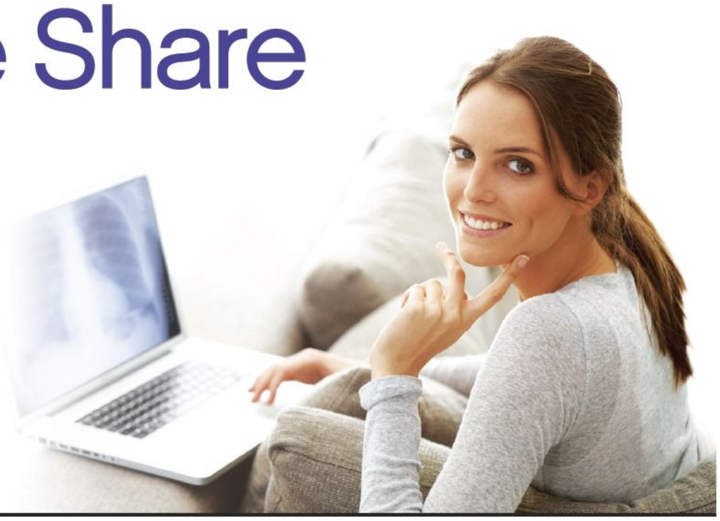
RSNA® Image Share



Letting patients
take control of their
medical images

Edge Server Installation, Upgrade and Administration Manual

Release 4.0.1
2017-05-19

Contents

1. Introduction

This document provides instructions intended for a system administrator to install, upgrade and manage an Edge Server release 4.0 device so that your site can participate in the RSNA Image Share Network (ISN). In order to manage the installation and operation of the device, you will need to understand the function of the Edge Server, which is described in the ***Image Share Network Executive Overview 4.0***.

There are several tasks required to integrate the Edge Server device with existing systems at your institution. The Edge Server administrator or other staff members will need to understand and complete tasks related to:

- DICOM configuration of existing PACS (added to RSNA ISN)
- HL7 V2 message feed from RIS for exam orders and reports (content)
- Allowing access to lifeImage

If you are installing the Edge Server for the first time, proceed to **Section 2. Installation**. If you are upgrading an existing installation, proceed to **Section 3. Upgrading Previous Releases of Edge Server to Release 4.0.**

1.1 New Features in Edge Server 4.0

The 4.0 release of the RSNA Image Share Edge Server is primarily intended as an upgrade to the latest stable versions of the components used in the Edge Server. Upgrading these components enhances the security, performance and maintainability of the Edge Server.

The versions of these components used in the previous release of the Edge Server (3.2) and the 4.0 release are shown below:

Release 3.2		**Release 4.0**	
Component	**Version**	**Component**	**Version**
Operating System	Ubuntu 10	Operating System	CentOS 7.2 or greater
Java	1.6	Java	1.8
Postgresql-server	8.4.22	Postgresql-server	9.2.18
Mirth	1.8.2	Mirth	3.4.0
Torquebox	3.x.incremental.1870	Torquebox	3.1.2
OpenAM	11	OpenAM	11.0
MIRC CTP		MIRC CTP	R39 103688eda6cd095aabe860da42c1c448230e31e3
OHT XDS Libraries	1.2.0	OHT XDS Libraries	1.2.0

2. Installation

2.1 Edge Server Delivery as Virtual Machine (VM)

The Edge Server is delivered as an image of a Virtual Machine (VM) that will operate using VMware. The site will download the VM image, install it in the existing site infrastructure, configure local PACS/RIS information and manage accounts on the Edge Server application.

2.1.1 Contents of the VM

Operating System
CentOS 7

PGAdmin3
VNC Server

2.1.2 User and Postgres Accounts

The Edge Server operates on a Linux operating system. In addition to the `root` account, we use a normal user account for day-to-day operations. The VM is configured to use the account with username `rsna`.

The default accounts/password are listed below.

`root`	**`JGK7@@ba$$Zbro`**
`rsna`	**`FT39bp#!@@Zcat`**

The PostgreSQL database uses three separate PostgreSQL roles that are not Linux accounts. The VM delivered by the RSNA has default passwords for these roles:

`postgres`	**`N3K647A`**
`mirth`	**`1947JAT$`**
`edge`	**`d17bK4#M`**

These roles are used as follows:

- `postgres`: Superuser, owner of the database
- `mirth`: Role used by the Mirth server that provides HL7 interfaces
- `edge`: Role used by the Edge Server components

There are also two default user accounts for managing and using the Edge Server via the web interface. During installation, you can set your own password for the `amAdmin` login:

`amAdmin`	**`<password set when the edge-config.sh script is run>`**
`admin`	**`password`**

Section 4.1 provides information on logging into components of the VM.

More details on the various types of accounts used by the Edge Server around found in Appendix G of this document. We recommend you read Appendix G for additional security information and instructions on changing passwords. We recommend that you change the passwords for all accounts that are listed here and in Appendix G.

Section 5.1 describes account management on the Edge Server interface in detail.

2.2 Network and Hardware Requirements

2.2.1 Edge Server Requires a Static IP Address

The Edge Server will need to communicate with several devices within the medical center (e.g. RIS and PACS). To enable this communication, the Edge Server will need a static IP address. As part of software configuration, the Edge Server will also need a fully qualified host name (e.g., edge.imaging-service.com). Before you begin installation, you will need to determine proper values for the following:

Fixed IP Address:
DNS Name:
Router/Gateway:
Net mask:
DNS Server:

The Edge Server will need to communicate with the Imaging Clearinghouse. Some institutions block outbound connections for secure reasons. You will need to allow outbound TCP connections to these ports:

```
clearinghouse.lifeimage.com:443
clearinghouse.lifeimage.com:8888
clearinghouse.lifeimage.com:8890
```

2.2.2 Hardware Requirements

The Edge Server software has been developed to run on standard desktop class PC hardware, but specific site requirements will vary based on volume of activity. The VM should deployed on a system with a base-line configuration containing:

a) Two or more cores, 2 GHz or faster CPU
b) 4 GB of RAM or more
c) 100 Mbps networking interface

2.3 Outline of the Installation Procedure - New Installation

This section provides an ordered list of installation steps for a new installation of the 4.0 Edge Server. If you are upgrading from a 3.x release, please refer to Section 3 of this document.

The 4.0 Edge Server software is distributed as a virtual machine. Instructions in this guide will refer to that VM.

1. Install the 4.0 Edge Server virtual machine (Section 2.4).
2. Login to the unix accounts on the virtual machine and change the passwords (Section 2.5).
3. Modify the hostname and establish network configuration for the virtual machine (Section 2.6).
4. Update the configuration for user management (Section 2.7).
5. Activate monitoring and email notification (Section 2.8).
6. Generate a digital certificate for and register with the lifeIMAGE Clearinghouse (Section 2.9).
7. Turn on the HL7 feed to the Edge Server (Section 2.10).

2.4 Install Edge Server 4.0 Virtual Machine

Download the Edge Server Release 4.0 Virtual Machine (in Open Virtualization Appliance [OVA]) from the following URL:

http://www.rsnaimageshare.org/downloads/4.0/rsnaedge-4.0.ova.zip

Unzip the VM.zip file. You will be directed to a single folder that contains one file:

a) rsnaedge-4.0.1.ova

The SHA-256 hash of the OVA file is:

```
8e5cc73602cd67e704a2c4aacf057945fc2a6da0b2fb63e7fa11152f014daa88
```

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) test the integrity of the file by computing the SHA-256 hash of the file you just downloaded; compare the value you computed to the value listed above with the file URL. See Appendix A for instructions on computing the SHA-256 hash.

After you have verified the integrity of the file, 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 environment has been tested:

- VMWare ESXi Server Version >= 5.x

Other OVF compliant hypervisors (such as VMware Workstation, Xen, VirtualBox and Microsoft Hyper-V) may also work, but have not been formally validated.

Boot the VM in your environment. You have the equivalent of the RSNA physical server.

2.5 Modify Unix Account Logins

The 4.0 VM is shipped with three Unix accounts. These are listed below with explanations and default passwords. You should change the password for the root and rsna accounts. The edge account is used to run applications, but is not a login account. Do not change the password for the edge account.

Account	Default Password	Description
root	`JGK7@@ba$$Zbro`	Standard unix root account.
rsna	`FT39bp#!@@Zcat`	A login account that we use to manage files and related tasks. This account does have sudo privileges.
edge		The applications on the Edge Server run under this account. Do not set or alter the password. Users do not login to this account.

2.6 Modify Hostname and Establish Network Configuration

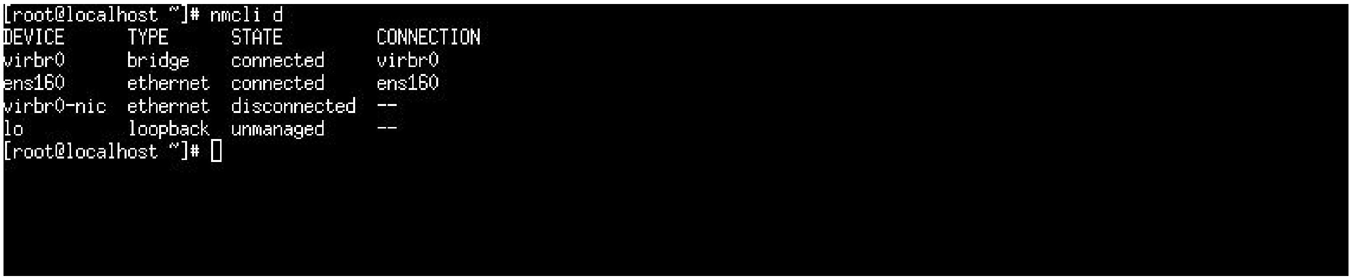
The Edge Server VM is distributed with the network configured for DHCP. This section describes the process for changing the network configuration to use a fixed IP address.

You need to change the hostname of the VM to match your local site configuration. The Edge Server does not require a specific hostname, but it DOES REQUIRE A FULLY QUALIFIED DOMAIN NAME. Using administrator privileges, edit the file /etc/hostname. Change the entry in that file to match the hostname of your VM or server.

The Edge Server needs to be able to resolve the fully qualified hostname (found in /etc/hostname) to an IP address. If your DNS does not resolve this for you, you can change the host entry in /etc/hosts to map the IP address of the server to the fully qualified host name.

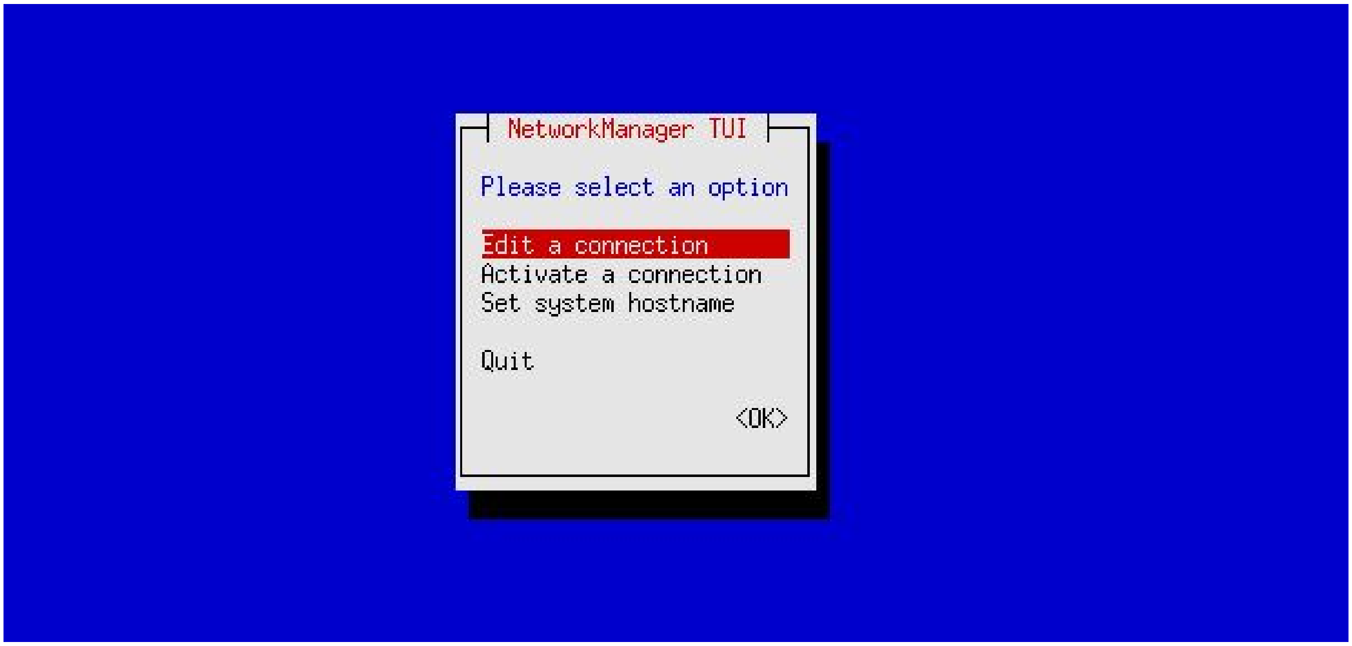
The detailed steps below describe how to configure your server for a fixed IP address. After you have completed all of the steps, reboot your server.

1. run ‘nmcli d’ command to find the connected ethernet device

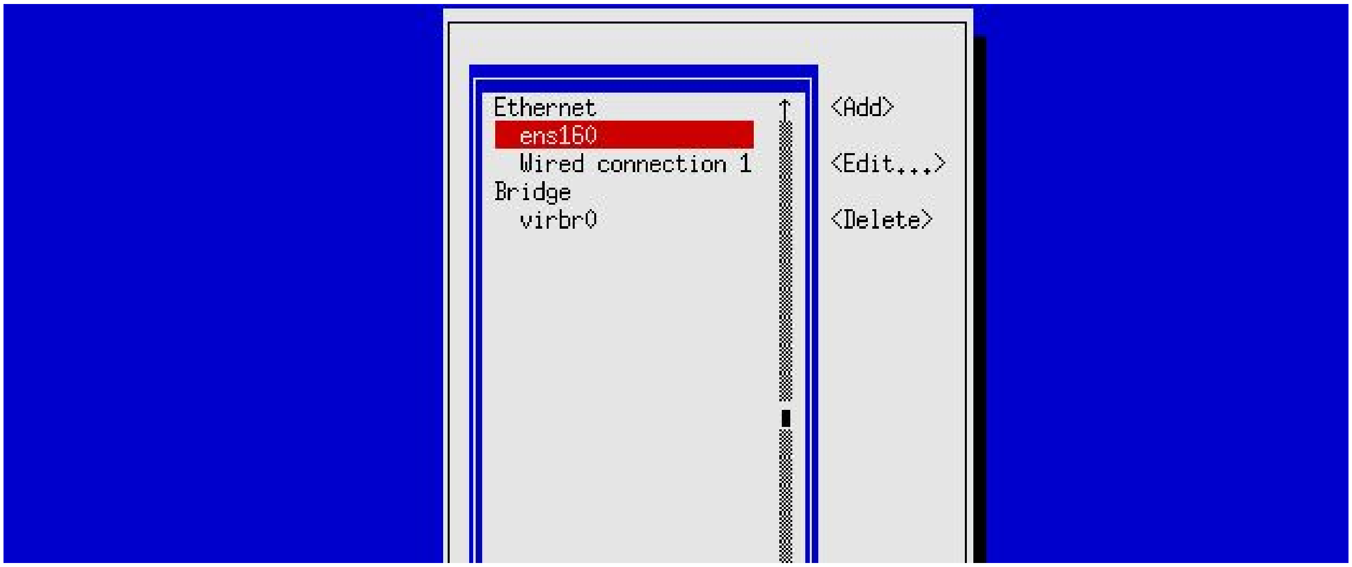


```
[root@localhost ~]# nmcli d
DEVICE      TYPE      STATE         CONNECTION
virbr0      bridge    connected     virbr0
ens160      ethernet  connected     ens160
virbr0-nic  ethernet  disconnected  --
lo          loopback  unmanaged     --
[root@localhost ~]# 
```

2. Run ‘nmtui’ or ‘sudo nmtui’ if not root

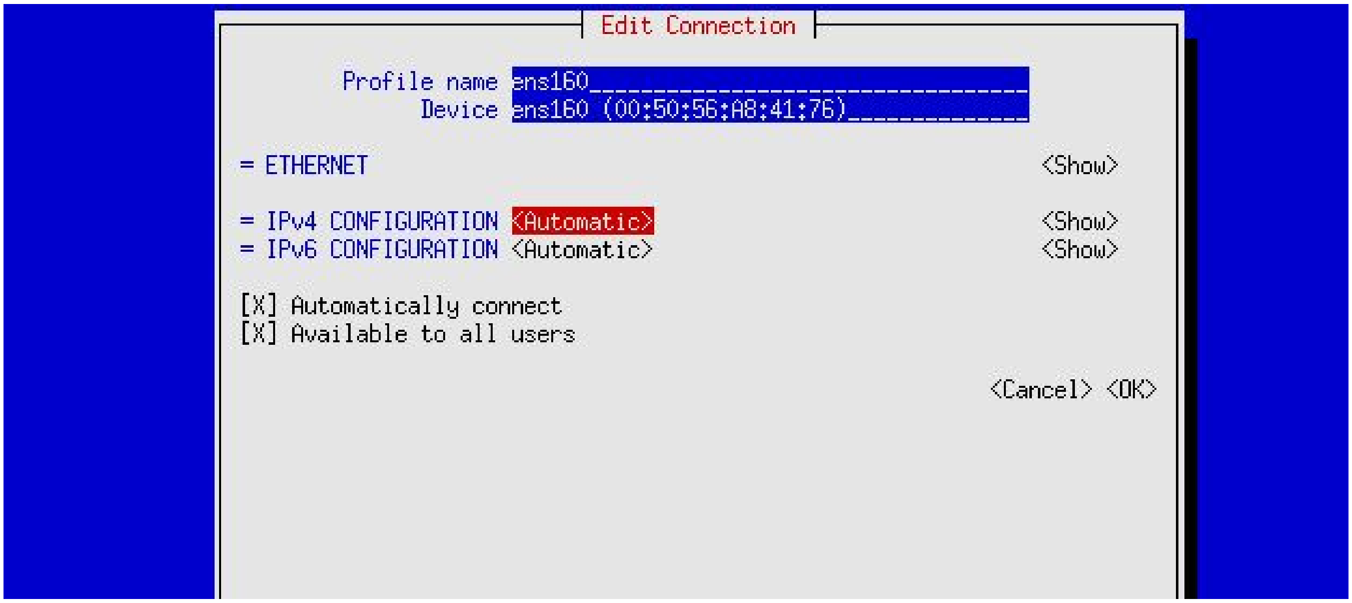


3. select ‘Edit a connection’



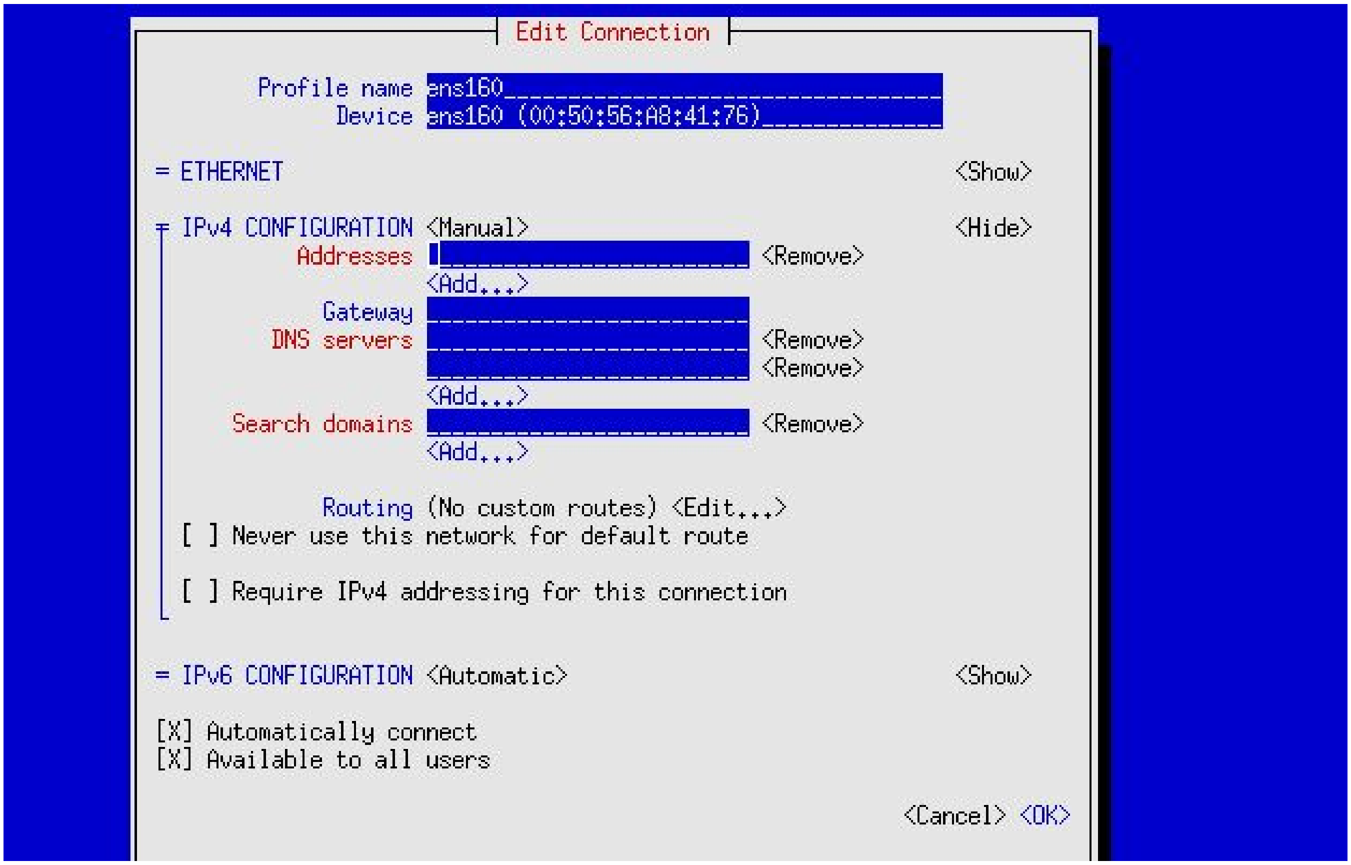
```
Ethernet                    <Add>
  ens160
  Wired connection 1        <Edit...>
Bridge
  virbr0                    <Delete>
```

4. select the connected ethernet device.



```
                        Edit Connection

       Profile name ens160________________________________
             Device ens160 (00:50:56:A8:41:76)____________

= ETHERNET                                          <Show>

= IPv4 CONFIGURATION <Automatic>                    <Show>
= IPv6 CONFIGURATION <Automatic>                    <Show>

[X] Automatically connect
[X] Available to all users

                                              <Cancel> <OK>
```

5. select configure network settings as needed.



```
┌───────────────────────────┤ Edit Connection ├───────────────────────────┐
│                                                                          │
│       Profile name ens160________________________________________        │
│             Device ens160 (00:50:56:A8:41:76)_____________________       │
│                                                                          │
│ = ETHERNET                                                      <Show>   │
│                                                                          │
│ ╤ IPv4 CONFIGURATION <Manual>                                   <Hide>   │
│ │          Addresses ▌_________________________ <Remove>                 │
│ │                    <Add...>                                            │
│ │            Gateway __________________________                          │
│ │        DNS servers __________________________ <Remove>                 │
│ │                    __________________________ <Remove>                 │
│ │                    <Add...>                                            │
│ │     Search domains __________________________ <Remove>                 │
│ │                    <Add...>                                            │
│ │                                                                        │
│ │            Routing (No custom routes) <Edit...>                        │
│ │ [ ] Never use this network for default route                           │
│ │                                                                        │
│ │ [ ] Require IPv4 addressing for this connection                        │
│ └                                                                        │
│                                                                          │
│ = IPv6 CONFIGURATION <Automatic>                                <Show>   │
│                                                                          │
│ [X] Automatically connect                                                │
│ [X] Available to all users                                               │
│                                                                          │
│                                                          <Cancel> <OK>   │
```

6. select ‘OK’

When complete, reboot the server.

