

RSNA Image Share Edge Server

Installation/User Manual

[1. Introduction: RSNA Edge Server](#)

[1.1 Intended Audience](#)

[2. Hardware Requirements](#)

[3. Software Requirements](#)

[Networking](#)

[Virtual](#)

[Physical](#)

[4. Build Instructions](#)

[4.1 Virtual](#)

[5. Setting up MIRTH](#)

[6. The Web UI](#)

[7. Retrieve Content Application](#)

[8. Maintenance](#)

[Appendix A. Edge Server Error Codes](#)

[Appendix B. Clearinghouse Error Codes](#)

[Appendix C: Upgrading from Version 2.0 to 2.1](#)

[Appendix D: Unix Hints](#)

[Unix Shell](#)

[Root or Administrative Account](#)

[Appendix E: DICOM Conformance](#)

[Appendix F: V2.1 Release Notes](#)

1. Introduction: RSNA Edge Server

The Edge Server is the gateway device to enable the Image Sharing Network. This partnership of the RSNA with the NIH aims to deliver on 3 primary use cases:

- a) patient initiated sends of their own imaging studies to the Clearing House for subsequent pickup by the patient via their PHR vendor (i.e. Microsoft HealthVault or <http://www.lifeimage.com/>)
- b) clinician initiated sends of identified studies to another care center in the performing site's Affinity Domain
- c) researcher initiated sends of anonymized studies from a source site, via the Clearing House, to a core lab in a multi-site research program

The last use case is not addressed with this release of the Edge Server manual. The next figure illustrates the workflow in the patient centric use case.

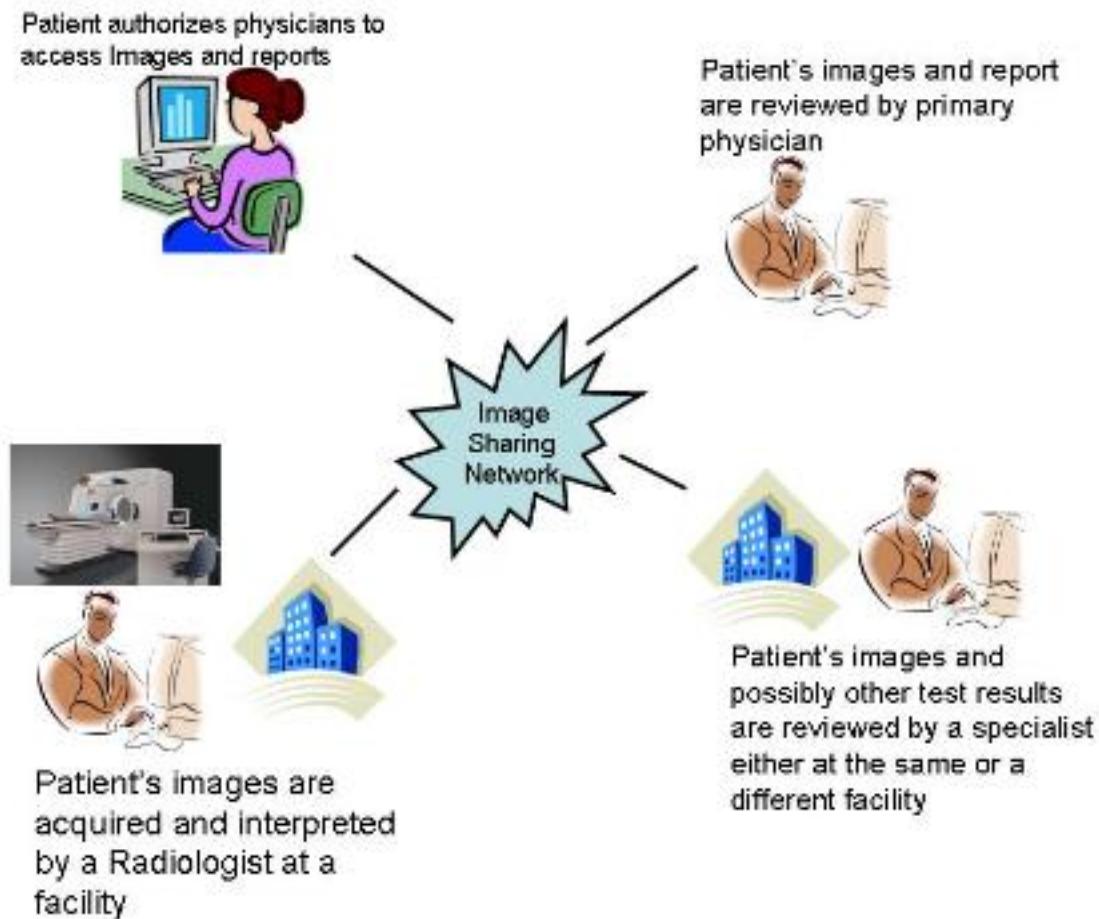


Figure 1-1: Image Sharing Workflow: Patient-centric Use Case

1.1 Intended Audience

This document is intended for users who are either installing Edge Server Version 2.1 from scratch, or are upgrading a V2.0 installation to 2.1. If you are in the latter camp, refer to Appendix C before reading the rest of this manual. For the former group, proceed to Chapter 2.

2. Hardware Requirements

The Edge Server software has been developed to run on standard desktop class PC hardware. However, experience will have to guide the provisioning of a system in any particular case. It is unlikely that the configuration for a 50 bed rural hospital performing 50,000 imaging studies per year would be adequate for a tertiary care center performing a million plus exams per year. There are also two possible methods to deploy the Edge Server software: a site may elect to download a Virtual Machine instance of the Edge Server (this is the easiest path for a site that already has a suitable virtual host) or it may also choose to deploy the software on a physical machine. In either case, a base-line configuration should contain:

- a) at least a dual core, 2 GHz CPU
- b) 4 GB of RAM
- c) a 100 Mbps networking card
- d) A 40 GB system disk and preferably a second data disk of 60 GB or more

3. Software Requirements

Networking

The Edge Server will need to communicate with several devices within the medical center (e.g. RIS and PACS). For these devices to “see” the appliance in predictable location, the Appliance will need at the very least a static IP address, and perhaps also a DNS name. Make sure these values are available at the time that the Appliance is being installed.

Fixed IP Address:

DNS Name:

Router/Gateway:

Net mask:

Virtual

As previously mentioned the Edge Server can be downloaded in a Virtual Machine (VM) format for running on a suitable environment. This is the least troublesome route to setting up a working Edge Server. If a site lacks the required virtual environment, the following physical machine requirements come into play.

Physical

Operating System

Currently only Ubuntu Server 10.04 LTS (32 bit version) has been vetted for this Edge Server release
site <http://www.ubuntu.com>

Java

Currently Java 1.6 is required for this Edge Server release. We have vetted this release using *only* the official Oracle JRE (formerly Sun) version “1.6.0_32”
site: <http://www.oracle.com/technetwork/java/javase/downloads>

PostgreSQL

Currently version 8.4.7 is required for this Edge Server release
site: <http://www.postgresql.org>

4. Build Instructions

4.1 Virtual

Download the latest Edge Server Virtual Machine (in OVF format) from here:
ftp://ftp.ihe.net/image_sharing/2.1_release

[Note to RSNA FTP users: The RSNA ftp server is based on Microsoft. You must force the transfer to be binary, else the .zip files will be corrupt.]

You will be directed to a single folder that contains several other files:

- a) the VM zip file
- b) an MD5 file with the same name as the above plus “.md5”
- c) an application called “hash-checker” (in both Linux and Windows versions)
- d) this User Manual
- e) a Windows md5 application (md5sums.exe)

To verify that the download was correct, you will have to:

- a) download the above mentioned files into a directory
- b) get into the resulting directory
- c) run the hash-checker (use the correct version for the operating system you are on)>hash-checker

If the hash checks out, use your VM environment’s OVF import tool to convert the OVF package into a VM on your current virtual host system. The following VM environments have been tested:

- VMWare ESXi Server 4.x
- VMWare Workstation 7.x

Other OVF compliant hypervisors (such as Sun/Oracle VirtualBox and Xen) may also work. The default accounts/password for Ubuntu are:

```
root    JGK7@ba
rsna   FT39bp# !
```

The default PostgreSQL account/passwords are:

postgres	N3K647A
mirth	1947JAT\$
edge	d17bK4#M

The system will initially boot using DHCP for its network address. This should be reassigned to the static IP and DNS name that was reserved for the Edge Server in Chapter 3. Change the network configuration for your environment from the Ubuntu menu System/Preferences/Network-Connections. Also, change the host entry in etc/hosts and make sure the IP matches the static IP assigned above. You can now continue to section 4.3 (Registering the Edge Server Certificate with the Clearing House).

4.2 Physical

If for some reason you cannot choose the virtual machine path, the following route must be taken.

4.2.1 Installing Ubuntu

1. You will perform the first step using a desktop or other system that is not your Edge Server. Use a web browser on your desktop to connect to the Ubuntu web site: <http://www.ubuntu.com>
2. Select the **Download** control and then **Download and install**
3. Select the 10.04 LTS release as shown in Figure 4-1. Download and save the ISO from the Ubuntu web site.
4. Follow the instructions provided on the Ubuntu web site for creating a DVD and installing the operating system.
5. Starting here, you will use the DVD to install the Ubuntu operating system on your hardware. These instructions assume you are starting with a blank system that will first boot from a DVD and then the hard drive. If your system does not default to the DVD or already has an operating system, you will need to modify the BIOS or boot sequence to boot from the Ubuntu installer DVD.
6. The DVD contains a bootable system. Load the DVD on the Edge Server hardware and boot from the DVD.
7. Continue through the installation. Make sure you use the Ubuntu documentation for your initial system load and configuration.
8. The Ubuntu installer will ask you to create at least one user account. At a minimum, create an account with the login name “rsna” with an appropriately secure password. That account will also have sudo privileges (can become root to perform administrative tasks).
9. Other user accounts will be added later as follows.
 - a. The PostgreSQL installation will add a postgres account.
 - b. The Edge Server installation will add an edge account.

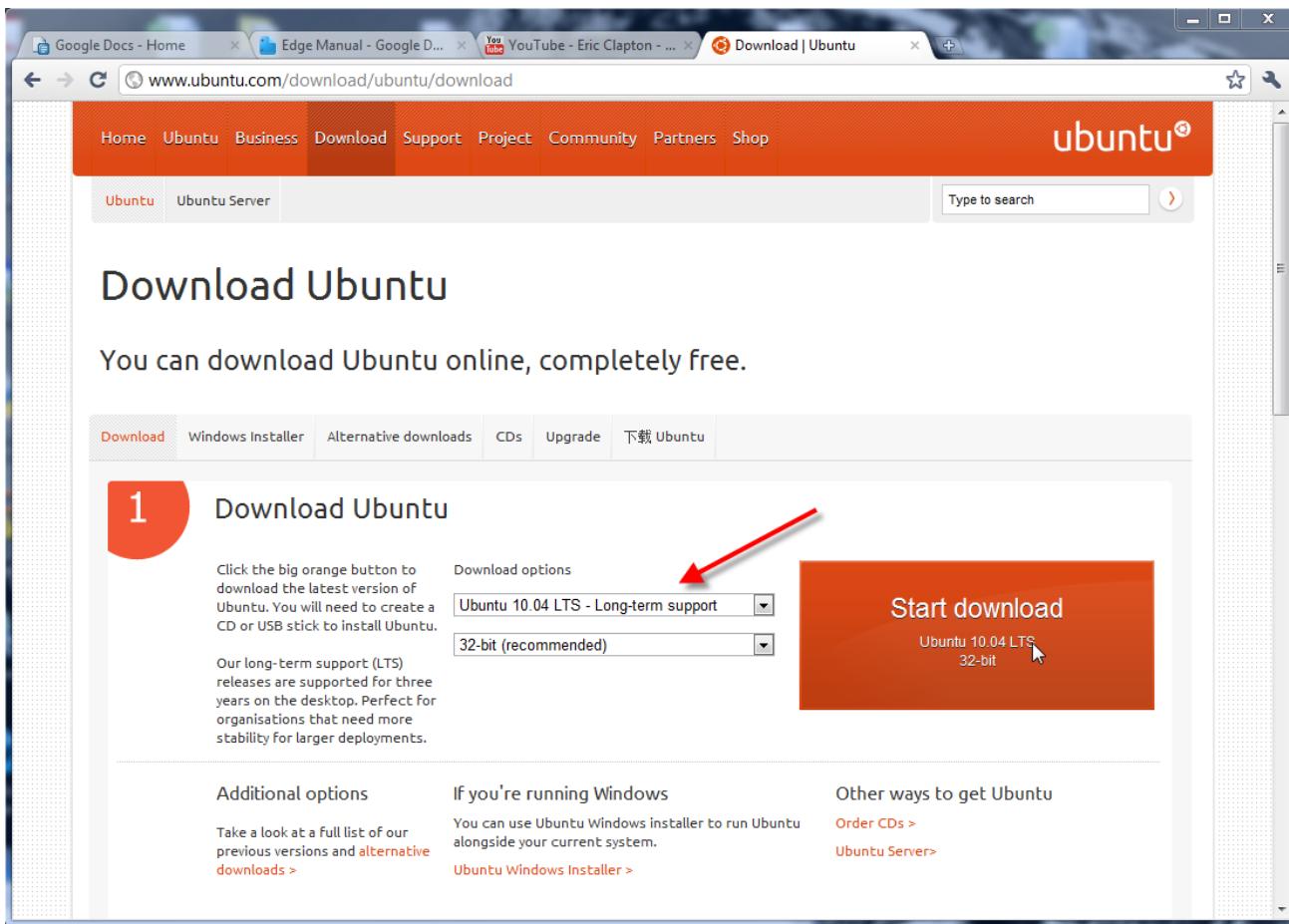


Figure 4-1: Ubuntu Download Page: Select Ubuntu 10.04 LTS

Installing Ubuntu Desktop

After you complete the base installation of Ubuntu Server, you will not have a desktop environment. You will need a desktop environment for installing the Edge Server. Login to the console using the **rsna** account you created during the installation process. You will then install the Ubuntu desktop:

```
sudo su - root  
apt-get install ubuntu-desktop
```

Change the root password to match your local security requirements. When you type the command below, you will be prompted for a new root password. Type the command exactly as listed:

```
sudo passwd root
```

Reboot the system. This will enable the desktop software:

```
sudo reboot
```

4.2.2 Installing Java

Do not use the Java packages that are managed by the Ubuntu Software Manager. Manually download the Sun Java Runtime Engine (JRE) found at <http://www.oracle.com/technetwork/java/javase/downloads/index.html>. We specify and test with the SE version of the Sun JRE; you do not need the EE version. Also, be sure to install the appropriate Java for the version of Ubuntu you have (64 bit versus 32 bit).

We install the JRE in **/usr/local** on the server; for example: /usr/local/jre_1.6.0_32. You may choose a different location. You will need to use the path to the JRE in configuration steps below for setting environment variables for the operating system (section 4.2.4)

4.2.3 Installing PostgreSQL

Install PostgreSQL using one of the two methods below.

1. From the command line (as root): **apt-get install postgresql-8.4**

or

2. **Recommended:** Graphical User Interface (Ubuntu):

- a. Run the Ubuntu Software Center (see Figure 4-2 below)
- b. In the left tab, select Get Software (see Figure 4-3 below)
- c. In the search window (upper right corner of window), search for **postgres**
- d. Select and install **object-relational SQL database, version 8.4 server** (see Figure 4-4 below)

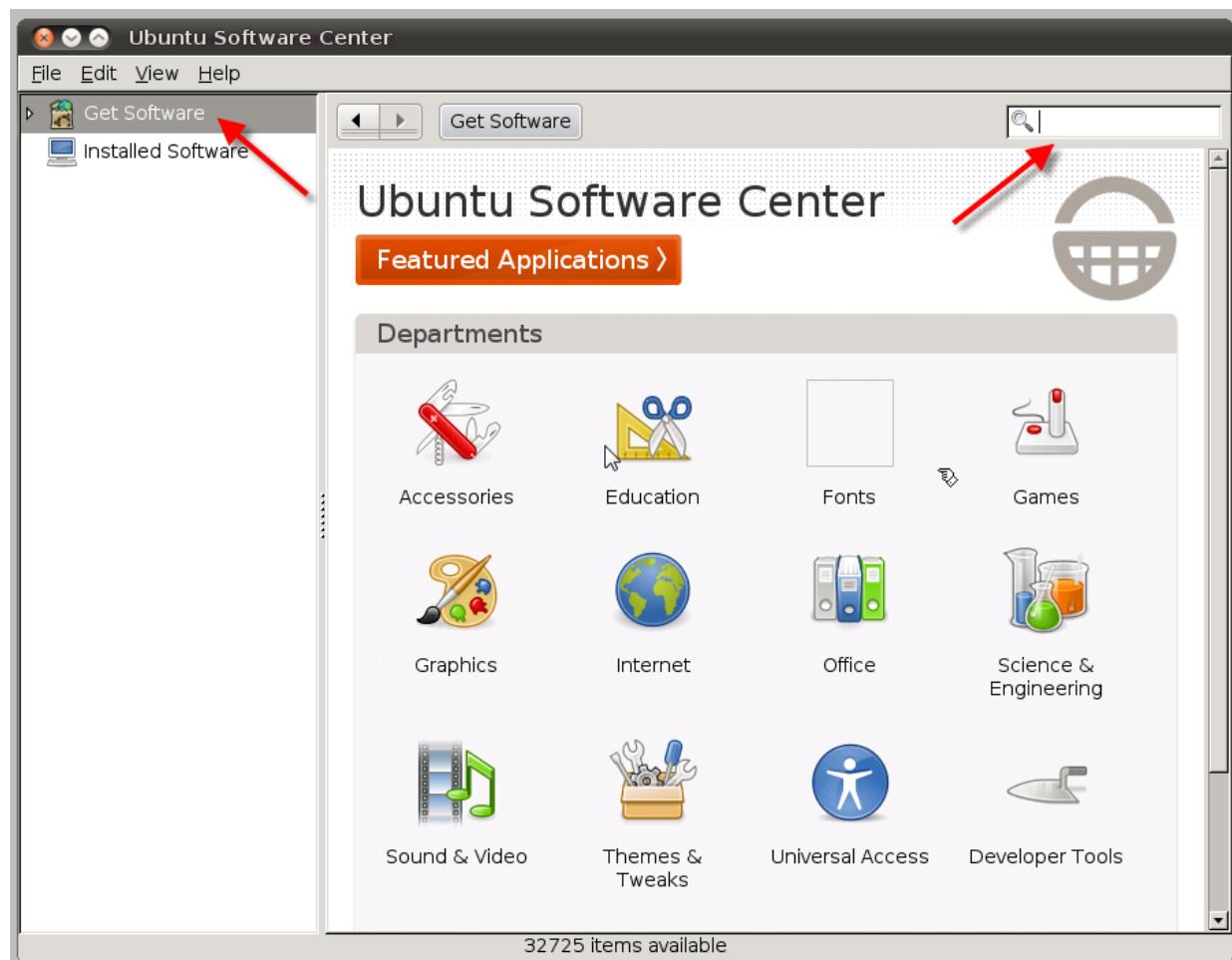


Figure 4-3: Ubuntu Software Center: Front Page

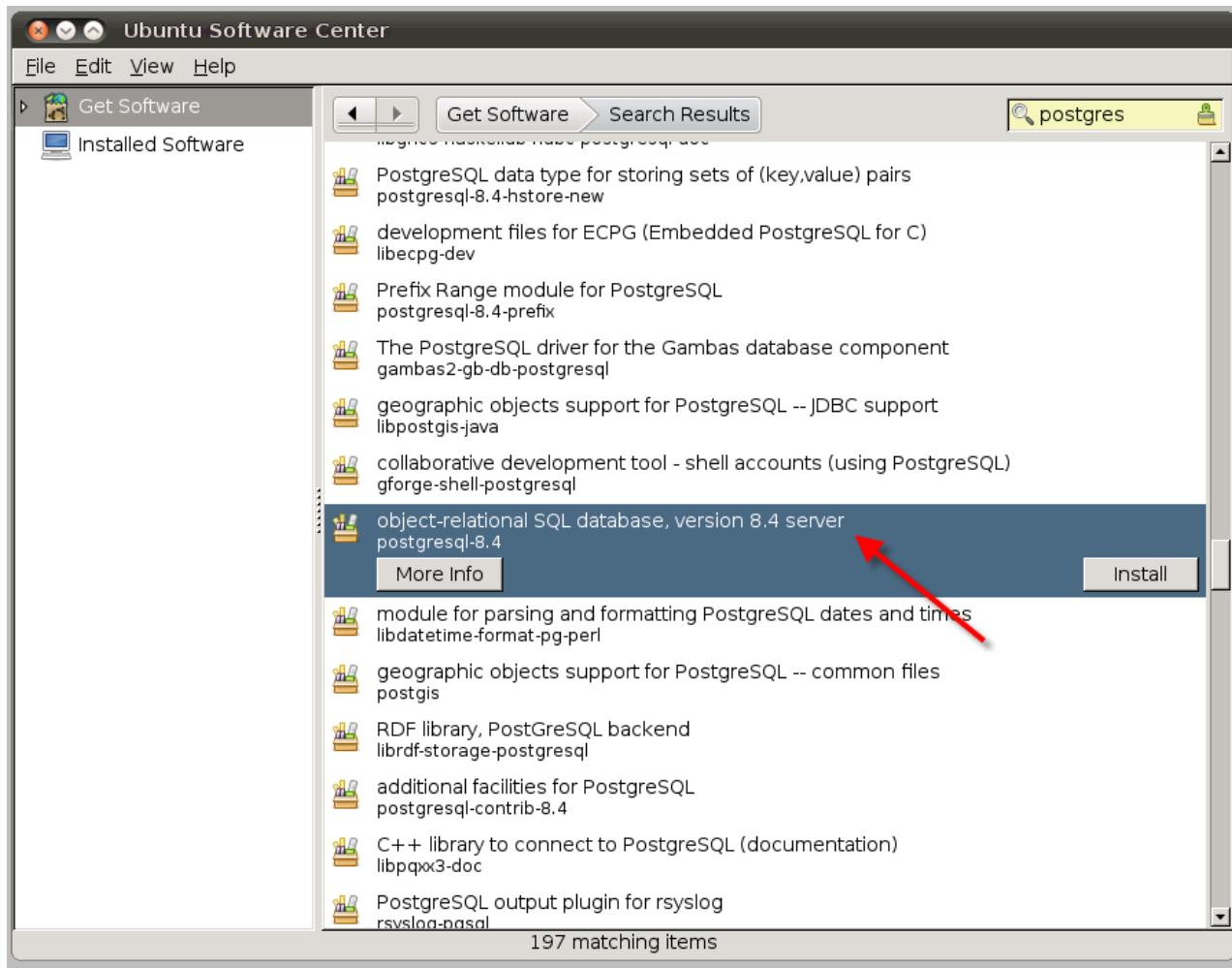


Figure 4-4: Ubuntu Software Center: Search for Postgres

After installation, run the following two commands

```
sudo update-rc.d -f postgresql-8.4 remove
sudo update-rc.d postgresql-8.4 defaults 20 80
```

Now, create a password in `postgres` for the super user account. This account is typically the “`postgres`” account. Use a terminal window and run this command:

```
sudo -u postgres psql postgres
```

The command above puts you into the `postgres` interpreter. In the interpreter, type:

```
\password postgres
```

You will be prompted for the password. You are encouraged to choose a secure password; you will need to record the value for use when installing the Edge Server Software (section 4.2.5).

4.2.4 Operating System Environment

The default shell for the root account is `/bin/bash`. The RSNA-Edge Installer will add the user account `edge` configured to use `/bin/sh`. You need to change some system-wide settings to properly support the installer.

1. Edit the file `/etc/environment`. If you have a new installation of Ubuntu Server, that file will contain one line

that configures the PATH variable. Add the path to the java executable to this PATH variable. If you use the suggested installation folder /usr/local/jre1.6.0_32 (section 4.2.2), the entry would be as follows:

- PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/usr/games:/usr/local/jre1.6.0_32/bin"
2. In the same environment file, add a variable that points to the installation folder for the Java Runtime Environment. If you use the suggested installation folder /usr/local/jre1.6.0_32 (section 4.2.2), the entry would be as follows:
- JAVA_HOME="/usr/local/jre1.6.0_32"
3. Next, in the environment file (/etc/environment), add a variable for the path of the Edge Server installation. For example, if installing the Edge Server to /usr/local/edgeserver:
- RSNA_ROOT="/usr/local/edgeserver"
4. In section 4.2.5 of this document, you will select a folder for the installation of the Edge Server software; see Figure 4-6. We recommend that you choose "/usr/local/edgeserver". Edit the file /etc/login.defs. Find the two PATH lines that start **ENV_SUPATH** and **ENV_PATH**. Append the path to the java executable to both PATH variables. Examples from a running system are:

```
ENV_SUPATH PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/usr/local/jre1.6.0_32/bin  
ENV_PATH PATH=/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/usr/local/jre1.6.0_32/bin
```

5. Alter the sudo path configuration:

```
$ sudo visudo
```

Comment out this line:

```
Defaults env_reset
```

And add the following line:

```
Defaults secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/local/jre1.6.0_32/bin
```

6. Reboot the computer to publish these variables throughout the system.

4.2.5 Running the RSNA Edge Installer

Once you have built the physical server to this point you need to obtain the RSNA Edge Server installer. This can be obtained using the following URL:

<https://github.com/RSNA/Image-Sharing-Network-Edge-Server/downloads/edgeserver-2.1.0-standard.zip>

If you are performing an upgrade from version 2.0 to version 2.1, please use the instructions in Appendix C. The information in this section is used for new installations.

Within the above zip file are several files:

- a) an installer ending in .zip
- b) an MD5 hash of the above ending in .md5
- c) hash-checkers for both Windows and Linux (and a support file for the Windows version)
- d) this Manual

To validate the installer has been downloaded without error, you may run the proper hash-checker for the operating system you are on, and it will validate if the download's hash agrees with the published value.

