Using {urn:ihe:iti:xds-b:
2007}DocumentRegistry_Port_Soap12.
9.
org.apache.cxf.frontend.AbstractWSDLBasedEndpointFactory#createEndpo
int(140) - Could not find endpoint/port for {urn:ihe:iti:xds-b:
2007}DocumentRegistry_PortTypePort in wsdl. Using {urn:ihe:iti:xds-b:
2007}DocumentRegistry_Port_Soap12.
10.
org.springframework.beans.GenericTypeAwarePropertyDescriptor#getWrit
eMethodForActualAccess WARN [WrapperStartStopAppMain] - Invalid
JavaBean property 'dao' being accessed! Ambiguous write methods
found next to actually used [public void
com.icw.ehf.usermgnt.service.UserSecretHistoryServiceImpl.setDao(com
.icw.ehf.usermgnt.dao.UserSecretHistoryDao)]: [public void
com.icw.ehf.usermgnt.service.CrudServiceImpl.setDao(com.icw.ehf.user
mgnt.dao.CrudDao)]
11.
 com.icw.ehf.authentication.cert.conf.Config#read WARN
[WrapperStartStopAppMain] - No resolver configuration found, neither
at URL null nor in file null.
```

```
12.
[java] 2011-01-05 14:11:54,879 WARN
[DefaultMessageListenerContainer-1] or
g.hibernate.util.JDBCExceptionReporter#logExceptions(77) - SQL
Error: 0, SQLStat e: null [java] 2011-01-05 14:11:54,894 ERROR
[DefaultMessageListenerContainer-1] or
g.hibernate.util.JDBCExceptionReporter#logExceptions(78) - failed
batch [java] 2011-01-05 14:11:54,894 ERROR
[DefaultMessageListenerContainer-1] or
g.hibernate.event.def.AbstractFlushingEventListener#performExecution
s(301) - Cou ld not synchronize database state with session ...
<stack trace> ...
```

10 Glossary

Term	Description
.NET	The Microsoft .NET Framework is a software technology available with several Microsoft Windows operating systems
ACK	Acknowledgement, or confirmation message
ActiveMQ	Open Source Implementation of JMS
ADT	Admission, Discharge and Transfer
API	Set of function calls an operating system (or other software generally) provides for use by application programmers Application Programming Interface: ● Set of function calls an operating system (or other software generally) provides for use by application programmers ● The defined specification for such a set of calls
ATNA	Audit Trail and Node Authentication, an IHE Integration Profile
ASN.1	Abstract Syntax Notation One
BPPC	basic patient privacy consents
CA	Certificate Authority
Deployment	Distribution, installation and configuration of software on target systems
DSUB	Document Metadata Subscription
Endpoint	Component of an integration middleware (enterprise service bus) directed at external systems.
Groovy	Object-oriented, dynamic programming language for the Java platform as an alternative to the Java programming language.
HIS	Hospital Information System A hospital information system (HIS) is the sum of all information processing units used to process medical and administrative data in a hospital. It includes computer programs, personnel and non IT-based information systems. The term is often restricted to mean the computer-based components of the HIS. Sometimes an additional distinction is made between the HIS as central system and specialized systems, such as radiological information systems (RIS), laboratory information systems (LIS), etc.
HL7 2	Health Level 7, Version 2 (also “Version 2.x”) Protocol for message exchange from Health Level Seven, Inc.
HL7 3	Health Level 7, Version 3 New messaging standard from Health Level Seven, Inc. A group of messaging specifications. It contains a generic model for healthcare objects (RIM) and a modeling methodology for new health care domains

Term	Description
HTTP	Hypertext Transfer Protocol The Hypertext Transfer Protocol (HTTP) is a protocol for the transfer of data over a network. It's primary use is for loading websites and other data from the World Wide Web (www) in a Web browser.
HTTPS	Hypertext Transfer Protocol Secure The Hypertext Transfer Protocol over SSL is a URI schema that defines an additional layer between HTTP and TCP. It serves to encrypt and authenticate communication between Web server and browser.
IHE Actor	Information systems or applications that produce, manage or act on information are represented as functional units called IHE Actors. Each actor supports a specific set of IHE transactions. A given information system may support one or more IHE actors.
IN1, IN2, IN3	HL7v2 segments that contain patient insurance information
IPF	Open eHealth Integration Platform. Extension to Apache Camel that adds a lot of eHealth-specific integration functionality.
JConsole	JMX client delivered together with JDK distributions. Enables monitoring and administration of target applications at runtime over JMX (MBeans).
JDK	Java Development Kit
JMS	Java Message Service
JMX	Java Management Extensions
JVM	Java Virtual Machine
Keystore	A repository for X.509 certificates used to authenticate SSL connections.
KILL signal	An instrument of an operating system to terminate a running process.
LDAP	Lightweight Directory Access Protocol, an application protocol for reading and editing directories over an IP network
MDT	Multi Disciplinary team, IHE profile
MLLP	Minimal Lower Layer Protocol
MPI	ICW Master Patient Index
MSB	Medical Service Bus
MSH-3	Field “Sending Application” in a HL7 v2 Message
MSH-4	Field “Sending Facility” in a HL7 v2 Message
NAK	Negative Acknowledgement
OID	Object Identifier Object Identifier: A hierarchical ID that uniquely identifies a device type or a source system.
OMI	Order Message for Imaging HL7 v2 Message format

Term	Description
PIX	Patient Identifier Cross-referencing, IHE profile
RMI	Remote Method Invocation
root user	Superuser/Administrator in UNIX-like operating systems
SOAP	Simple Object Access Protocol SOAP is a protocol for sharing XML-based files between systems and for performing remote procedure calls
TCP	Transmission Control Protocol, a network protocol used in the Internet
Truststore	A repository of X.509 certificates used for authentication in secure connections (SSL).
VMR	Virtual Medical Record
XML	Extensible Markup Language Hierarchical modeling standard for semi-structured data defined by the World Wide Web Consortium (W3C).
XDS	Cross Enterprise Document Sharing, IHE profile

List of Figures