2.7 Configure User Management

Edge Server user management uses OpenAM for Single Sign-On (SSO) functions. By default users are authenticated with a local user database. Role permissions are handled by group membership of the OpenAM user profile.

Optionally OpenAM can be configured to authenticate with an Active Directory server. In this case, role permissions are still handled by appropriate group memberships managed by OpenAM.

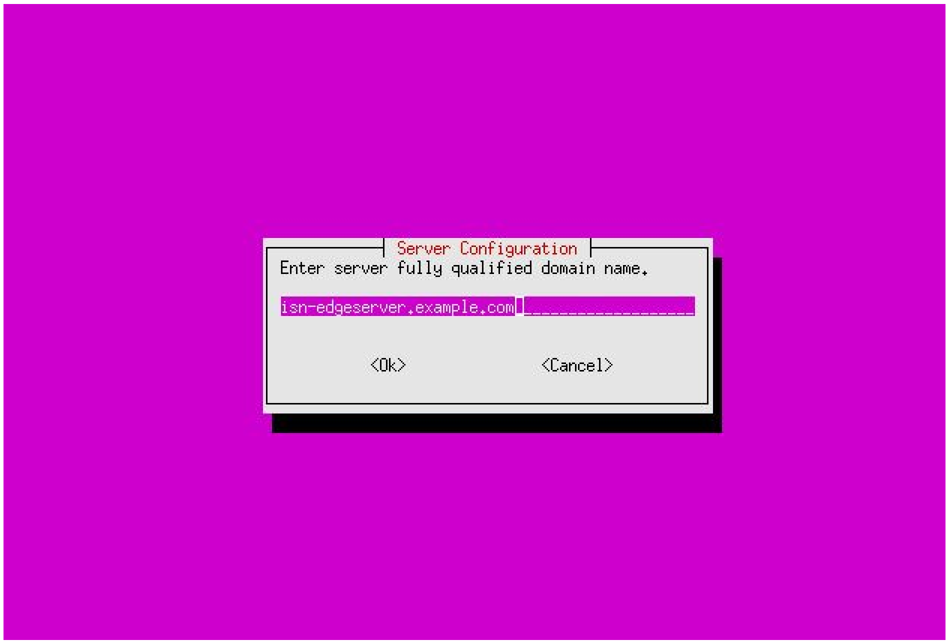
Note:

- It is not necessary to manually configure OpenAM via its web interface at this point.
- Before starting the configuration below, we recommend you take a snapshot of your installed VM. If you make an error during the OpenAM configuration, it is easier to restore from a snapshot than to reset the files that were updated by the edge-config.sh script below.
- OpenAM configuration is tightly coupled to the fully qualified domain name of your server (e.g., edge.eastern-imaging.org). Please make sure you have selected and configured the full hostname for your system before executing the in this section. Appendix H of this document provides instructions on modifying the user management (OpenAM) configuration should you decide to change your host name after initial installation.

To start configuring OpenAM, run the script $RSNA_ROOT/scripts/edge-config.sh:

```
sudo -u root $RSNA_ROOT/scripts/edge-config.sh
```

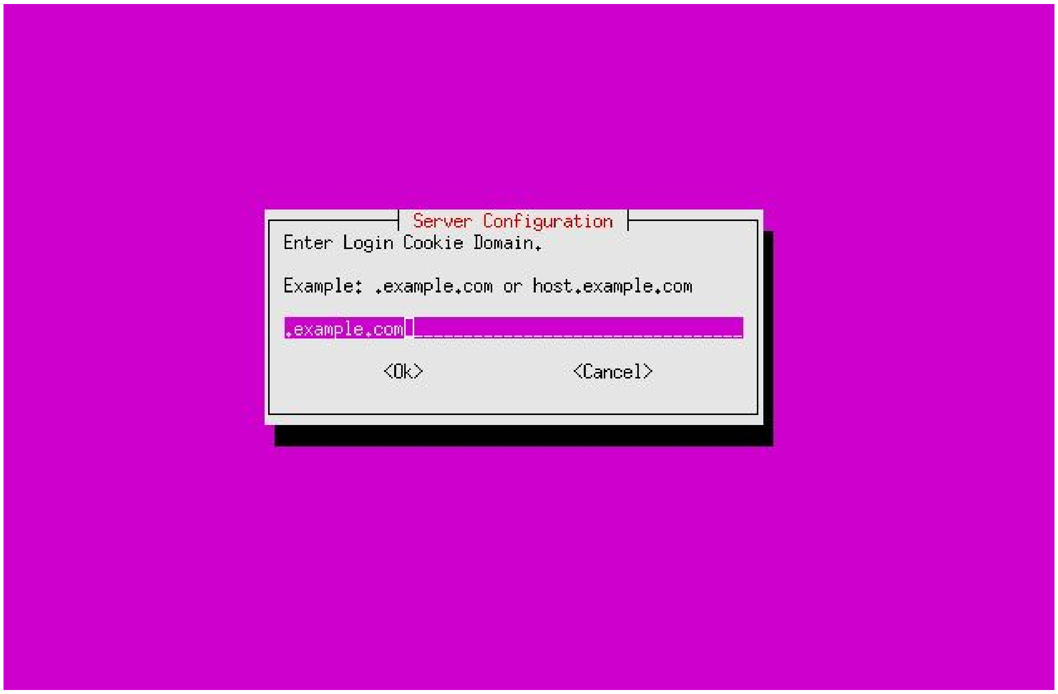
Enter server's fully qualified domain name:



```
Server Configuration
Enter server fully qualified domain name.

isn-edgeserver.example.com
```

Figure 2-7.1: Server Configuration DNS

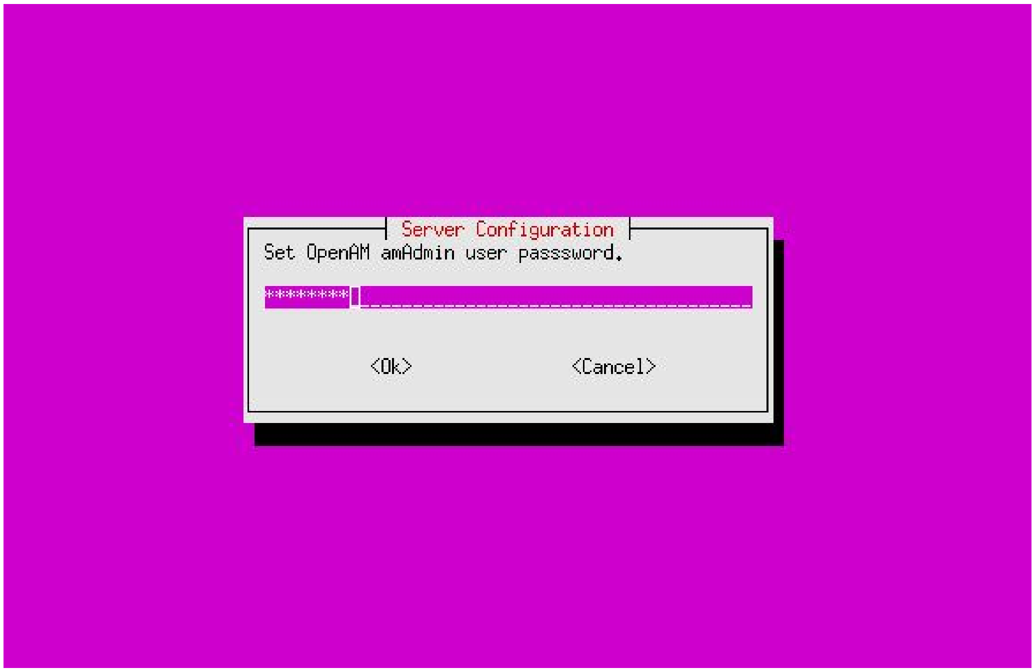
Enter cookie domain used by OpenAM. Note the single . character if you enter only the domain name.



```
Server Configuration
Enter Login Cookie Domain.

Example: .example.com or host.example.com

.example.com
```

Figure 2-7.2: Server Configuration Cookie Domain

Set OpenAM amAdmin user password:



```
Server Configuration
Set OpenAM amAdmin user password.

*********
```

Figure 2-7.3: Server Configuration AmAdmin User Password

When all the input is entered the configuration process will start. When it is finished, it will display “Setup Complete.”

Restart the VM to apply the new configuration to all the components.

Now, open a Web browser, you can visit the URL http://<your server's fully qualified domain name>:3000/openam to login to the OpenAM control panel by using the admin user "amAdmin" and the password you just set.

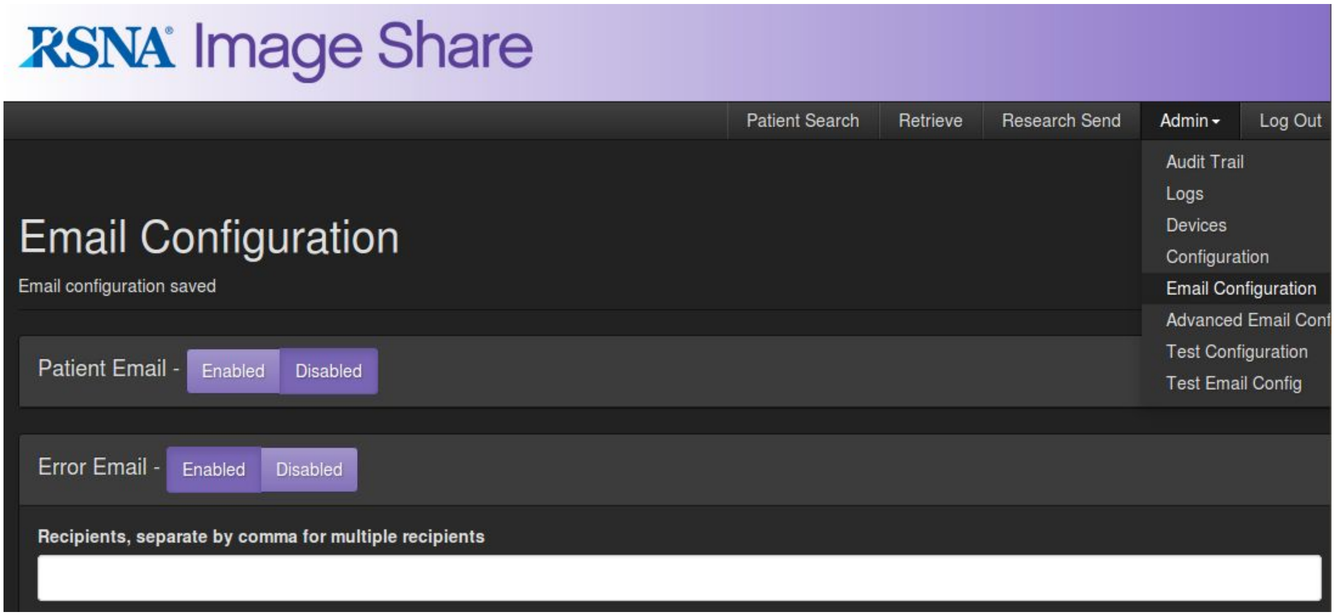
See Appendix F for information on setting up Active Directory for user authentication if that is required.

See Appendix H for information on setting up Active Directory for user authentication if that is required.

See Section 7 for instructions on administering user accounts.

2.8 Activate Monitoring and Email Notifications

A monitor script can be installed to run as a cron job to monitor the status of the Edge Server. Whenever an error is detected, an email notification will be sent to the recipients configured via the Email Configuration under the `Admin` menu of the Web interface of edge server Select Email Configuration from the Admin dropdown menu and enter a recipient for the notifications.



Email Configuration

Email configuration saved

Patient Email - Enabled Disabled

Error Email - Enabled Disabled

Recipients, separate by comma for multiple recipients

Figure 2.8-1: Configuring email recipients to receive error notifications for monitor script

The script monitors three critical services of the Edge Server:

- `postgresql-9.2`
- `ctpService`
- `edge-server (which includes the following processes in` Torquebox: prepare content, transfer content and Mirth).

The script also checks the connections to the `rsnadb` and `mirthdb` databases in the Edge Server using the credentials stored in the following two (2) files:

- `$RSNA_ROOT/conf/database.properties`
- `$RSNA_ROOT/mirthconnect/conf/postgres-SqlMapConfig.properties.`

To assure the monitor script is working, you need to do the following steps:

- Test run the script manually
- Make sure that a “cron” job is set up to make it run automatically

2.8.1 Test Run the Monitor Script

Now you can test run the script by typing the following from the command line (as root or using sudo from the rsna account):

```
# cd /usr/local/edge-server/monitor-scripts
# chmod u+x edgeserver_monitor.sh
# sudo -u edge ./edgeserver_monitor.sh
```

If your Edge Server is running normally, you should have a successful output, as shown in the following:

```
root@rsnaedge-vm:~# ./edgeserver_monitor.sh
All required services are running!

DB connectivity testing result(s):
Testing connection to database "rsnadb" succeeded.
Testing connection to database "mirthdb" succeeded.

Diagnosed Reason(s):
No reason found.
```

If an error is detected by the monitor script, it will be visible in the output, as shown in the following example:

```
root@rsnaedge-vm:~# ./edgeserver_monitor.sh
Here are the problem(s) I found:
true
true
false : Service "edge-server: torquebox" is not running.
true
true
```

```
true

DB connectivity testing result(s):
Testing connection to database "rsnadb" succeeded.
Testing connection to database "mirthdb" succeeded.

Diagnosed Reason(s):
No reason found.

An email notification has been sent to the configured recipient(s).
```

In this example, the Edge Server's `torquebox` service is not running.

Note: If you get an error in regarding to sending emails when running the monitor script, check for the file `$RSNA_ROOT/sendemail-isn-1.0.jar` to make sure it exists.

2.8.2 Set Up a Cron Job for the Monitor Script

After successfully running the monitor script manually, you can install the monitor as a cron job to run periodically and automatically. For the example, the following setting

```
0 0-23 * * * /root/edgeserver_monitor.sh
```

for the monitor script as a cron job will make the script run at the beginning of every hour (the first column indicates the 0’th minute of the hour). You can manually change this schedule if you wish.

Assuming you are logged in as user “rsna” and that the path to the monitor script is as above, you would do the following at the command prompt:

```
> sudo crontab -u root ./edgeserver_monitor.crontab
```

Now, the monitor script has been scheduled to run as a cron job. You can see that the cron job has been setup by running this command:

```
>sudo crontab -l -u root
```

2.9 Registering the Edge Server Certificate with the

Clearinghouse

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. *In order to connect to the Clearinghouse, your institution must establish a HIPAA-compliant BAA (Business Associates Agreement) with lifeIMAGE. If you have not done so, please contact Jim Phllips (jphillips@lifeimage.com) to initiate the process.*

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.

2.9.1 Generating Edge Server Digital Certificate

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 su edge
```

You will be prompted for the rsna password.

Remove the temporary installed certificate by issuing the following command on line line:

```
keytool -delete -alias edge -storepass edge1234 -keystore
$RSNA_ROOT/conf/keystore.jks
```

Next, create a new certificate by issuing the following command on line line:

```
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. 1095 for 3 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 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.

2.9.2 Exporting and Registering the Certificate

To send the Edge Server certificate to lifeIMAGE, 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. *Note: if you are logged in as* `edge` *you must exit and login as the* `rsna` *user.* Then, on one line:

```
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 support@lifeimage.com to have it registered with the clearinghouse.

It is strongly recommended you send some test exams to the clearinghouse after completing the configuration of the Edge Server. If you choose to send test exams, make sure to send lifeIMAGE the DOB and Access Code 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.

2.10 Setting Up Mirth

Mirth provides HL7 interfaces for the Edge Server for the clinical use cases. Mirth enables the Edge Server to receive information about clinical orders and reports. These data are used to build the patient and exam lists on the Edge web interface, and package reports when studies are sent to the Clearinghouse.

1. You will need to find the specification for HL7 V2 messages exported by your RIS for the following events:
    a. Merge Patient (ADT^A18)
    b. Order Exam (ORM^O01)
    c. Schedule Exam (ORM^O01)
    d. Complete Exam (ORM^O01)
    e. Cancel Exam (ORM^O01)
    f. Prelim Report (ORU^R01)
    g. Finalize Report (ORU^R01)
    h. Addend Report (ORU^R01)
2. Use the specification of your messages and determine how the map to the Edge Server's database columns (see **2.11.3 HL7 Specification** for detailed specifications).
3. Verify that the Edge Server web services are running. If you cannot connect to the Mirth administrator web page, reboot the Edge Server or restart the services manually:

```
        sudo service edge-server restart
```

4. Follow the instructions in **2.11.2 Configuration and Management** on configuring Mirth. There are detailed screen shots.
5. Configure your RIS to send messages for the events listed above to the Edge Server. The Edge Server receives HL7 V2 messages using the standard MLLP at port 20000.
6. You will need to test the interface to ensure the mapping has been setup correctly. This is best done by sending a sequence of messages that steps through the entire order lifecycle (i.e. from ordering an exam to finalizing a report).

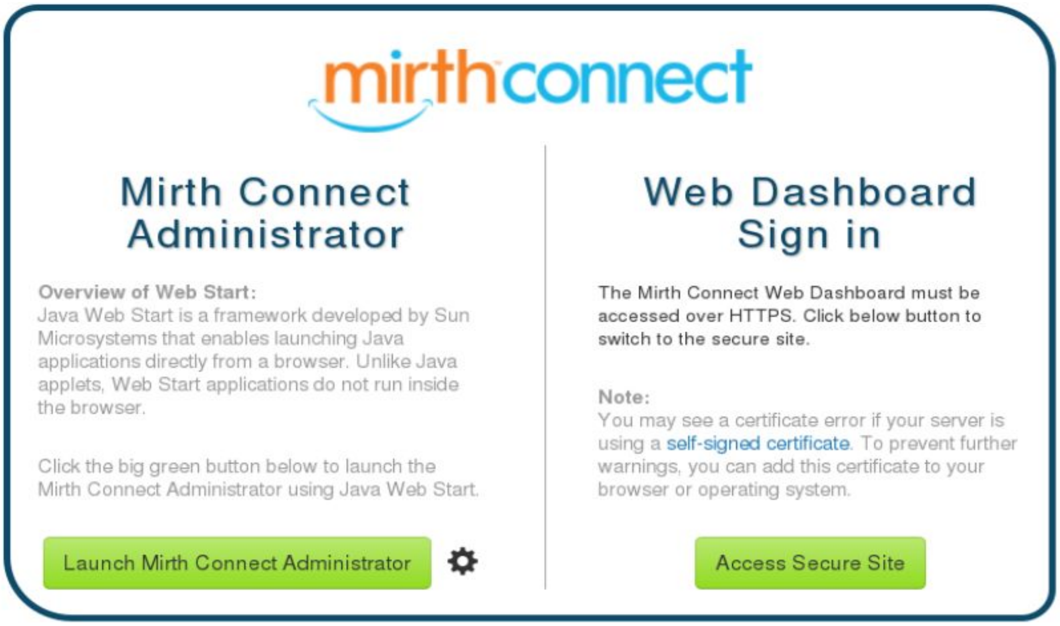
2.10.1 Accessing Mirth via the Web Interface

Mirth configuration is accomplished via a Web interface; the web browser can be on either a remote machine (**strongly recommended**) or locally on the Edge Server.

Before you continue, please verify Mirth has been configured to use PostgreSQL (see 2.4.1 Configure Mirth to Use Postgres).

If accessing locally from the server, **you will need to be running Java 8.**

Navigate your browser to: `http://isn.example.com:8080` (substituting your actual FQDN for `isn.example.com`). You will see the landing page with `Launch` button (Figure 2.10-1).



Mirth Connect Administrator

Overview of Web Start:
Java Web Start is a framework developed by Sun Microsystems that enables launching Java applications directly from a browser. Unlike Java applets, Web Start applications do not run inside the browser.

Click the big green button below to launch the Mirth Connect Administrator using Java Web Start.

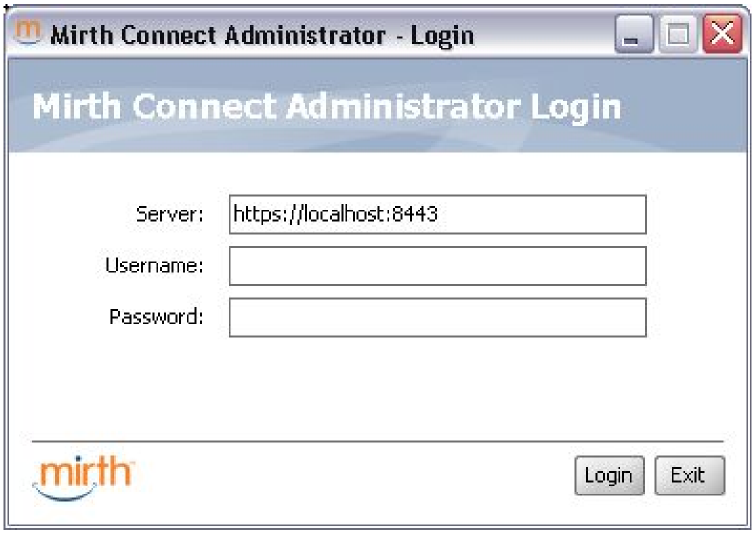
Web Dashboard Sign in

The Mirth Connect Web Dashboard must be accessed over HTTPS. Click below button to switch to the secure site.

Note:
You may see a certificate error if your server is using a self-signed certificate. To prevent further warnings, you can add this certificate to your browser or operating system.

Figure 2.10-1: The Mirth Administrator Java Web Start page

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: `/opt/jdk1.8.0_77/bin/javaws`. A Java Web Start app should launch and you should see a login dialog (Figure 2.10-2).


Mirth Connect Administrator - Login
Mirth Connect Administrator Login
mirth
Login
Exit

Server: https://localhost:8443

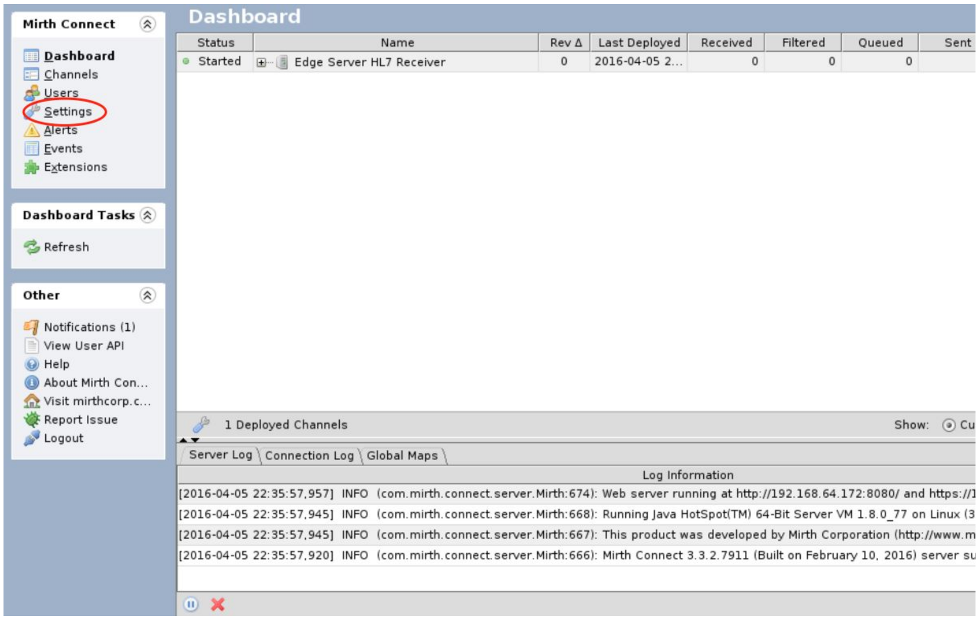
Username:

Password:

Figure 2.10-2: The Mirth Administrator login dialog

2.10.2 Configuration and Management

1. Login using username = “admin”, password = “admin”. After logging in you should see a screen similar to:

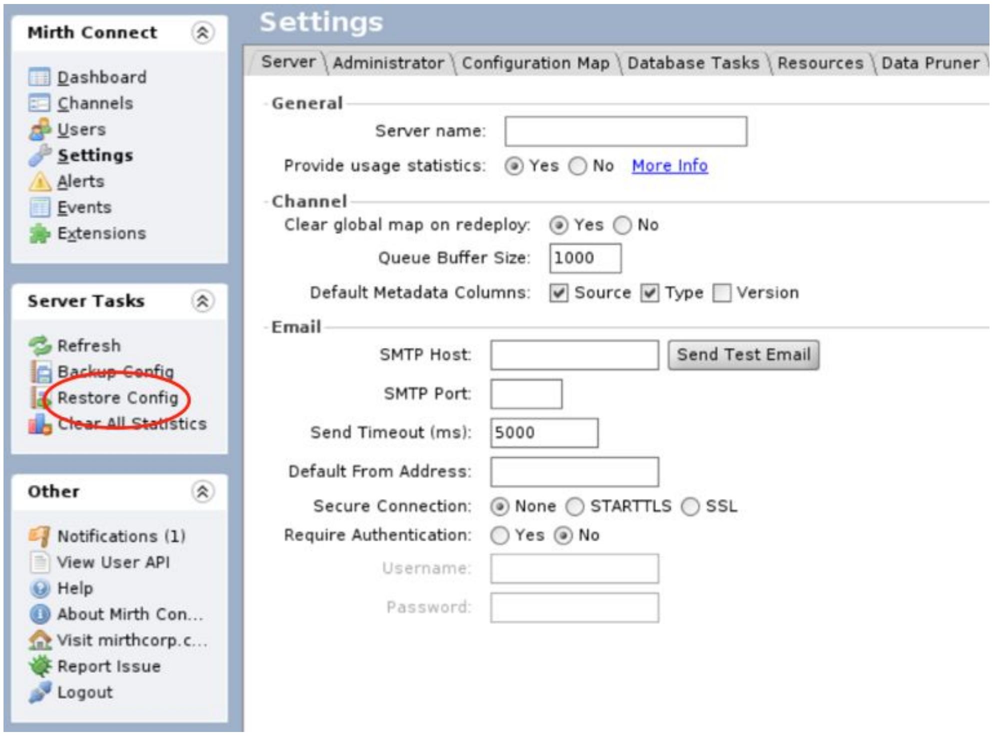


Status	Name	Rev Δ	Last Deployed	Received	Filtered	Queued	Sent
● Started	Edge Server HL7 Receiver	0	2016-04-05 2...	0	0	0	

```
Log Information
[2016-04-05 22:35:57,957]  INFO  (com.mirth.connect.server.Mirth:674): Web server running at http://192.168.64.172:8080/ and https://1
[2016-04-05 22:35:57,945]  INFO  (com.mirth.connect.server.Mirth:668): Running Java HotSpot(TM) 64-Bit Server VM 1.8.0_77 on Linux (3
[2016-04-05 22:35:57,945]  INFO  (com.mirth.connect.server.Mirth:667): This product was developed by Mirth Corporation (http://www.m
[2016-04-05 22:35:57,920]  INFO  (com.mirth.connect.server.Mirth:666): Mirth Connect 3.3.2.7911 (Built on February 10, 2016) server su
```

Figure 2.10-3: Mirth Administrator

2. Initialize the base Mirth setup. In the left column, click on the “Settings” link. You should see a screen similar to:



General

Server name:

Provide usage statistics: ● Yes ○ No

Channel

Clear global map on redeploy: ● Yes ○ No

Queue Buffer Size: 1000

Default Metadata Columns: ☑ Source ☑ Type □ Version

Email

SMTP Host:

SMTP Port:

Send Timeout (ms): 5000

Default From Address:

Secure Connection: ● None ○ STARTTLS ○ SSL

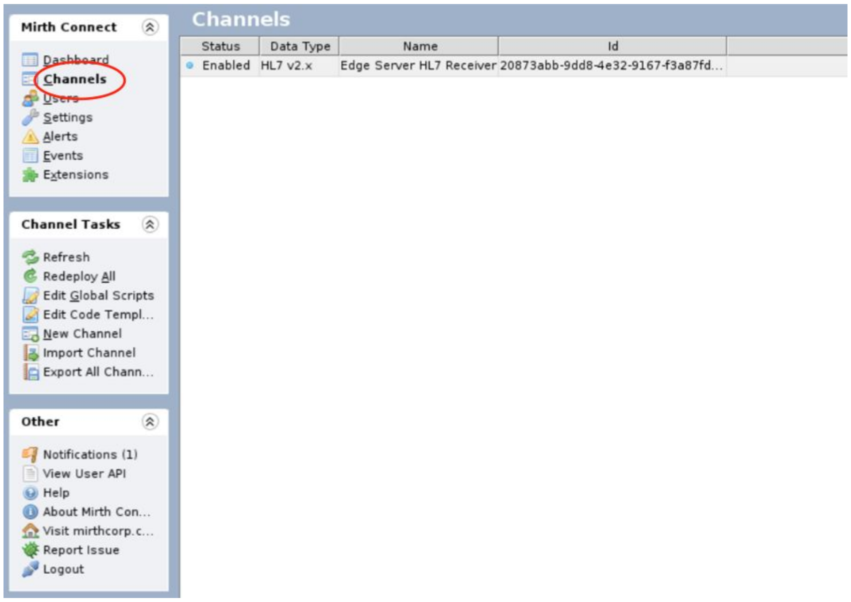
Require Authentication: ○ Yes ● No

Username:

Password:

Figure 2.10-4: Installing the default Mirth configuration

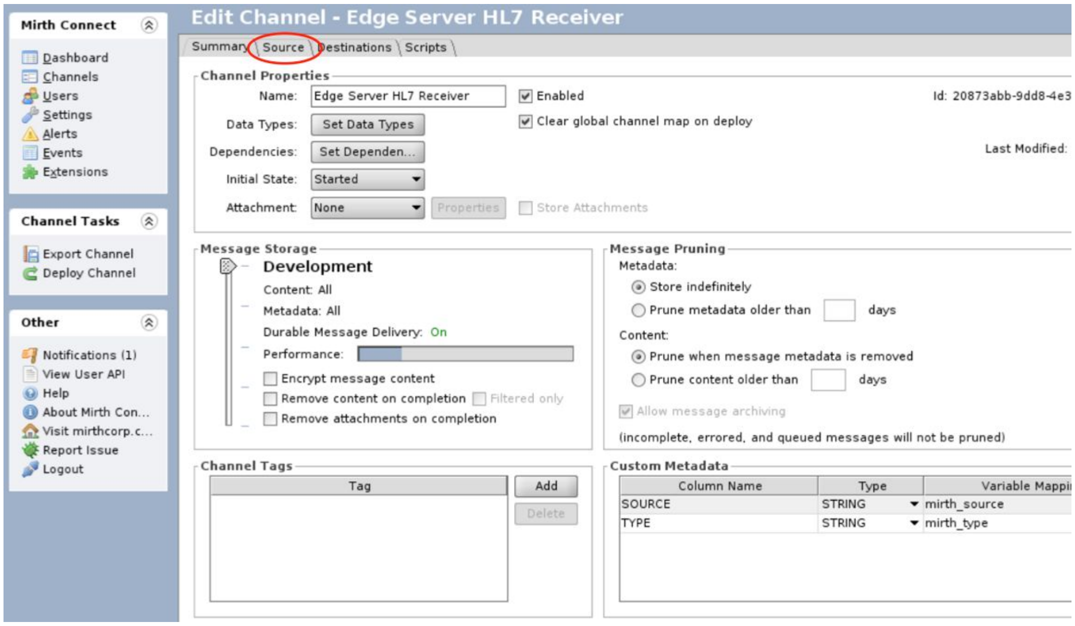
3. Click the “Restore Config” button at the bottom of the page and select the “Mirth Backup.xml” file located in the in the home folder of the rsna linux account (/home/rsna); see Figure 2.10-4. You may be prompted to convert the imported server configuration, if so accept by pressing “Yes”. You should get a message saying your configuration was successfully restored.
4. Now switch to the channels page by click the “Channels” link in the left column. You should see the screen pictured below:



Status	Data Type	Name	Id
● Enabled	HL7 v2.x	Edge Server HL7 Receiver	20873abb-9dd8-4e32-9167-f3a87fd...

Figure 2.10-5: Mirth Channel Listing

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



Edit Channel - Edge Server HL7 Receiver

Channel Properties

Name: Edge Server HL7 Receiver ☑ Enabled Id: 20873abb-9dd8-4e3

Data Types: Set Data Types ☑ Clear global channel map on deploy

Dependencies: Set Dependen... Last Modified:

Initial State: Started

Attachment: None Properties □ Store Attachments

Message Storage

Development

Content: All

Metadata: All

Durable Message Delivery: On

Performance:

□ Encrypt message content

□ Remove content on completion □ Filtered only

□ Remove attachments on completion

Message Pruning

Metadata:

● Store indefinitely

○ Prune metadata older than days

Content:

● Prune when message metadata is removed

○ Prune content older than days

☑ Allow message archiving

(incomplete, errored, and queued messages will not be pruned)

Channel Tags

Tag

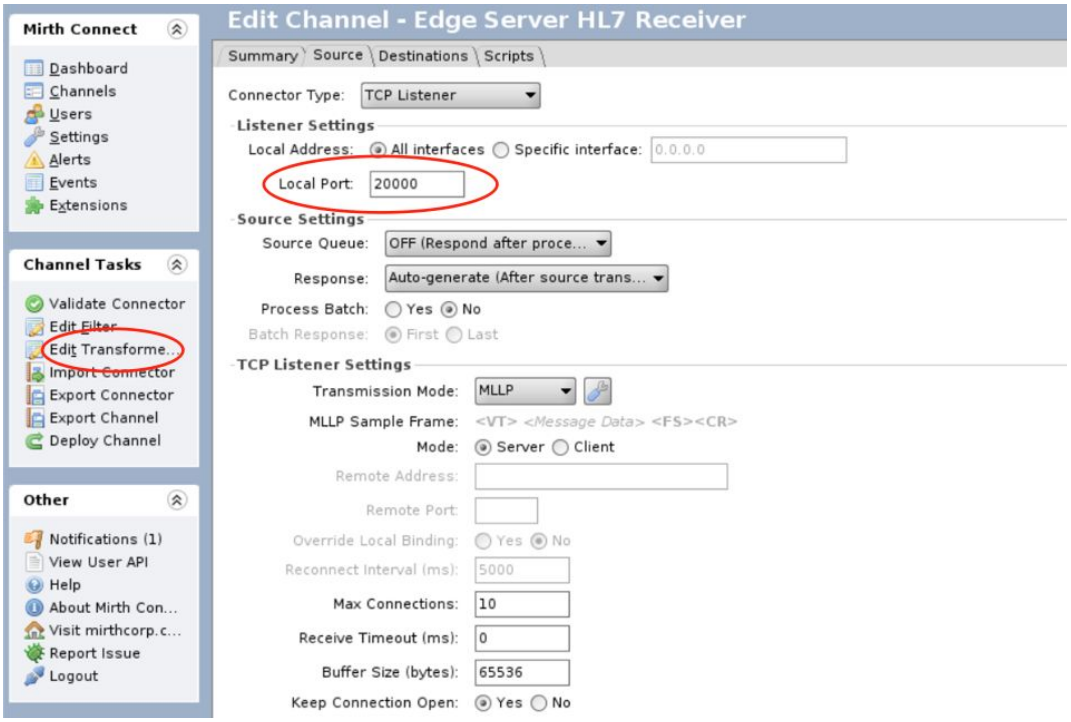
Add Delete

Custom Metadata

Column Name	Type	Variable Mappi
SOURCE	STRING	mirth_source
TYPE	STRING	mirth_type

Figure 2.10-6: Configuring the HL7 Channel

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



Edit Channel - Edge Server HL7 Receiver

Connector Type: TCP Listener

Listener Settings

Local Address: ● All interfaces ○ Specific interface: 0.0.0.0

Local Port: 20000

Source Settings

Source Queue: OFF (Respond after proce...

Response: Auto-generate (After source trans...

Process Batch: ○ Yes ● No

Batch Response: ● First ○ Last

TCP Listener Settings

Transmission Mode: MLLP

MLLP Sample Frame: <VT> <Message Data> <FS><CR>

Mode: ● Server ○ Client

Remote Address:

Remote Port:

Override Local Binding: ○ Yes ● No

Reconnect Interval (ms): 5000

Max Connections: 10

Receive Timeout (ms): 0

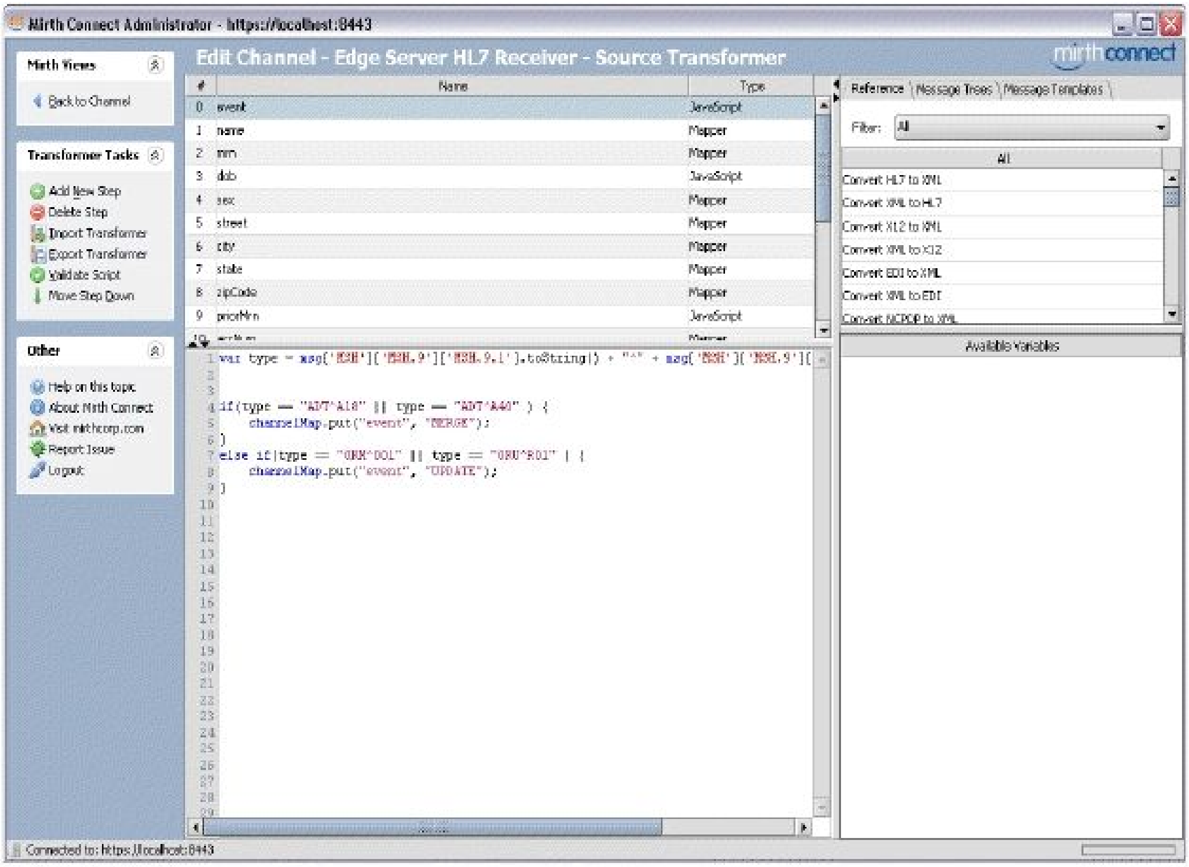
Buffer Size (bytes): 65536

Keep Connection Open: ● Yes ○ No

Figure 2.10-7: Configuring the HL7 Network Parameters

7. Set the the Listener Port value to the appropriate value for your installation. The default value is 20,000.

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



#	Name	Type
0	event	JavaScript
1	name	Mapper
2	mrn	Mapper
3	dob	JavaScript
4	sex	Mapper
5	street	Mapper
6	city	Mapper
7	state	Mapper
8	zipCode	Mapper
9	priorMrn	JavaScript