When running the installer, you will be asked for configuration information:

Database Superuser Password: The password you entered for postgres above

Password for RSNA Database user: Choose a (different) secure value for this user account
For example: d17bK4#M

Password for Mirth Database user: Choose a separate, secure database password for Mirth
For example: 1947JAT\$

Make sure that **JAVA_HOME** points to the installation folder of the Java JRE. Open a terminal emulator, change to the folder that contains the downloaded zip file and extract it. As user 'root' change to the extracted directory and run the shell script:

```
$ unzip edgeserver-2.1.0-standard.zip  
$ cd edgeserver-2.1.0  
$ sh ./install.sh
```

The installer will launch with a splash screen (Figure 4-5):

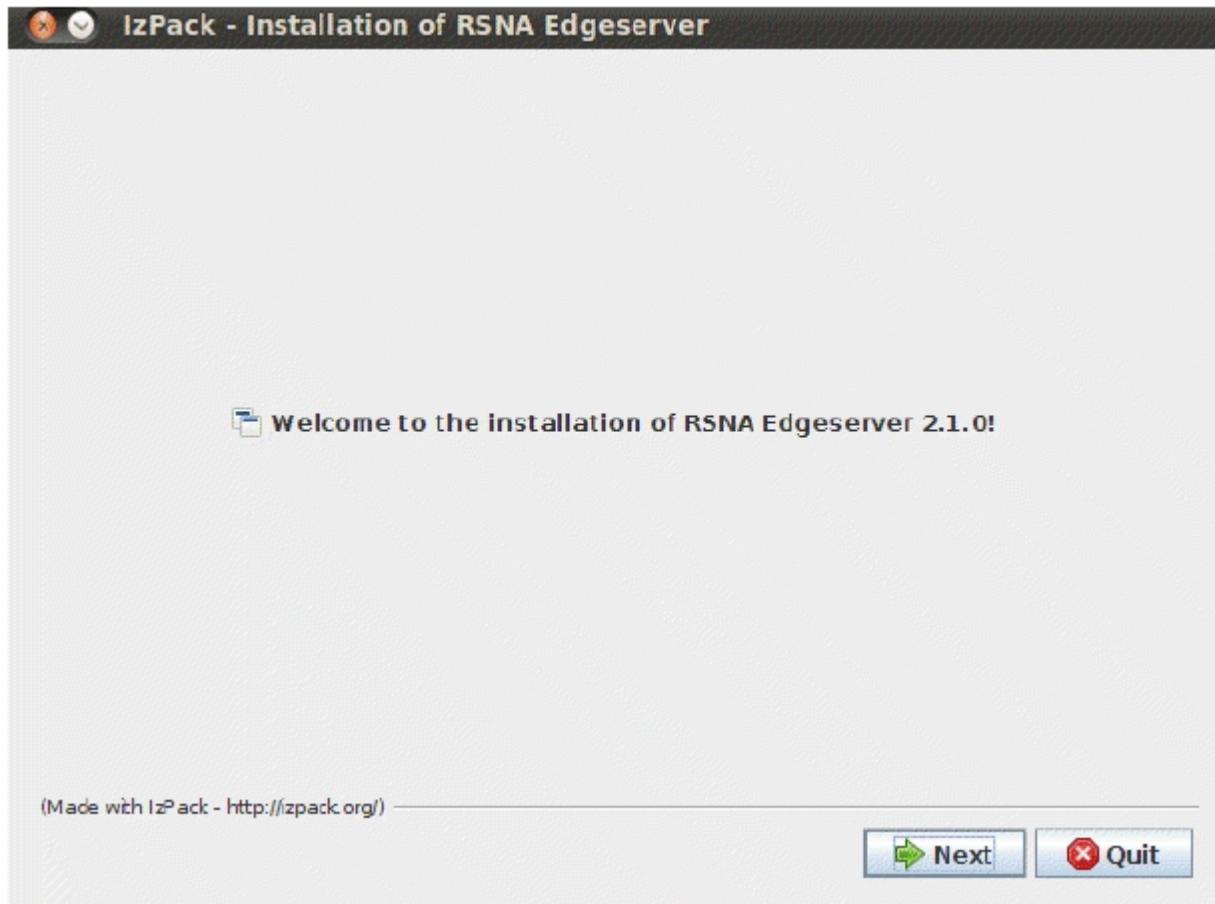


Figure 4-5: Installer splash screen

After the splash screen, you are asked if you are upgrading from a previous version (Figure 4-6). If you are performing an upgrade, this section of the document is not relevant. Please refer to Appendix C.

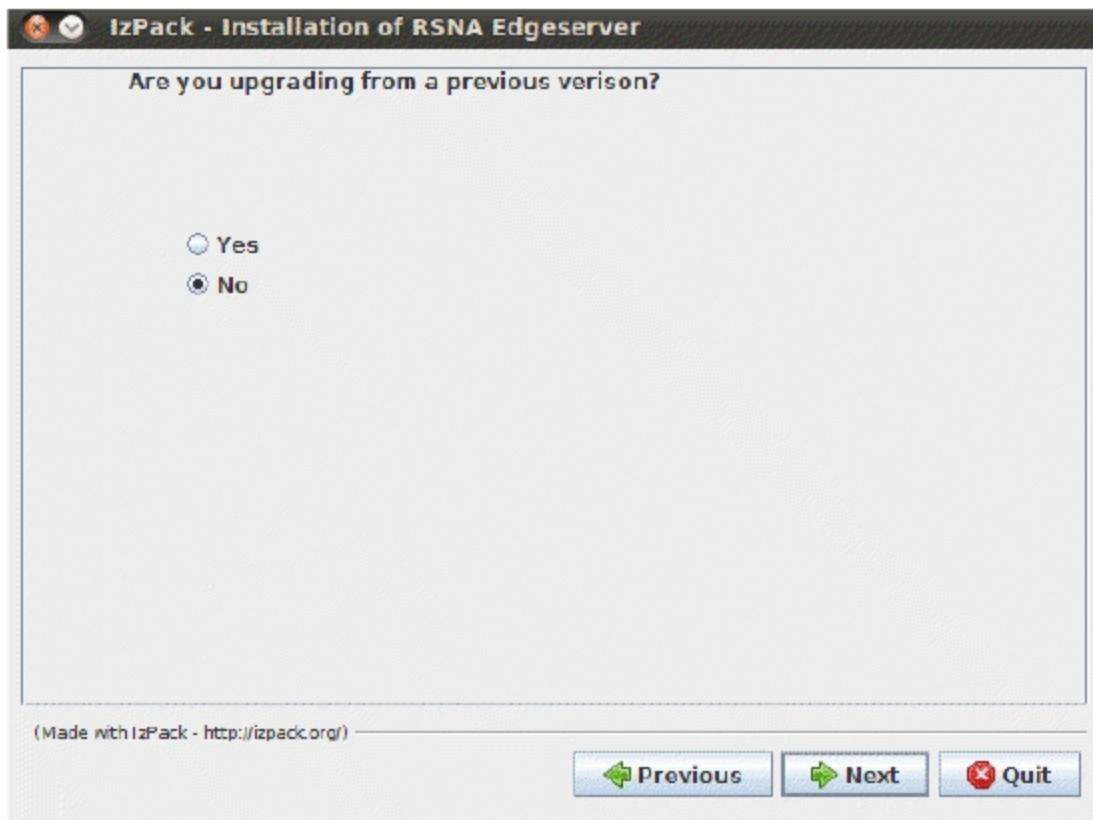


Figure 4-6: Upgrade query screen

Next you are prompted to select the installation path for the software (Figure 4-7):

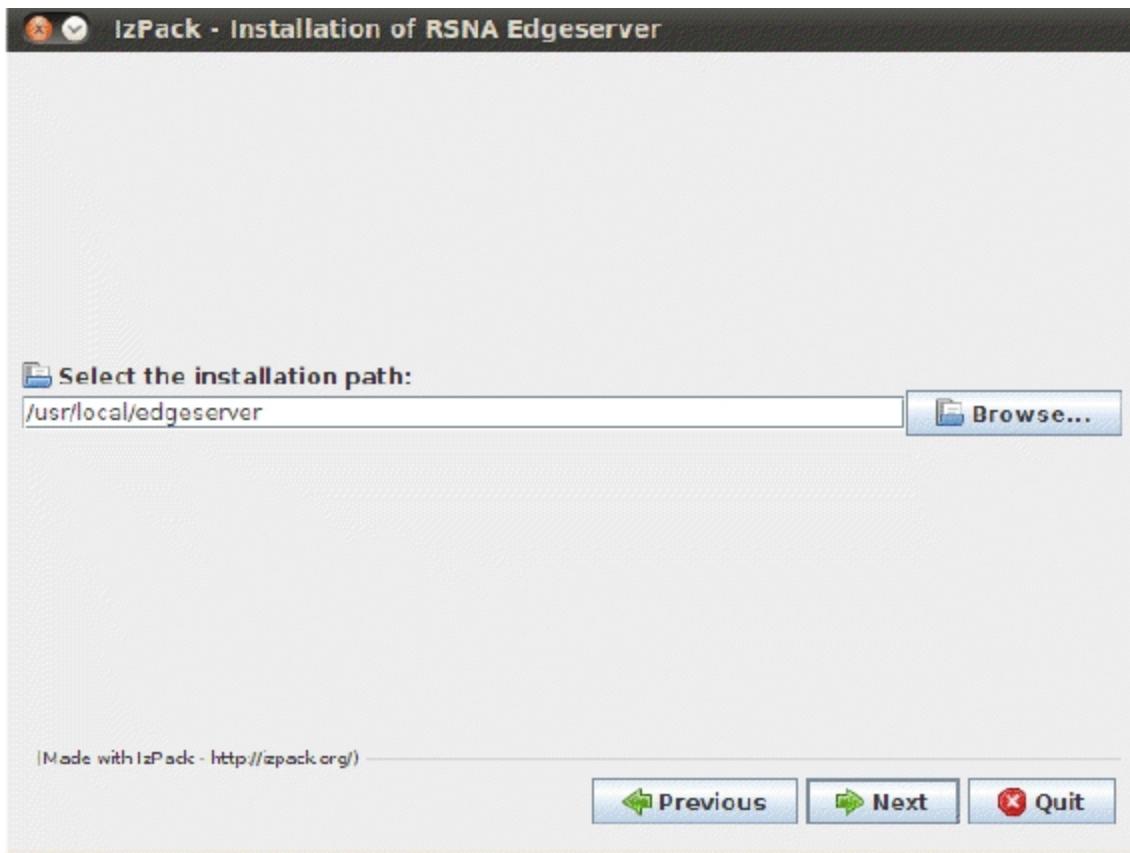


Figure 4-7: Installation Path

A message will appear informing you that the target directory will be created (Figure 4-8):

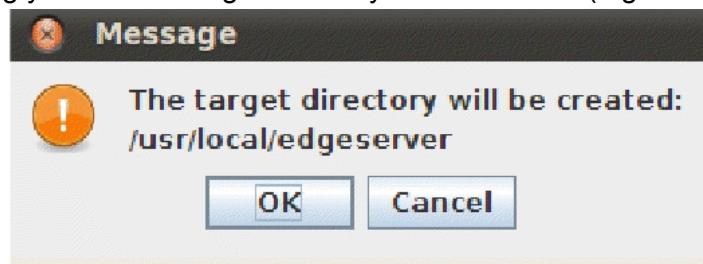


Figure 4-8: Target Directory Creation

Next you will be prompted about which components to install (Figure 4-9). For new installations, the default options of all components should remain selected. For upgrade installations (see Chapter 8: Upgrades), you can safely de-select Glassfish, Mirth, and Generate Client Certificate.

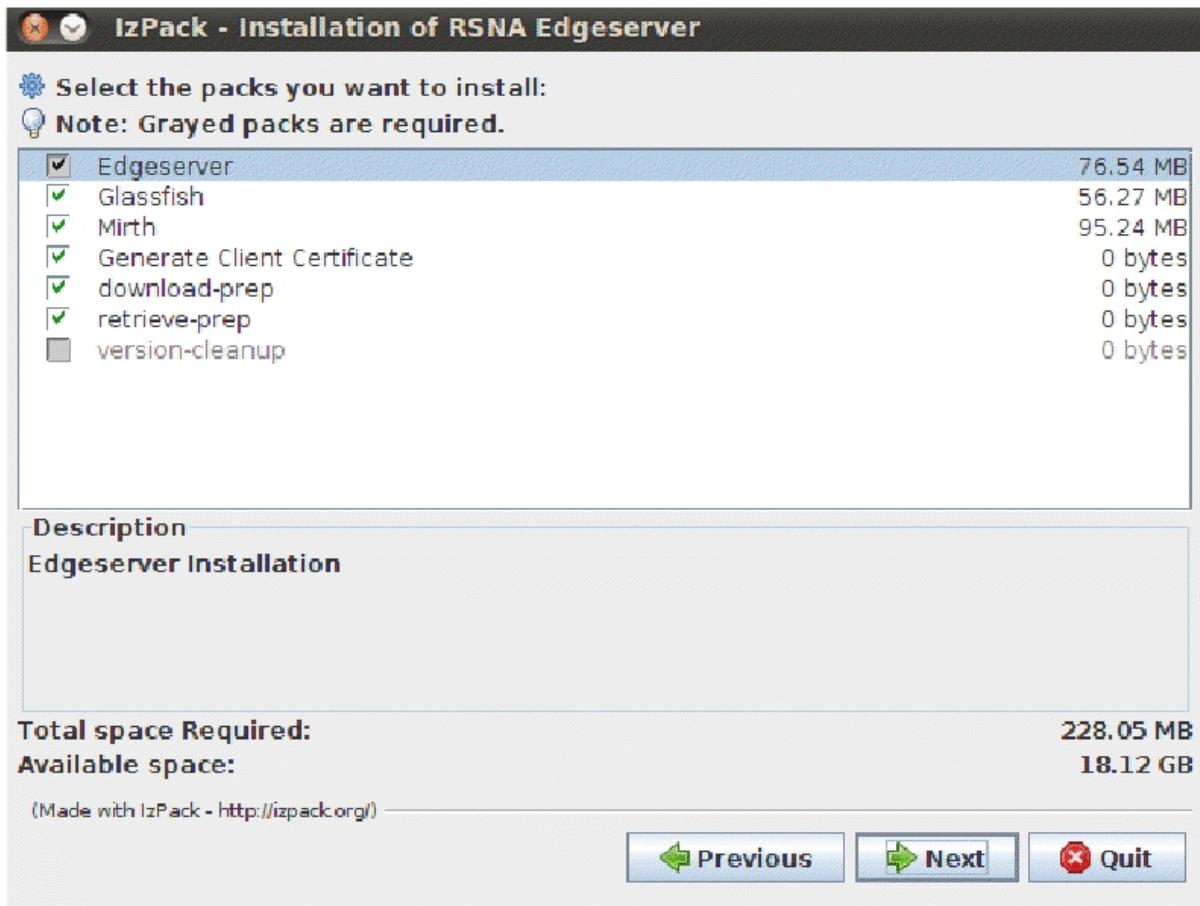


Figure 4-9: Component selection

Configure the database connection as shown in (Figure 4-10). For the Host, Port and Database Superuser Name, use the default values presented by the installer. For *Database Superuser Password*, enter the password created for the postgres account in Section 4.2.3. The edge account is also referred to as the RSNA Database user. For the *Password for RSNA Database user*, enter the password you selected for the edge account; this is the first time you enter that password in the system.

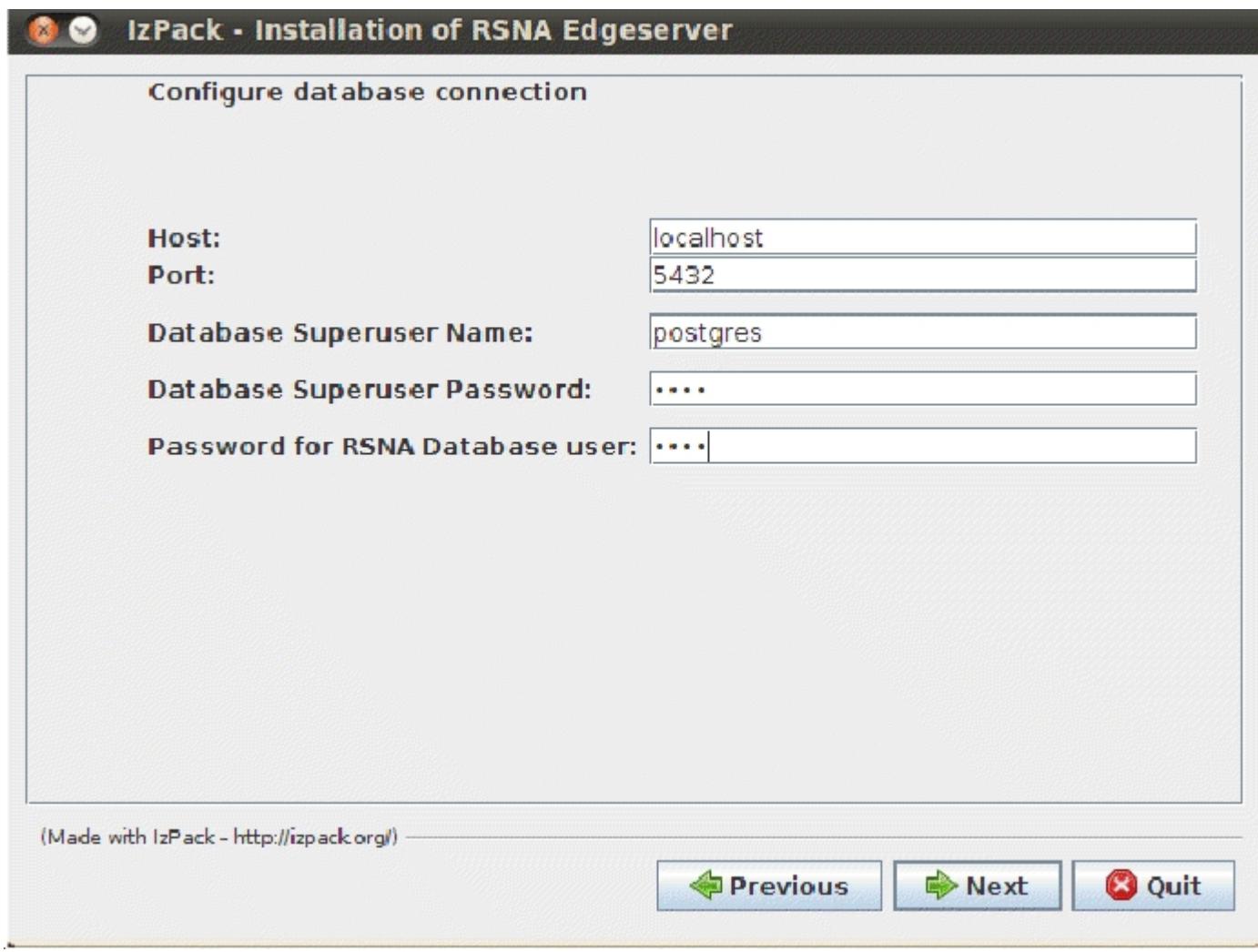


Figure 4-10: Database configuration

You will create a digital certificate on the initial installation. Fill out the certificate subject information (Figure 4-11). This will create a certificate, which is necessary to communicate with the Clearing House, and place it in the root application directory (specified above as the install path). We make these recommendations:

- For *Full server name*, enter the fully qualified hostname for the server
- For *Number of days the certificate is valid*, enter 1095 (equivalent to three years)

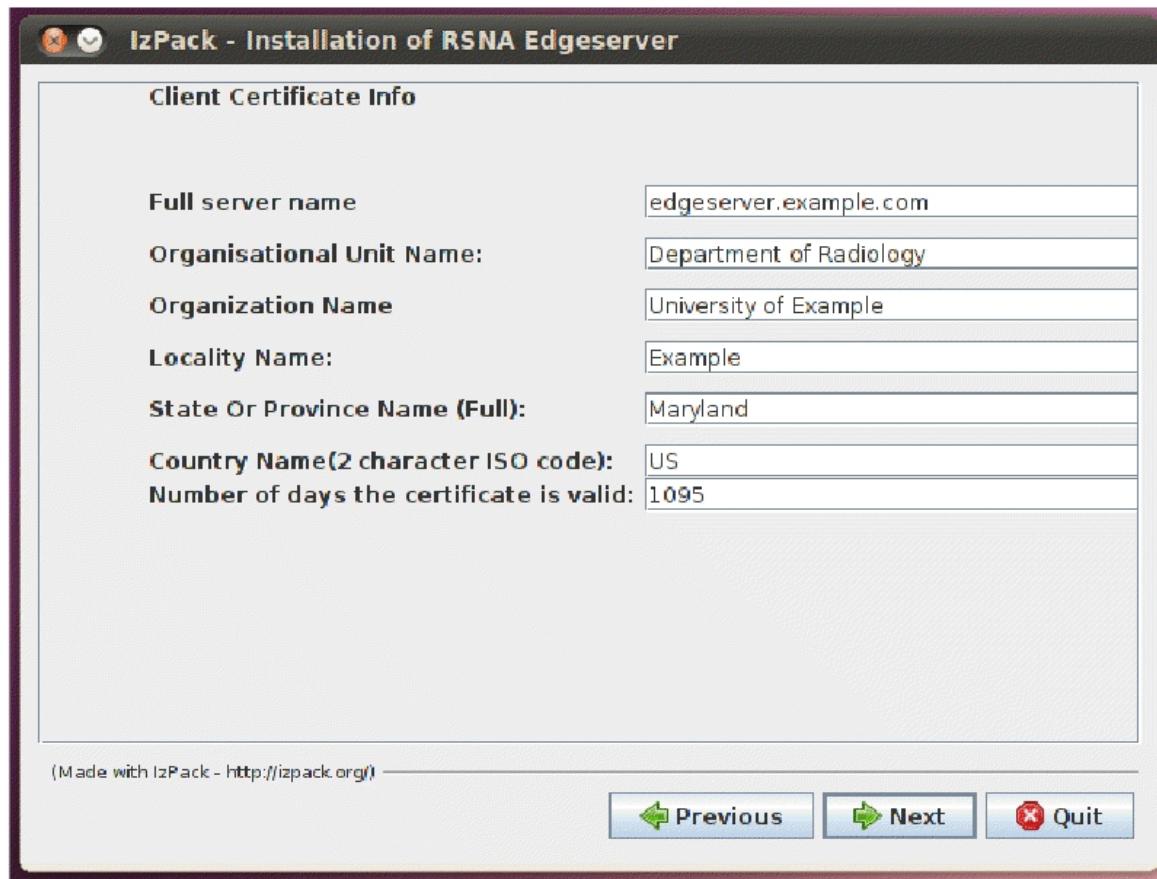


Figure 4-11: Certificate Generation

Configure the MIRTH database connection as shown in (Figure 4-12). You will only need to enter a value in the last line: Password for Mirth Database user. Enter the value you chose previously; this is the first time you enter it in the system.

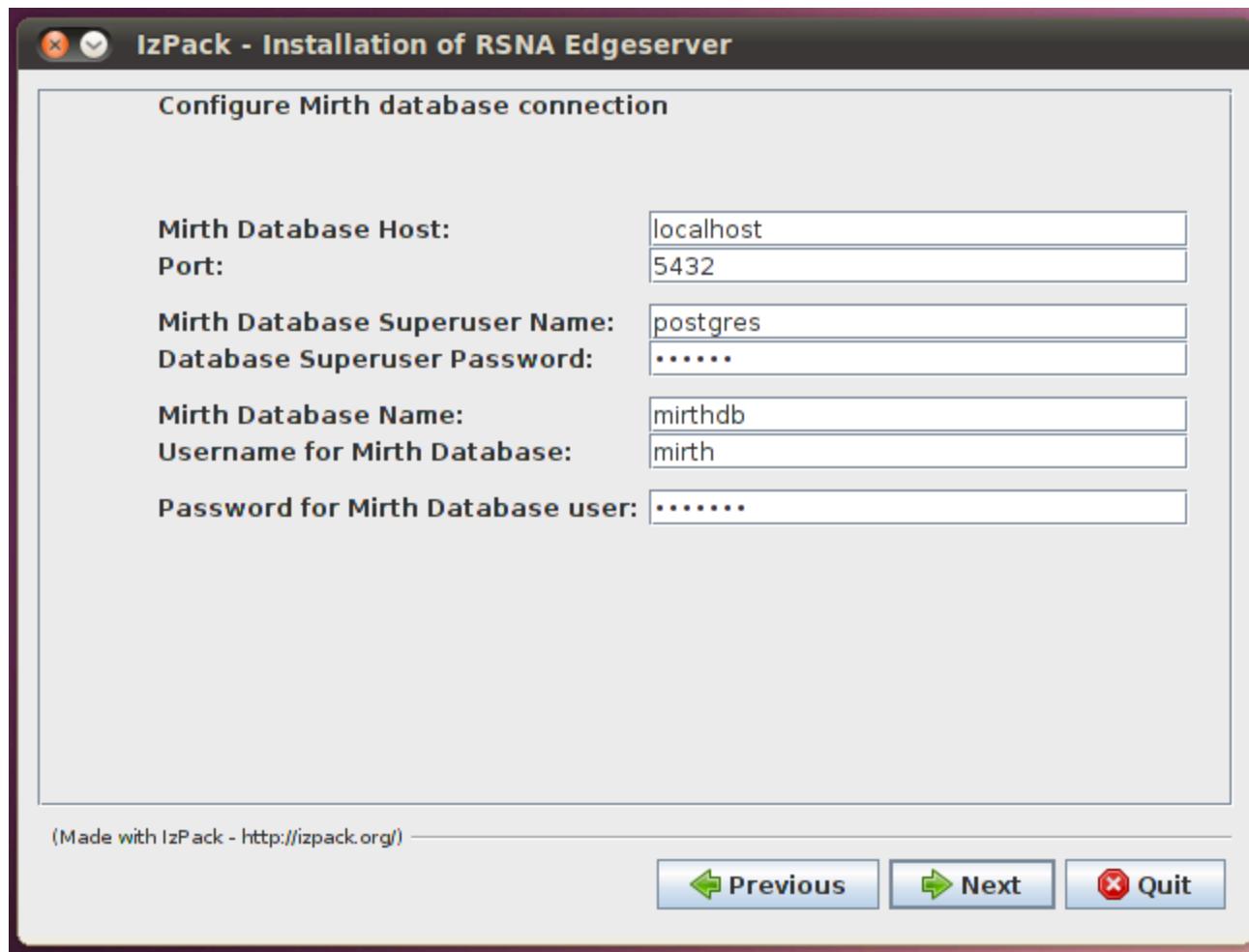


Figure 4-11: Configure MIRTH Database

Before the installer begins to execute its tasks, it presents a summary screen of what will be installed (Figure 4-13) and where, giving you one last chance to revise configuration settings before install.

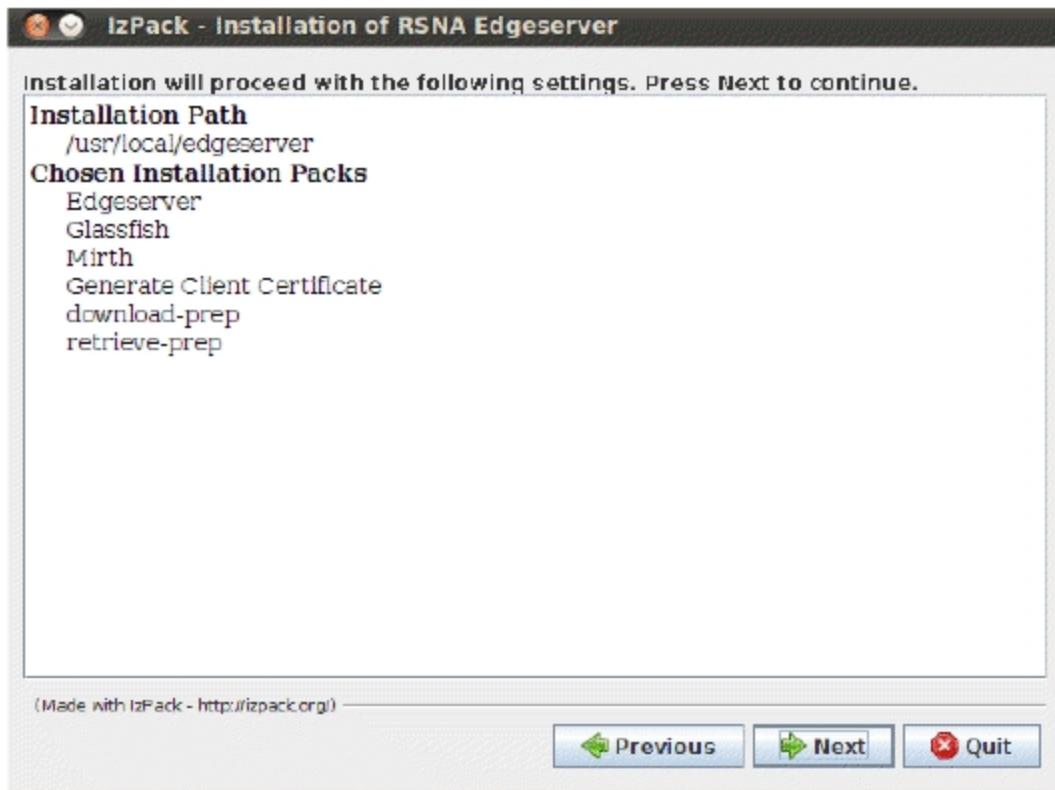


Figure 4-13: Pre-installation task summary

The installer will run through several screens, first setting up the Edge Server application (Figure 4-14) and then support applications (Figure 4-15). The final screen after installation has a “Done” button to click (Figure 4-16) which closes the installer.

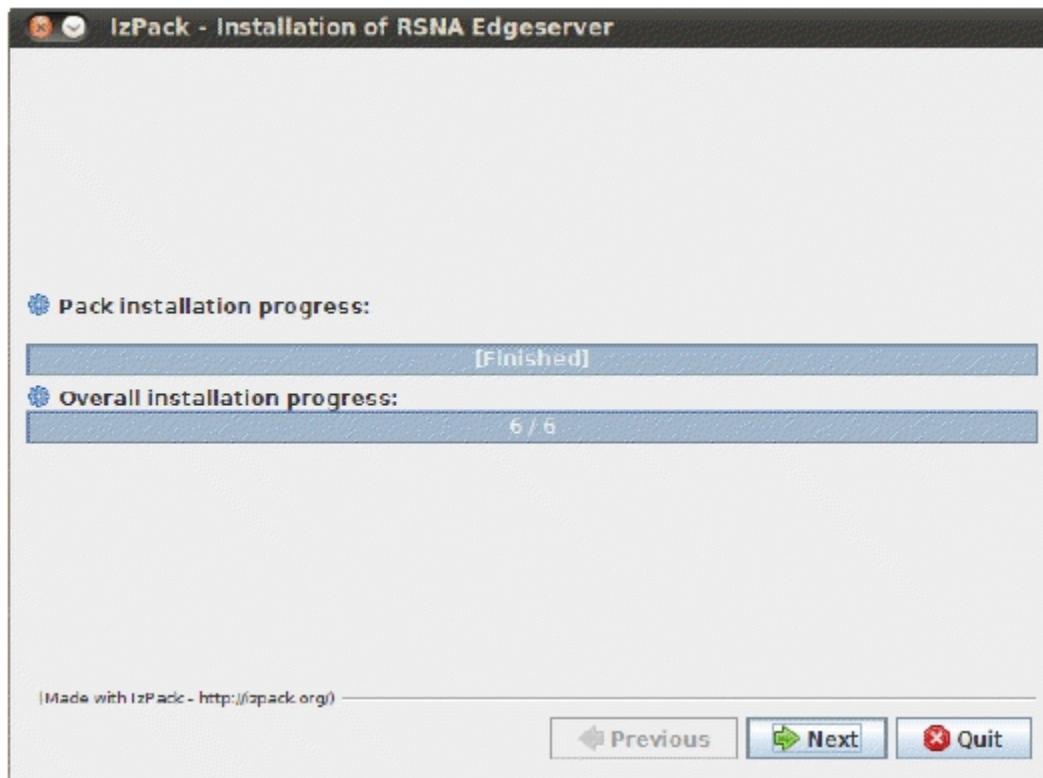


Figure 4-14: Edge server installation progress

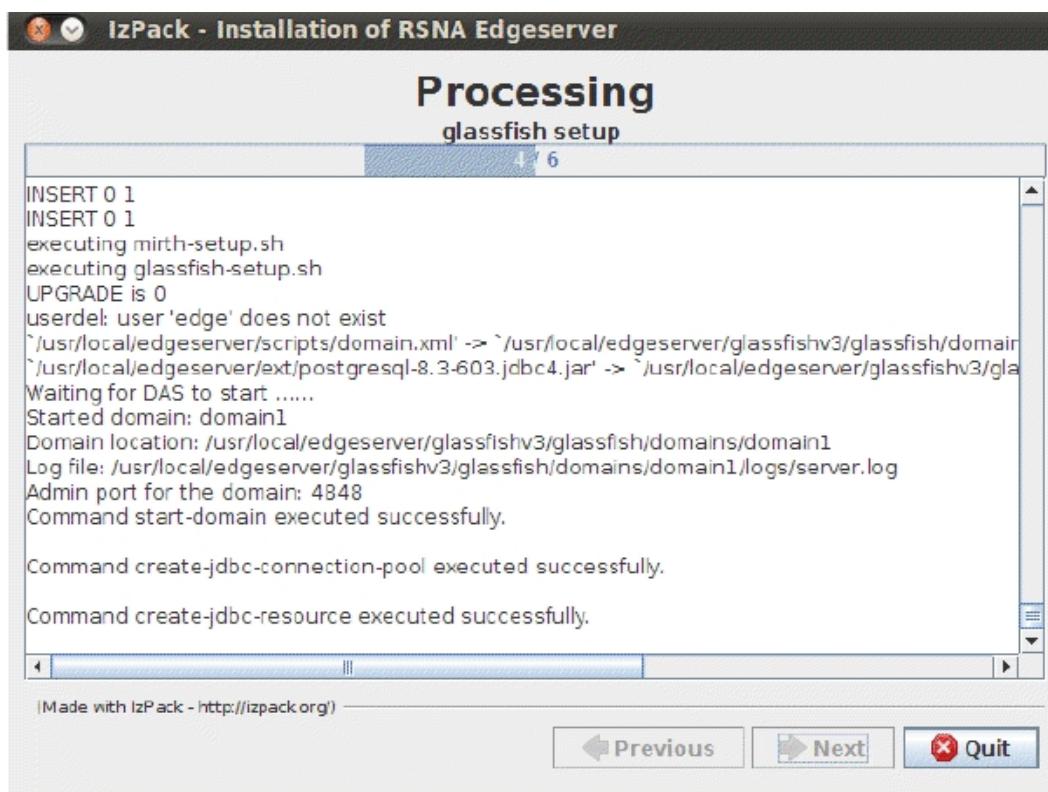


Figure 4-15: Application install progress

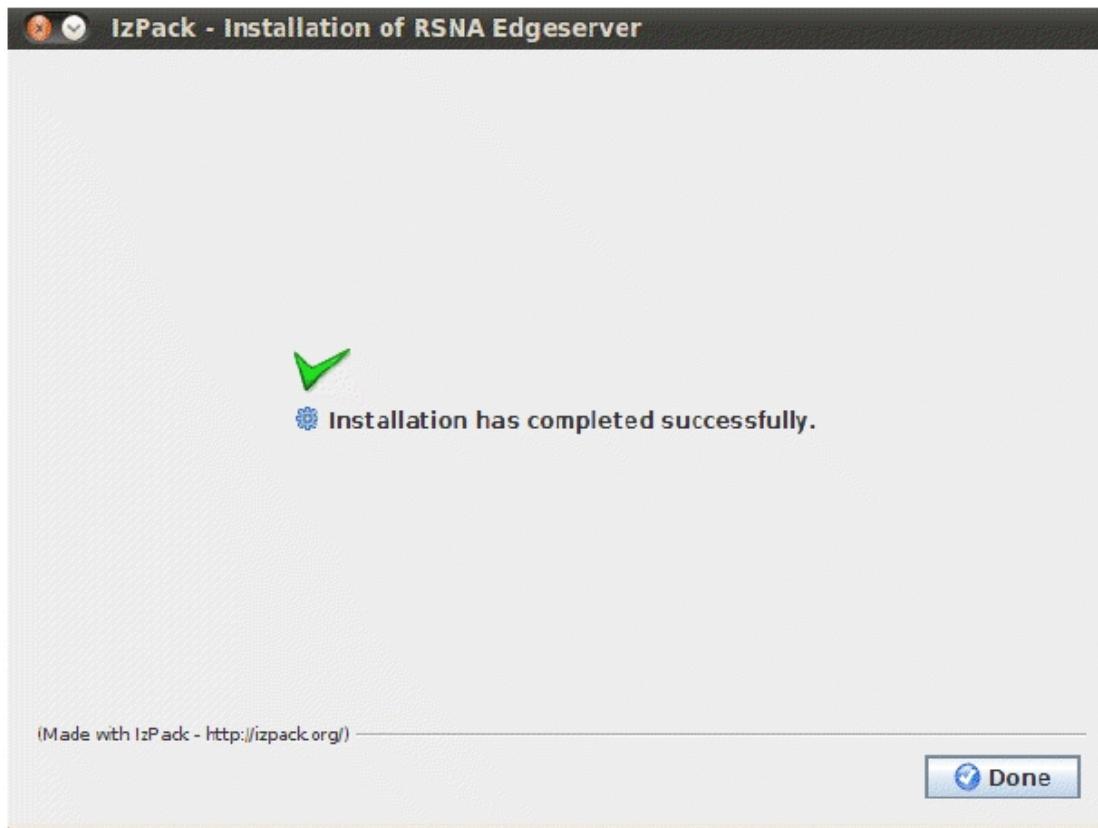


Figure 4-16: Installation complete

4.2.6 Configure the RSNA-Edge Server as an Ubuntu Service

From your command line window:

```
Sudo update-rc.d edge-server defaults 98 02
```

Reboot the system. All Edge Server services should now be running. You can now continue to section 4.3 (Registering the Edge Server Certificate with the Clearing House).

4.3 Registering the Edge Server Certificate with the Clearing House

In order for your institution's RSNA Edge Server to communicate with the lifeIMAGE Clearinghouse, SSL security certificates must be exchanged between your institution and lifeIMAGE. *Please note: it is assumed your institution has established a HIPAA BAA (Business Associates Agreement) with LifeIMAGE. If not, please contact David Wilkins (dwilkins@lifeimage.com) to get the process started.*

A copy of the lifeIMAGE's certificate is preinstalled in the \$RSNA_ROOT/conf/truststore.jks file To complete the exchange, you will need to send lifeIMAGE a copy of your site's Edge Server certificate. If you ran the installer (i.e. followed the Physical build process) then the certificate has already been generated (Figure 4-10) and you can skip to section 4.3.2: *Exporting and registering the certificate*. However, if you are using a virtual machine (VM) you will need to generate the certificate manually (see section 4.3.1)

4.3.1 Generating a certificate (VM users only)

To generate the certificate you will need to use the Java keytool utility. If you haven't already done so, start by logging into the Edge Server as the "rsna" user and opening a command line window. You need to assume the role of the edge account to be able to write into the Edge Server software folder. At the prompt, type:

```
sudo - edge
```

You will be prompted for the rsna password. Then, on one line:

```
$JAVA_HOME/bin/keytool -genkey -alias edge -keyalg RSA -keypass edge1234 -  
storepass edge1234 -validity <days> -keystore $RSNA_ROOT/conf/keystore.jks
```

where <days> is the number of days you want the certificate to be valid, e.g. 3650 for 10 years. Once the keytool utility starts, it will prompt you for information about your certificate. Note: FQDN means "Fully Qualified Domain Name" like edge.hospital.com. At the prompts enter the following (making sure to put the appropriate values in the brackets):

```
What is your first and last name?: <FQDN of Edge Server>  
What is the name of your organizational unit?: <Lab or department name>  
What is the name of your organization?: <University or Company name>  
What is the name of your City or Locality? <Your city (no abbreviations)>  
What is the name of your State or Province? <Your state or province (no  
abbreviations)>  
What is the two-letter country code for this unit? <Your country code, enter "US"  
(no quotes) for the United States>
```

When asked, verify the information you've entered is correct by typing "**yes**". Enter "**no**" if you need to go back and

reenter anything. At this point the keytool will generate the certificate and save it in \$RSNA_ROOT/conf/keystore.jks. You can now continue to section 4.1.2 (Exporting and registering the certificate).

4.3.2 Exporting and registering the certificate

To send LifeIMAGE the Edge Server certificate, you will first need to export it and convert it to a format LifeIMAGE can understand. If you haven't already done so, log into the Edge Server as the "rsna" user and open a command line window. At the prompt, type:

```
sudo - edge
```

You will be prompted for the rsna password. Then, on one line:

```
$JAVA_HOME/bin/keytool -export -alias edge -storepass edge1234 -file client.der -keystore $RSNA_ROOT/conf/keystore.jks
```

You should have a file called "client.der" in your current directory. This file contains the certificate in DER (Distinguished Encoding Rules) format. In order for LifeIMAGE to accept the certificate, it must be converted to PEM (Privacy-enhanced Electronic Mail) format. To convert the certificate run the following command:

```
openssl x509 -inform DER -in client.der -outform PEM -out client.pem
```

At this point you should have a file called "client.pem" in the current directory. You will need to email this file to David Wilkins (dwilkins@lifeimage.com) and support@lifeimage.com. You have now completed the installation of the Edge Server software and can continue to Chapter 5: Setting up MIRTH.

Please note: it is strongly recommended you send some test exams to the clearinghouse after completing the configuration of the Edge Server (Chapters 5 & 6). If you choose to send test exams, make sure to send LifeIMAGE the DOB, token and password for the job set as well as information on the exams included (e.g. modality, study date/time, image count). They will need this information to verify receipt by the clearinghouse.

5. Setting up MIRTH

Assumptions:

1. You have either run the Edge Server installer (Chapter 4, Physical) or installed and configured the Edge Server VM (Chapter 4, Virtual).
2. You have defined your HL7 message format and determined how they map to the Edge Server's database columns (see mappin spreadsheet).
3. That the Edge Server Web services are running. If you do not see the web page shown below, you may have to start the web services manually by typing “>/etc/init.d/edge-server start”

Setup:

1. MIRTH configuration is accomplished via a web interface; the web browser can be on either a remote machine or local on the Edge Server. If remote, open the browser (IE 8 is best avoided) and navigate to: <http://<address of Edge Server>:8080>. If local, open FireFox and navigate to: <http://localhost:8080>. You should see a page similar to the one pictured below:

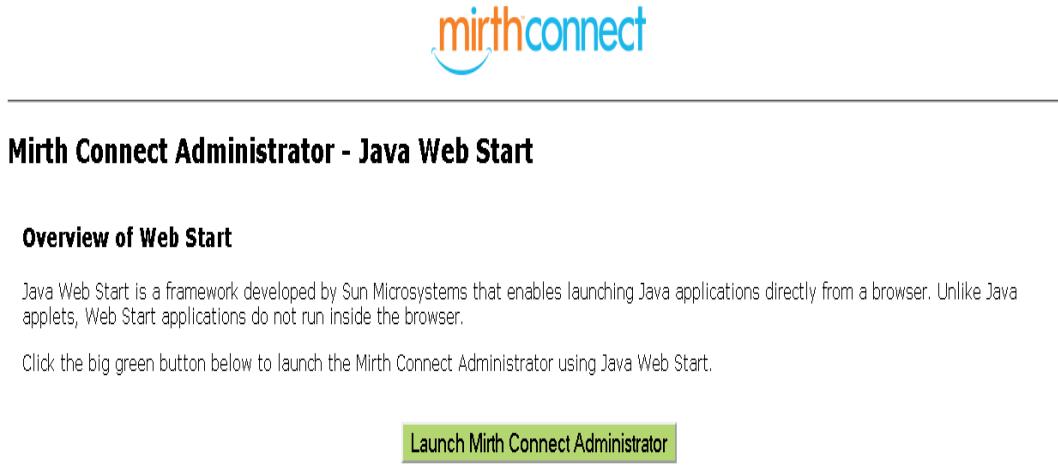


Figure 5-1: The Mirth Administrator Java Web Start page

2. Click the “Launch Mirth Connect Administrator” button. [Note: The first time this is done on the Edge Server’s local browser the path to the Java Web Start application is unknown. When FireFox asks what to use to open the file, select “other” on the drop down and navigate to Filesystem:/usr/local/jre-1.6-xx/javaws/javaws]. A Java Web Start app should launch and you should see the dialog pictured below:

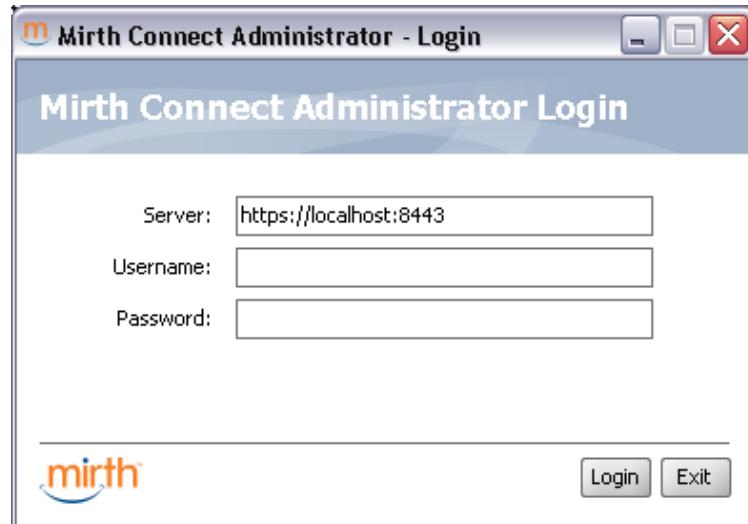


Figure 5-2: The Mirth Administrator login dialog

3. Login using username = "admin", password = "admin". After logging in you should see a screen similar to:

A screenshot of the Mirth Connect Administrator dashboard. The title bar says "Mirth Connect Administrator - https://localhost:8443". The left sidebar has sections for "Mirth Connect" (Dashboard, Channels, Users, Settings, Notes, Events, Plugins), "Status Tasks" (Refresh, Start All Channels, Stop All Channels, Reset All Channels), and "Other" (Help on this topic, About Mirth Connect, Visit mirthcorp.com, Report Issue, Logout). The main area is titled "Dashboard" and shows a table with columns "Status", "Name", "Received", and "Filtered". There are no rows in the table.

Figure 5-3: Mirth Administrator

4. You will first need to initialize the base Mirth setup. In the left column, click on the "Settings" link. You should see a screen similar to:

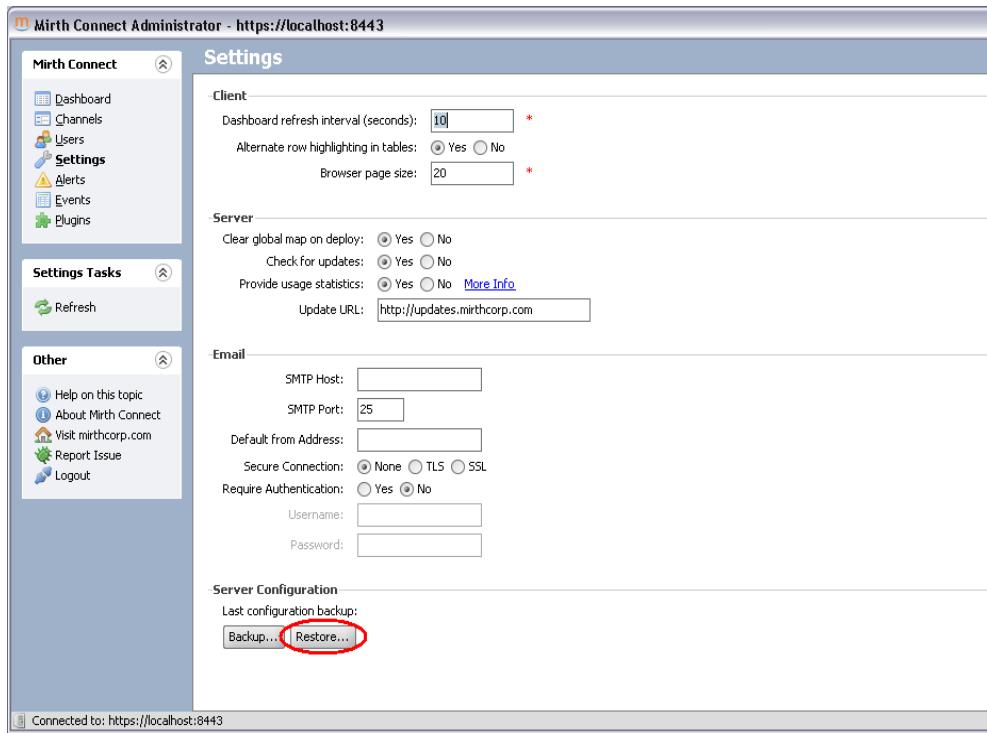


Figure 5-4: Installing the default Mirth configuration

5. Click the “Restore...” button at the bottom of the page and select the “Mirth Backup.xml” file located in the Edge Server installation directory (see Figure 5-4). You should get a message saying your configuration was successfully restored.
6. You will now need to configure the database connection password. To do so first switch “Channels” under the Mirth Connect heading on the left, then click the “Edit Code Templates” link under the “Channel Tasks” heading.
7. Then open the “Get Database Connection” template by double clicking on its entry. You should see the screen below.

Code Templates

Name	Type	Context	Description
Get Database Connection	Function	Global	Returns a connection to the RSNA results database
Insert or Update Patient	Function	Channel	Adds a new patient or updates an existing patient's demographic i...
Insert or Update Exam	Function	Channel	Adds a new exam or updates an existing exam.
Insert Status Change	Function	Channel	Adds a new entry into the reports table

CodeTemplate Tasks

- New CodeTemplate
- Import Code Templa...
- Export Code Templa...
- Delete CodeTemplate
- Validate Script

Other

- Help on this topic
- About Mirth Connect
- Visit mirthcorp.com
- Report Issue
- Logout

Connected to: https://192.9.69.124:8443

```

Type: Function
Context: Global
Description: Returns a connection to the RSNA results database
Function:
1 // modify function_name and parameters as you wish.
2 // one function per template is recommended. i.e.) create a new code template for each new funct:
3 function getConnection() {
4     var con = DatabaseConnectionFactory.createDatabaseConnection('org.postgresql.Driver',
5         'jdbc:postgresql://localhost:5432/rsnadb','edge01');
6
7
8     return con;
9 }
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30

```

Figure 5-5: Configuring database connection parameters

8. Replace the fourth parameter with the password you defined for the RSNA database user.
9. Now switch to the channels page by click the “Channels” link in the left column. You should see the screen pictured below:

Channels

Status	Protocol	Name	Id	Description
Enabled	HL7 v2.x	Edge Server HL7 Receiver	20873abb-9dd9-4e32-9167-f3a82fd99fb6	

Channel Tasks

- Refresh
- Deploy
- Edit Global Scripts
- Edit Code Templates
- New Channel
- Import Channel
- Export All Channels
- Export Channel
- Clone Channel
- Edit Channel
- Delete Channel
- Disable Channel

Other

- Help on this topic
- About Mirth Connect
- Visit mirthcorp.com
- Report Issue
- Logout