```
var type = msg['MSH']['MSH.9']['MSH.9.1'].toString() + "^" + msg['MSH']['MSH.9'][


if(type == "ADT^A18" || type == "ADT^A40" ) {
    channelMap.put("event", "MERGE");
}
else if(type == "ORM^O01" || type == "ORU^R01" ) {
    channelMap.put("event", "UPDATE");
}
```

Figure 2.10-8: Configuring the HL7 Channel Variables

9. 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")	The exam status. Sites need to map their exam status codes to the following values: ORDERED SCHEDULED IN-PROGRESS COMPLETED DICTATED PRELIMINARY FINALIZED REVISED ADDENDED CANCELED NON-REPORTABLE
statusChangeTimestamp ("reports")	The timestamp of the exam status change. Cannot be null. Value must be of type java.sql.Timestamp.
report ("reports")	Full text of the report. *The value must be plain text and cannot contain any formatting character sequences*.
signer("reports")	The report signer.
dictator("reports")	The report dictator.
transcriber("reports")	The report transcriber.

10. When you are done click "Back to Channel" on the top left then "Save Changes" link in the left column and switch back to the Channels panel.
11. Next you will need to update/verify the password Mirth will use to connect to the rsnadb database for storing patient & exam info. Start by selected the channel as before and clicking on the "Edit Code Templates" link to open the Code Templates tab:

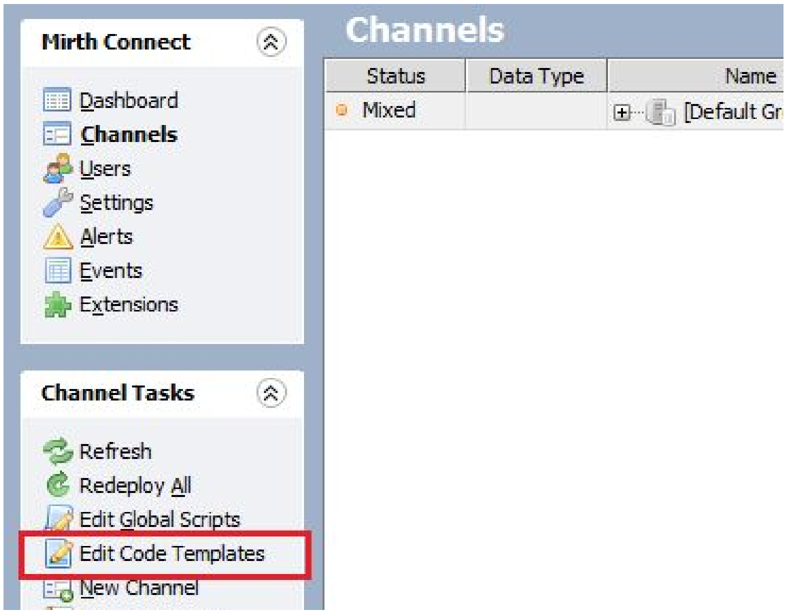
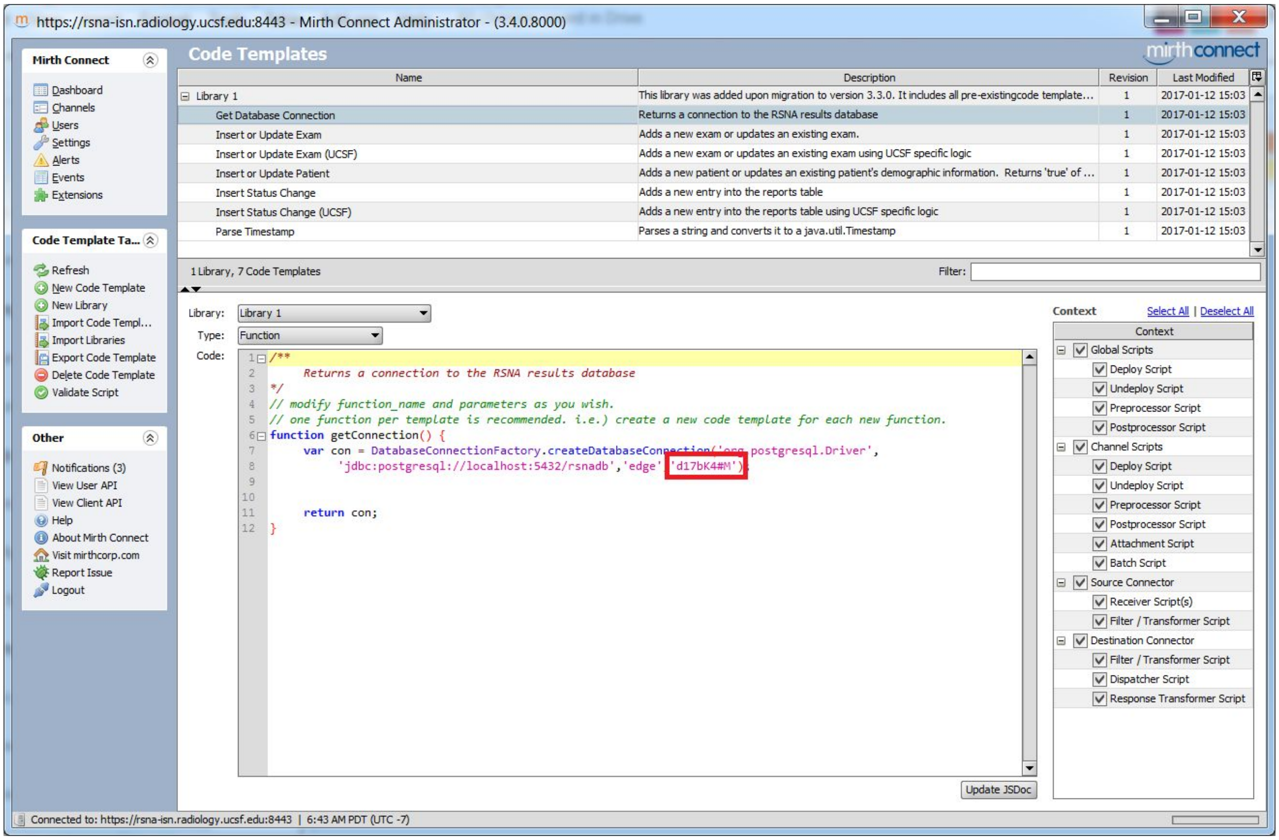


Figure 2.10-9: How to Open the Edit Code Templates Tab

12. Once you have opened the edit code templates tab, you should see a screen similar to the one pictured below.



Name	Description	Revision	Last Modified
⊟ Library 1	This library was added upon migration to version 3.3.0. It includes all pre-existingcode template...	1	2017-01-12 15:03
Get Database Connection	Returns a connection to the RSNA results database	1	2017-01-12 15:03
Insert or Update Exam	Adds a new exam or updates an existing exam.	1	2017-01-12 15:03
Insert or Update Exam (UCSF)	Adds a new exam or updates an existing exam using UCSF specific logic	1	2017-01-12 15:03
Insert or Update Patient	Adds a new patient or updates an existing patient's demographic information. Returns 'true' of ...	1	2017-01-12 15:03
Insert Status Change	Adds a new entry into the reports table	1	2017-01-12 15:03
Insert Status Change (UCSF)	Adds a new entry into the reports table using UCSF specific logic	1	2017-01-12 15:03
Parse Timestamp	Parses a string and converts it to a java.util.Timestamp	1	2017-01-12 15:03

1 Library, 7 Code Templates

Library: Library 1

Type: Function

Code:

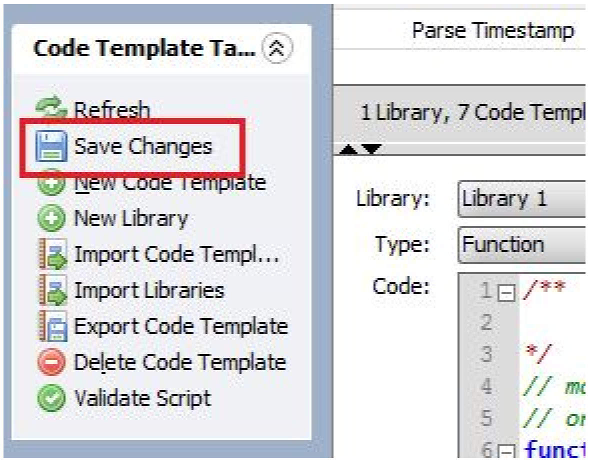
```
/**
	Returns a connection to the RSNA results database
*/
// modify function_name and parameters as you wish.
// one function per template is recommended. i.e.) create a new code template for each new function.
function getConnection() {
	var con = DatabaseConnectionFactory.createDatabaseConnection('org.postgresql.Driver',
		'jdbc:postgresql://localhost:5432/rsnadb','edge','d17bK4#M');


	return con;
}
```

Context
⊟ ☑ Global Scripts
☑ Deploy Script
☑ Undeploy Script
☑ Preprocessor Script
☑ Postprocessor Script
⊟ ☑ Channel Scripts
☑ Deploy Script
☑ Undeploy Script
☑ Preprocessor Script
☑ Postprocessor Script
☑ Attachment Script
☑ Batch Script
⊟ ☑ Source Connector
☑ Receiver Script(s)
☑ Filter / Transformer Script
⊟ ☑ Destination Connector
☑ Filter / Transformer Script
☑ Dispatcher Script
☑ Response Transformer Script

Figure 2.10-10: Updating “Get Database Connection” code template

13. Click on the “Get Database Connection” code template under the code library and verify/update the value of password parameter to the one used for the `edge` PostgreSQL user.

14. If you make any changes you will need to click the “Save Changes” link in the left column to ensure the channel configuration is updated correctly:



Library: Library 1

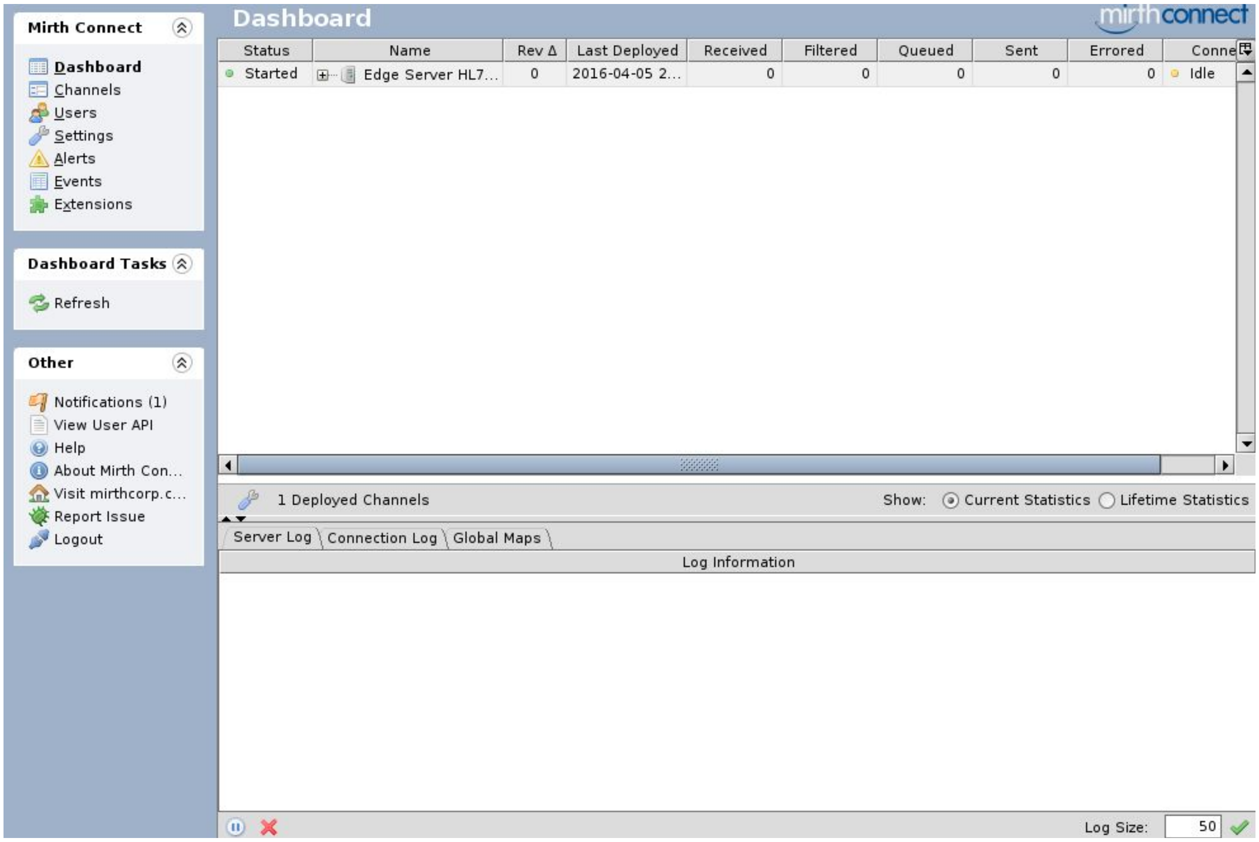
Type: Function

Code:

```
/**

*/
// mo
// or
funct
```

Figure 2.10-11: Saving updates to “Get Database Connection” code template

15. Right click on the list of channels and select “Deploy All” from the context menu.
16. You will then see the Dashboard panel pictured below. Verify the HL7 channel is listed as “Started”.



Status	Name	Rev Δ	Last Deployed	Received	Filtered	Queued	Sent	Errored	Conne
● Started	⊞ Edge Server HL7...	0	2016-04-05 2...	0	0	0	0	0	● Idle

1 Deployed Channels

Show: ● Current Statistics ○ Lifetime Statistics

Log Size: 50

Figure 2.10-12: The Mirth Administrator Dashboard for Monitoring Channel Status

2.10.3 HL7 Specification

The EdgeServer currently uses the following messages:

1. ORM - used to create the patient and the exam or report status
2. ORU - used to receive the report and report status
3. ADT (A18 or A40) – used for patient merge

The message fields are shown below:

	Message Type		
Edgeserver DB Field	**ORU^R01**	**ORM^O01**	**ADT^A18**
Patient Name	PID-5	PID-5	
Medical Record Number	PID-3-1	PID-3-1	
Prior Medical Record Number			MRG-1-1
Date of Birth	PID-7-1	PID-7-1	
Sex	PID-8-1	PID-8-1	
Street	PID-11-1	PID-11-1	
City	PID-11-3	PID-11-3	
State	PID-11-4	PID-11-4	
Zip Code	PID-11-4	PID-11-4	
Acc Number ● **(DICOM tag 0008,0050)**	OBR-3-1	OBR-3-1	
Description	OBR-4-2	OBR-4-2	
Exam Status			
ORDERED			
SCHEDULED		OBR-25-1 (status code = 'S')	
IN-PROGRESS		OBR-25-1 (status code = 'I')	

COMPLETED		OBR-25-1 (status code = 'C')	
DICTATED	OBR-25-1 (status code = 'D')		
PRELIMINARY	OBR-25-1 (status code = 'P')		
FINALIZED	OBR-25-1 (status code = 'F')		
REVISED	OBR-25-1 (status code = 'R')		
ADDENDED	OBR-25-1 (status code = 'A')		
NON-REPORTABLE	OBR-25-1 (status code = 'N')		
CANCELED		OBR-25-1 (status code = 'X')	
Status Change Timestamp	OBR-22-1	OBR-22-1	
Report Text	OBX-5-1		
Report Dictator	ZRI-2 & ZRI-3		
Report Transcriber	OBR-35		
Report Signer	OBR-32		

2.11 Configuring for Site-to-site Sending and Retrieval

The Edge Server contains a module called the Clinical Trials Process (or CTP) that is used to retrieve images from the Clearinghouse for site-to-site sharing of clinical images with partner institutions in the Image Share Network and for sending and retrieval of de-identified images for imaging-based clinical trials. If your site uses the Edge Server exclusively for sending images for patient retrieval (the site-to-patient use case), you can skip this section.

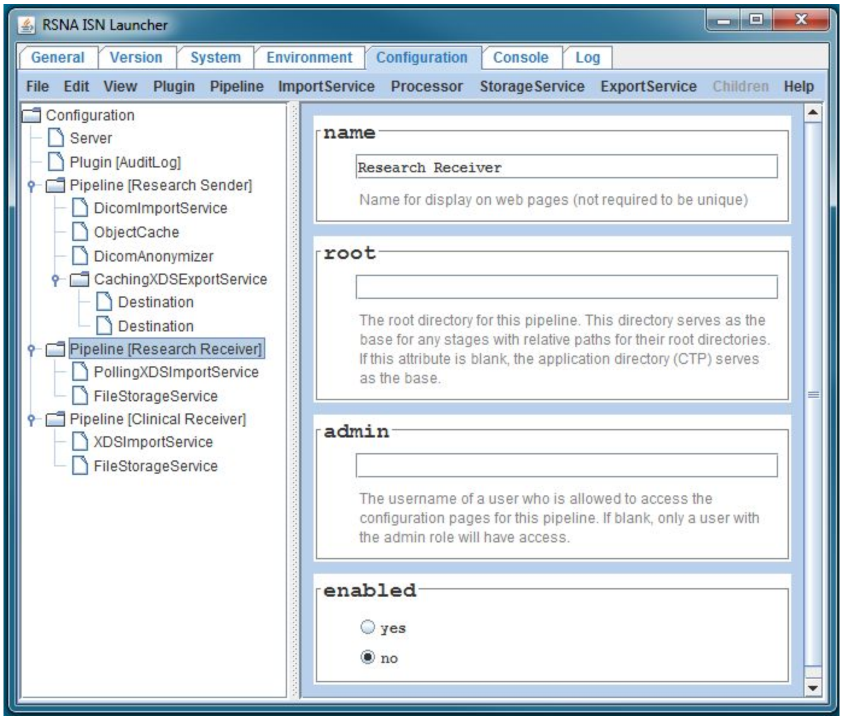
The Edge Server delegates certain image transmission and reception tasks to the CTP program. These are clinical study retrieval, research study transmission, and research study retrieval. Each task is implemented in a CTP pipeline. CTP and pipelines are described on the RSNA MIRC Wiki at http://mircwiki.rsna.org/index.php?title=CTP-The_RSNA_Clinical_Trial_Processor.

The pipelines are designed to be configurable using the Configuration Editor in the Launcher program, as described at http://mircwiki.rsna.org/index.php?title=The_CTP_Launcher_Configuration_Editor.

Pipelines that are not necessary for a specific site should be disabled to reduce both local processing and communication overhead. To disable a pipeline, start the Launcher.jar program using the command:

```
cd /usr/local/ctp/CTP/
java -jar Launcher.jar
```

In the GUI window, click the Configuration tab. In the left pane, click the pipeline to be enabled or disabled. The window will then look like this:



name

Research Receiver

Name for display on web pages (not required to be unique)

root

The root directory for this pipeline. This directory serves as the base for any stages with relative paths for their root directories. If this attribute is blank, the application directory (CTP) serves as the base.

admin

The username of a user who is allowed to access the configuration pages for this pipeline. If blank, only a user with the admin role will have access.

enabled

○ yes

● no

In the right pane, click the appropriate radio button in the **enabled** field, then type Ctrl-S or select Save in the File menu.

2.11.1 Clinical Study Transfer

Clinical study retrieval is performed by the Clinical Receiver Pipeline in the CTP program. As initially delivered, that pipeline receives the requested studies and stores them in a local directory tree. It provides access to the images via a webserver on port 1086.

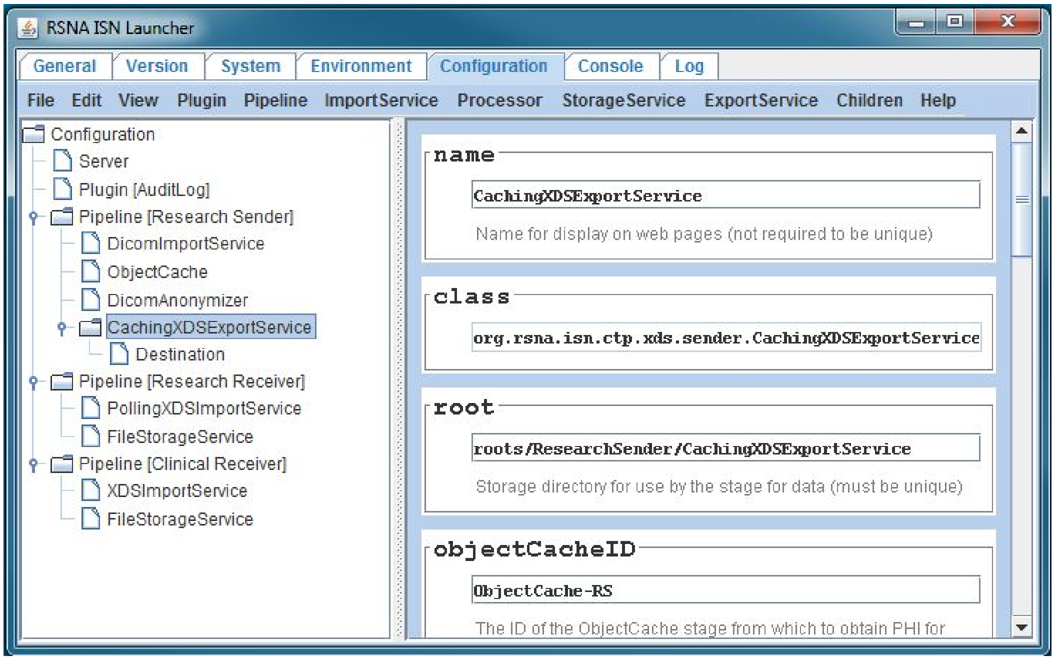
In a real clinical situation, it may be desirable to configure the pipeline to forward the images to a local DICOM workstation or a PACS. This is done by adding a DicomExportService at the end of the pipeline, using the Configuration Editor in the Launcher program.

2.11.2 Research Study Transmission

Research study transmission is performed by the Research Sender Pipeline in the CTP program.

To contribute de-identified studies to a research program at a destination site, the destination site must supply a text key that must be inserted into the configuration of the Research Sender Pipeline. The key must be communicated by some means outside the program (phone, email, etc.). Each key configured into the pipeline produces one entry in the destination drop-down list on the Send Studies pane.

As in the Clinical Study Transfer case, CTP configuration changes are best accomplished using the Configuration Editor in the Launcher.jar program. To add a destination, start the Launcher.jar program located in the CTP directory and click the Configuration tab. In the Research Sender Pipeline in the left pane, click the CachingXDSExportService line. The window will then look like this:



name: CachingXDSExportService

Name for display on web pages (not required to be unique)

class: org.rsna.isn.ctp.xds.sender.CachingXDSExportService

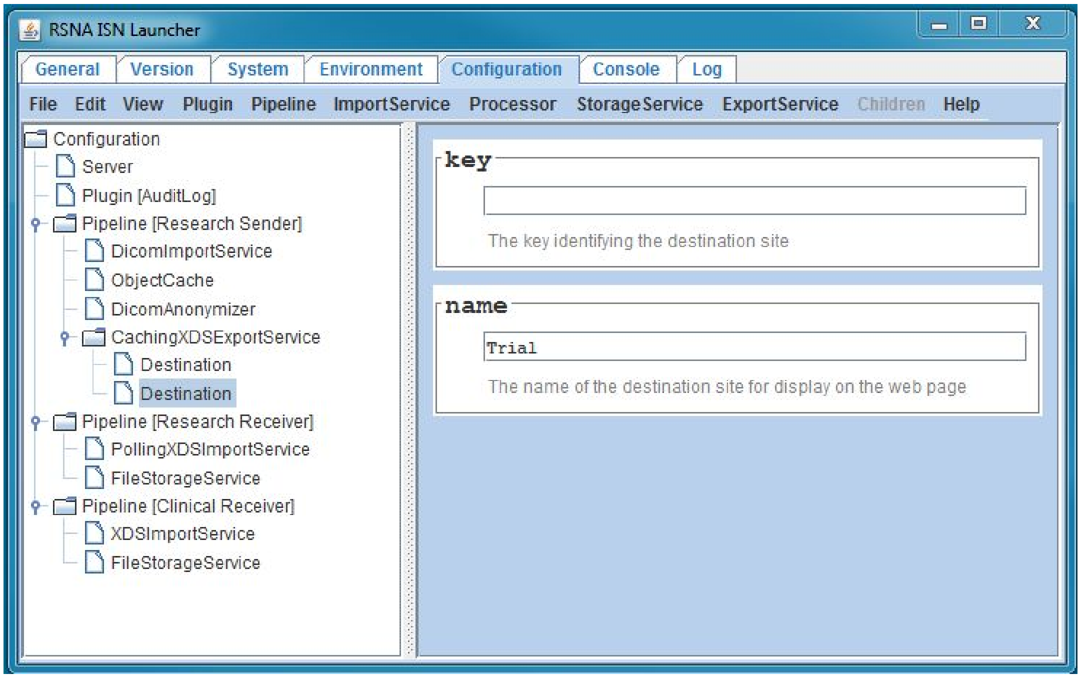
root: roots/ResearchSender/CachingXDSExportService

Storage directory for use by the stage for data (must be unique)

objectCacheID: ObjectCache-RS

The ID of the ObjectCache stage from which to obtain PHI for

To edit an existing destination, click its entry in the left pane. To add another destination, select Destination In the Children menu. The window will then look like this:



key:

The key identifying the destination site

name: Trial

The name of the destination site for display on the web page

Enter the key provided by the destination site in the key field and enter a meaningful name for the destination in the name field, then type Ctrl-S or select Save in the File menu. When CTP is started, the destination will be available.

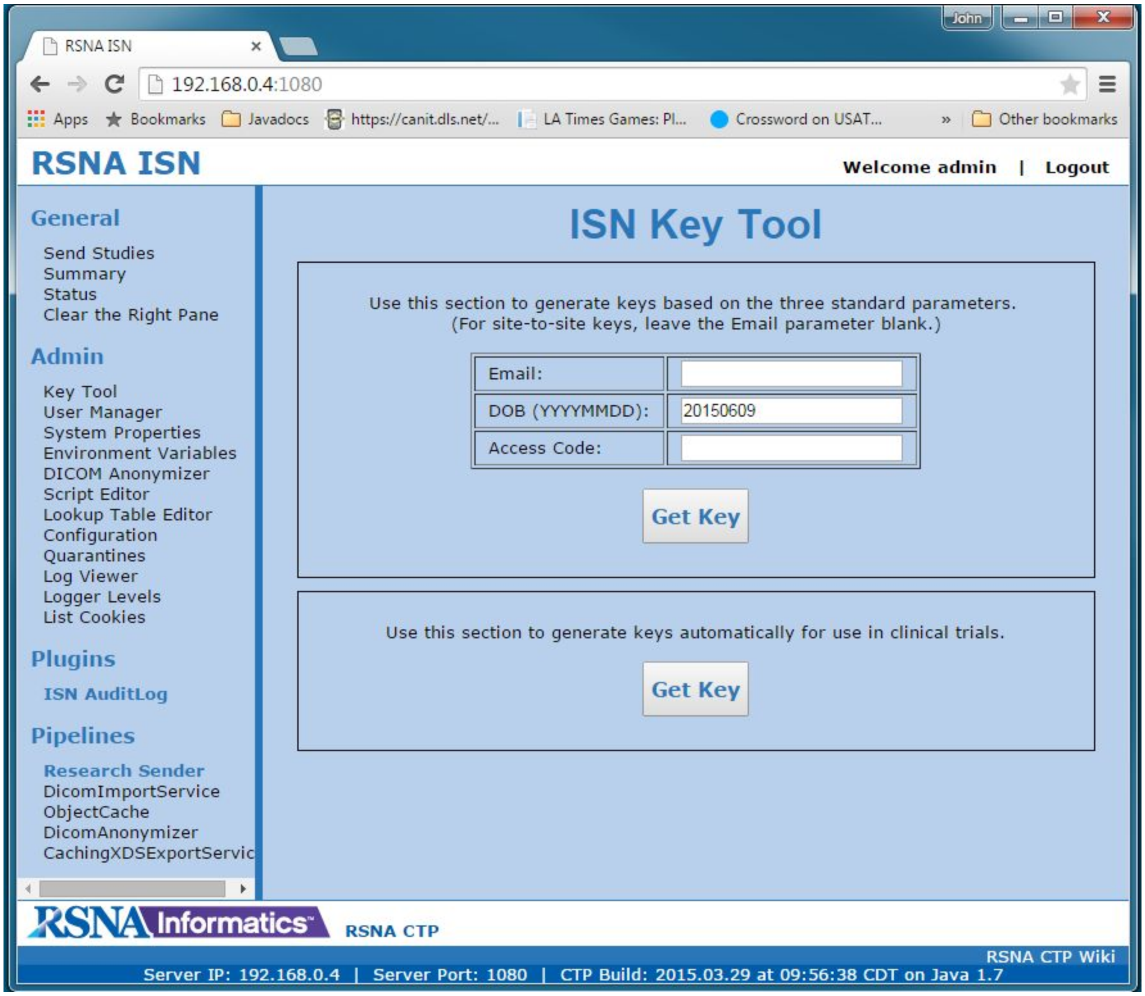
2.11.3 Research Study Retrieval

The receiving site in a research program is responsible for creating the key(s) used by the transmitting sites. There are two strategies, each with its own advantages and disadvantages:

- The simplest strategy is to create one key for the entire research program and provide that key to all the sites contributing studies. The principal advantage is that managing and configuring one key is easier than configuring many. The disadvantage is that every site in the program can see the contributions of all the contributors.

- A more secure strategy is to create a unique key for each contributing site. This makes the key management problem a little more complex, but it ensures that any contributing site can only see its own contributions.

To create keys, a user must be logged into the OpenAM management system and be a member of the Admin group. To access the Key Tool, go to the CTP home page on port 1080 and click the Key Tool link in the left pane. The window will then look like this:



ISN Key Tool

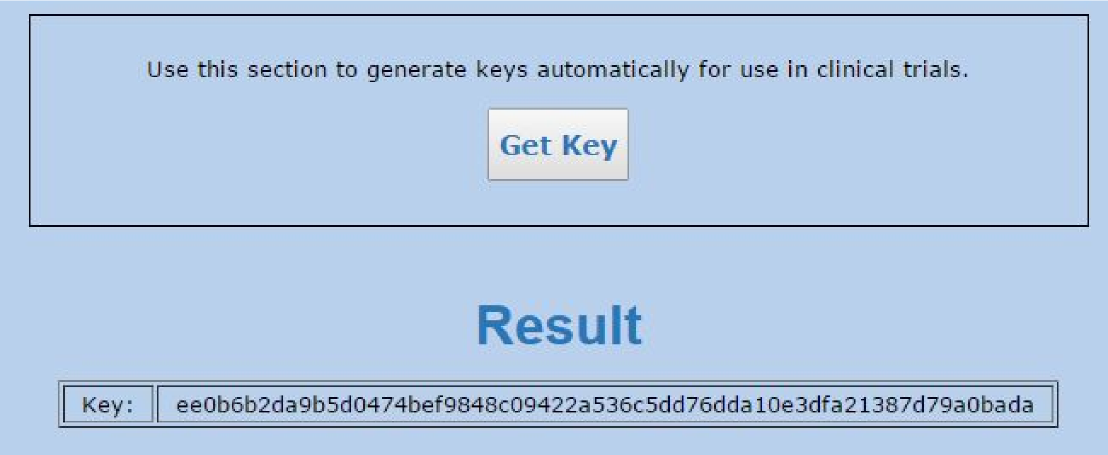
Use this section to generate keys based on the three standard parameters.
(For site-to-site keys, leave the Email parameter blank.)

Email:	
DOB (YYYYMMDD):	20150609
Access Code:	

Use this section to generate keys automatically for use in clinical trials.

Server IP: 192.168.0.4 | Server Port: 1080 | CTP Build: 2015.03.29 at 09:56:38 CDT on Java 1.7

Click the Get Key button in the lower box. A result field will then appear at the bottom of the right pane:



Use this section to generate keys automatically for use in clinical trials.

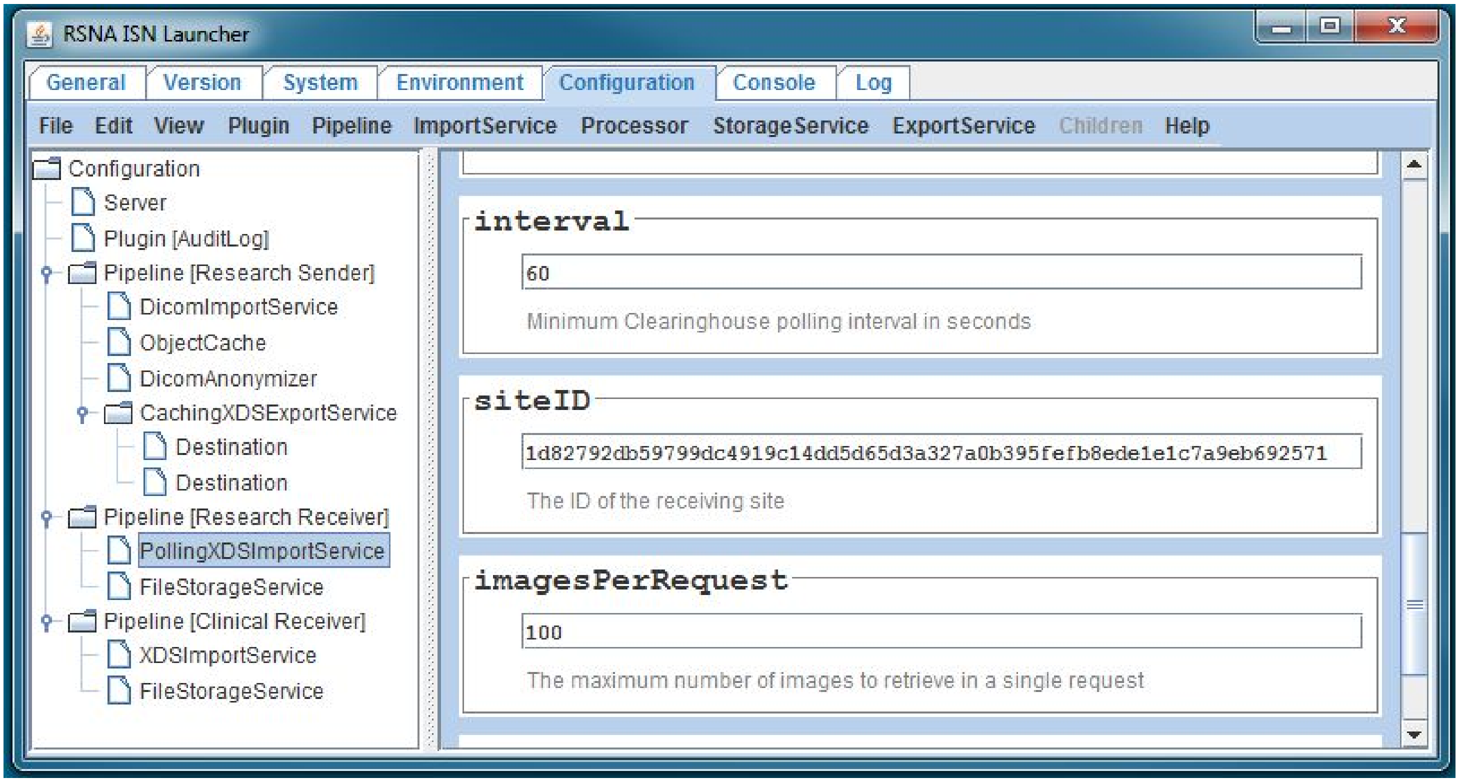
Result

Key: ee0b6b2da9b5d0474bef9848c09422a536c5dd76dda10e3dfa21387d79a0bada

Each time the Get Key button is clicked, a new key is generated. This may be copied and pasted into a record for later configuration work.

Each contributing site must be sent its key. The site will insert the key into its CTP configuration as described in the section above.

The receiving site must insert all the keys to be monitored into its CTP configuration. To do so, run the Launcher.jar application, click the Configuration tab, and click the PollingXDSImportService in the left pane. In the right pane, scroll down to the siteID field. The window will then look like this:



interval: 60
Minimum Clearinghouse polling interval in seconds

siteID: 1d82792db59799dc4919c14dd5d65d3a327a0b395fefb8ede1e1c7a9eb692571
The ID of the receiving site

imagesPerRequest: 100
The maximum number of images to retrieve in a single request

If there is only one key, enter it in the siteID field. If there are multiple keys, enter them all in the field, separated by spaces.

It may be convenient to add a DicomExportService to the Research Receiver Pipeline to forward the received images to a local workstation or PACS. This is done by adding a DicomExportService at the end of the pipeline, using the Configuration Editor in the Launcher.jar program.

In some situations, it may also be convenient to add an EmailService at the end of the pipeline to send an email to the administrator when studies are received. See http://mircwiki.rsna.org/index.php?title=Using_the_CTP_EmailService_Pipeline_Stage for details.

2.11.4 Using the CTP EmailService Pipeline Stage

This section describes how to configure the CTP EmailService pipeline stage to send emails when studies are processed. This function may be useful if your site will use the Edge Server to receive imaging data for use in clinical trials.

The EmailService is a processor stage. For each DicomObject it receives, it stores the identifier of the study (StudyInstanceUID) and the time the object was encountered. If no object is encountered for a study after 10 minutes, the stage considers the study to be complete, and it then sends an email to the recipients identified in the stage's configuration element.

The EmailService is only capable of sending to SMTP email servers.

Use the Configuration Editor in the Launcher program to configure the EmailService stage into a pipeline. See the article on the CTP Launcher Configuration Editor for details.

The emails sent by the stage contain the numbers of objects, series, and images in the study, plus any additional information specified by the **include**... attributes.

The placement of the pipeline stage in the pipeline determines whether the additional information will be PHI. To be specific, if the object received has not been de-identified, either before receipt by the pipeline or by a preceding anonymizer in the pipeline itself, then the values included in the emails will be PHI. This may be appropriate in some circumstances, but care must be taken because email transmission should not be considered to be secure.

The emails have the MIME type **multipart/alternative**, and include both HTML and plain text parts.

The script attribute can be used to select which studies are tracked by the EmailService stage. For details on the script language, see the article on the CTP DICOM Filter.

In the unusual situation where email notifications are to be sent to different destinations depending on the characteristics of the study, the best configuration is to include multiple EmailService stages in the pipe and use different scripts to select which EmailService stage will track which study type.

3. Upgrading Previous Releases of Edge Server to Release 4.0

The upgrade procedure from an existing Edge Server 3.x device to a 4.0 device requires more steps than can be accomplished with a single automated script. This section provides the instructions needed to execute the upgrade while maintaining existing data in the Edge Server.

3.1 Outline of the Upgrade Procedure

The Edge Server release 4.0 uses a different operating system (Centos 7) than prior versions (Ubuntu 12.4) and also different software packages. You will thus not be able to use the server or virtual machine running a previous version of the Edge Server to run this release. The 4.0 Edge Server software is distributed as a virtual machine (VM). Instructions in this guide will refer to that VM. Several steps in the process are described in the Installation section above.

1. Install the 4.0 Edge Server virtual machine. (See section 2.4 above.)
2. Login to the Unix accounts on the virtual machine and change the passwords. (Section 2.5 above and Appendix G)
3. Modify the network configuration for the virtual machine. (Section 2.6 above)
4. Copy the digital certificate from your existing system to the 4.0 VM. (Section 3.2)
5. Copy and test the configuration for MIRTH from your existing system to the 4.0 VM. (Section 3.3)
6. Suspend the HL7 feed to your existing 3.x system until the new system is operational.
    a. This step is typically performed at the RIS to disable the HL7 feed to the Edge Server. The instructions depend on the RIS.
7. Copy the Edge Server database (rsnadb) from your existing system to the 4.0 VM. (Section 3.4)
8. Update the configuration for user management. (Section 2.7)
9. Turn on the HL7 feed to your new system. That might mean changing the IP address of the new system to match your 3.x system, or you might configure the sending system to send to a different IP address.
    a. This step is performed at the RIS. The instructions to enable the new feed will depend on the RIS.

3.2 Copy Digital Certificate from Existing System

After you have completed installation of the VM, logged into the Unix accounts to change the passwords and modified the network configuration on the VM (see above), you will copy certificates from the 3.x server to 4.0. On the 3.x server, copy /usr/local/edge-server/conf/truststore.jks and /usr/local/edge-server/conf/keystore.jks to /usr/local/edge-server/conf on your 4.0 server. Verify the jks file ownership belongs to user edge.

If the owner is not edge, issues the following commands:

```
chown edge:edge /usr/local/edge-server/conf/keystore.jks
chown edge:edge /usr/local/edge-server/conf/truststore.jks
```

3.3 Transfer Mirth Configuration

The Edge Server uses two separate PostgreSQL databases. In this section, you will prepare the PostgreSQL database on the new virtual machine and copy over the configuration for the Mirth application. We leave the clinical data for Section 3.4.

The instructions below require you to execute Postgres commands from the command line. The instructions match the packaged 4.0 VM configuration. If you have modified the Postgres configuration file (i.e., pg_hba.conf), your command line syntax may differ slightly. See Appendix G for a discussion of security information and password management.

1. Stop the Mirth service on the 4.0 VM. Using root privileges, run the following command:
   ```
   systemctl stop mirthconnect
   ```
2. Copy over pg_hba.conf from your existing system to the 4.0 VM. This allows you maintain connections that you may have previously configured.
   a. In the 3.x VM, you should find the file in this folder: /etc/postgreql/8.4/main
   b. In the 4.0 VM, the file will be found in this folder: /data
3. Manually move any configuration options in postgresql.conf on the 3.x server to 4.0 VM. Do not overwrite the new 4.0 configuration file but add options individually in the postgresql.conf file on the 4.0 VM. The postgresql.conf file should be located in the same folder as the pg_hba.cof file (item 1).
   a. Restart the Postgresql database: `systemctl restart postgresql`
4. Extract the mirth database on the 3.x system using the rsna account (or other user account):
   ```
   pg_dump -U postgres -Fc -f mirthdb.sql mirthdb
   ```
5. Copy the file mirthdb.sql to the new system.
   a. Note that this file contains PHI. Follow your standard, internal procedures when copying these files between systems.
6. In the 4.0 VM, drop mirthdb and import the database from 3.x server; run these two steps using the rsna login:
   ```
   dropdb -U postgres mirthdb
   pg_restore -Fc --create -d postgres -U postgres mirthdb.sql
   ```
7. Copy the preconfigured Mirth configuration file to the conf directory. This will enable Mirth to use PostgreSQL instead of the default Derby database.
   ```
   cd /usr/local/mirthconnect
   sudo cp mirth.properties conf
   ```
8. Start the MIRTH service. Using root privileges, run the following command using root privileges:
   ```
   systemctl start mirthconnect
   ```
9. You can discard the mirthdb.sql file.

3.4 Transfer Clinical Data to New Virtual Machine

As part of the transfer defined in Section 3.3, you modified the PostgreSQL configuration to match your 3.x installation. This section provides instructions on copying the clinical data from the 3.x system to the 4.0 Edge Server.

The instructions below require you to execute Postgres commands from the command line. The instructions match the packaged 4.0 VM configuration. If you have modified the Postgres configuration file (i.e., pg_hba.conf), your command line syntax may differ slightly.

1. Stop the MIRTH service and the Torquebox service on the 4.0 VM. Using root privileges, run the following commands:
   ```
   systemctl stop edge-server
   systemctl stop mirthconnect
   systemctl stop torquebox
   ```
2. Extract the RSNA database on the 3.x system:
   ```
   pg_dump -U postgres -Fc -f rsnadb.sql rsnadb
   ```
3. Copy the file rsnadb.sql to the new system.
   a. Note that this file contains PHI. Follow your standard, internal procedures when copying these files between systems.
4. On 4.0 VM drop rsnadb; run this command using the rsna login account:
   ```
   dropdb -U postgres rsnadb
   ```
5. Restore the rsnadb database on the new system. *The follow command will generate an error stating “plpgsql already exists”. This can be ignored.*
   ```
   pg_restore -Fc --create -d postgres -U postgres rsnadb.sql
   ```
6. Update rsnadb schema to 4.0
   ```
   psql -U postgres -d rsnadb -f $RSNA_ROOT/db/RSNADB.rollout.v4.0.0.sql
   ```
7. Restart the services on the Edge Server. Using root privileges, run the following commands:
   ```
   systemctl start mirthconnect
   systemctl start torquebox
   systemctl start edge-server
   ```
8. Discard the rsnadb.sql file.

3.5 Migrate 3.x User Accounts

3.5.1 For User Accounts From a 3.2 System

Copy the $RSNA_ROOT/scripts/3.2-export-users.sh file from the 4.0 VM to the old 3.2 install.
Run the 3.2-export-users.sh script to export the users from the 3.2 system.