Connected to: https://localhost:9443

Figure 5-6: Mirth Channel Listing

10. Double click the HL7 channel to edit it. You'll see the page below:

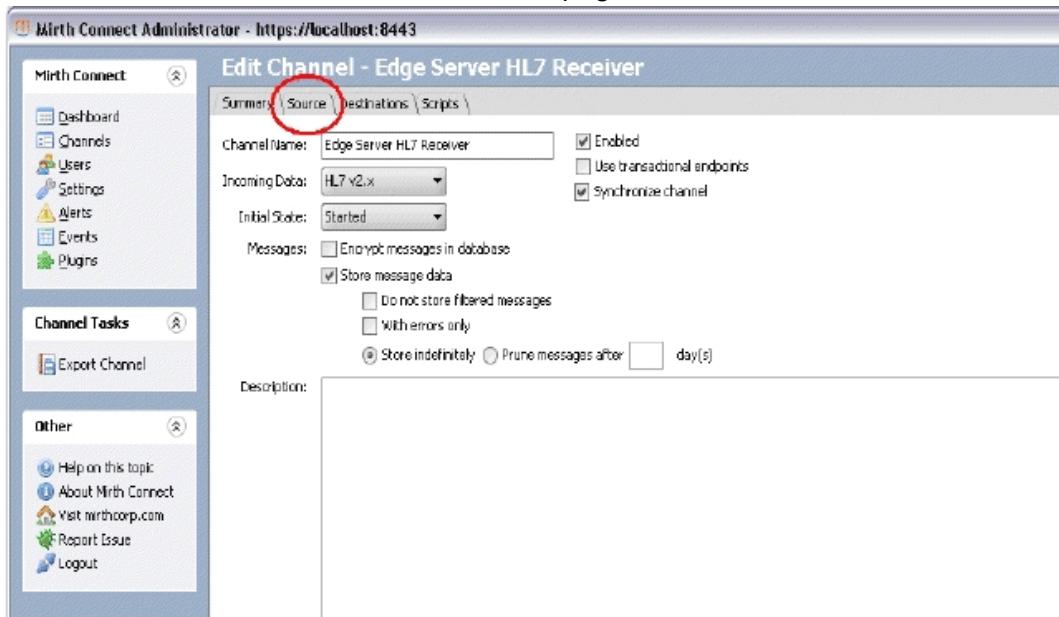


Figure 5-7: Configuring the HL7 channel

11. Click on the Source tab and you will see the screen below:

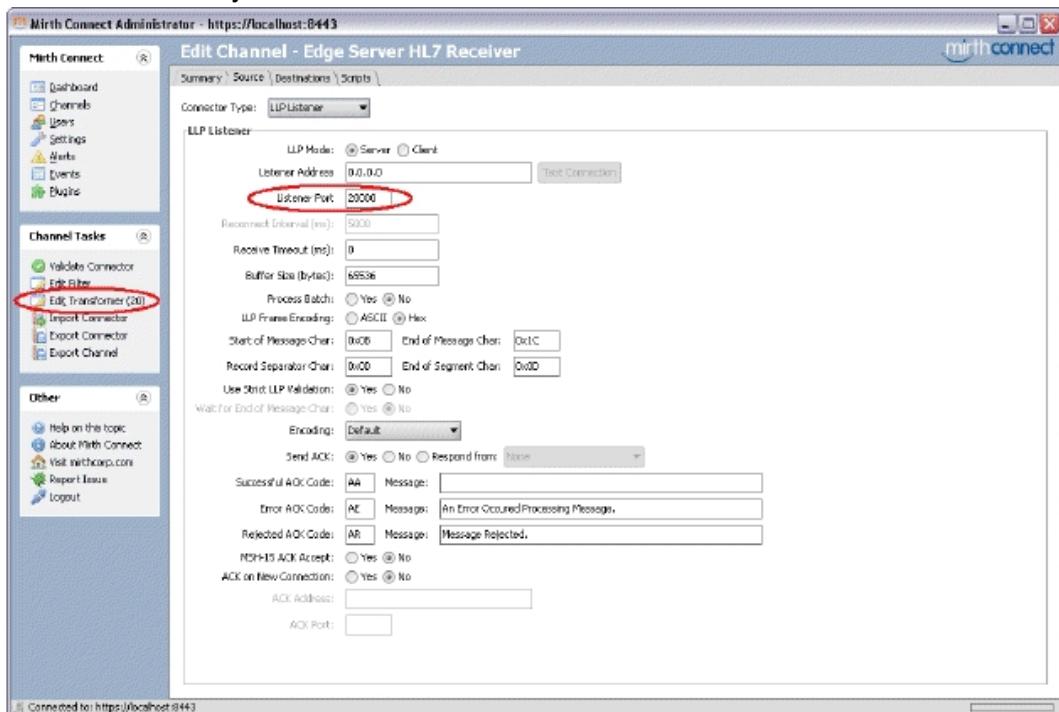


Figure 5-8: Configuring the HL7 network parameters

12. Set the the Listener Port value to the appropriate value for your installation.

13. After you are done, click the "Edit Transformer" link in the left column. You will see the screen pictured below:

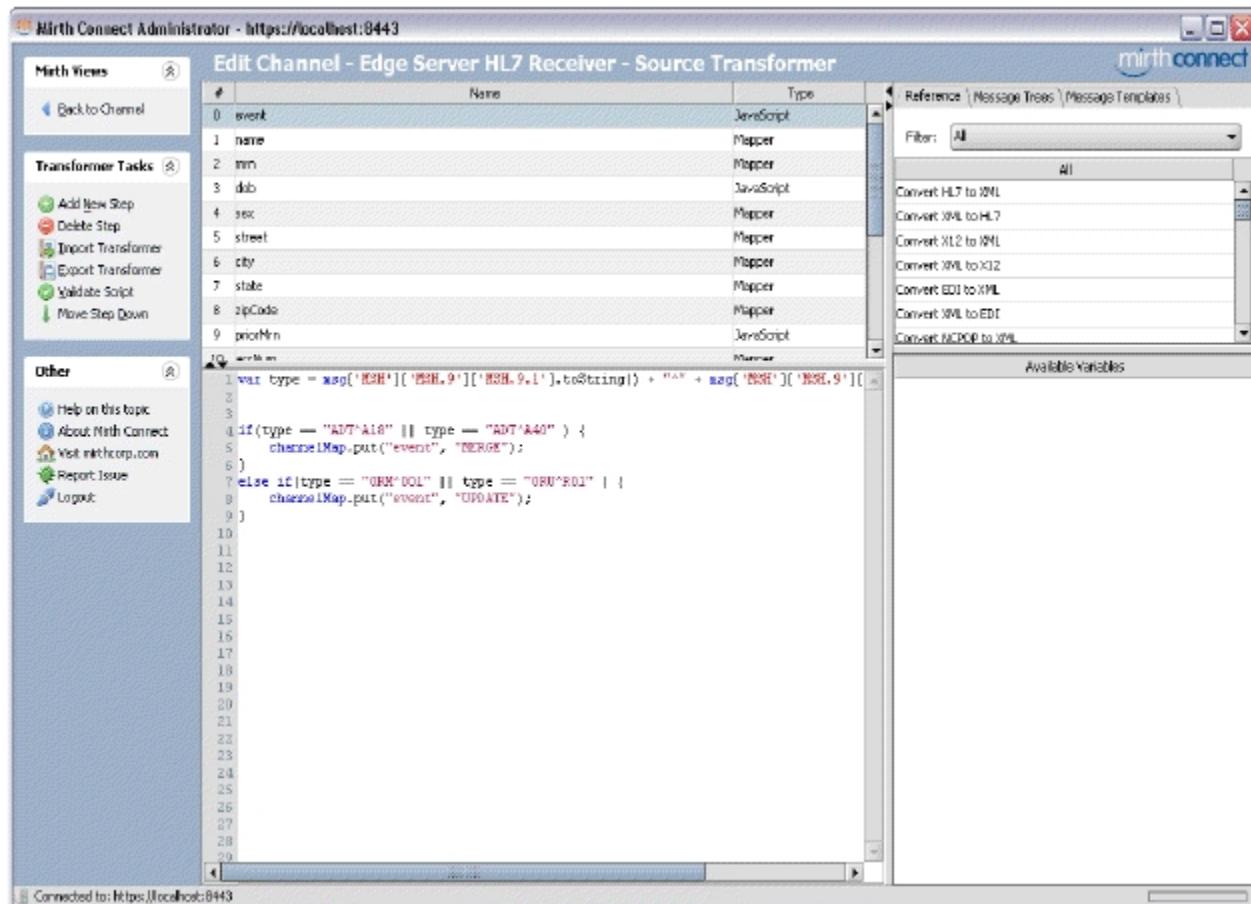


Figure 5-9: Configuring the HL7 channel variables

14. You will need to adjust the mapping between your HL7 messages and the channel variables used to populate the Edge Server database. The following variables require customization:

Variable	Notes
event	Type of event associated with the incoming message. Permitted values are: UPDATE MERGE Determines whether the incoming message is for an exam status UPDATE or a patient MERGE.
name ("patients")	The patient's name. Must not be blank.
mrn ("patients")	The patient's medical record number. This value will unique identify the patient on the Edge Server and is used to retrieve images from the site's PACS. Must not be blank.
dob ("patients")	The patient date of birth. Cannot be null. Value must be of type java.sql.Date
sex ("patients")	The patient's sex. Must not be blank.
street ("patients")	The street component of a patient's address. Used by the token app to help site staff verify a patient's identity before their images are queued for transmission.

city ("patients")	The city component of a patient's address. Used by the token app to help site staff verify a patient's identity before their images are queued for transmission.
state ("patients")	The state component of a patient's address. Used by the token app to help site staff verify a patient's identity before their images are queued for transmission.
zipCode ("patients")	The zip code component of a patient's address. Used by the token app to help site staff verify a patient's identity before their images are queued for transmission.
priorMrn ("patient_merge")	Used when merging 2 patients. Should be populated for a patient merge message.
accNum ("exams")	The exam's accession number. This value will uniquely identify an exam on the Edge Server and is used to retrieve images from the site's PACS.
studyDescription ("exams")	The exam description.
status ("reports")	<p>The exam status. Sites need to map their exam status codes to the following values:</p> <p style="text-align: center;">ORDERED SCHEDULED IN-PROGRESS COMPLETED DICTATED PRELIMINARY FINALIZED REVISED ADDED CANCELED NON-REPORTABLE</p>
statusChangeTimestamp ("reports")	The timestamp of the exam status change. Cannot be null. Value must be of type java.sql.Timestamp.
report ("reports")	<p>Full text of the report. <i>The value must be plain text and cannot contain any formatting character sequences.</i></p> <p>To convert from RTF to plain text, use Mirth's built-in FileUtils.rtfToPlainText method. Other formats will require the development of site specific conversion methods, which are beyond the scope of this document.</p>
signer ("reports")	The report signer.
dictator ("reports")	The report dictator.
transcriber ("reports")	The report transcriber.

15. When you are done click the "Save Changes" link in the left column and switch back to the Channels panel.
16. Right click on the list of channels and select "Deploy All" from the context menu.
17. You will then see the Dashboard panel pictured below. Verify that both channels are listed as "Started".

The screenshot shows the Mirth Connect Administrator interface at the URL <https://localhost:8443>. The main area is titled "Dashboard" and displays a table of channel status. The table has columns for Status, Name, Received, Filtered, Queued, Sent, Errored, Alerted, and Connection. Two channels are listed:

Status	Name	Received	Filtered	Queued	Sent	Errored	Alerted	Connection
Started	Edge Server HL7 Receiver	0	0	0	0	0	0	Waiting
Started	RSNA Edge Appliance DICOM SCP	0	0	0	0	0	0	Waiting

On the left sidebar, there are sections for "Status Tasks" (Refresh, Start All Channels, Stop All Channels, Reset All Channels) and "Other" (Help on this topic, About Mirth Connect, Visit mirthcorp.com, Report Issue, Logout). At the bottom, a status bar indicates "Connected to: https://localhost:8443". A large central panel is labeled "Server Log | Dashboard Status Panel \ Log Information" and contains a large empty white area.

Figure 5-10: The Mirth Administrator dashboard for monitoring channel status

6. The Web UI

Initial Login and Account Management:

As in Chapter 5, configuration is done via a web browser which can be local to the Edge Server or remote. Currently the supported browsers are:

- a) Firefox versions > V3.5
- b) Google Chrome (latest version)
- c) Internet Explorer > V7.0
- d) Safari (latest version)

If you are local on the Edge server, one can use the URL **http://localhost:3000**, if remote use **http://edge-hostname-or-ip:3000/** and enter the initial login credentials:

- Username: **admin**
- Password: **changeme**



Figure 6-1: Login Screen

The initial landing page is the patient search interface. For security reasons, it is suggested your first activity is to

change the administrator password, so click the “Change Password” button to change your password.



Figure 6-2: Successful Login and Patient Search

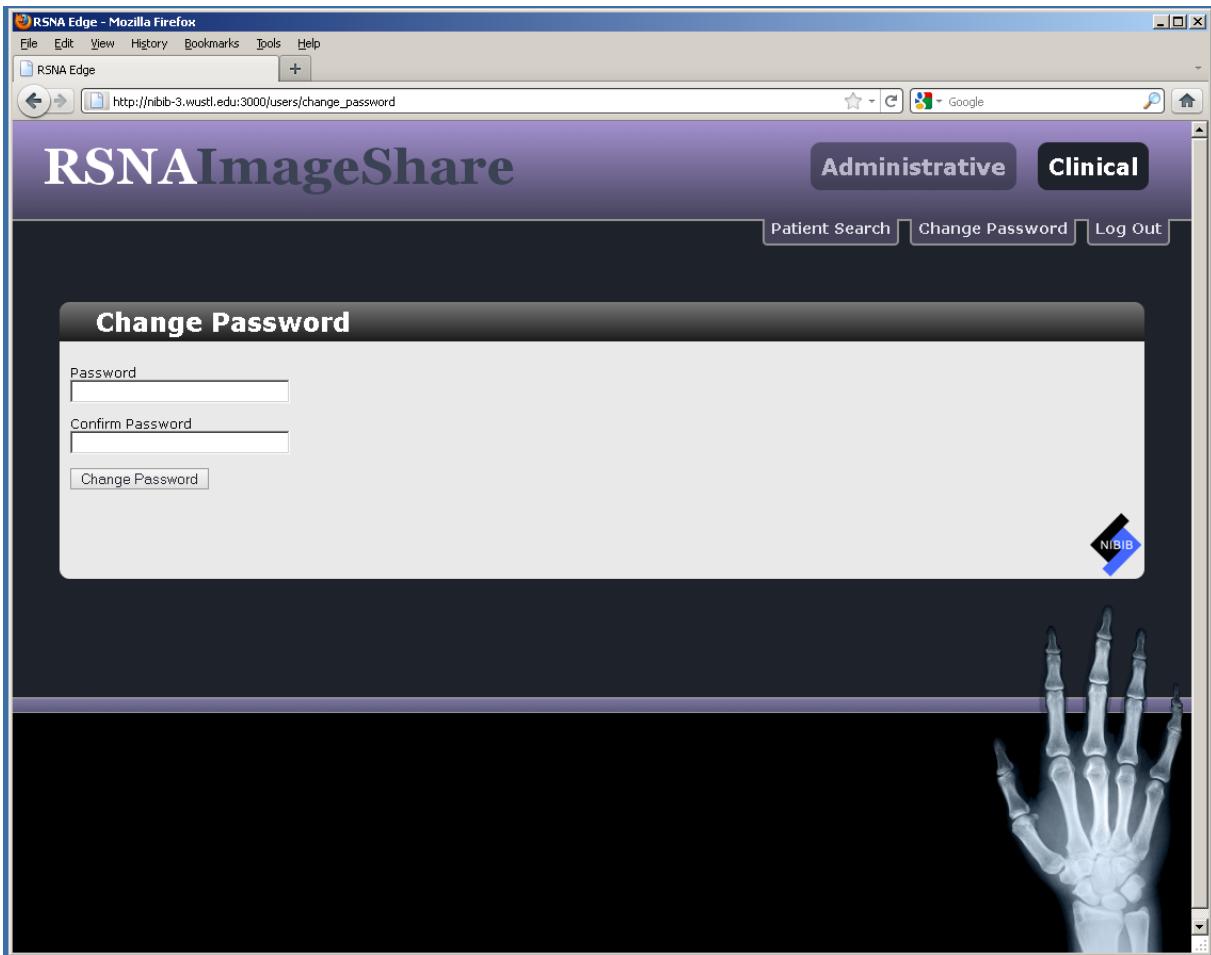


Figure 6-3: Changing Password

The **admin** user has full privileges, including the ability to create other users, change system configuration options, and view logs. To create a new user, click the "Administrative" button, then click the "New User" button.

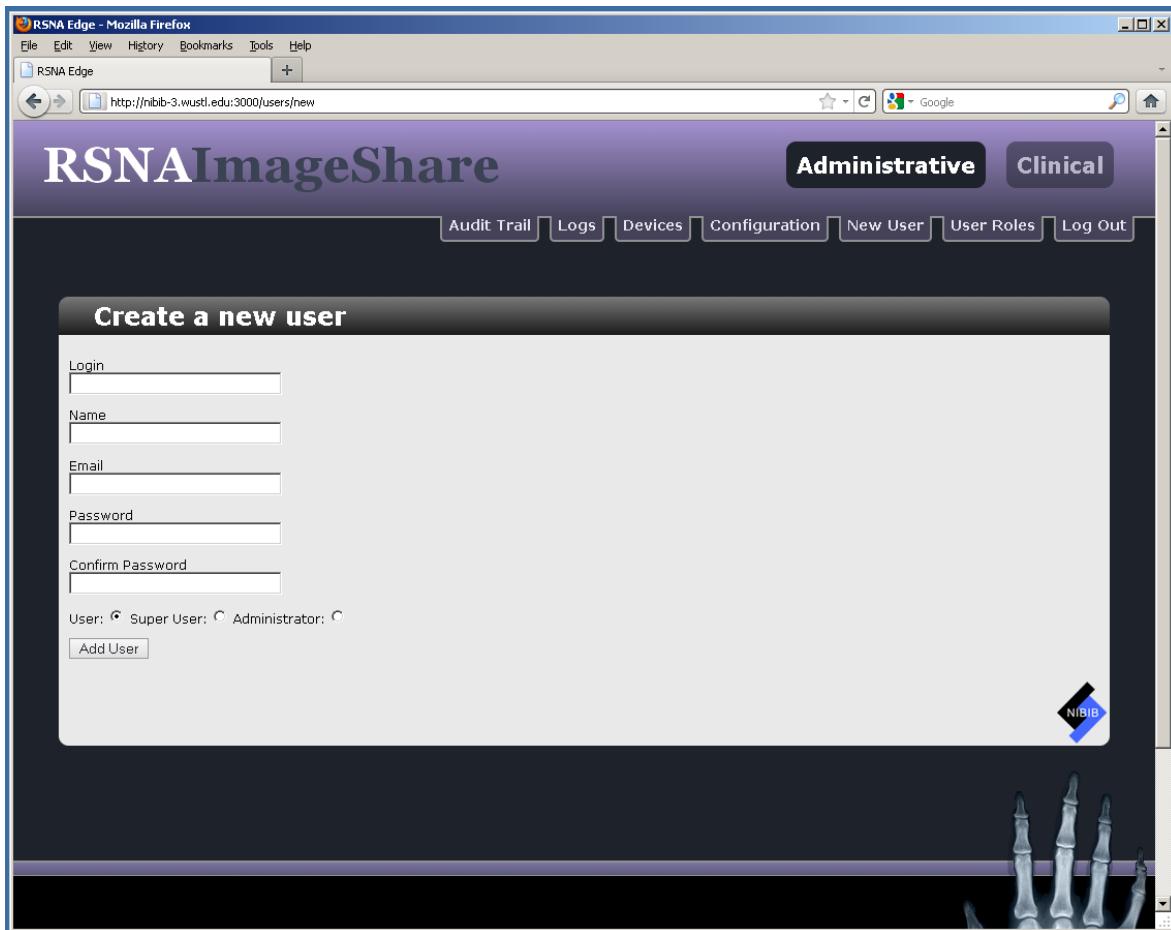


Figure 6-4: Creating a new user

When creating the user, note that there are 3 roles to choose from:

- **Administrator:** create/delete/edit users, modify devices and site config, view jobs (all privileges)
- **Super User:** same as user, with ability to view all jobs
- **User:** look up patients and create RSNA IDs, reset PINs, submit jobs, and view their own jobs

These roles can always be adjust by clicking the "User Roles" buttons.

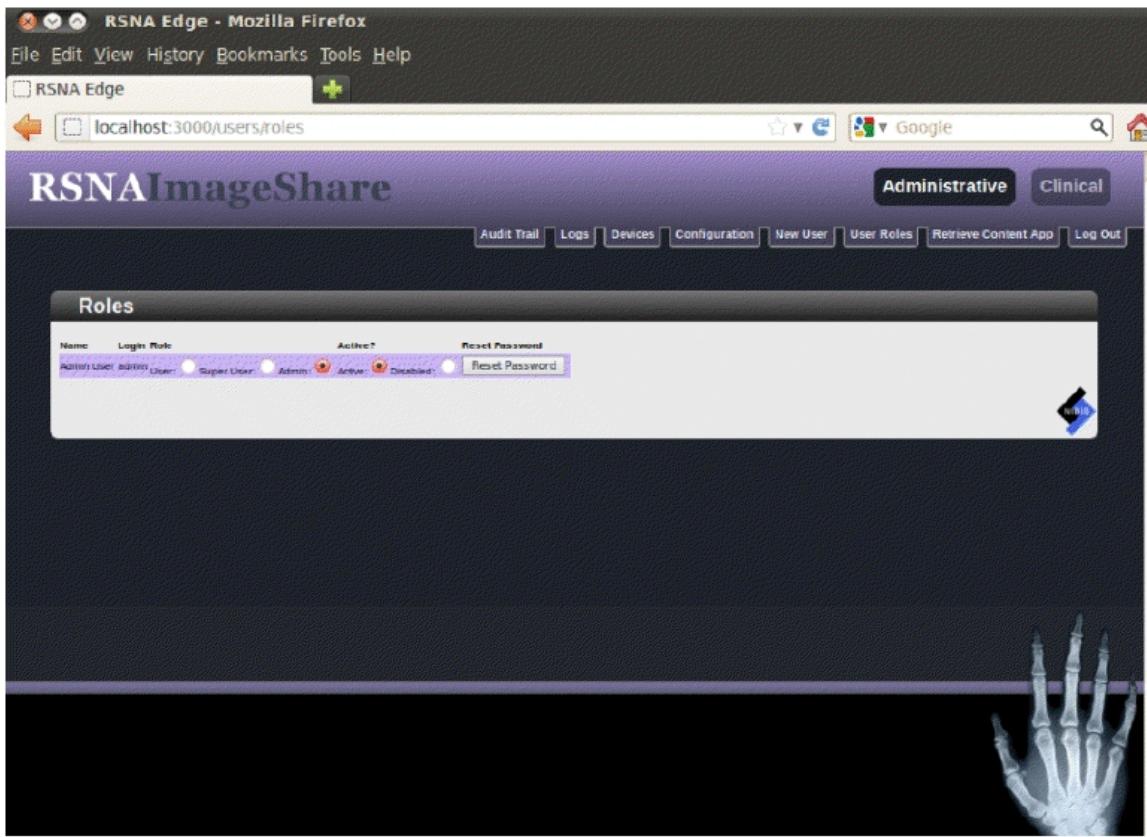


Figure 6-5: Adjusting User Roles

Configuration Options:

The Administrative interface can be used to configure information about the DICOM device by clicking the "Devices" link.

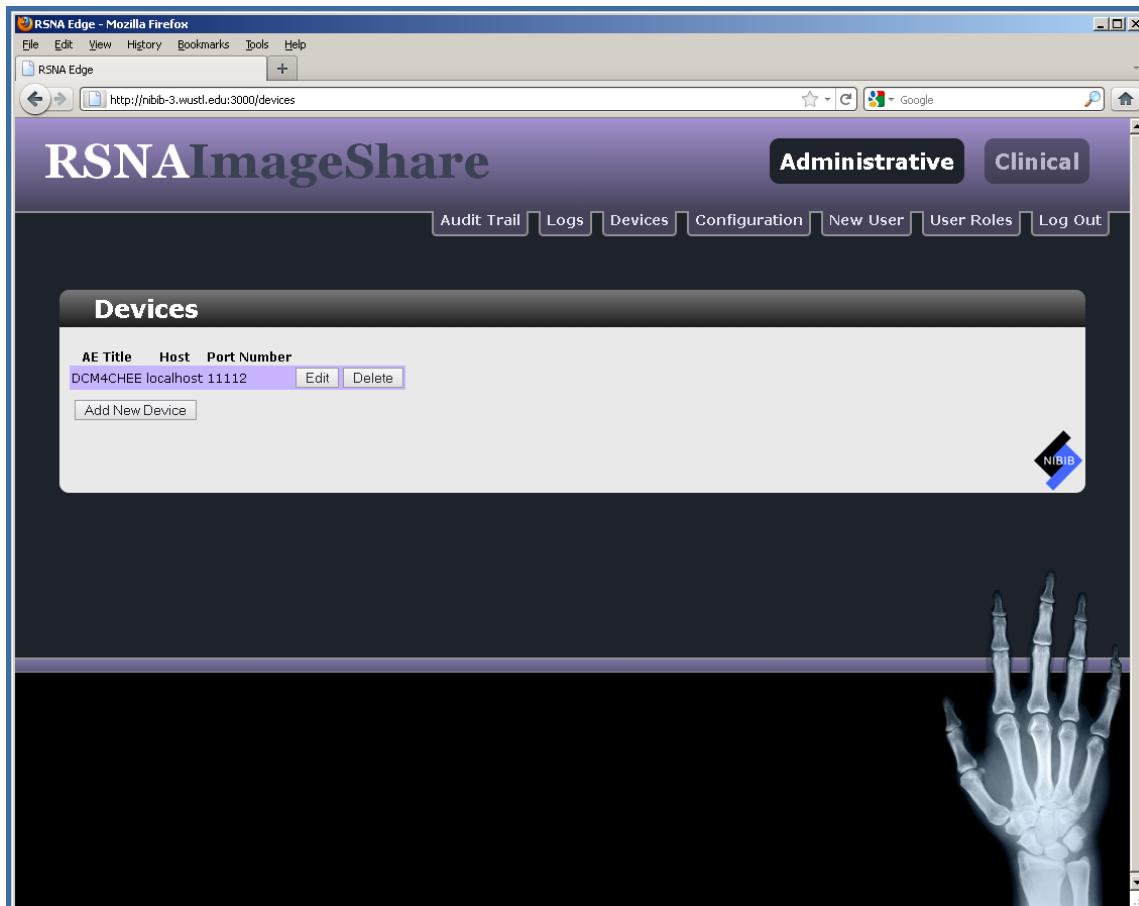


Figure 6-6: DICOM Device Configuration

In addition, other system settings can be adjusted by clicking the "Configuration" button.

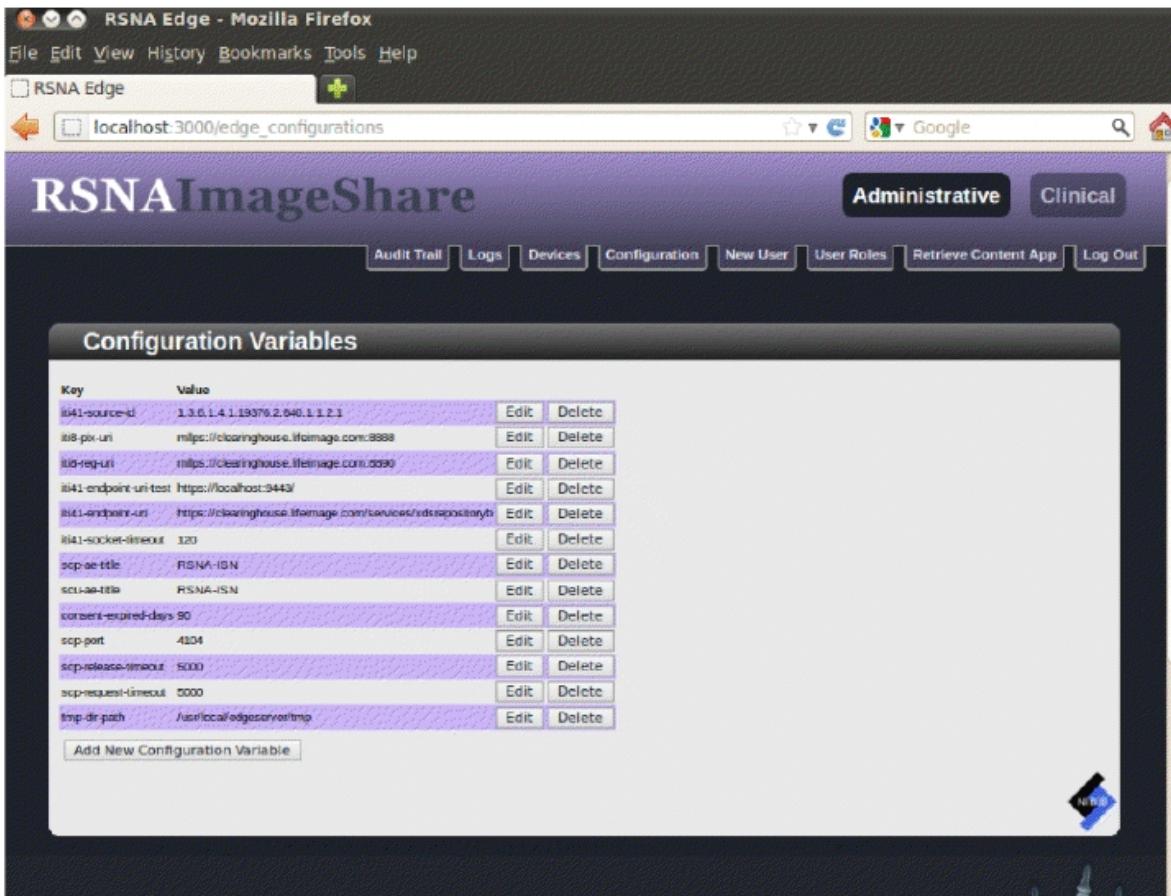


Figure 6-7: System Configuration Options

Configuration:

The Edge Server relies on several variables specified in the database and editable using the Administrative configuration page. To get there click on the “Administrative” menu and then “Configuration”. One variable that should be set by each site is the “help_desk_message” variable. This value will appear on the printout given to patients. The default message is: “Please contact helpdesk@imsharing.org or call 1-855-IM-SHARING (467-4274) for support” Another variable which should be considered is the “delay_in_hours” variable. Setting this variable will override the default 72 hour delay.

DICOM Configuration:

The following variables are required to ensure DICOM connectivity between the Edge Server and your institution’s PACS:

- scu-ae-title: The AE title of the Edge Server’s SCU. Used to initiate C-FIND and C-MOVE requests against your institution’s PACS.
- scp-ae-title: The AE title of the Edge Server’s SCP. Used to handle C-STORE requests from your institution’s PACS.
- scp-port: The TCP/IP port to use for the Edge Server’s SCP.

After making any changes, you will need to restart the Edge Server. You should also test connectivity by performing a C-ECHO from your PACS to the Edge Server.

Furthermore, the following optional variables are available for debugging and performance tuning. As with the previous settings, you will need to restart the Edge Server for them to take effect:

- scp-request-timeout: Maximum number of milliseconds the SCP will wait for the initial request on an

association. Default value is 5000.

- scp-release-timeout: Maximum number of milliseconds the SCP will wait to release an association. Default value is 5000.
- scp-max-send-pdu-length: Limits the maximum send PDU length (in bytes) negotiated by the SCP. Default value is 16364.
- scp-max-receive-pdu-length: Limits the maximum receive PDU length (in bytes) negotiated by the SCP. Default value is 16364.

For more information on these setting please consult the DCM4che2 toolkit documentation:

<http://www.dcm4che.org/confluence/display/d2/dcm4che2+DICOM+Toolkit>

Administrative Overview:

The Administrative interface also provides audit and application log views by clicking the “Audit Trail Button” and the “Logs” buttons.

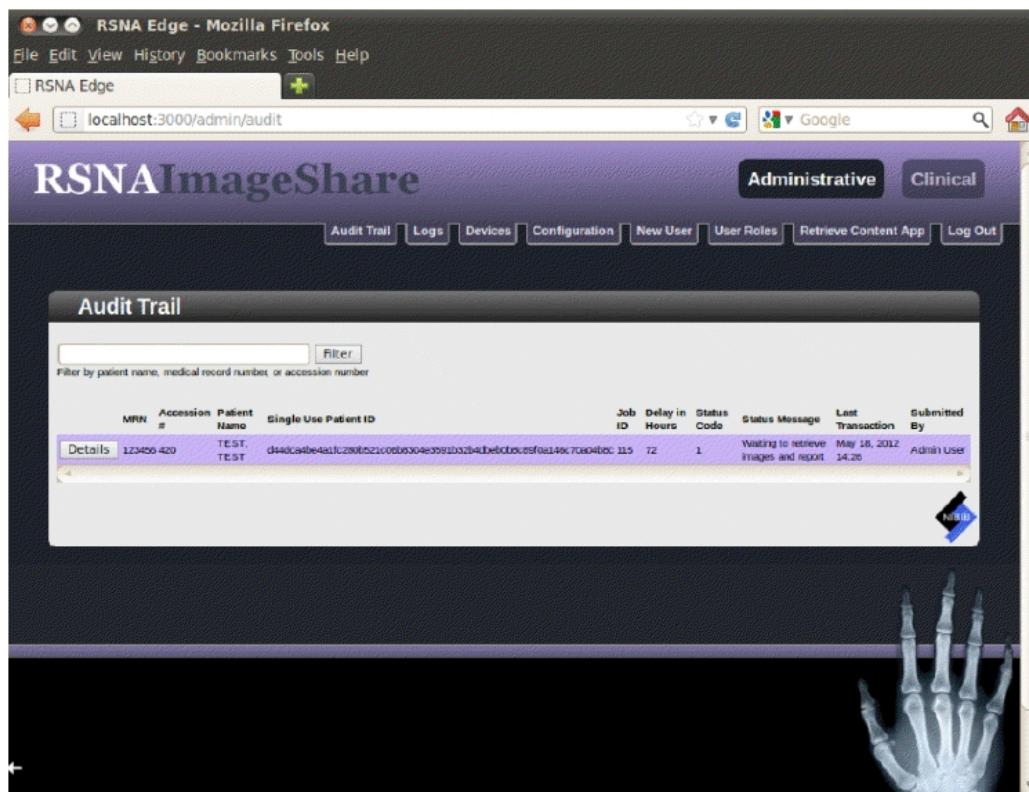


Figure 6-8: Audit Trail Interface

If a job has failed (indicated by status code < 0), a “Retry Job” button will appear on the Audit Details screen. Pressing this button will create a new transaction for the job with status code “1” and comments “Retry”. The screen will refresh and the new transaction details will display in the Audit Trail.

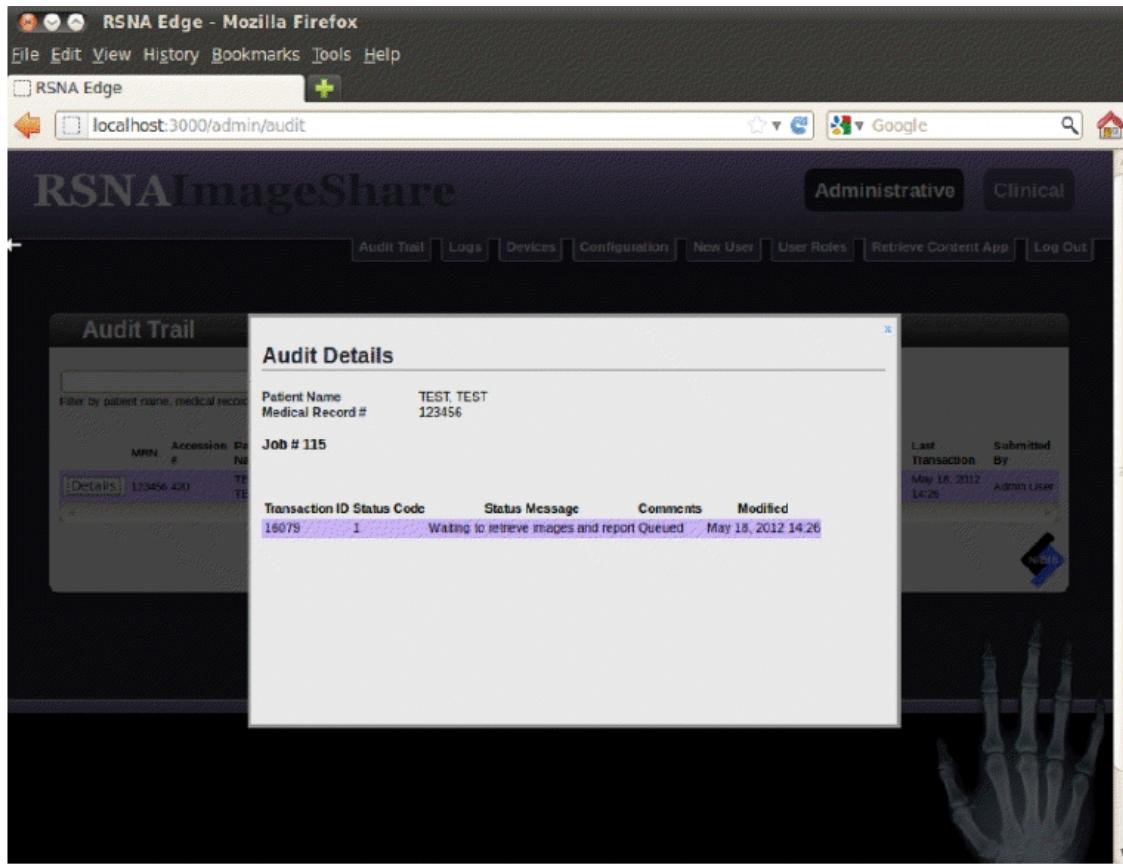


Figure 6-9: Retry Failed Jobs

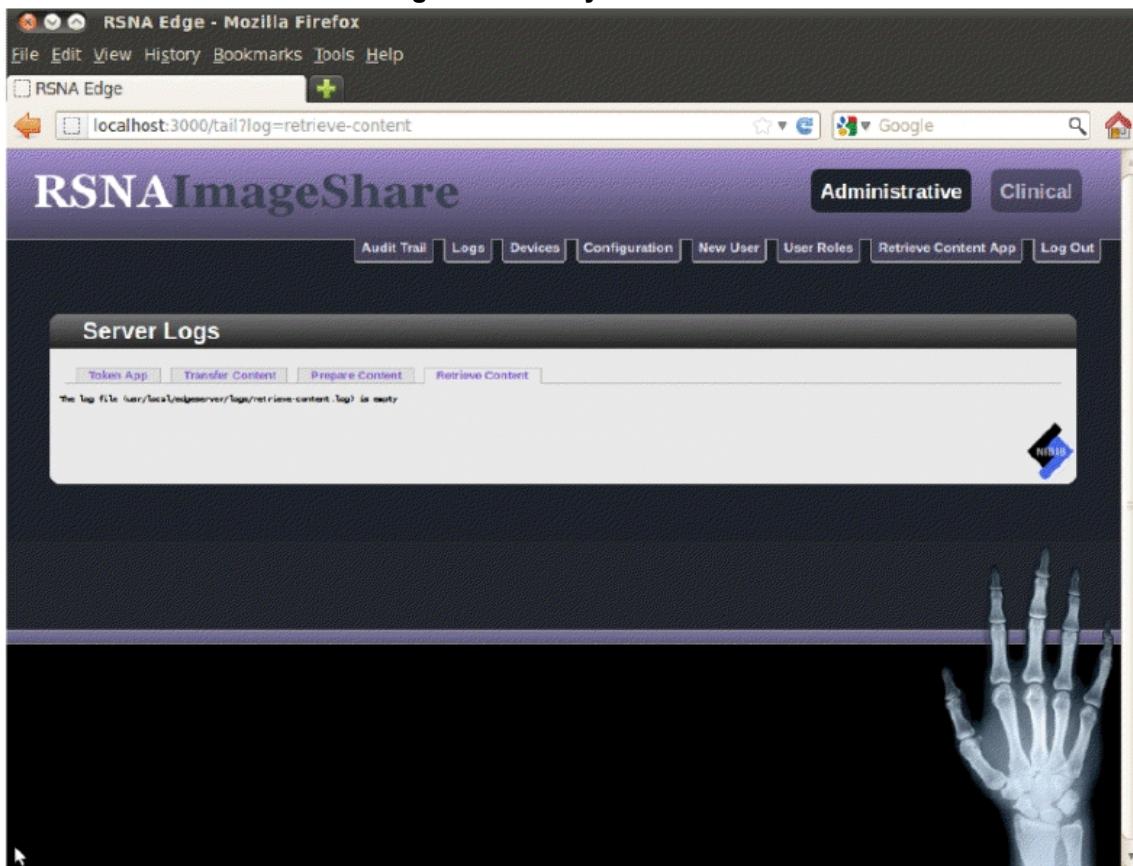


Figure 6-10: Application Logs

Normal Usage:

Normal workflow is to search for a patient under the Clinical interface by clicking the “Patient Search” button. There is also an Advanced Search link you can use on this page.

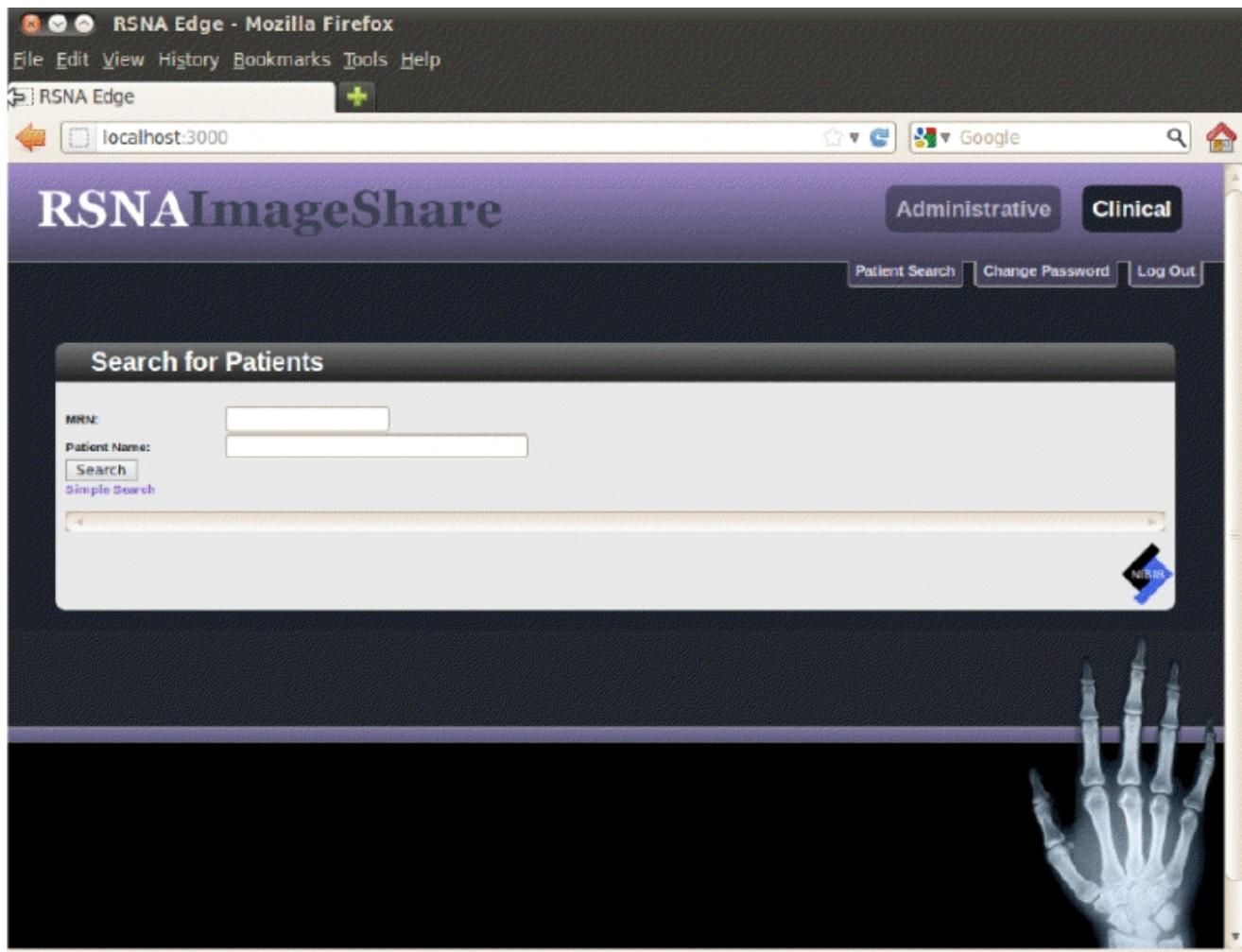


Figure 6-11: Advanced Patient Search

Once you search for a patient, results are presented and you can choose a patient. This prompts for a patient confirmation and consent acknowledgement. After the confirmation is acknowledged, a list of the selected patients exams are presented. These exams are added to a “shopping-cart” style interface.

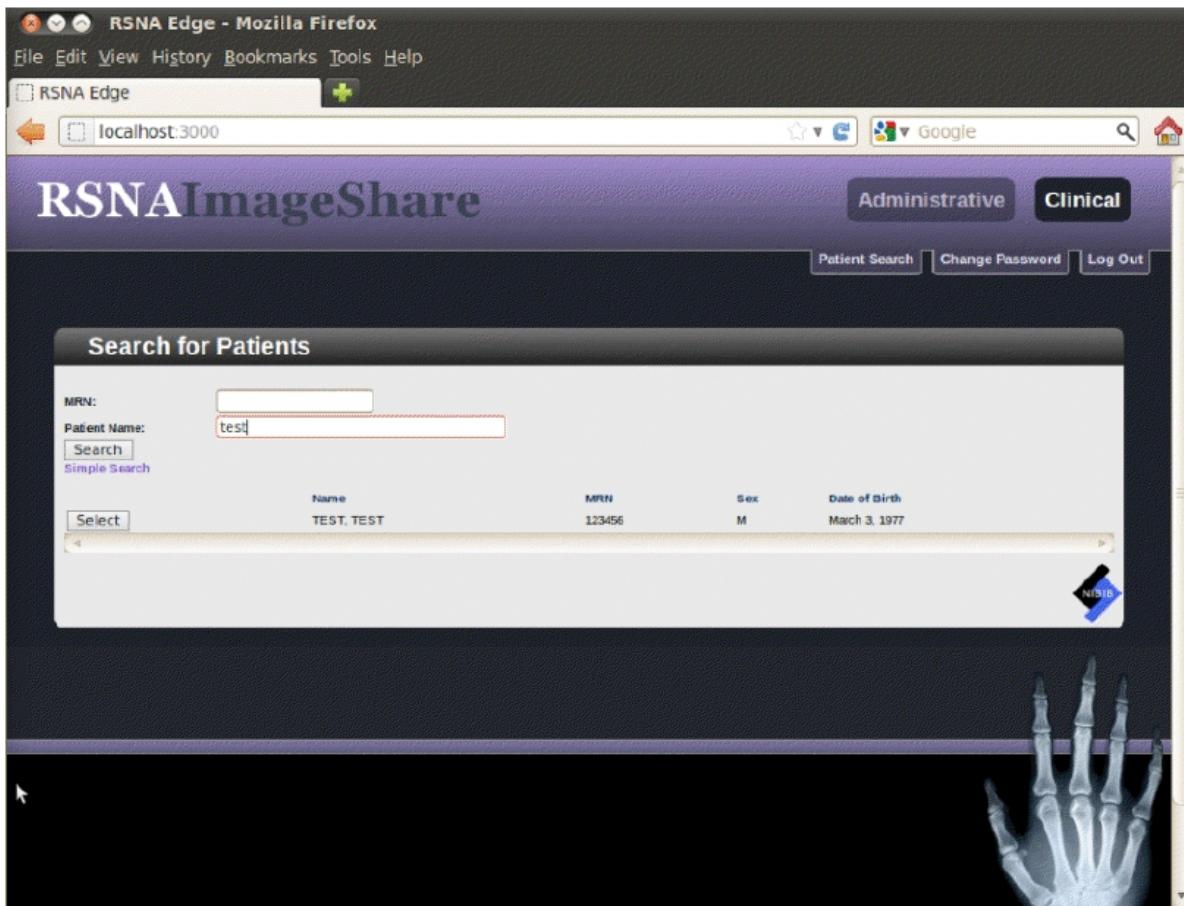


Figure 6-12: Search Results

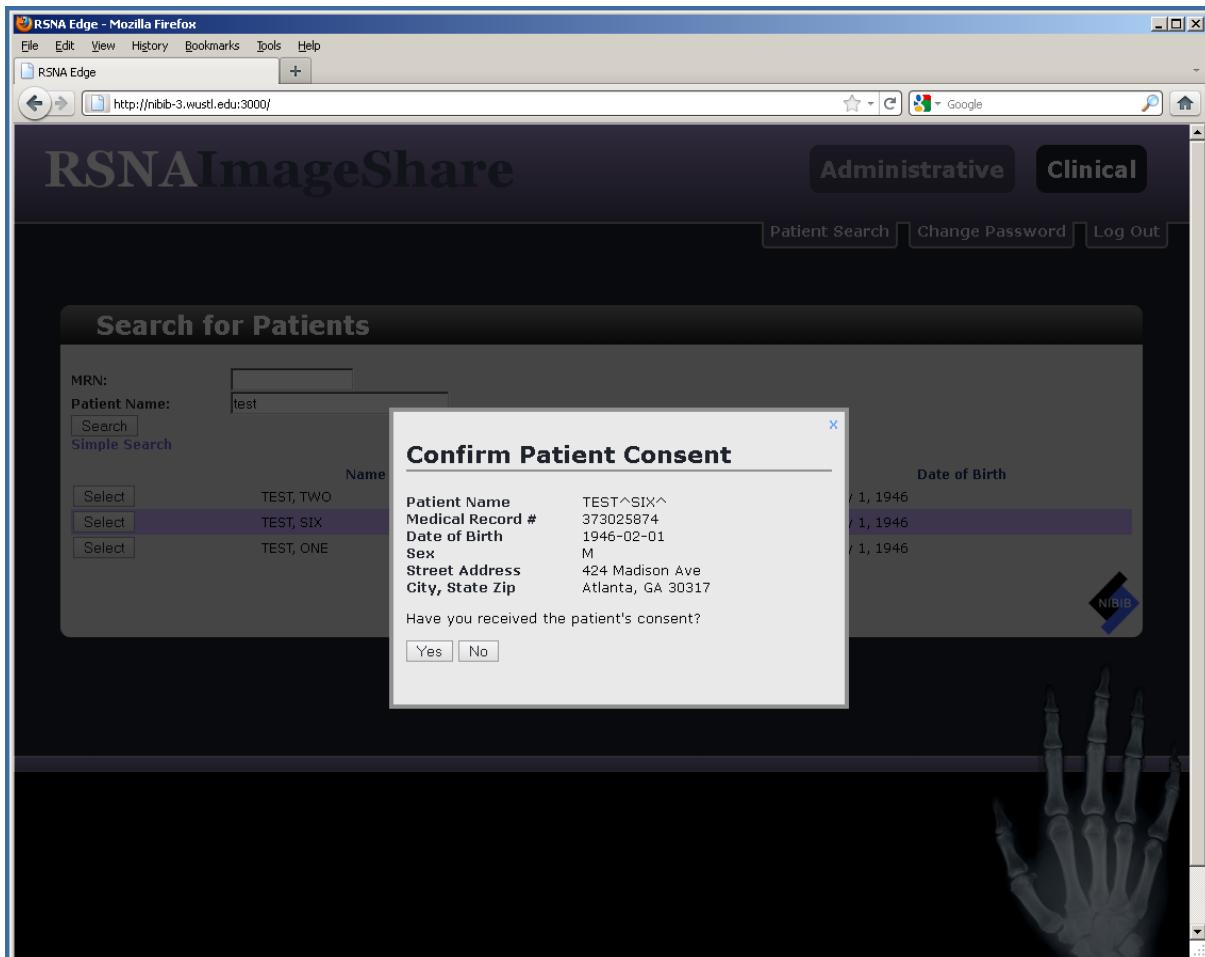


Figure 6-13: Patient Confirmation and Consent Acknowledgment

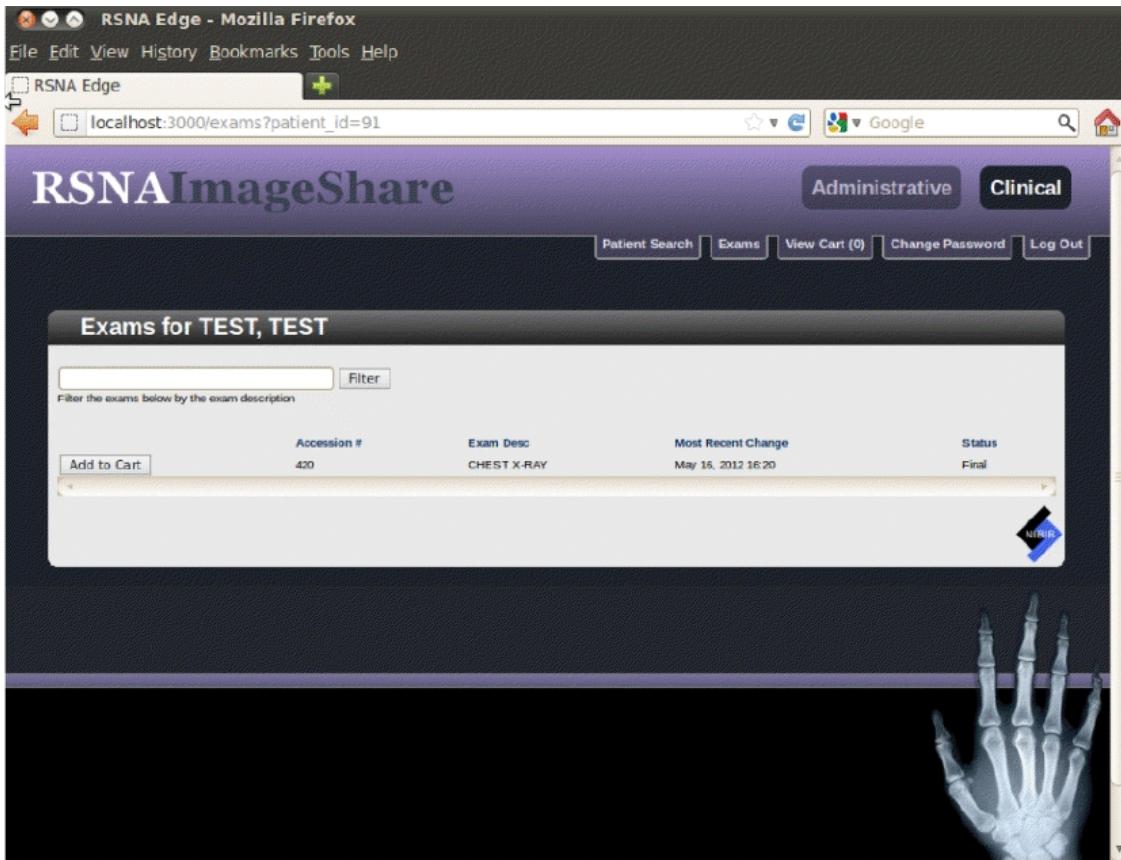


Figure 6-14: Exam Selection

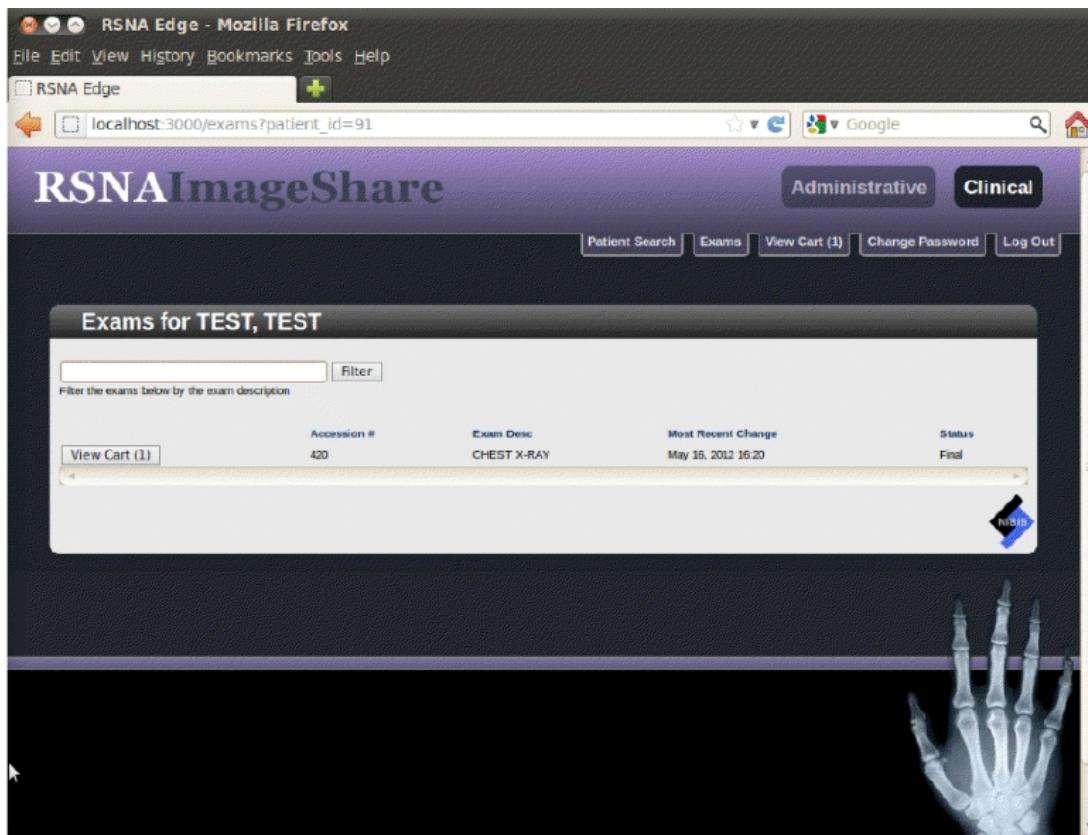


Figure 6-15: Selected Exams in the Cart

Clicking the “Send Cart” button will prompt for creation of an RSNA ID. After creation, the job is put in the queue and the user is prompted to print the RSNA ID for the patient. **Please note that pop-up blockers are popular in modern browsers and an exception will need to be made to allow the PDF printout to appear.**