```
sudo -u edge ./3.2-export-users.sh
```

Copy the /tmp/user-export.ldif file to the 4.0 VM

Import the users. This MUST be done AFTER OpenAM is configured via the edge-config.sh script (see Section 2.7 of this document).

```
$RSNA_ROOT/scripts/user-import.sh user-export.ldif
```

3.5.2 For User Accounts Prior to Version 3.2

If 3.1 and earlier db-based user accounts need to be imported. After OpenAM is configured run:

```
sudo -u edge $RSNA_ROOT/scripts/enable-db-users.sh
```

4. Default Accounts

4.1 User and Postgres Accounts

The Edge Server operates on a Linux operating system. In addition to the `root` account, we use a normal user account for day-to-day operations. The VM is configured to use the account with username `rsna`.

The default accounts/password are listed below. You should change these passwords as part of installation:

`root`	**`JGK7@@ba$$Zbro`**
`rsna`	**`FT39bp#!@@Zcat`**

The PostgreSQL database uses three separate PostgreSQL roles that are not Linux accounts. The VM delivered by the RSNA has default passwords for these roles:

`postgres`	**`N3K647A`**
`mirth`	**`1947JAT$`**
`edge`	**`dl7bK4#M`**

These roles are used as follows:

- `postgres`: Superuser, owner of the database
- `mirth`: Role used by the Mirth server that provides HL7 interfaces
- `edge`: Role used by the Edge Server components

There are also two default user accounts for managing and using the Edge Server via the web interface. During installation, you can set your own password for the `amAdmin` login:

`amAdmin`	**`<password set when the edge-config.sh script is run>`**
`admin`	**`password`**

Section 4.1 provides information on logging into components of the VM.

More details on the various types of accounts used by the Edge Server around found in Appendix G of this document. We recommend you read Appendix G for additional security information and instructions on changing passwords. We recommend that you change the passwords for all accounts that are listed here and in Appendix G.

Section 5.1 describes account management on the Edge Server interface in detail.

5. Edge Server Administration Using the Web User Interface

The Edge Server's Web user interface provides both clinical and administrative functions. It is used to set up the DICOM devices that the Edge Server will use as sources for clinical studies, it is used to create and manage users, and it is used to create and track studies that are sent for clinical purposes.

Configuration is done via a web browser which can be local to the Edge Server or remote. Currently the supported browser versions are:

a) Mozilla Firefox >= 3.5
b) Google Chrome >= 35.0
c) Microsoft Internet Explorer >= 9.0
d) Apple Safari >= 7.0

5.2 Administrative login

Hit the light blue `Log Out` button on the top right corner of the OpenAM interface to log out and resume normal Edge Server functionality. The logout page will present a return link in green titled `Return to Login page` which you can click. This will take you to the login page and you can enter the following credentials:

- Username: `admin`
- Password: `password`

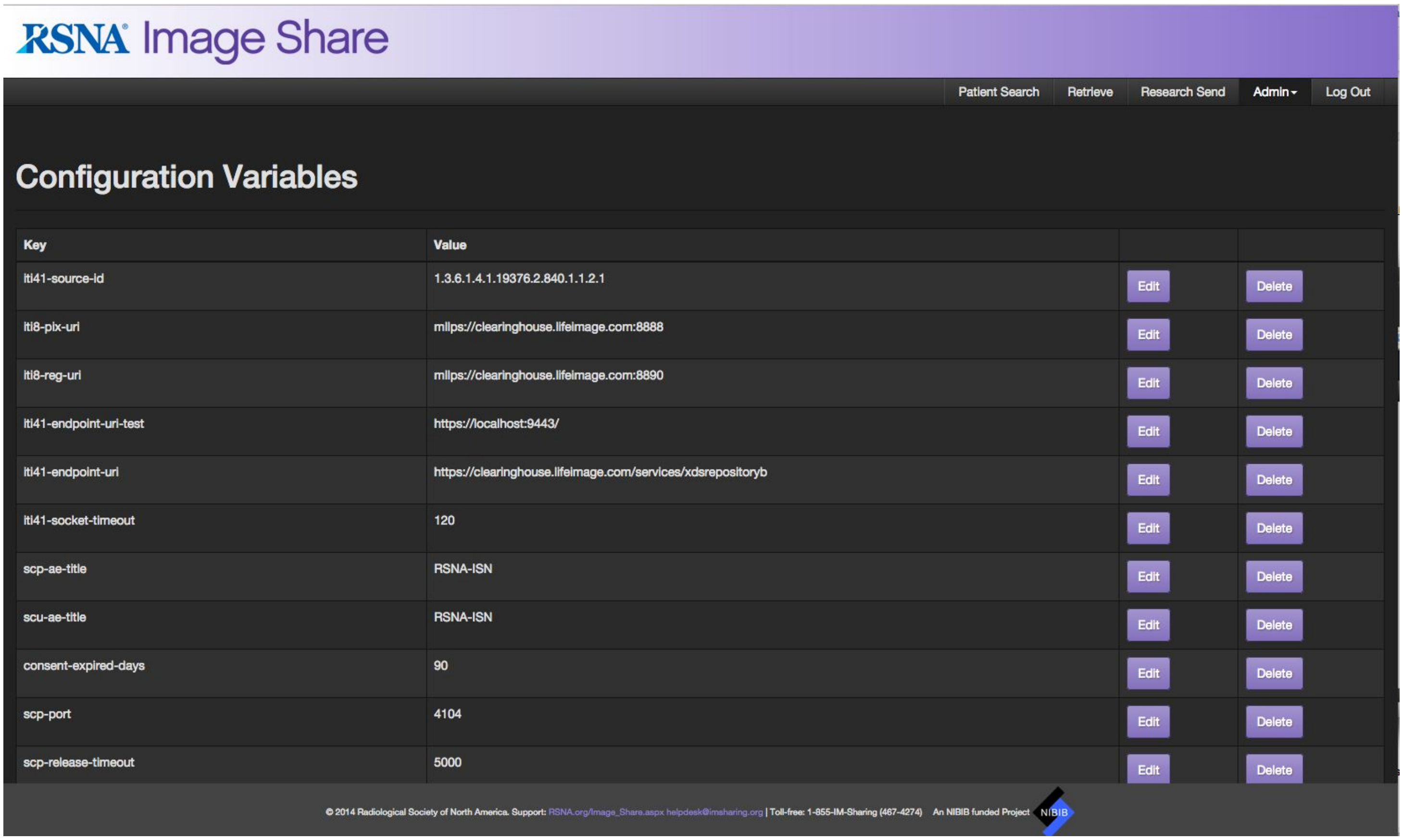
This is the default admin account (role of Admin), and will allow you to edit the system configuration.

5.3 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 "Admin" menu and then "Configuration" (Figure 5-9). Variables that should be set by each site are "site_id" and "help_desk_message" variables.

- "site_id is the name of your site as it will appear in printouts and emails to patients. When the software is installed, there is a variable in the configuration database with the value "TBD". Use the Administration configuration page to change the value of this variable.
- The default message for "help_desk_message" is: "Please contact helpdesk@imsharing.org or call 1-855-IM-SHARING (467-4274) for support". This value will appear on the printout given to patients. If you would prefer to have a different message, you will need to use the Add New Configuration Variable button to add the variable **help_desk_message** with the appropriate message.
- The system has a delay of 72 hours after the report is signed before images are sent to the Clearinghouse. This is designed to provide time for consultation between the radiologist and ordering physician. If you wish to change the default value, use the Administration configuration page to add the variable **delay_in_hours** with an appropriate delay (as measured in hours, whole numbers only).

- consent-expired-days: Number of days patient consent expires. A patient consent notification will display after expiration. Default value is 90.
- fail-on-incomplete-study: Fail transfers that retrieve fewer images than expected from a DICOM device. Default value is false.
- max-retries: Number of times jobs to be retried before it fails. Default value is 10.
- retrieve-timeout-in-secs: The time to wait for images to be transferred. After the timeout expires the job will be considered complete. Default value is 600.
- retry-delay-in-mins: Time in minutes in between each job retry. Default is 10.
- assume_last_name_first: Unused settings for future search feature.



Configuration Variables

Key	Value		
iti41-source-id	1.3.6.1.4.1.19376.2.840.1.1.2.1	Edit	Delete
iti8-pix-uri	mllps://clearinghouse.lifeimage.com:8888	Edit	Delete
iti8-reg-uri	mllps://clearinghouse.lifeimage.com:8890	Edit	Delete
iti41-endpoint-uri-test	https://localhost:9443/	Edit	Delete
iti41-endpoint-uri	https://clearinghouse.lifeimage.com/services/xdsrepositoryb	Edit	Delete
iti41-socket-timeout	120	Edit	Delete
scp-ae-title	RSNA-ISN	Edit	Delete
scu-ae-title	RSNA-ISN	Edit	Delete
consent-expired-days	90	Edit	Delete
scp-port	4104	Edit	Delete
scp-release-timeout	5000	Edit	Delete

© 2014 Radiological Society of North America. Support: RSNA.org/Image_Share.aspx helpdesk@imsharing.org | Toll-free: 1-855-IM-Sharing (467-4274)   An NIBIB funded Project NIBIB

```
    1.2.840.10008.5.1.4.1.1.2 = 1.2.840.10008.1.2, 1.2.840.10008.1.2.1
```

The default list of present contexts are listed in Appendix I (Extended DICOM Configuration).

After making any changes, you will need to restart the Edge Server by running `sudo restart edge-server` from the command line.

5.3.1 Clearinghouse Configuration Variables

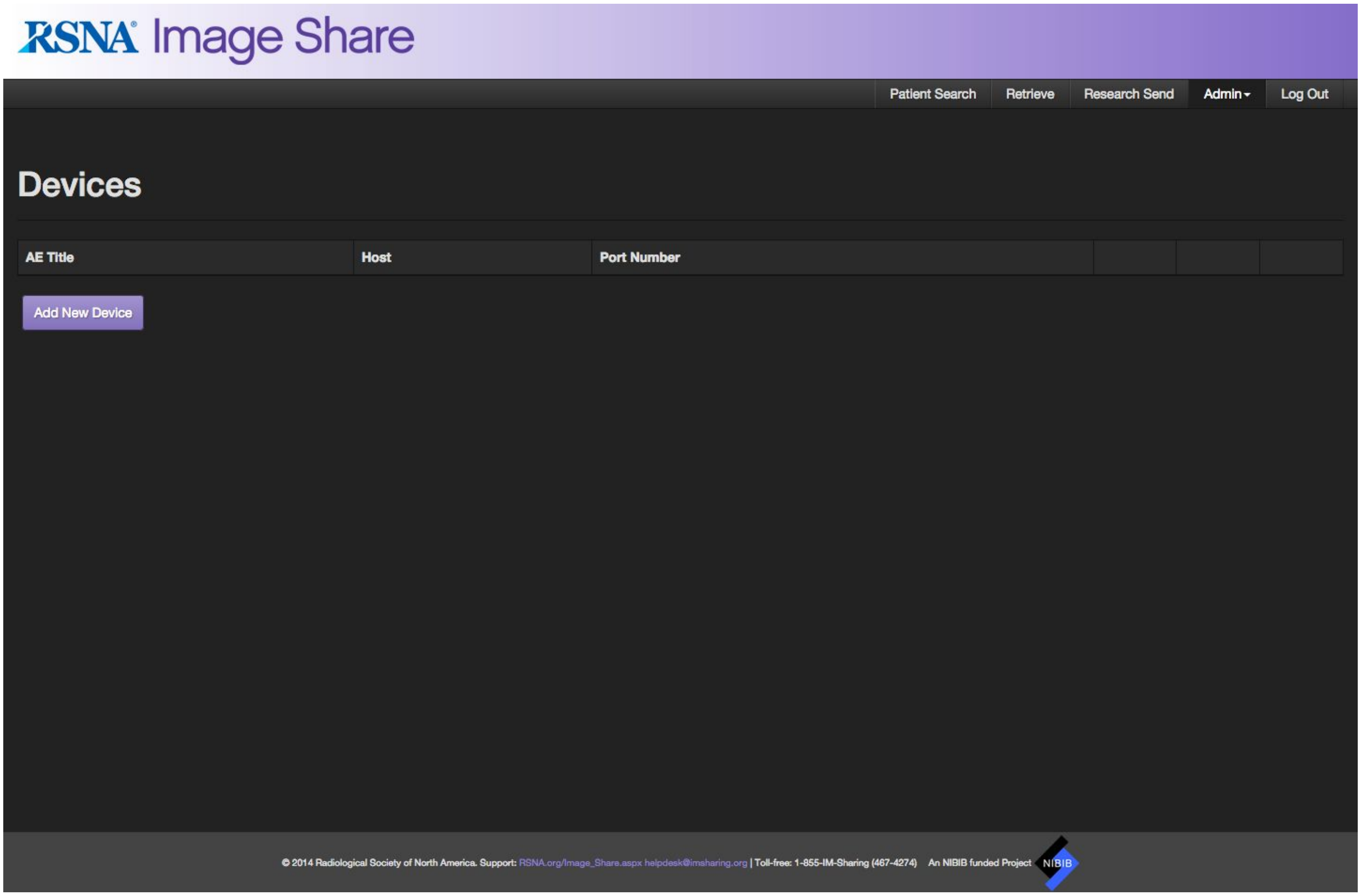
The following variables are required to ensure connectivity between the Edge Server and the Clearinghouse:

- iti41-endpoint-uri: URI endpoint for Provide and Register Set-b transaction. Default value is https://clearinghouse.lifeimage.com/services/xdsrepositoryb.
- iti41-endpoint-uri-test: Test endpoint for Provide and Register Set-b transaction.
- iti8-pix-uri: The URI of the PIX Manager being accessed. Default value is mllps://clearinghouse.lifeimage.com:8888.

- iti8-reg-uri: The URI of the registry being accessed.Default value is mllps://clearinghouse.lifeimage.com:8890.

5.3.2 DICOM Device Configuration

Click the `Admin` button in the top right corner, then click `Devices` on the menu to configure information about the DICOM device (Figure 5-10). Additional devices may be added. If a study is not found the next device will be queried.



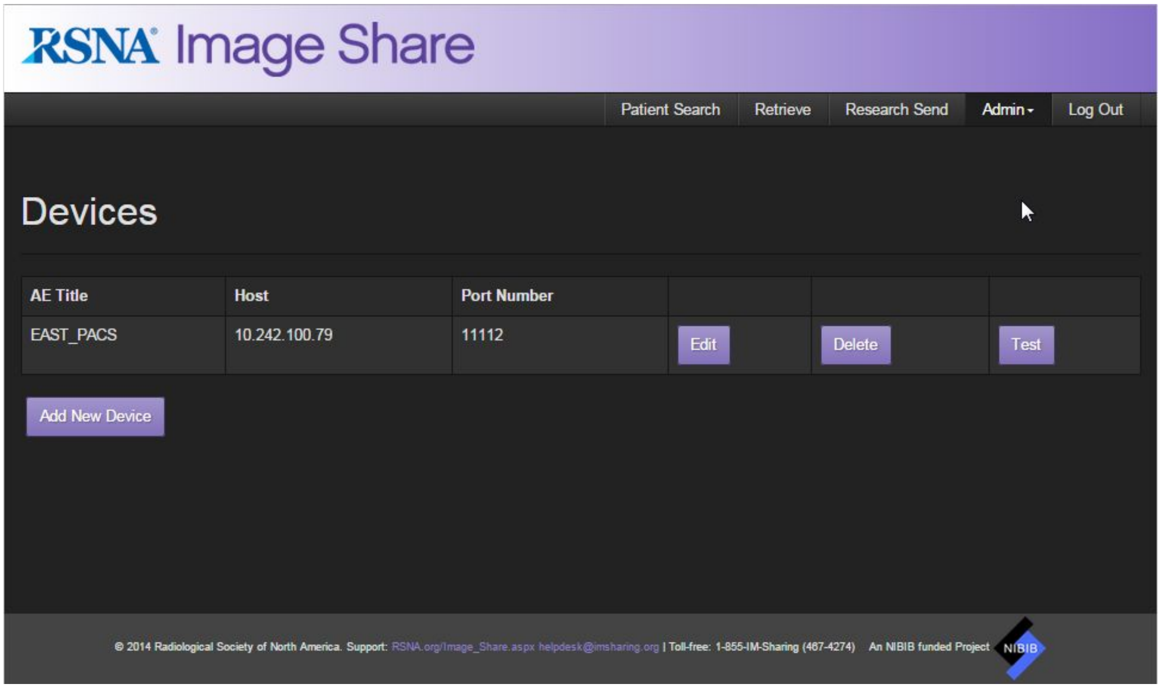
Devices

AE Title	Host	Port Number			

© 2014 Radiological Society of North America. Support: RSNA.org/Image_Share.aspx helpdesk@imsharing.org | Toll-free: 1-855-IM-Sharing (467-4274) An NIBIB funded Project

Figure 5-10: DICOM Device Configuration

Once a device is added a `Test` button will appear (Figure 5-11). To test connectivity to PACS devices, click `Test` button.



Devices

AE Title	Host	Port Number			
EAST_PACS	10.242.100.79	11112	Edit	Delete	Test

© 2014 Radiological Society of North America. Support: RSNA.org/Image_Share.aspx helpdesk@imsharing.org | Toll-free: 1-855-IM-Sharing (467-4274) An NIBIB funded Project

Figure 5-11: Test connection for devices

5.3.3 DICOM Connectivity 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. The default value is RSNA-ISN.
- scp-ae-title: The AE title of the Edge Server's SCP. Used to handle C-STORE requests from your institution's PACS. The default value is RSNA-ISN.
- scp-port: The TCP/IP port to use for the Edge Server's SCP. The default value is 4104. Note: values under 1024 are not permitted.

These additional variables are available for debugging and performance tuning:

- 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.
- scp-idle-timeout: The maximum time in milliseconds that an association may remain idle. Default value is 60000.

For more information on these setting please consult the DCM4CHE2 toolkit documentation:

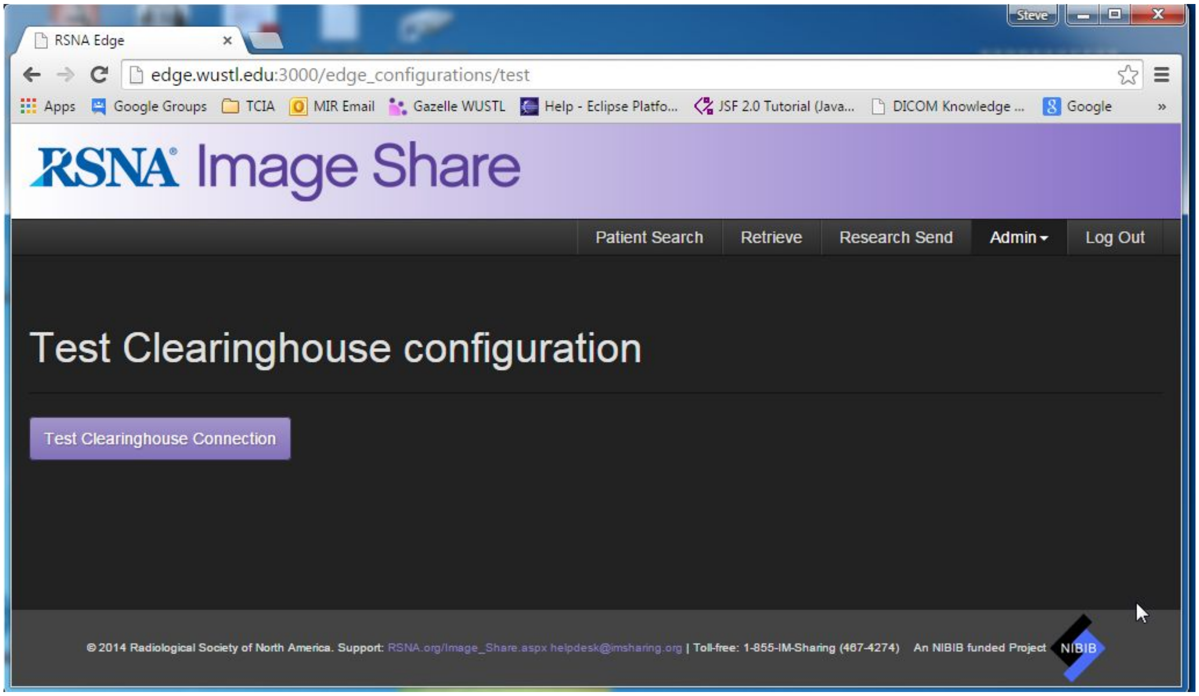
http://www.dcm4che.org/confluence/display/d2/dcm4che2+DICOM+Toolkit

The DICOM presentation contexts supported by the SCP during association negotiation are specified in a properties file located at: `$RSNA_ROOT/conf/scp.properties`. This file conforms to the Java properties file syntax and is automatically generated when the SCP is first run. Each key in the properties file represents a SOP class UID and each value is a comma separated list of transfer syntax UIDs. For example, to enable support for receiving CT images in either LEI or LEE format, the following line would need to appear in the properties file:conversion methods, which are beyond the scope of this document.

5.3.4 Testing Clearinghouse connectivity

Once all the configuration changes have been made and the Edge Server restarted, you should test connectivity to the Clearinghouse.

To test connectivity to the Clearinghouse, navigate to “Test Configuration” under the Admin tab. Click on “Test Clearinghouse connection” (Figure 5-12).



Test Clearinghouse configuration

© 2014 Radiological Society of North America. Support: RSNA.org/Image_Share.aspx helpdesk@imsharing.org | Toll-free: 1-855-IM-Sharing (467-4274) An NIBIB funded Project

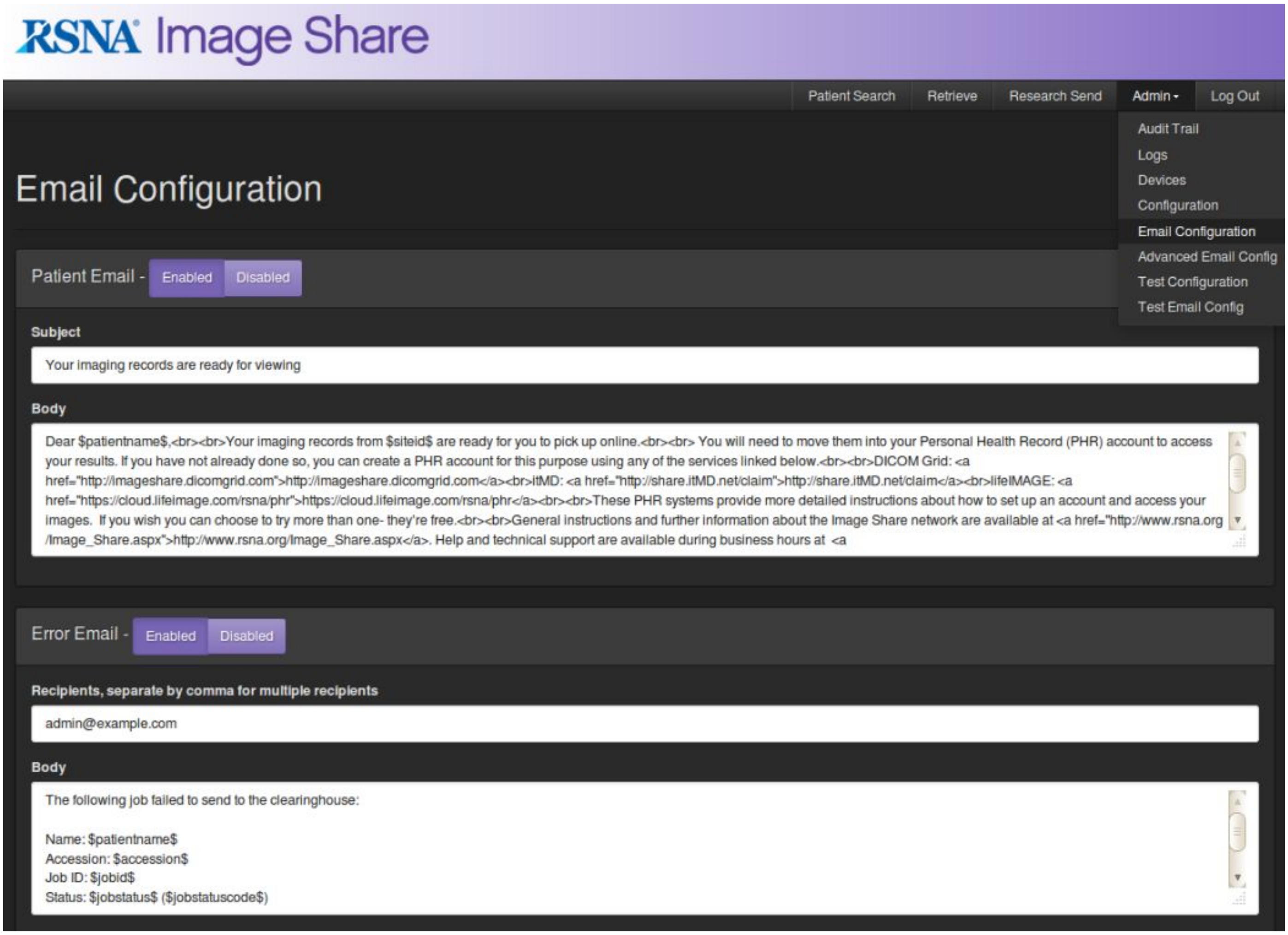
Figure 5-12: Test Clearinghouse connection

5.3.5 Email configuration

The RSNA Edge Server can be configured to send two types of notification emails:

a) Patient notification emails are sent when the job set has been completed and submitted to the clearinghouse.
b) Administrative emails notify an administrative contact when transfer issues occur.

To enable these email notifications, first select Email Configuration from the Admin drop down. Then, click the appropriate "Enabled" control button for Patient Email and/or Error Email. Email(s) in the recipient field are required if "Error Email" is enabled. To send to multiple recipients, separate the emails with a comma (Figure 5-13).



Email Configuration

Subject

Your imaging records are ready for viewing

Body