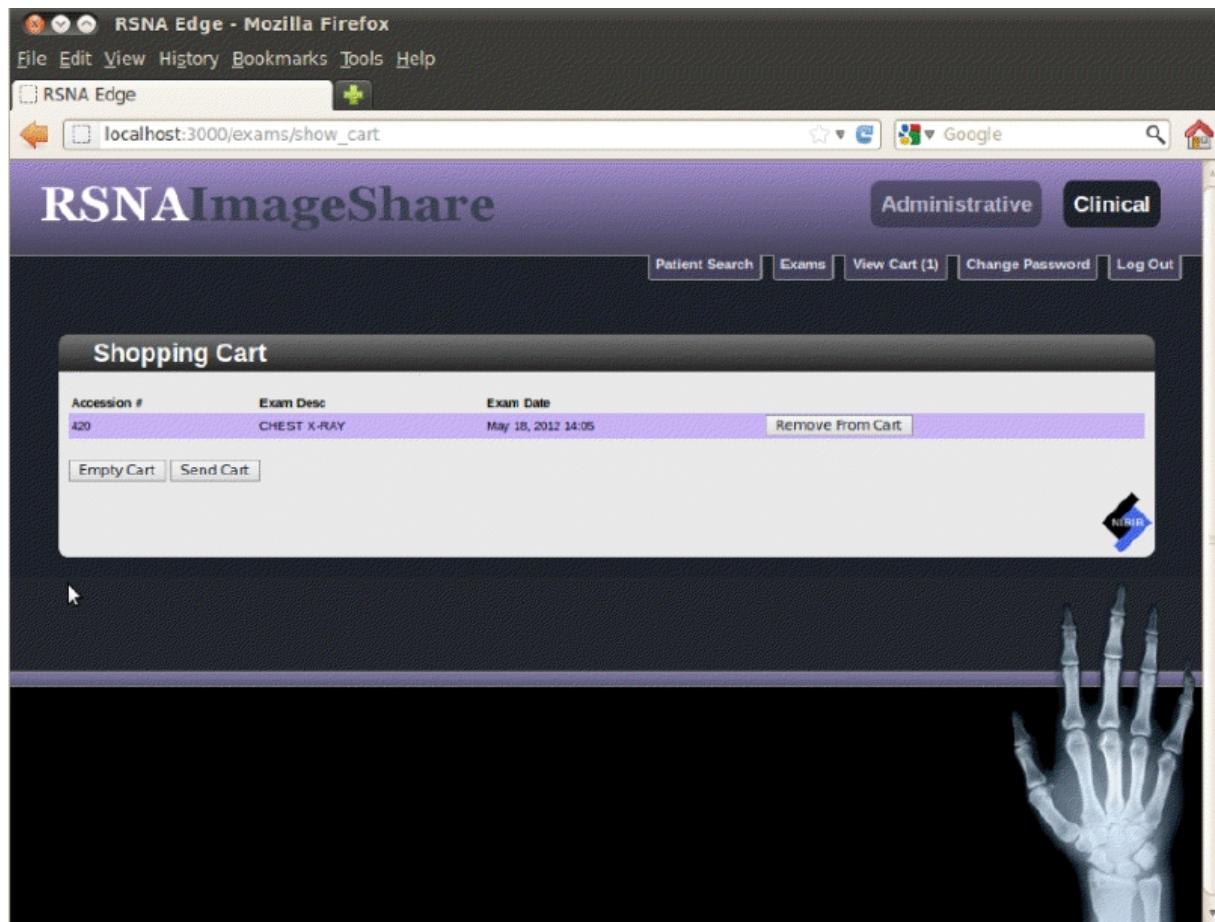


Figure 6-16: Sending Cart

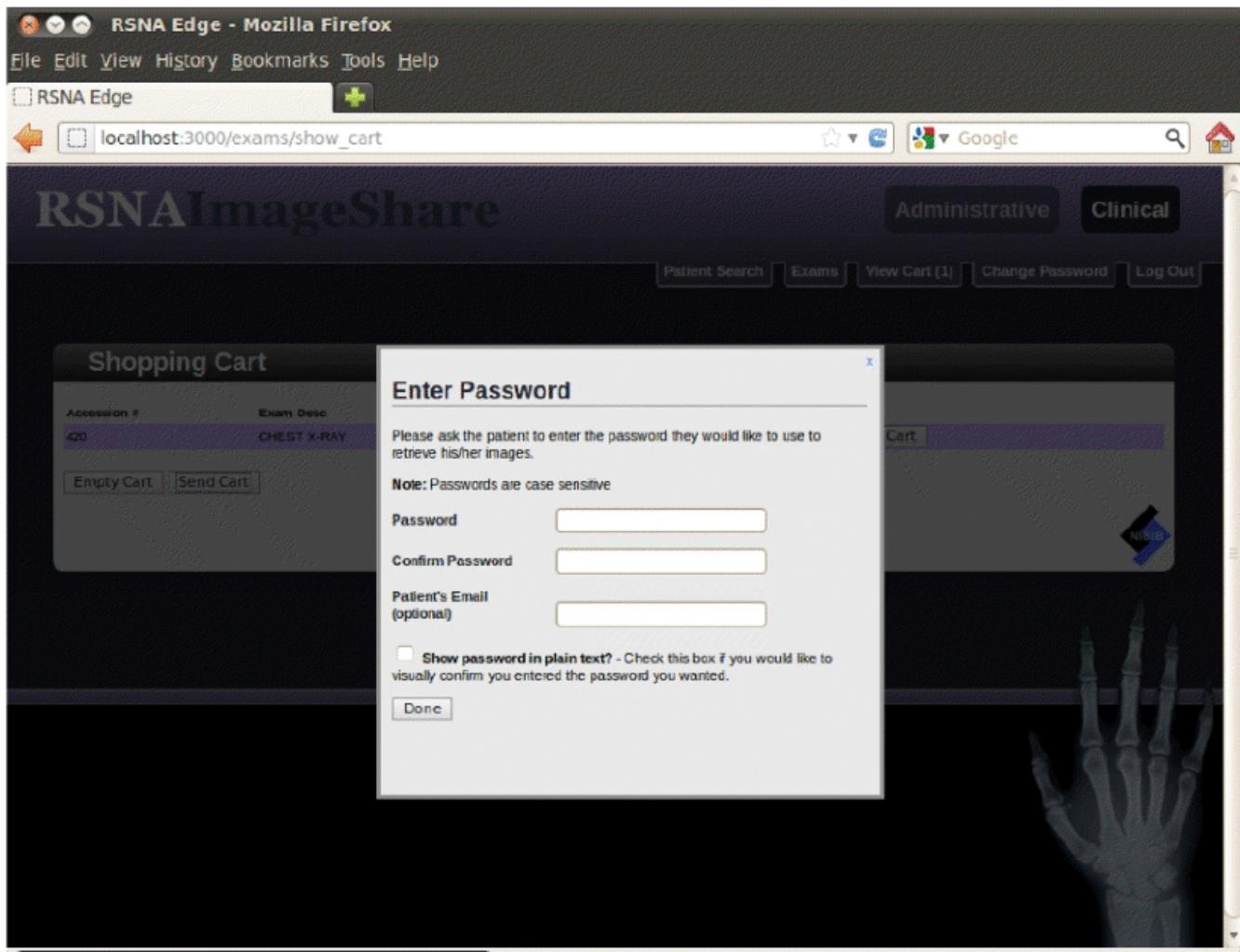


Figure 6-17: Creating the RSNA ID

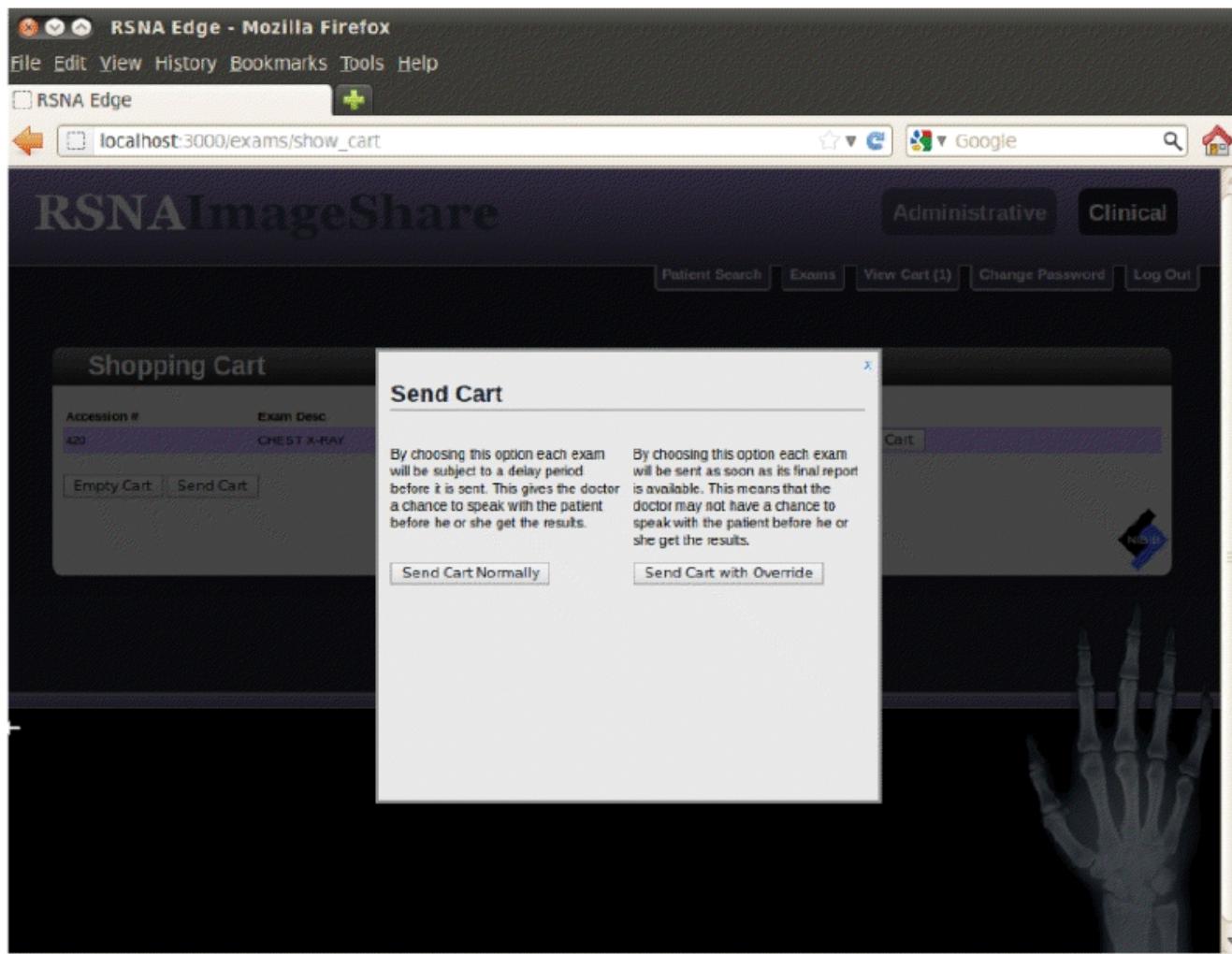


Figure 6-18: Option to override send delay

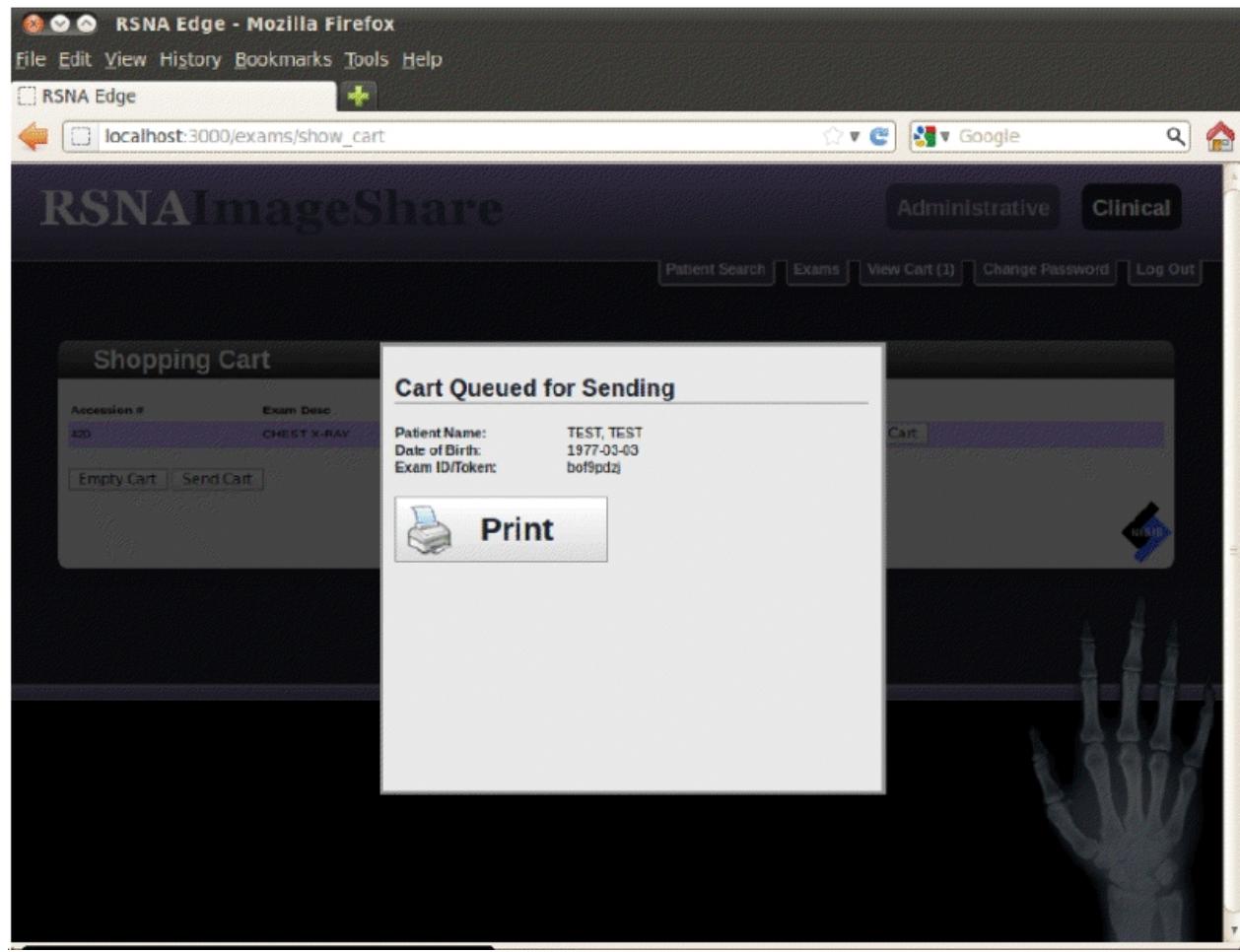


Figure 6-19: Exam Queued to be Sent, Print Dialog Prompt for RSNA ID

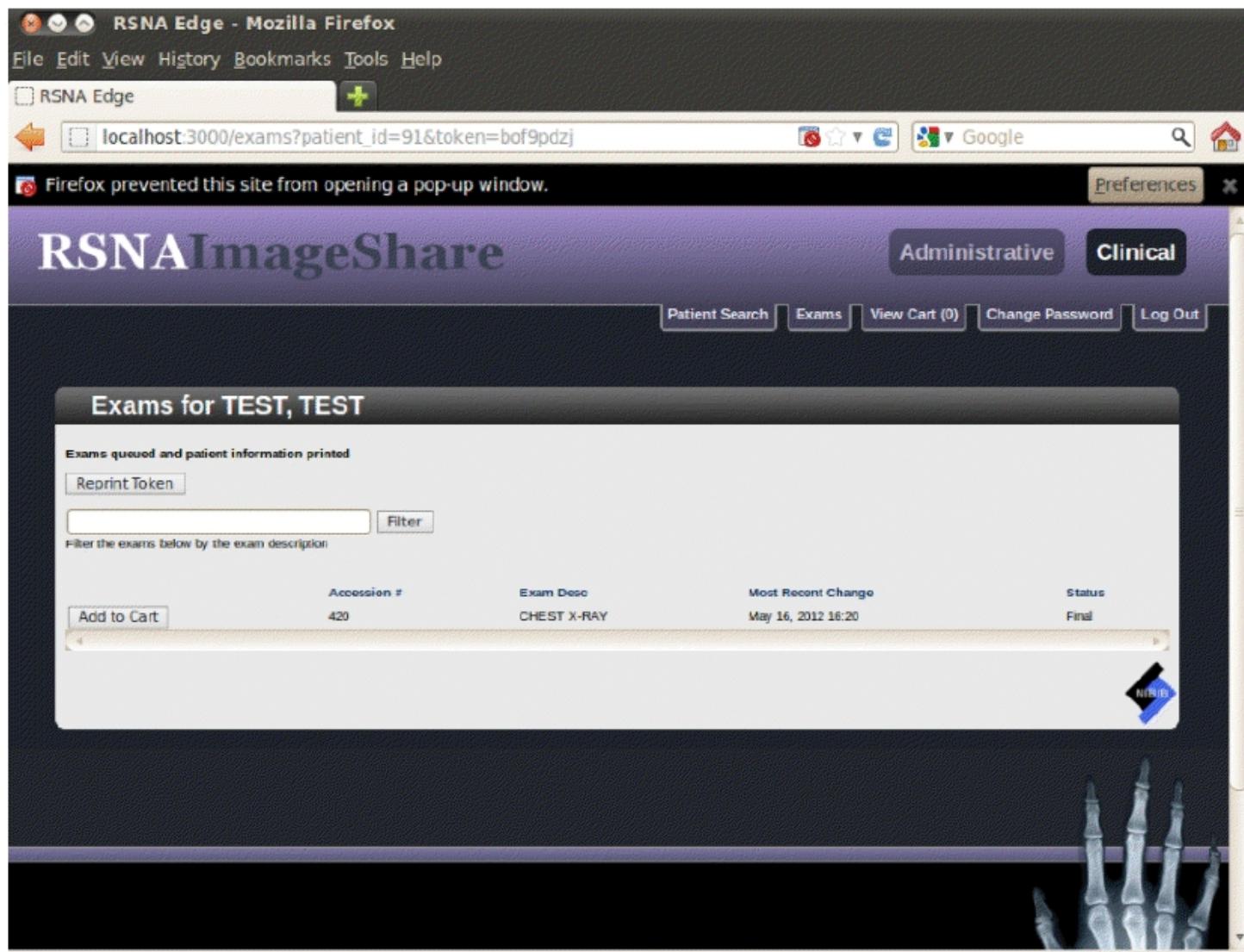


Figure 6-20: Pop-up blockers will prevent the RSNA ID from printing

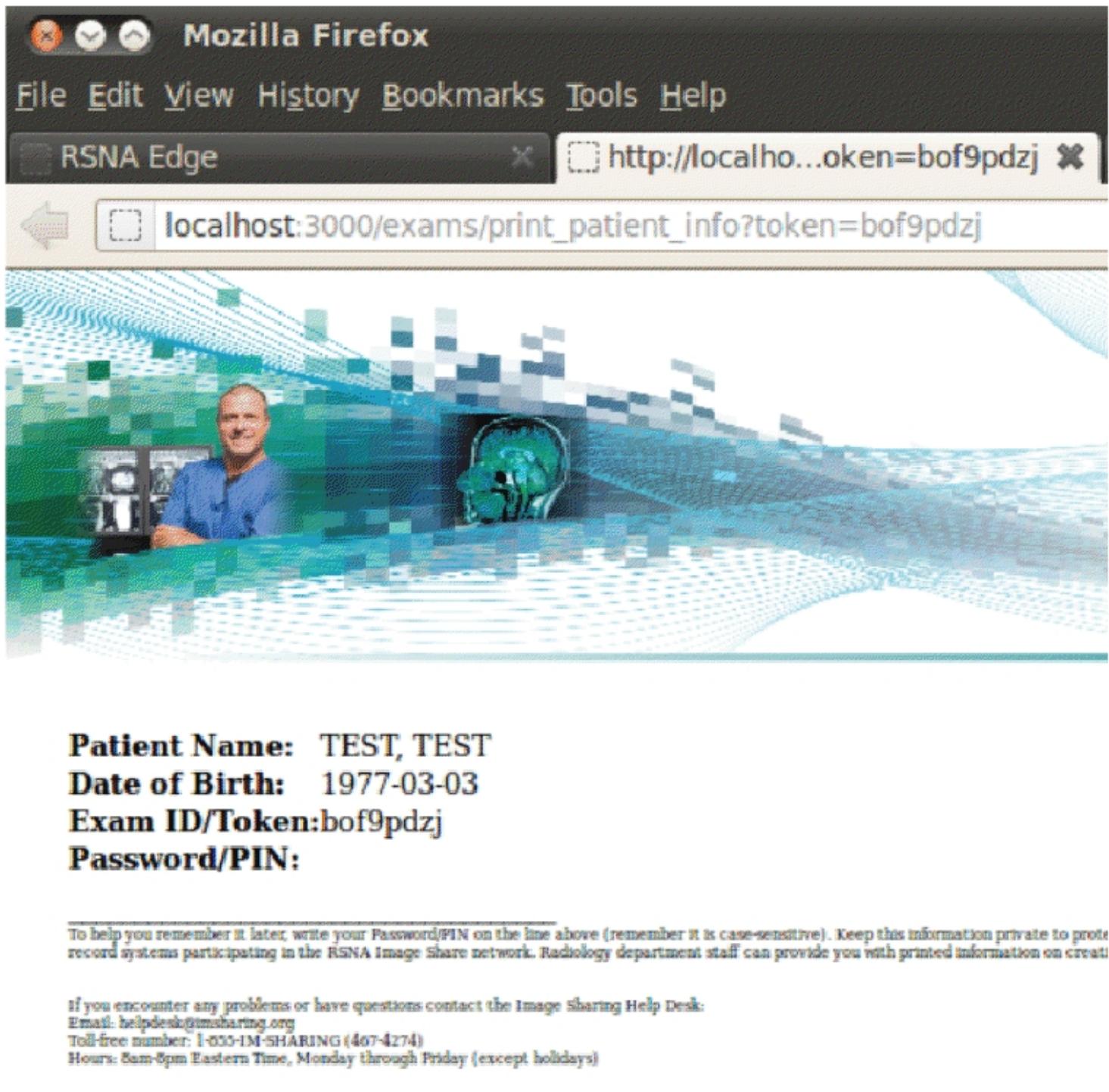


Figure 6-21: Sample RSNA ID PDF print out

7. Retrieve Content Application

Version 2.1 of the RSNA Edge Server adds a new component to enable retrieval of studies that have been previously sent to the RSNA Clearing House [<https://clearinghouse.lifeimage.com>], enabling transfer of cases from site to site without going through a patient's Personal Health Record account. This uses the same security model as the PHR—that is the patient must provide the same security token and password at a participating site to enable this transfer. This chapter covers this new component.

7.1 Installation:

Note: This section assumes a clean V2.1 install, if you are upgrading from V2.0 refer to Appendix C, and then skip to 7.2 for usage instructions.

7.1.1 Edge Server:

If you are running the Retrieve Content application from a V2.1 Edge Server, the application should already be installed under \$RSNA_ROOT folder.

7.1.2 Installing to Another Machine (Microsoft Windows):

Log in to the Edge Server web application (see Chapter 6) using the administrator account and go to Administration Tool. Click on the tab labeled “Retrieve Content Application.” The page will show a link to download two files: retrieve-content.zip and keystore.jks.

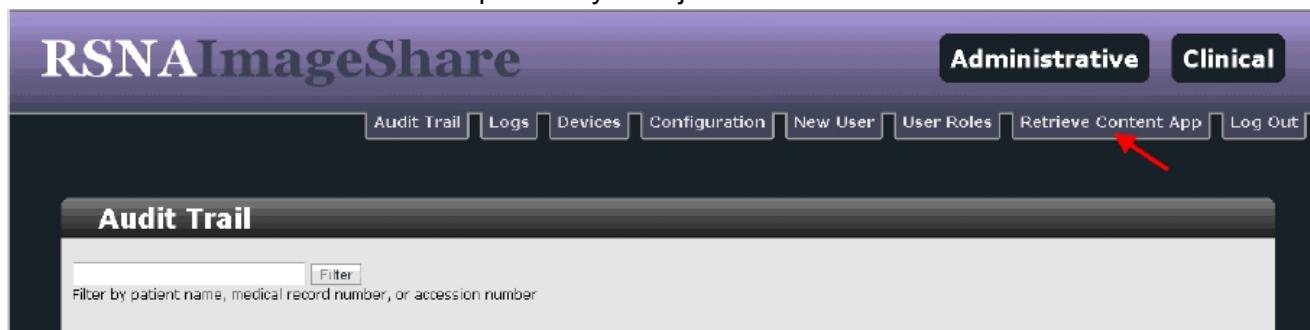


Figure 7-1: Retrieve Content App Tab

Download and unzip retrieve-content.zip, it contains:

- retrieve-content-2.1.1.jar
- folder “conf” which contains retrieve-log4j.properties and retrieve-content.properties with application configuration settings
- folder “ext” which contains jar dependencies
- start.bat

Download keystore.jks and truststore.jks to folder “conf”.

To run Retrieve Content app on Windows, simply double click on start.bat, you will see the screens depicted in section 7.2. [Note: This assumes that there is a recent (> V1.6) version of the Java Runtime environment on the Windows PC] The Application log file will be in logs folder. Retrieved exams will be found in images folder.

7.2 Running on Edge Server:

You will start the RetrieveContent application from a terminal. You will need to be in the folder where the jar file exists to reference properties files. You also need to make sure you and others can share folders. As

user "rsna" use these commands:

```
> cd $RSNA_ROOT  
> umask 0  
> java -Xmx1024M -jar retrieve-content-2.1.1.jar
```

Application log file can be found in \$RSNA_ROOT/logs/retrieve-content.log. This log file will keep growing, so we suggest user to backup by changing the file name to retrieve-content-YYYY-MM.log every month or more frequently according to the file growth. Application will automatically create a new log after the name change.

7.2.1 Start RetrieveContent application:

When the application starts, it displays the Retrieve Studies window:

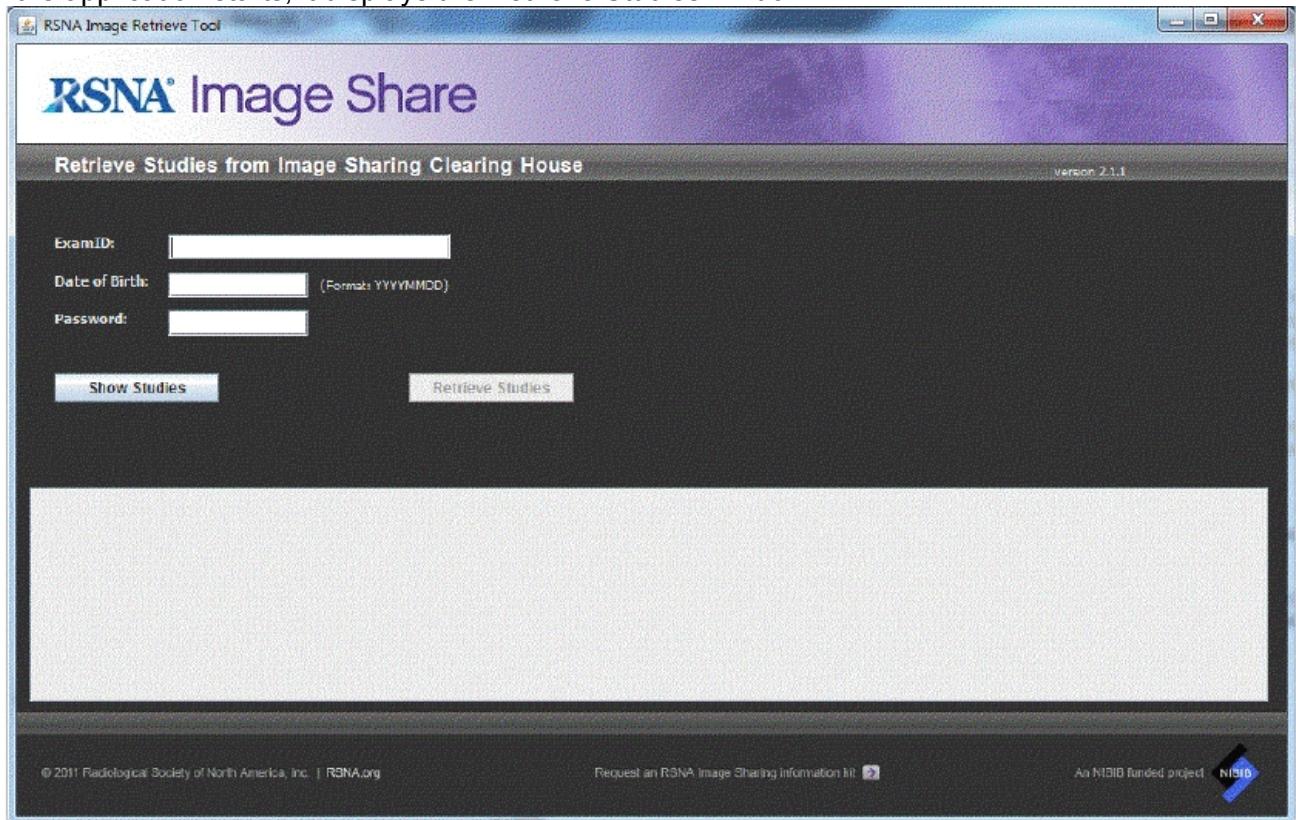


Figure 7-2: Retrieve Studies Window

7.2.2 Search Studies:

After the user inputs the retrieve criteria (the once used patient's ID hash that was written on the paper form created by the Edge Server job creation GUI) and clicks the Show Studies button, the tool will get the KOS and report files from Clearing House and save the retrieved document sets into \$RSNA_ROOT/images folder. You'll notice a subfolder with patient name was created under that folder.

If there are any reports, they will be saved in \$RSNA_ROOT/images/[patient name]/StudyDesc-StudyDate-StudyUID/other/

Note: at this point the DICOM images have not yet been retrieved.

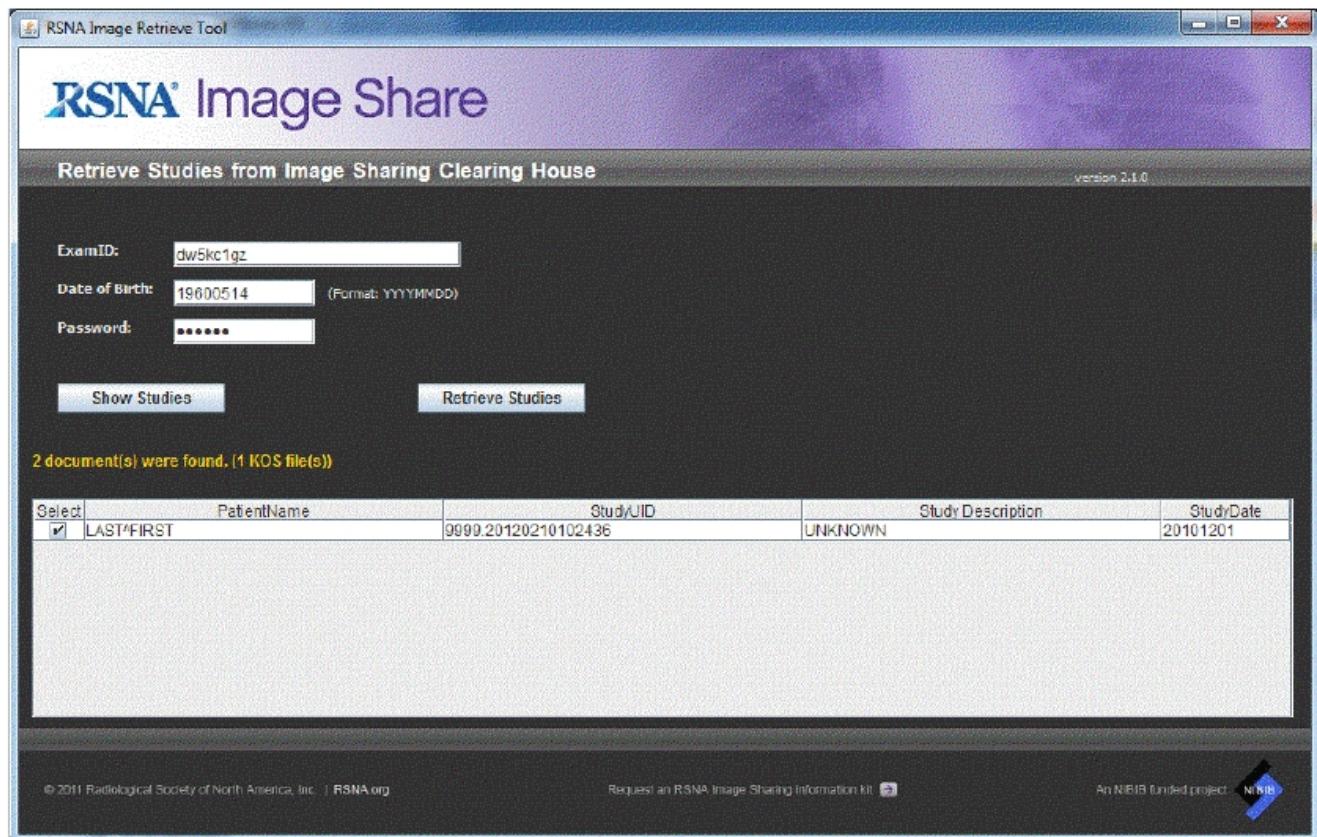


Figure 7-3: Retrieve Studies Search Results

7.2.3 Retrieve Studies:

The user then selects the needed studies and clicks Retrieve Study button. The site can customize the number of images per request in \$RSNA_ROOT/conf/retrieve-content.properties to adjust memory usage. (Tool needs to be restarted to apply this change).

Once images are retrieved, they will be saved in \$RSNA_ROOT/images/[patient name]/StudyDesc-StudyDate-StudyUID where the StudyUID(s) are the folders corresponding to the studies downloaded for that patient.

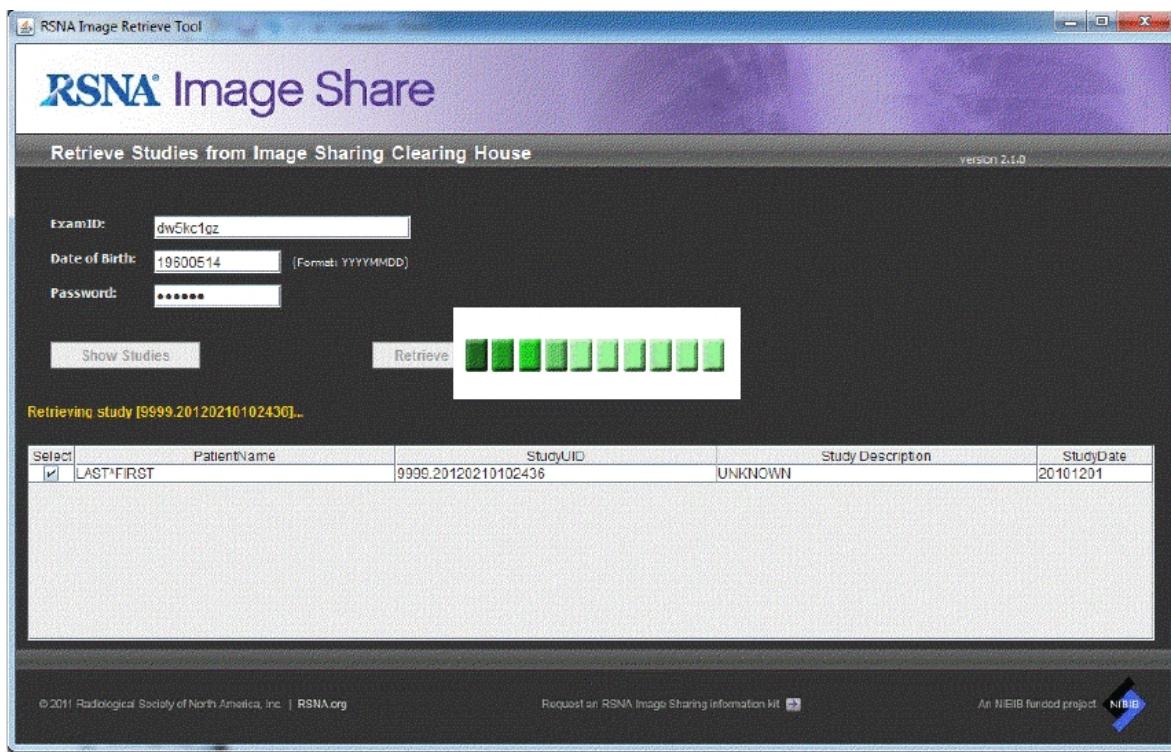


Figure 7-4: Retrieve Studies in Progress

8. Maintenance

8.1 Backups:

There are multiple levels of backups. The entire system (i.e. system level backups) or just sub-components (i.e. the MIRTH configuration and database). Taking each in turn:

8.1.1 System:

the site can always use any standard backup tools they normally have. Or if there is no preference an excellent free choice is CloneZilla at <http://clonezilla.org/>

8.1.2 MIRTH:

To backup Mirth you will need to backup both the Mirth database in PostgreSQL as well as the Mirth installation. To backup the Mirth database, open a command shell within Ubuntu and make a dump of the database by typing the following (these commands will prompt for the mirth database password):

```
pg_dump -h 127.0.0.1 -U mirth -W -C -f mirthdb.sql mirthdb
```

Note: the above syntax creates a .sql file that contains both the database schema and the data. The -C option assures that the .sql file can recreate the named database (as long as a placeholder of the same name exists on PostgreSQL). If one desires only the schema and no data (yet still have creation ability) one can use:

```
pg_dump -h 127.0.0.1 -U mirth -W -C -s -f mirthdb.sql mirthdb
```

To restore the Mirth database to PostgreSQL use the following command:

```
psql -h 127.0.0.1 -U mirth -W -d mirthdb < mirthdb.sql
```

Note: the above command will recreate the named database as long as the database name exists in PostgreSQL (owner Edge)

To backup the Mirth installation, you will need to make a copy of the following directory:

```
/usr/local/edgeserver-1.0-SNAPSHOT/mirth
```

8.1.2 RSNA Database:

Within Ubuntu open a command shell. To make a dump of the RSNA database in PostgreSQL type (this command will prompt for the edge database password):

```
> pg_dump -h 127.0.0.1 -U edge -W -C -f rsnadb.sql rsnadb
```

To restore the rsnadb to PostgreSQL use

```
> psql -h 127.0.0.1 -U edge -W -d rsnadb < rsnadb.sql
```

8.2 Update/Upgrade

Not applicable to this release.

8.3 Help Desk:

If at any time you need assistance with the RSNA Edge Server feel free to email helpdesk@imgsharing.org or call 1-855-IM-SHARING (467-4274).

If you would like to escalate support you may also call (203) 981-0195

Appendix A. Edge Server Error Codes

The following errors are reported by the RSNA Edge-Server software.

Code	Description	Explanation
-20	Failed to prepare content	Indicates a general error with retrieving images and/or reports. Consult the associated comments (in the job details dialog, see Figure 6-8: Audit Trail Interface) for specific error information.
-21	Unable to find images	Indicates the Edge Server was unable to find any images under the job's MRN/acc # combo. Verify that the MRN/acc # combo is correct and that all remote PACS are configured in the devices table (see Figure 6.6)
-23	DICOM C-MOVE failed	Indicates an error with the C-MOVE operation used to retrieve a job's images. Possible causes include network or protocol errors. Consult the associated comments (in the job details dialog, see Figure 6-8: Audit Trail Interface) for specific error information.
-30	Failed to transfer to clearinghouse	Indicates a general error with a job's submission to the clearinghouse. Consult the associated comments (in the job details dialog) for specific error information.
-32	Failed to generate KOS	Indicates an error within the KOS generation process. Possible causes include invalid DICOM objects and disk errors. Consult the associated comments (in the job details dialog, see Figure 6-8: Audit Trail Interface) for specific error information.
-33	Failed to register patient with clearinghouse.	Indicates an error within the ITI-8 transaction with the clearinghouse. Consult the associated comments (in the job details dialog) for specific error information. For assistance with diagnosing the cause, please contact David Wilkins (dwilkins@lifeimage.com)
-34	Failed to submit documents to clearinghouse	Indicates an error within the ITI-41 transaction with the clearinghouse. Consult the associated error comment and Appendix B for more information. For assistance with diagnosing the cause, please contact David Wilkins (dwilkins@lifeimage.com)

Appendix B. Clearinghouse Error Codes

The following codes are reported by the clearinghouse when there is an error with the ITI-41 transaction. For assistance with diagnosing the cause, please contact David Wilkins (dwilkins@lifeimage.com).

1. Registry Error Codes

Code	Description
E01000001	The XDS Registry does not support action or transaction
E01000002	The Patient Global ID cannot be found in the XDS Metadata.
E01000003	The Patient Global ID is not registered in XDS registry.
E01000004	Database access error
E01000005	The slot parameter of this method must not be null.
E01000006	The ValueList of slot must not be null.
E01000007	The Values of slot must not be null.
E01000008	The ValueList size must not be zero
E01000009	The StoredQuery with multiple parameters must start with "(" and end with ")" .
E01000010	The StoredQuery with string parameters must start with ' and end with ' .
E01000011	The StoredQuery parameter of type "string" must start with the '!
E01000012	The StoredQuery parameter of type "string" must end with the '!
E01000013	The StoredQuery Slot valueList must not be null.
E01000014	The StoredQuery Slot valueList values must not be null.
E01000015	The StoredQuery Slot valueList values must not be null.
E01000016	The AdhocQueryRequest must not be NULL.
E01000017	The AdhocQuery element of the AdhocQueryRequest must not be NULL.
E01000018	The ID attribute of the AdhocQuery element must not be NULL.
E01000020	The DocumentEntry metadata should not be null.
E01000021	This ExtrinsicObjectType provided in the metadata is not identified to DocumentEntry
E01000022	The ExtrinsicObject ID must not be null.
E01000023	The ExtrinsicObject status must not be null.
E01000024	The DocumentEntry must be of a valid ExtrinsicObject type.
E01000025	The docData of DocumentEntryExtractor must not be null.
E01000026	If authorPerson Info is provided then the value should not be null.
E01000027	If authorPerson Info is provided then there should only be one attribute value.
E01000028	The Slot name should not be null.
E01000029	The Slot name should not be blank.
E01000030	The creationTime Slot ValueList should not be null.
E01000031	The creationTime Slot Value Elements should not be null.
E01000032	The creationTime Slot Value Elements must not be less than one value.
E01000033	The creationTime Slot Value Elements must not be more than one value.
E01000034	The creationTime Slot Value must not be the right format.
E01000035	The serviceStartTime Slot ValueList should not be null.
E01000036	The serviceStartTime Slot Value Elements should not be null.
E01000037	The serviceStartTime Slot Value Elements must not be less than one value.
E01000038	The serviceStartTime Slot Value Elements must not be more than one value.

E01000039	The serviceStartTime Slot Value must not be the right format.
E01000040	The serviceStopTime Slot ValueList should not be null.
E01000041	The serviceStopTime Slot Value Elements should not be null.
E01000042	The serviceStopTime Slot Value Elements must not be less than one value.
E01000043	The serviceStopTime Slot Value Elements must not be more than one value.
E01000044	The serviceStopTime Slot Value must not be the right format.
E01000045	The sourcePatientInfo Slot ValueList should not be null.
E01000046	The sourcePatientInfo Slot Value Elements should not be null.
E01000047	The metadata of document entry must not be null.
E01000048	The Folder metadata should not be null.
E01000049	The Folder status should not be null.
E01000050	The registryObject is not identified to the folder
E01000051	The Folder metadata must not be null.
E01000052	The SubmitObjectsRequest to extractMetadata must not be null.
E01000053	Submit objects list must not be null.
E01000055	The ObjectType Attribute of the ExtrinsicObjectType should not be null.
E01000057	The Patient Global Id is not consistent in the Submit metadata.
E01000058	The ObjectType Attribute of the ExtrinsicObjectType should be the correct value
E01000059	The ID Attribute of the RegistryPackageType should not be null.
E01000060	The XDS.b Registry does not support the ObjectType in the SubmitObjectsRequest.
E01000061	The Classification object must be provided to classify the SubmissionSet
E01000063	The Classification object must be provided to classify the Folder
E01000065	The patient info must be provided in the Metadata.
E01000066	The Patient Global ID is not provided
E01000067	This RegistryPackageType should not be null.
E01000068	The SubmissionSet ID should not be null.
E01000069	The SubmissionSet status should not be null.
E01000070	This object is not a RegistryPackageType.
E01000071	The submissionset metadata must not be null.
E01000072	The submissionTime Slot ValueList should not be null.
E01000073	The submissionTime Slot Value Elements should not be null.
E01000074	There must be at least one value in the submissionTime Slot Value Elements
E01000077	The submissionTime Slot Value is the incorrect format
E01000078	The metadata for the submissionset does not comply with the IHE xds.b profile.
E01000079	The old Patient ID must not be null.
E01000080	The new Patient ID must not be null.
E01000081	The existing Patient ID not exist when updating the Patient ID
E01000082	An exception when fetching the new Patient ID from ResultSet encounter
E01000083	An exception when querying for the new Patient ID
E01000086	The old Patient ID not exist.
E01000105	The UUID is unknown

2. Repository Error Codes

Code	Description
E02000003	Submission set meta data is incorrect.

E02000004	The SubmissionSet UniqueId is not provided
E02000005	The DocumentEntry UniqueId is not provided
E02000006	The Folder UniqueId is not unique!
E02000007	Database Connection Encounter Error – When submitting documents.
E02000010	Database Connection Encounter Error – When fetching the repository UniqueId
E02000013	Database Connection Encounter Error – When fetching document content from the database
E02000014	Database Connection Encounter Error – When fetching documents
E02000015	The DocumentEntry metadata is null.
E02000016	This ExtrinsicObjectType is not a valid DocumentEntry.
E02000017	The ExtrinsicObject ID is null.
E02000018	The ExtrinsicObject type is null.
E02000019	This RegistryPackageType is null.
E02000020	The SubmissionSet ID is null.
E02000021	SubmitObjectsRequest in ProvideAndRegisterDocumentSetRequest is null
E02000022	The Document Element SubmitObjectsRequest in ProvideAndRegisterDocumentSetRequest is null.
E02000024	RegistryObjectList in SubmitObjectsRequest is null
E02000025	The Document Element RegistryObjectList in SubmitObjectsRequest is null.

Appendix C: Upgrading from Version 2.0 to 2.1

Assumptions: There is an upgrade script that automates

- a) updating the send_content and prep_content apps
- b) updating the Web GUI
- c) updating the retrieve_content app
- d) updates the database non-destructively with new features and indices

If you are reading this it is assumed you have a running 2.0 system. The instructions here are to use the installer to upgrade your current installation.

After completing the following steps, you may jump back to Chapters 6 and 7 to learn about the new features in this release. Note to RSNA FTP users: The RSNA ftp server is based on Microsoft. You must force the transfer to be binary, else the .zip files will be corrupt.

a) Database backup

Best practices for any update include backing up existing data. Use the procedures defined in Section 8 to backup both the rsnadb and the mirthdb. Copy the backup files to a separate server. That data will contain PHI, so use appropriate procedures per your institution.

b) Updating Mirth

As part of the V2.1 upgrade, the DICOM SCP functionality has been merged into the prep-content app. As a result the Mirth DICOM channel is no longer needed and must be disabled. The instructions for doing so are as follows:

1. Login to Mirth (see Chapter 5)
2. Once in Mirth, switch to the Dashboard panel (see Figure 5-3)
3. Right click on the dashboard and select “Stop All Channels” from the context menu
4. Once stopped, switch to the Channels panel (see Figure 5-6)
5. Right click on the “RSNA Edge Server DICOM SCP” channel and select “Disable Channel” from the context menu
6. Once disabled, right click anywhere on the panel and select “Deploy All”
7. You’ll be automatically switched to the Dashboard where you should see only the “Edge Server HL7 Receiver” channel running.

c) Updating prep-content app

As part of the V2.1 upgrade, the DICOM SCP functionality has been merged into the prep-content app. As a result you will need to verify the SCP configuration using the instructions listed in the DICOM Configuration section of Chapter 6.

d) Upgrade Procedure

Obtain the installer software from the RSNA GitHub site:

<https://github.com/RSNA/Image-Sharing-Network-Edge-Server/downloads/edgeserver-2.1.0-standard.zip>

Within the above zip file are several files:

- a) an installer ending in .zip
- b) an MD5 hash of the above ending in .md5
- c) hash-checkers for both Windows and Linux (and a support file for the Windows version)

d) this Manual

To validate the installer has been downloaded without error, you may run the proper hash-checker for the operating system you are on, and it will validate if download's hash agrees with the published value.

When running the installer, you will be asked for configuration information you used during your previous installation.

Database Superuser Password: The password you entered for postgres above

Password for RSNA Database user: Choose a (different) secure value for this user account

For example: d17bK4#M

Make sure that JAVA_HOME points to the installation folder of the Java JRE. Open a terminal emulator, change to the folder that contains the downloaded zip file and extract it. Change to the extracted directory and run the shell script:

```
$ unzip edgeserver-2.1.0-standard.zip  
$ cd edgeserver-2.1.0  
$ sh ./install.sh
```

You are asked if you are upgrading from a previous version (Figure AC-1):

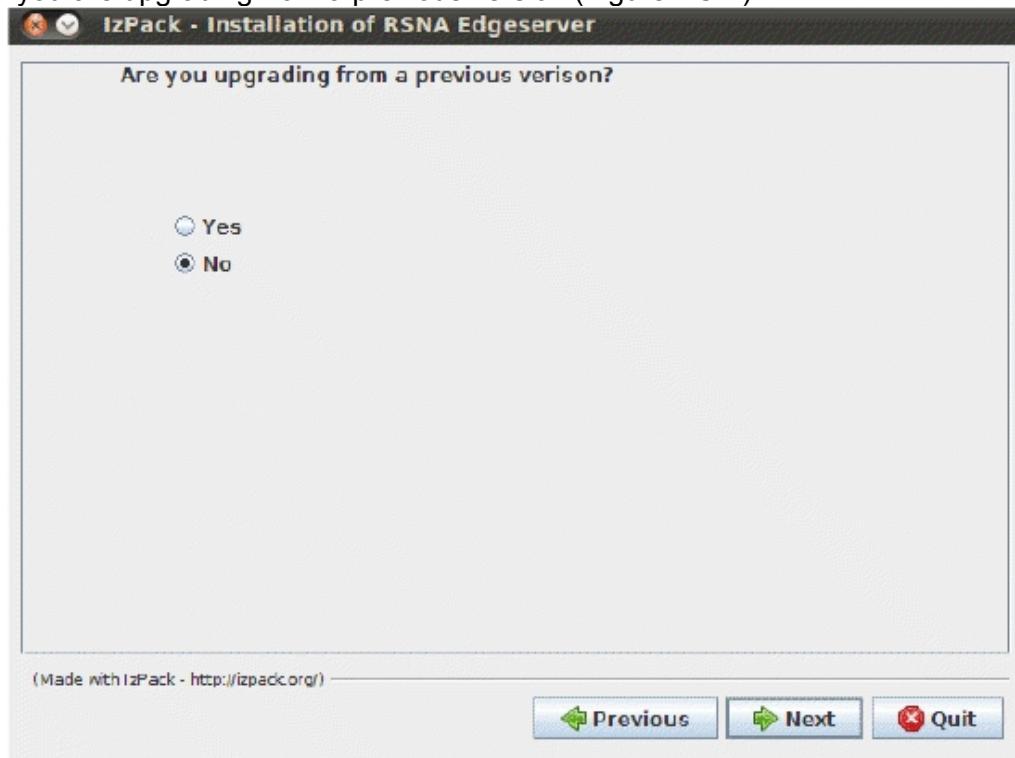


Figure AC-1: Upgrade Query Screen

Next you are prompted to select the installation path for the software (Figure AC-2)

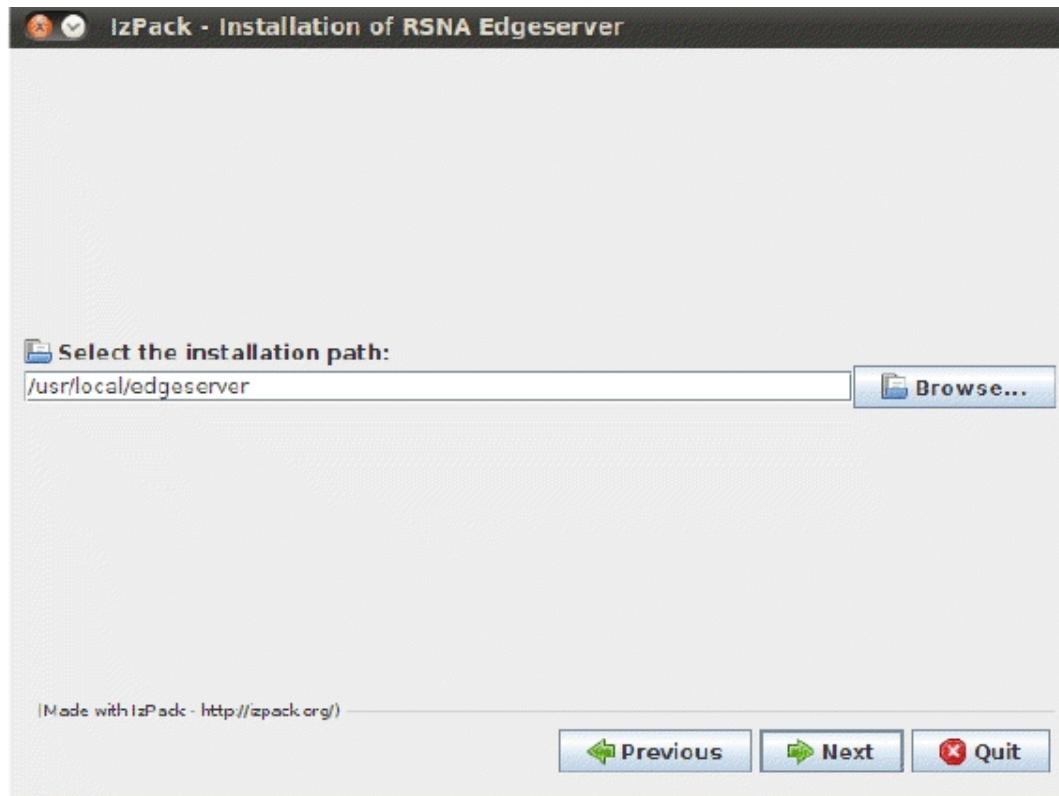


Figure AC-2: Installation Path

A pop-up will appear alerting you that you are overwriting the directory. Click “yes” to continue with install (Figure AC-3).



Figure AC-3: Overwrite Directory

Figure AC-4 shows the component selection window. For the 2.1 upgrade, the software removes the options to install Mirth and generate a client certificate. Leave each of the remaining components selected as shown in Figure AC-4.

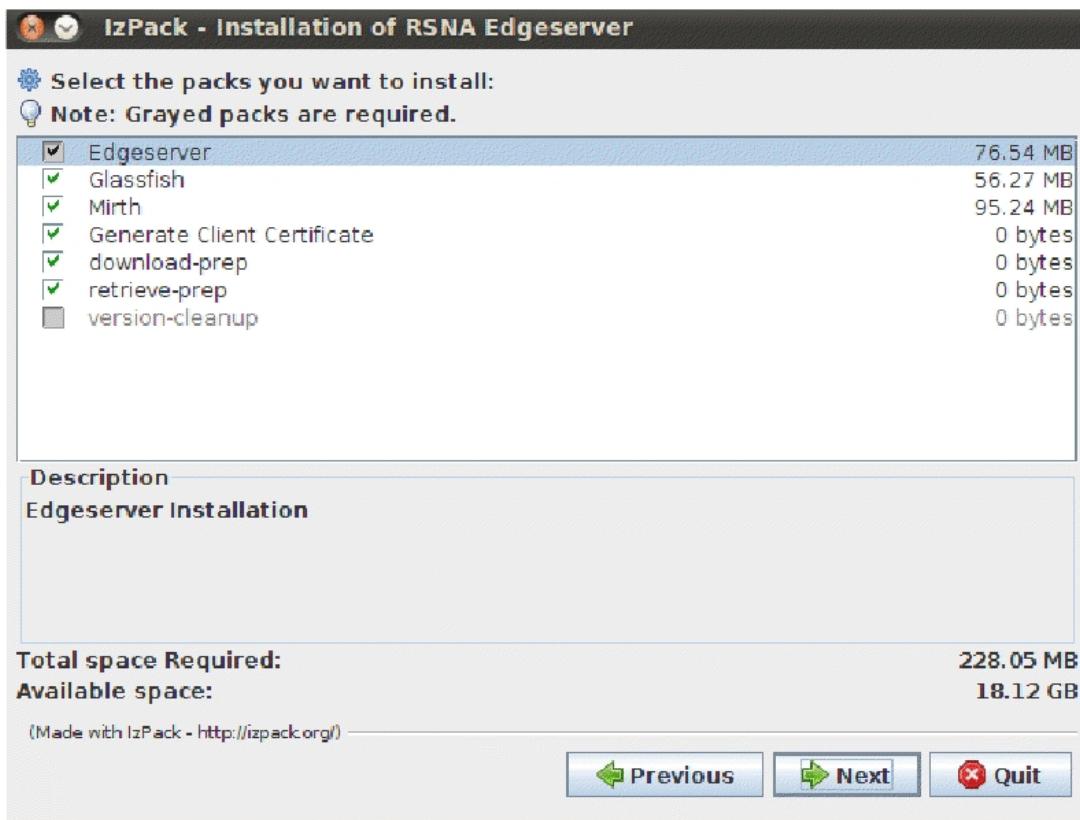


Figure AC-4: Component Selection

Figure AC-5 shows the next screen which is used to configure the database connection. You will enter the passwords that you are currently using for the Database Superuser (postgres account) and the RSNA Database user (edge account). These are the passwords you entered during your initial installation.

The screenshot shows the 'IzPack - Installation of RSNA Edgeserver' window with the title 'Configure database connection'. It contains fields for database connection settings:

Setting	Value
Host:	localhost
Port:	5432
Database Superuser Name:	postgres
Database Superuser Password:	[Redacted]
Password for RSNA Database user:	[Redacted]

(Made with IzPack - <http://izpack.org/>)

Buttons at the bottom: Previous, Next, Quit.

Figure AC-5: Upgrade, Database Connection

After you have successfully entered the passwords for the database connection, the installer software will show you the installation path and components you have chosen as shown in Figure AC-6. Select Next to continue.

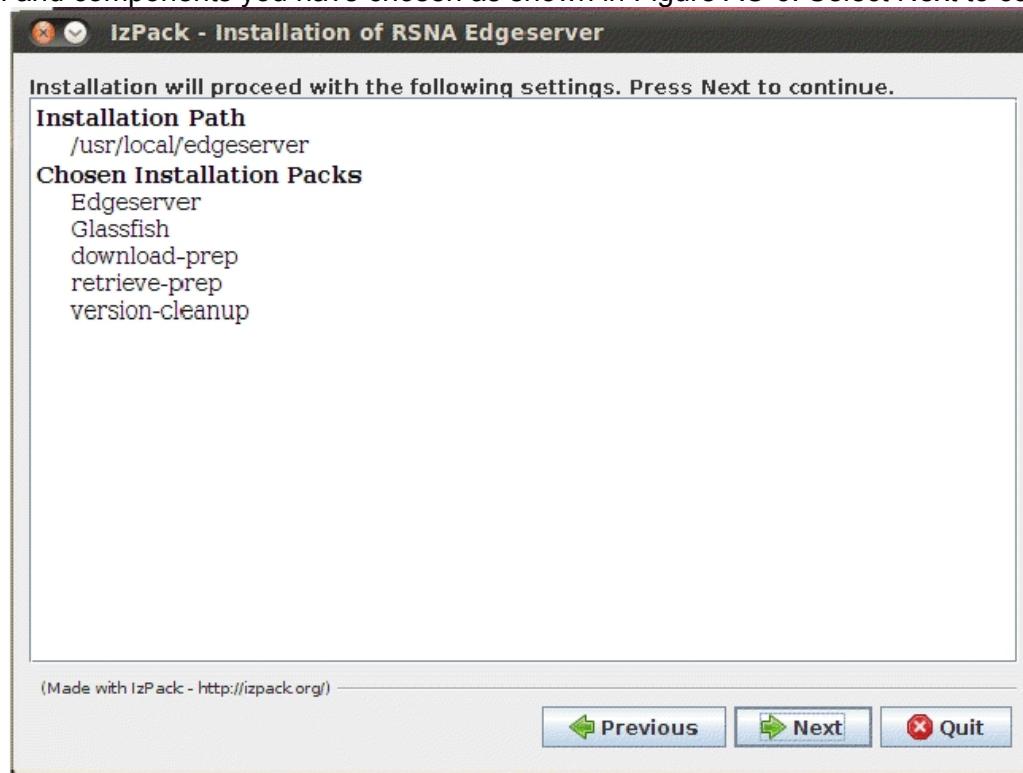


Figure AC-6: Upgrade, Confirmation Screen

The actual installation starts, and the first phase is completed as shown in Figure AC-7.

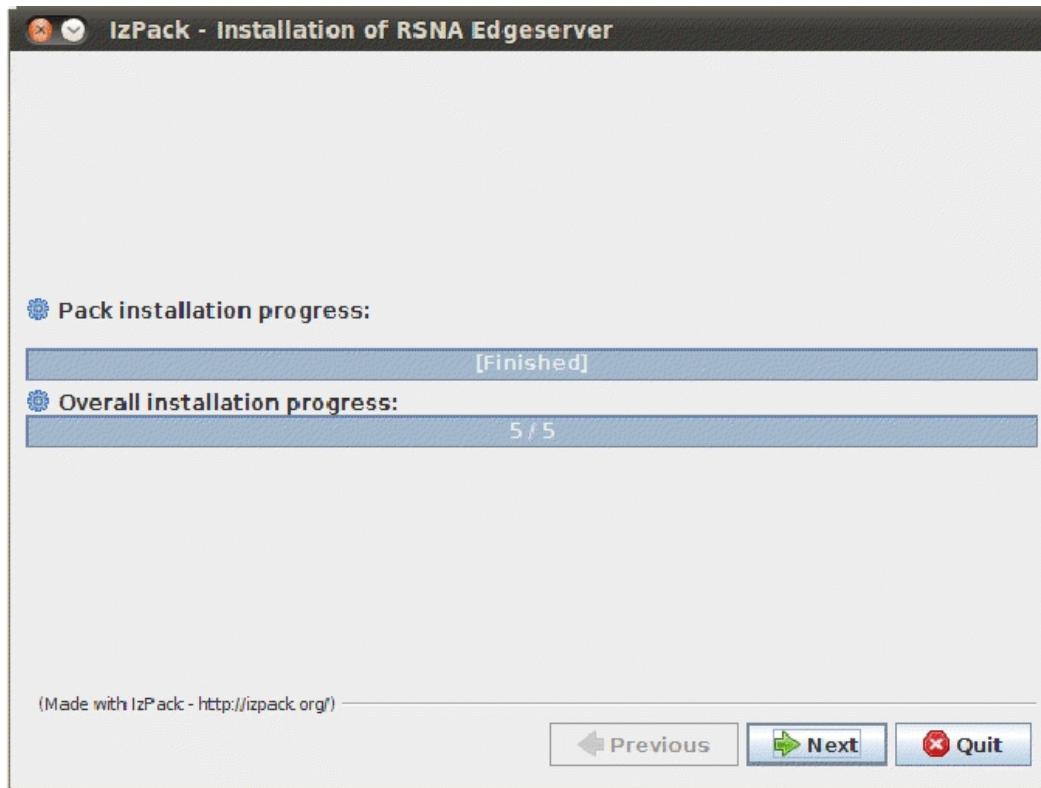


Figure AC-7: Upgrade, Completion One

The next installer screen provides many more details as the installer processes more of the configuration steps (Figure AC-8).

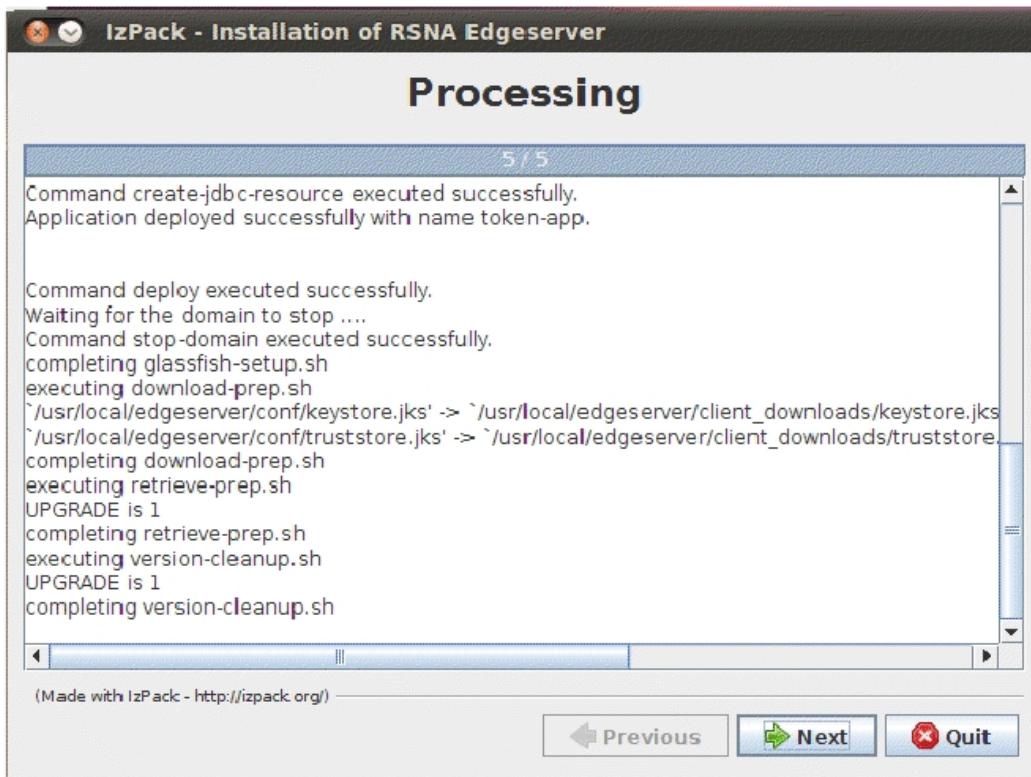


Figure AC-8: Upgrade, Completion Two

Figure AC-9 shows the last screen when the installer has completed. When you select the Done button, the installer will exit. The script that you executed (./install.sh) will restart the Edge Server software.

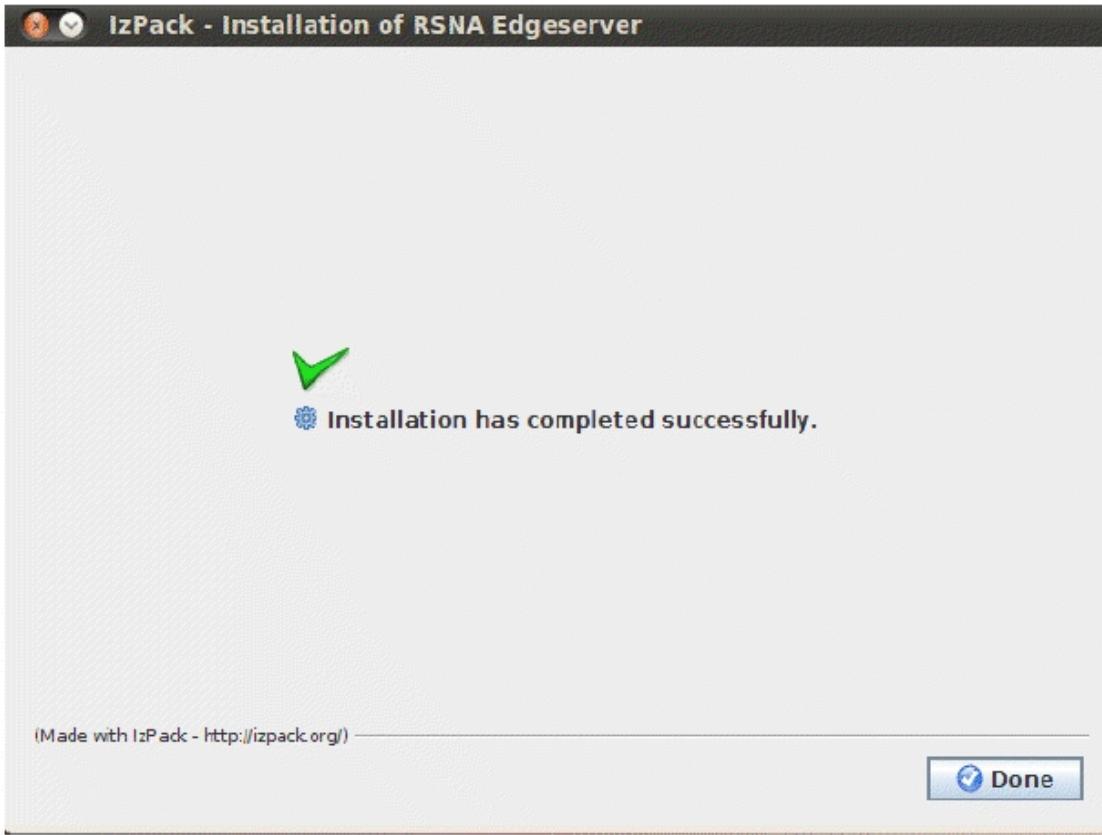


Figure AC-9: Upgrade, Completion Three

Congratulations! Your 2.1 upgrade is complete.

Appendix D: Unix Hints

Unix Shell

This is taken directly from Wikipedia (http://en.wikipedia.org/wiki/Unix_shell). It is a reasonable introduction:

The most generic sense of the term *shell* means any program that users employ to type commands. A shell hides the details of the underlying operating system with the shell interface and manages the technical details of the operating system *kernel* interface, which is the lowest-level, or 'inner-most' component of most operating systems. In Unix-like operating systems users typically have many choices of command-line interpreters for interactive sessions. When a user *logs in* to the system, a shell program is automatically executed. The login shell may be customized for each user. In addition, a user is typically allowed to execute another shell program interactively.

The Unix shell was unusual when it was introduced. It is both an interactive *command language* as well as a *scripting programming language*, and is used by the operating system as the facility to control (*shell script*) the execution of the system. Shells created for other *operating systems* than Unix, often provide similar functionality.

On systems with a *windowing system*, some users may never use the shell directly. On Unix systems, the shell is still the implementation language of system startup scripts, including the program that starts the windowing system, the programs that facilitate access to the *Internet*, and many other essential functions.

Graphical user interfaces for Unix, such as *GNOME*, *KDE*, and *Xfce* are often called *visual* or *graphical* shells.

Root or Administrative Account

Linux (and Unix) systems are designed with an administrative account known as *root*. The account name is literally *root*, and the password will be under your control. When you login with this account, you will have system / administrative privileges.

Linux users will say or write “become root”; by this they mean to login as root or to assume the role of root. There are several ways to assume this role from a terminal emulator if you are logged in with a normal Linux account:

```
su - root
```

The *su* command will invoke a shell with a different user ID. You want to type the command as typed (*su <dash> root*). You will be prompted for the password of the root account. You can also assume other roles by using a different account name.

```
sudo "command"
```

The *sudo* command allows you to execute a command as another user. In the default mode, that other user is the root account. You will be prompted for your password, not the password of the other account. This is a way to give users administrative privileges without giving them the password of the root account. In order for this to work, the administrator must add your account to a list of trusted accounts in the file */etc/sudoers*.

Appendix E: DICOM Conformance

The following presentation contexts are supported by the Edge Server's SCP (note: LEI = little endian implicit, LEE = little endian explicit). Additional presentation contexts can be added using the procedure described below.

SOP Class	Description	Tx
1.2.840.10008.1.1	Verification SOP Class	LEI, LEE
1.2.840.10008.1.9	Basic Study Content Notification SOP Class (Retired)	LEI, LEE
1.2.840.10008.5.1.1.27	Stored Print Storage SOP Class (Retired)	LEI, LEE
1.2.840.10008.5.1.1.29	Hardcopy Grayscale Image Storage SOP Class (Retired)	LEI, LEE
1.2.840.10008.5.1.1.30	Hardcopy Color Image Storage SOP Class (Retired)	LEI, LEE
1.2.840.10008.5.1.4.1.1.1	Computed Radiography Image Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.1.1	Digital X-Ray Image Storage - For Presentation	LEI, LEE
1.2.840.10008.5.1.4.1.1.1.1.1	Digital X-Ray Image Storage - For Processing	LEI, LEE
1.2.840.10008.5.1.4.1.1.1.2	Digital Mammography X-Ray Image Storage - For Presentation	LEI, LEE
1.2.840.10008.5.1.4.1.1.1.2.1	Digital Mammography X-Ray Image Storage - For Processing	LEI, LEE
1.2.840.10008.5.1.4.1.1.1.3	Digital Intra-oral X-Ray Image Storage - For Presentation	LEI, LEE
1.2.840.10008.5.1.4.1.1.1.3.1	Digital Intra-oral X-Ray Image Storage - For Processing	LEI, LEE
1.2.840.10008.5.1.4.1.1.10	Standalone Modality LUT Storage (Retired)	LEI, LEE
1.2.840.10008.5.1.4.1.1.104.1	Encapsulated PDF Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.11	Standalone VOI LUT Storage (Retired)	LEI, LEE
1.2.840.10008.5.1.4.1.1.11.1	Grayscale Softcopy Presentation State Storage SOP Class	LEI, LEE
1.2.840.10008.5.1.4.1.1.11.2	Color Softcopy Presentation State Storage SOP Class	LEI, LEE

1.2.840.10008.5.1.4.1.1.11.3	Pseudo-Color Softcopy Presentation State Storage SOP Class	LEI, LEE
1.2.840.10008.5.1.4.1.1.11.4	Blending Softcopy Presentation State Storage SOP Class	LEI, LEE
1.2.840.10008.5.1.4.1.1.12.1	X-Ray Angiographic Image Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.12.1.1	Enhanced XA Image Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.12.2	X-Ray Radiofluoroscopic Image Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.12.2.1	Enhanced XRF Image Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.12.3	X-Ray Angiographic Bi-Plane Image Storage (Retired)	LEI, LEE
1.2.840.10008.5.1.4.1.1.128	Positron Emission Tomography Image Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.129	Standalone PET Curve Storage (Retired)	LEI, LEE
1.2.840.10008.5.1.4.1.1.2	CT Image Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.2.1	Enhanced CT Image Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.20	Nuclear Medicine Image Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.3	Ultrasound Multi-frame Image Storage (Retired)	LEI, LEE
1.2.840.10008.5.1.4.1.1.3.1	Ultrasound Multi-frame Image Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.4	MR Image Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.4.1	Enhanced MR Image Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.4.2	MR Spectroscopy Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.481.1	RT Image Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.481.2	RT Dose Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.481.3	RT Structure Set Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.481.4	RT Beams Treatment Record Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.481.5	RT Plan Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.481.6	RT Brachy Treatment Record Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.481.7	RT Treatment Summary Record Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.5	Nuclear Medicine Image Storage (Retired)	LEI, LEE

1.2.840.10008.5.1.4.1.1.6	Ultrasound Image Storage (Retired)	LEI, LEE
1.2.840.10008.5.1.4.1.1.6.1	Ultrasound Image Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.66	Raw Data Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.66.1	Spatial Registration Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.66.2	Spatial Fiducials Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.67	Real World Value Mapping Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.7	Secondary Capture Image Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.7.1	Multi-frame Single Bit Secondary Capture Image Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.7.2	Multi-frame Grayscale Byte Secondary Capture Image Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.7.3	Multi-frame Grayscale Word Secondary Capture Image Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.7.4	Multi-frame True Color Secondary Capture Image Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.77.1	VL Image Storage - Trial (Retired)	LEI, LEE
1.2.840.10008.5.1.4.1.1.77.1.1	VL Endoscopic Image Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.77.1.1. 1	Video Endoscopic Image Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.77.1.2	VL Microscopic Image Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.77.1.2. 1	Video Microscopic Image Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.77.1.3	VL Slide-Coordinates Microscopic Image Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.77.1.4	VL Photographic Image Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.77.1.4. 1	Video Photographic Image Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.77.1.5. 1	Ophthalmic Photography 8 Bit Image Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.77.1.5. 2	Ophthalmic Photography 16 Bit Image Storage	LEI, LEE

1.2.840.10008.5.1.4.1.1.77.1.5. 3	Stereometric Relationship Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.77.2	VL Multi-frame Image Storage - Trial (Retired)	LEI, LEE
1.2.840.10008.5.1.4.1.1.8	Standalone Overlay Storage (Retired)	LEI, LEE
1.2.840.10008.5.1.4.1.1.88.11	Basic Text SR Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.88.22	Enhanced SR Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.88.33	Comprehensive SR Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.88.40	Procedure Log Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.88.50	Mammography CAD SR Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.88.59	Key Object Selection Document Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.88.65	Chest CAD SR Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.88.67	X-Ray Radiation Dose SR Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.104.1	Encapsulated PDF Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.104.2	Encapsulated CDA Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.9	Standalone Curve Storage (Retired)	LEI, LEE
1.2.840.10008.5.1.4.1.1.9.1.1	12-lead ECG Waveform Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.9.1.2	General ECG Waveform Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.9.1.3	Ambulatory ECG Waveform Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.9.2.1	Hemodynamic Waveform Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.9.3.1	Cardiac Electrophysiology Waveform Storage	LEI, LEE
1.2.840.10008.5.1.4.1.1.9.4.1	Basic Voice Audio Waveform Storage	LEI, LEE
1.2.840.10008.5.1.4.38.1	Hanging Protocol Storage	LEI, LEE
1.3.12.2.1107.5.9.1	Siemens CSA Non-Image Storage	LEI, LEE

The following procedure can be used to add additional presentation contexts:

1. Using your preferred text editor (e.g. vi, emacs, gedit, etc) open the following file on the Edge Server (if the file does not exist you must create it first):

\$RSNA_ROOT/conf/dicom.properties

2. For each presentation context, you will need to add a line with the following format:

scp.sop_class.<n> = <sop class UID>

where <n> is the line number starting from zero and <sop class UID> is the actual UID of the SOP class

you're adding. For example if you're adding two hypothetical SOP classes, 1.2.3.4.5 and 9.8.7.6.5, you would add the following lines:

```
scp.sop_class.0 = 1.2.3.4.5  
scp.sop_class.1 = 9.8.7.6.5
```

3. Save the file and restart the Edge Server. You must make sure the file is readable by the edge user.

Appendix F: V2.1 Release Notes

Feature	Comment
DICOM Store SCP moved from MIRTH to prepare-content app	Should improve DICOM fetch from PACS by at least 10x's
retrieve-content app submission set based	Query Clearinghouse by submission set, so the report can be associated with corresponding study and saved under study folder
retrieve-content app installer on Edge GUI	user can now install retrieve-content on any Windows PC
Edge GUI retry stuck job	In "Audit Trail" page, when press "Details" button can locate the broken job and press a "Retry" button
Edge dbase new features and indexes	Adding db indexes on exams, patients and reports tables, so to improve HL7 feed performance. Also adding configurations for DICOM SCP function.

In addition to the features described above, we offer these queries as a method to track a site's traffic. To ascertain how many patients have signed up for the service use this:

```
select * from patients where consent_timestamp is not null;
```

To see how many patients have actually had exams sent to the Clearing House, use this:

```
select DISTINCT  
    job_sets.patient_id  
from  
    transactions ,  
    jobs,  
    job_sets  
where  
    (transactions.status_code = 40) AND  
    (transactions.job_id = jobs.job_id) AND  
    (jobs.job_set_id = job_sets.job_set_id)  
order by  
    job_sets.patient_id ;
```

Finally, to see how many studies have been sent to the Clearing House use this:

```
select * from transactions where status_code = 40 ;
```