```
Dear $patientname$,<br><br>Your imaging records from $siteid$ are ready for you to pick up online.<br><br> You will need to move them into your Personal Health Record (PHR) account to access your results. If you have not already done so, you can create a PHR account for this purpose using any of the services linked below.<br><br>DICOM Grid: <a href="http://imageshare.dicomgrid.com">http://imageshare.dicomgrid.com</a><br>itMD: <a href="http://share.itMD.net/claim">http://share.itMD.net/claim</a><br>lifeIMAGE: <a href="https://cloud.lifeimage.com/rsna/phr">https://cloud.lifeimage.com/rsna/phr</a><br><br>These PHR systems provide more detailed instructions about how to set up an account and access your images.  If you wish you can choose to try more than one- they're free.<br><br>General instructions and further information about the Image Share network are available at <a href="http://www.rsna.org/Image_Share.aspx">http://www.rsna.org/Image_Share.aspx</a>. Help and technical support are available during business hours at  <a
```

Recipients, separate by comma for multiple recipients

admin@example.com

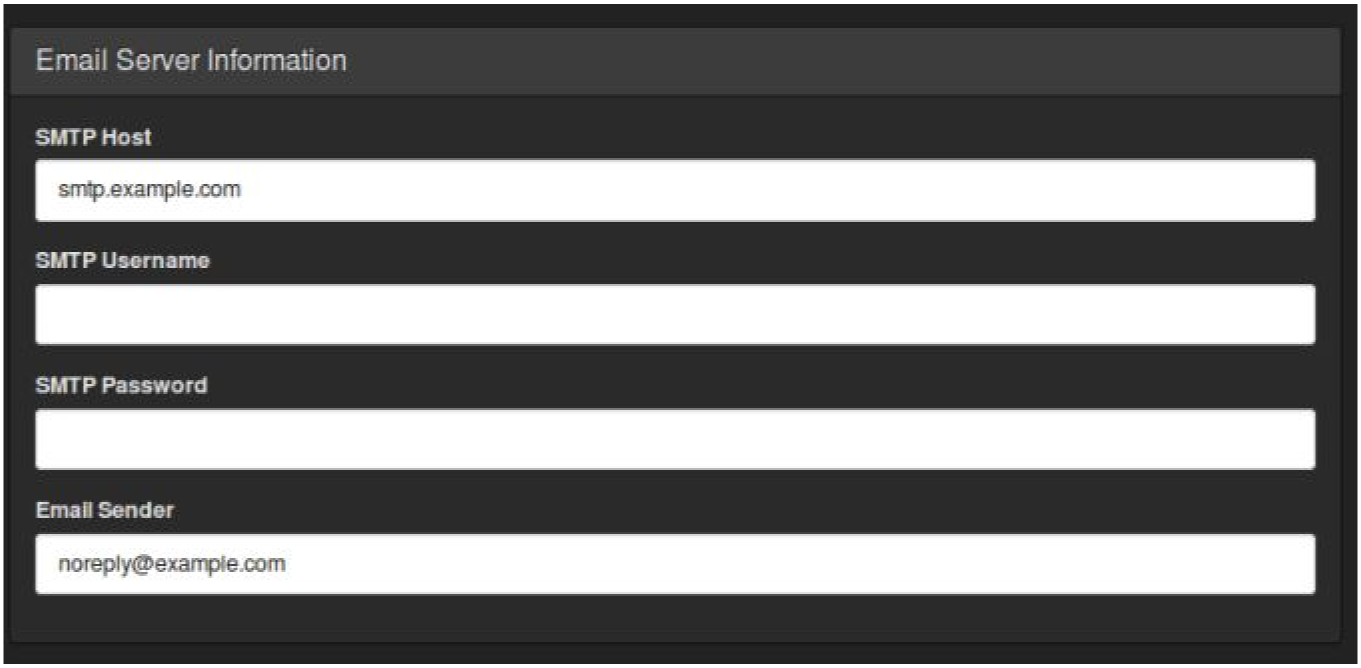
Body

```
The following job failed to send to the clearinghouse:

Name: $patientname$
Accession: $accession$
Job ID: $jobid$
Status: $jobstatus$ ($jobstatuscode$)
```

Figure 5-13: Enabling email

The default configuration is setup to use your institution's relay server. This method is the most common and recommended; however, other email services are supported. The follow section describes how to setup email using a relay server. For advanced setup, refer to section 5.3.6.

- Under the section "Email Server Information" on the Email Configuration page, enter your SMTP Host and Email Sender information. SMTP Username and SMTP Password are used in advanced setup.
- SMTP Host - The mail relay server
- Email Sender - Shows up as the "from" address on outbound email



Email Server Information

SMTP Host

smtp.example.com

SMTP Username

SMTP Password

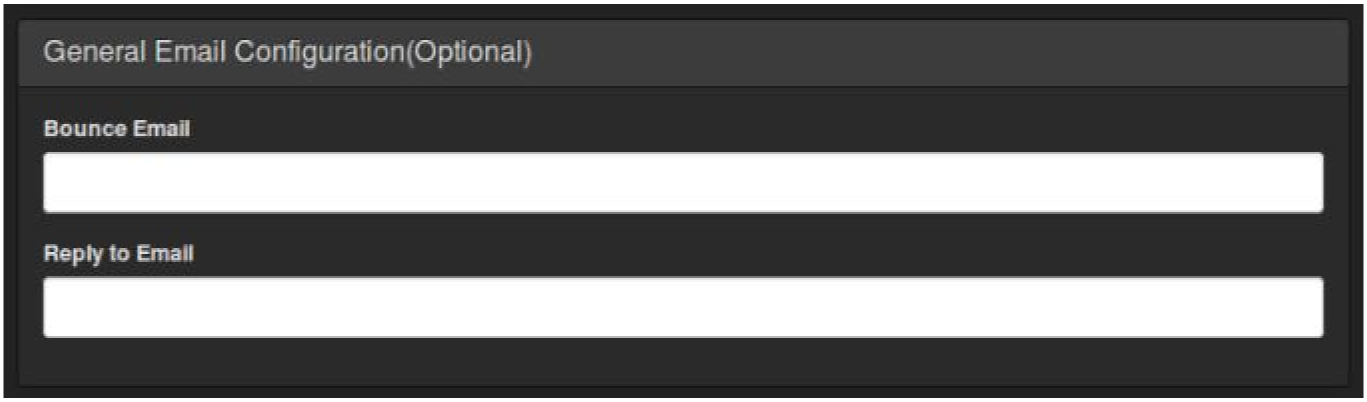
Email Sender

noreply@example.com

Figure 5-14: Email Configuration

The “General Email Configuration” section contains optional fields.

- Bounce Email - Email address to receive notification that the message can not be delivered.
- Reply To Email - Becomes the “reply to” field in outbound email



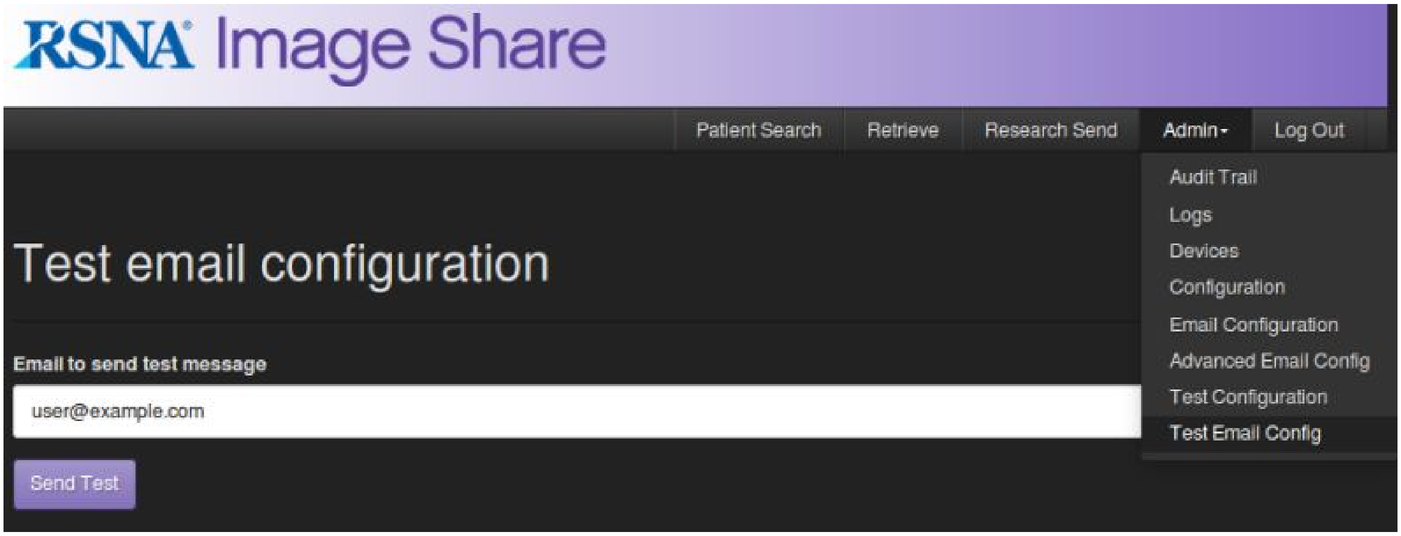
General Email Configuration(Optional)

Bounce Email

Reply to Email

Figure 5-15: General Email Configuration

After you have saved your configuration setting, you should verify has been setup correctly. To perform an email test, Click on “Test Email Config” under the Admin tab. Submit a test email by entering an email address and clicking the “Send Test” button.



Test email configuration

Email to send test message: user@example.com

Figure 5-16: Email Testing

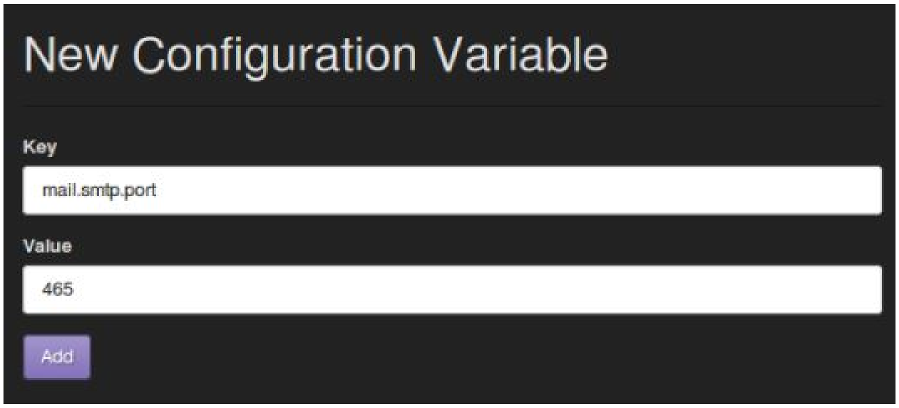
5.3.6 Advanced Email Configuration

The Edge email feature is built off the JavaMail API and uses the same property variables. Consult the JavaMail documentation for a detailed list of supported configuration options.

https://javamail.java.net/nonav/docs/api/com/sun/mail/smtp/package-summary.html

To add configuration variables, click on "Advanced Email Config" under the Admin tab. Next click on "Add New Configuration Variable" on the bottom on the page. Enter the key and value appropriate for your email server. Then click "Add". **Please note that if a key is not part of JavaMail API or mistyped it will not work.**

+



New Configuration Variable

Key: mail.smtp.port

Value: 465

Figure 5-17: Adding new configuration variables

As an example, to setup email for Exchange, you would add variables listed in Figure 5-18. to the Advanced Email Config page.

Variable	Values
username	myUsername
password	myPassword

`mail.smtp.from`	user@example.com
`mail.smtp.host`	mail.example.com
`mail.smtp.port`	465
`mail.smtp.ssl.enable`	true
`mail.smtp.auth`	true
`mail.smtp.auth.mechanisms`	ntlm
`mail.smtp.auth.ntlm.domain`	DOMAIN

Figure 5-18: Example of configuration variables for setting up Exchange with Authentication

5.3.7 Email Templates

Patient and administrative email notifications can be customized in the email configuration page. The body of the email body supports HTML or plain text. The content type is automatically detected; for example, if HTML tags are detected, carriage returns are ignored and <BR> tags should be used instead.

Emails are sent as multipart MIME messages that include both HTML and plain text parts.

A number of variables are supported for use within the email body. Email variables are denoted by a string starting and ending with a dollar sign.

Supported email variables

Variable	Description
`$patientname$`	Full name of the patient
`$accession$`	Accession Number
`$jobid$`	Referring ID for Job
`$errormsg$`	Supported in administrative template only. Returns error message.
`$jobstatus$`	Job Status
`$jobstatuscode$`	Reference code for Job status
`$site_id$`	Name of your site. User defined in Section 5.3

Figure 5-19: Description of email variables

5.3.8 Utilization Reporting

To help us improve and better understand how the network is being utilized, there is the option to enable the transmission of aggregate usage statistics to RSNA. The following statistics are transmitted (**Please note that no ePHI is ever sent**):

1. Name of your site (Via site_id variable. See Section 9.3)
2. Number of patients consented.
3. Number of exams sent to the lifeIMAGE ClearingHouse
4. Number of patients sent to the lifeIMAGE ClearingHouse

By default this feature is turned off; however, if you would like to participate, you will need to do the following:

1. Under the Admin->Configuration tab, change the `submit-stats` variable to ‘true’.
2. Copy the file `gdoc.properties` to your `conf` directory (`/usr/local/edge-server/conf`)
   a. Change the owner of the file to the edge account:
      `sudo chown edge:edge /usr/local/edge-server/conf/gdoc.properties`
3. Install cron job from the command line by running the following command:

```
sudo /usr/local/edge-server/scripts/utilization-report.sh --install
```

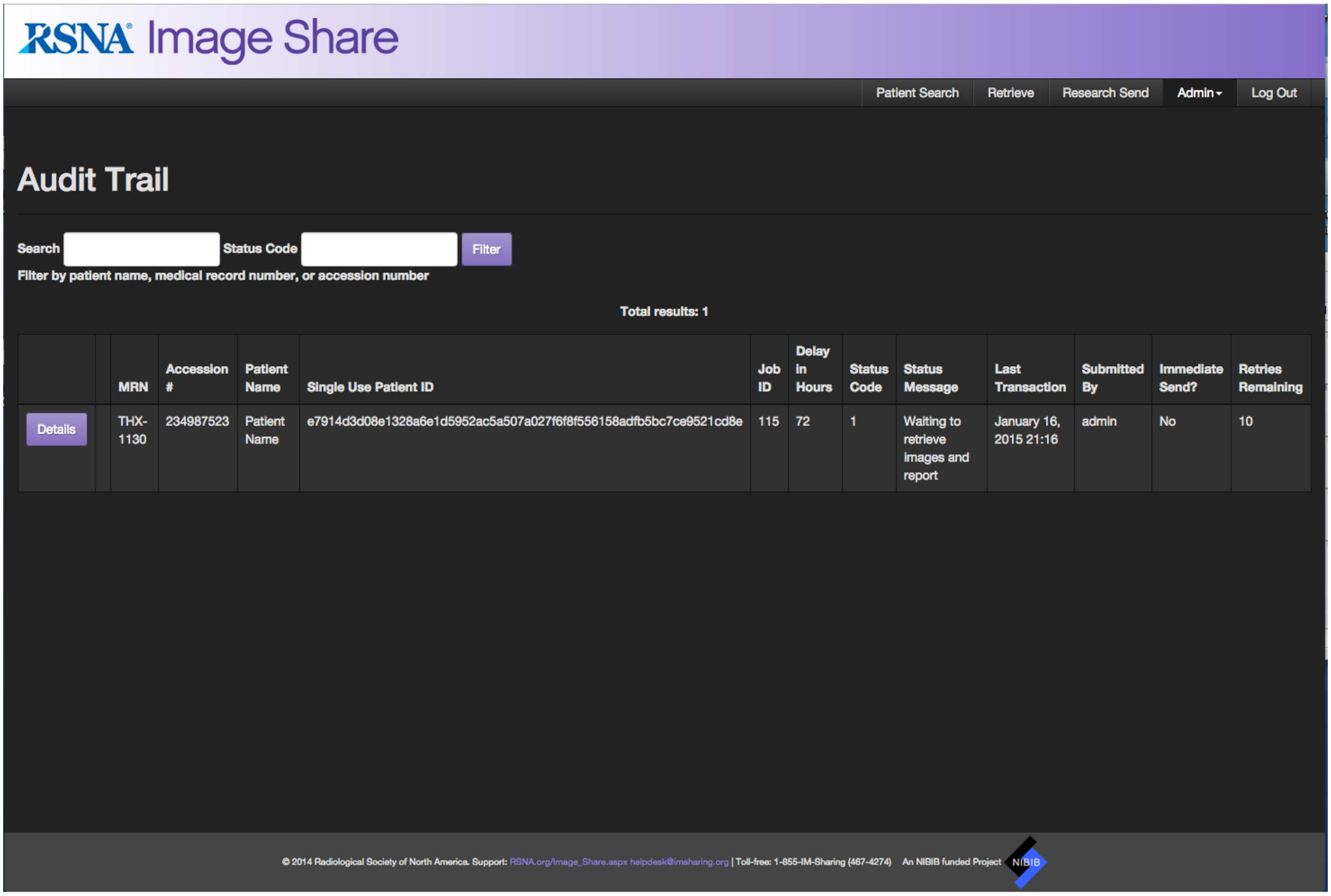
4. Allow outbound connection from the ImageShare server to IP: **192.203.117.40** and Port: **3128**
5. Contact Celeste Garcia (celeste_g@msn.com) to register the external IP address of your ImageShare server with the RNSA proxy server.
6. Test connectivity by running the following command:

```
sudo /usr/local/edge-server/scripts/utilization-report.sh --test
```

The data is transferred and is sent through a TLS connection. Your server will automatically transmit the utilization report every Sunday at midnight.

5.4 Administrative Overview

The Administrative interface also provides audit and application log views by clicking the `Audit Trail` and `Logs` buttons (Figure 5-20).



Audit Trail

Search Status Code Filter

Filter by patient name, medical record number, or accession number

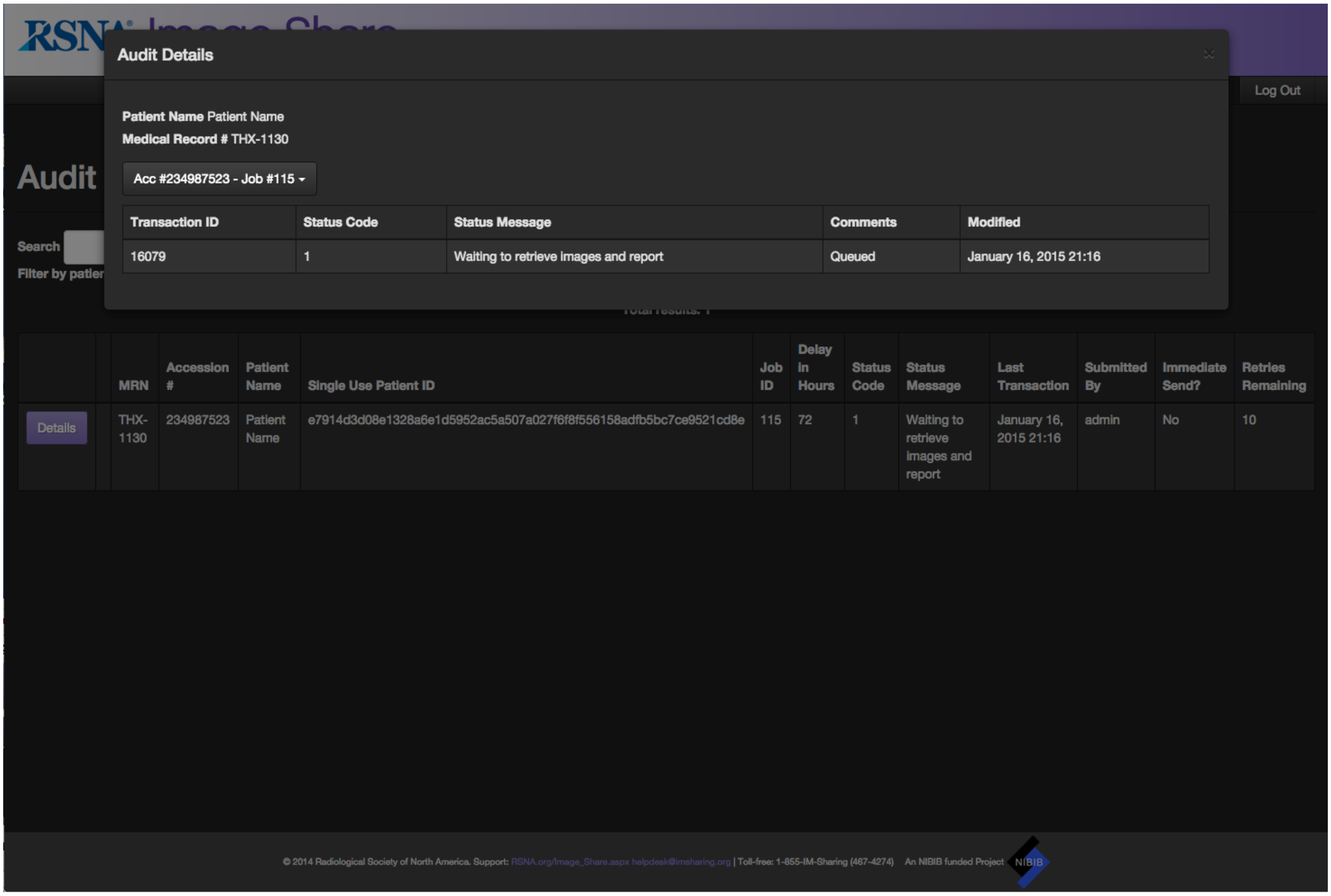
Total results: 1

		MRN	Accession #	Patient Name	Single Use Patient ID	Job ID	Delay in Hours	Status Code	Status Message	Last Transaction	Submitted By	Immediate Send?	Retries Remaining
Details		THX-1130	234987523	Patient Name	e7914d3d08e1328a6e1d5952ac5a507a027f6f8f556158adfb5bc7ce9521cd8e	115	72	1	Waiting to retrieve images and report	January 16, 2015 21:16	admin	No	10

© 2014 Radiological Society of North America. Support: RSNA.org/Image_Share.aspx helpdesk@imsharing.org | Toll-free: 1-855-IM-Sharing (467-4274) An NIBIB funded Project

Figure 5-20: Audit Trail Interface

If a job has failed (indicated by status code < 0), a `Retry Job` button will appear on the Audit Details modal dialog. 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 5-21).



Audit Details

Patient Name Patient Name
Medical Record # THX-1130

Acc #234987523 - Job #115

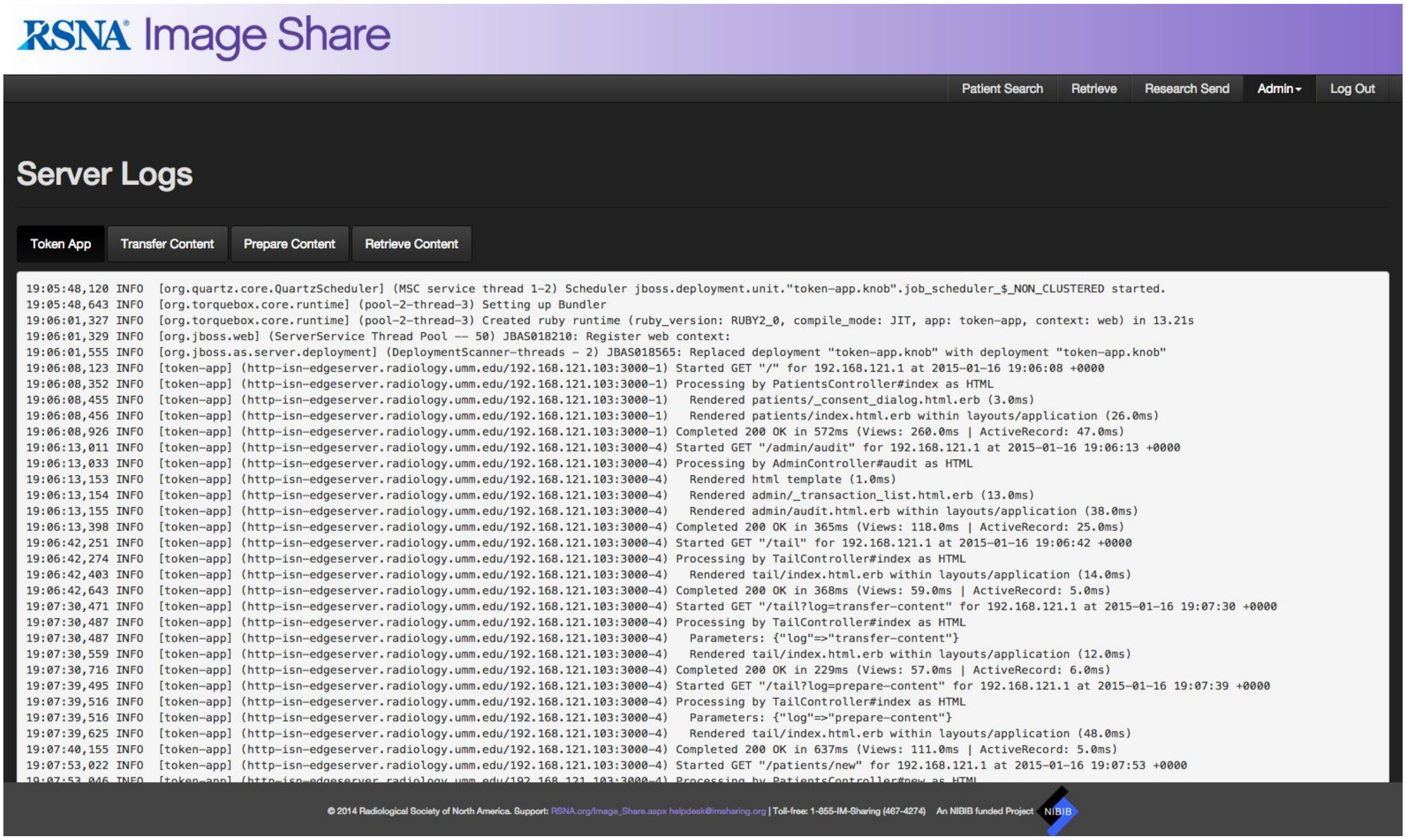
Transaction ID	Status Code	Status Message	Comments	Modified
16079	1	Waiting to retrieve images and report	Queued	January 16, 2015 21:16

		MRN	Accession #	Patient Name	Single Use Patient ID	Job ID	Delay in Hours	Status Code	Status Message	Last Transaction	Submitted By	Immediate Send?	Retries Remaining
Details		THX-1130	234987523	Patient Name	e7914d3d08e1328a6e1d5952ac5a507a027f6f8f556158adfb5bc7ce9521cd8e	115	72	1	Waiting to retrieve images and report	January 16, 2015 21:16	admin	No	10

© 2014 Radiological Society of North America. Support: RSNA.org/Image_Share.aspx helpdesk@imsharing.org | Toll-free: 1-855-IM-Sharing (467-4274) An NIBIB funded Project

Figure 5-21: Job Details / Retry Failed Jobs Interface

Application logs are available under the `Logs` link and show detailed application information per service that runs on the Edge server (Figure 5-22). These are useful for troubleshooting and viewing more detailed information than the summaries provided by the Job Details view (Figure 5-21).



Server Logs

```
19:05:48,120 INFO  [org.quartz.core.QuartzScheduler] (MSC service thread 1-2) Scheduler jboss.deployment.unit."token-app.knob".job_scheduler_$_NON_CLUSTERED started.
19:05:48,643 INFO  [org.torquebox.core.runtime] (pool-2-thread-3) Setting up Bundler
19:06:01,327 INFO  [org.torquebox.core.runtime] (pool-2-thread-3) Created ruby runtime (ruby_version: RUBY2_0, compile_mode: JIT, app: token-app, context: web) in 13.21s
19:06:01,329 INFO  [org.jboss.web] (ServerService Thread Pool -- 50) JBAS018210: Register web context:
19:06:01,555 INFO  [org.jboss.as.server.deployment] (DeploymentScanner-threads - 2) JBAS018565: Replaced deployment "token-app.knob" with deployment "token-app.knob"
19:06:08,123 INFO  [token-app] (http-isn-edgeserver.radiology.umm.edu/192.168.121.103:3000-1) Started GET "/" for 192.168.121.1 at 2015-01-16 19:06:08 +0000
19:06:08,352 INFO  [token-app] (http-isn-edgeserver.radiology.umm.edu/192.168.121.103:3000-1) Processing by PatientsController#index as HTML
19:06:08,455 INFO  [token-app] (http-isn-edgeserver.radiology.umm.edu/192.168.121.103:3000-1)   Rendered patients/_consent_dialog.html.erb (3.0ms)
19:06:08,456 INFO  [token-app] (http-isn-edgeserver.radiology.umm.edu/192.168.121.103:3000-1)   Rendered patients/index.html.erb within layouts/application (26.0ms)
19:06:08,926 INFO  [token-app] (http-isn-edgeserver.radiology.umm.edu/192.168.121.103:3000-1) Completed 200 OK in 572ms (Views: 260.0ms | ActiveRecord: 47.0ms)
19:06:13,011 INFO  [token-app] (http-isn-edgeserver.radiology.umm.edu/192.168.121.103:3000-4) Started GET "/admin/audit" for 192.168.121.1 at 2015-01-16 19:06:13 +0000
19:06:13,033 INFO  [token-app] (http-isn-edgeserver.radiology.umm.edu/192.168.121.103:3000-4) Processing by AdminController#audit as HTML
19:06:13,153 INFO  [token-app] (http-isn-edgeserver.radiology.umm.edu/192.168.121.103:3000-4)   Rendered html template (1.0ms)
19:06:13,154 INFO  [token-app] (http-isn-edgeserver.radiology.umm.edu/192.168.121.103:3000-4)   Rendered admin/_transaction_list.html.erb (13.0ms)
19:06:13,155 INFO  [token-app] (http-isn-edgeserver.radiology.umm.edu/192.168.121.103:3000-4)   Rendered admin/audit.html.erb within layouts/application (38.0ms)
19:06:13,398 INFO  [token-app] (http-isn-edgeserver.radiology.umm.edu/192.168.121.103:3000-4) Completed 200 OK in 365ms (Views: 118.0ms | ActiveRecord: 25.0ms)
19:06:42,251 INFO  [token-app] (http-isn-edgeserver.radiology.umm.edu/192.168.121.103:3000-4) Started GET "/tail" for 192.168.121.1 at 2015-01-16 19:06:42 +0000
19:06:42,274 INFO  [token-app] (http-isn-edgeserver.radiology.umm.edu/192.168.121.103:3000-4) Processing by TailController#index as HTML
19:06:42,403 INFO  [token-app] (http-isn-edgeserver.radiology.umm.edu/192.168.121.103:3000-4)   Rendered tail/index.html.erb within layouts/application (14.0ms)
19:06:42,643 INFO  [token-app] (http-isn-edgeserver.radiology.umm.edu/192.168.121.103:3000-4) Completed 200 OK in 368ms (Views: 59.0ms | ActiveRecord: 5.0ms)
19:07:30,471 INFO  [token-app] (http-isn-edgeserver.radiology.umm.edu/192.168.121.103:3000-4) Started GET "/tail?log=transfer-content" for 192.168.121.1 at 2015-01-16 19:07:30 +0000
19:07:30,487 INFO  [token-app] (http-isn-edgeserver.radiology.umm.edu/192.168.121.103:3000-4) Processing by TailController#index as HTML
19:07:30,487 INFO  [token-app] (http-isn-edgeserver.radiology.umm.edu/192.168.121.103:3000-4)   Parameters: {"log"=>"transfer-content"}
19:07:30,559 INFO  [token-app] (http-isn-edgeserver.radiology.umm.edu/192.168.121.103:3000-4)   Rendered tail/index.html.erb within layouts/application (12.0ms)
19:07:30,716 INFO  [token-app] (http-isn-edgeserver.radiology.umm.edu/192.168.121.103:3000-4) Completed 200 OK in 229ms (Views: 57.0ms | ActiveRecord: 6.0ms)
19:07:39,495 INFO  [token-app] (http-isn-edgeserver.radiology.umm.edu/192.168.121.103:3000-4) Started GET "/tail?log=prepare-content" for 192.168.121.1 at 2015-01-16 19:07:39 +0000
19:07:39,516 INFO  [token-app] (http-isn-edgeserver.radiology.umm.edu/192.168.121.103:3000-4) Processing by TailController#index as HTML
19:07:39,516 INFO  [token-app] (http-isn-edgeserver.radiology.umm.edu/192.168.121.103:3000-4)   Parameters: {"log"=>"prepare-content"}
19:07:39,625 INFO  [token-app] (http-isn-edgeserver.radiology.umm.edu/192.168.121.103:3000-4)   Rendered tail/index.html.erb within layouts/application (48.0ms)
19:07:40,155 INFO  [token-app] (http-isn-edgeserver.radiology.umm.edu/192.168.121.103:3000-4) Completed 200 OK in 637ms (Views: 111.0ms | ActiveRecord: 5.0ms)
19:07:53,022 INFO  [token-app] (http-isn-edgeserver.radiology.umm.edu/192.168.121.103:3000-4) Started GET "/patients/new" for 192.168.121.1 at 2015-01-16 19:07:53 +0000
19:07:53,046 INFO  [token-app] (http-isn-edgeserver.radiology.umm.edu/192.168.121.103:3000-4) Processing by PatientsController#new as HTML
```

© 2014 Radiological Society of North America. Support: RSNA.org/Image_Share.aspx helpdesk@imsharing.org | Toll-free: 1-855-IM-Sharing (467-4274) An NIBIB funded Project

Figure 5-22: Application Logs

6. Maintenance

6.1 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:

6.1.1 System

The site can always use any standard backup tools they normally have. If there is no local preference an excellent free choice is CloneZilla at http://clonezilla.org/

6.1.2 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/mirthconnect
```

6.1.2 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
```

6.2 Vacuuming

Vacuuming is another PostgreSQL maintenance task that should be performed on a regular basis. The procedures is described in the PostgreSQL documentation. For PostgreSQL version 9.2 used by the Edge Server, the URL is:

http://www.postgresql.org/docs/9.2/static/maintenance.html

6.3 Help Desk

A help desk is available during regular business hours to provide support to users of the Edge Server and patients attempting to create and use personal health record accounts. Email helpdesk@imsharing.org or call 1-855-IM-SHARING (467-4274).

7. Administration of User Accounts

User accounts and privileges are managed using the OpenAM server on the Edge Server and an optional Active Directory server. User logins can be authenticated by the OpenAM server or by an Active Directory server. User privileges on the Edge Server are always managed by the OpenAM system on the Edge Server.

Section 7.1 describes how to manage user authentication.

Section 7.2 describes how to manage user privileges in OpenAM. Those privileges are managed in OpenAM even if authentication is managed with Active Directory.

7.1 User Authentication Management in OpenAM

Section 2.7 of this document describes the initial configuration of the OpenAM software. During the process of completing that configuration, the account **amAdmin** is created with a password of your choice. You may then choose to authenticate other users to an Active Directory server or to authenticate users with the OpenAM server. Appendix F of this document describes how to couple the Edge Server to an existing Active Directory server.

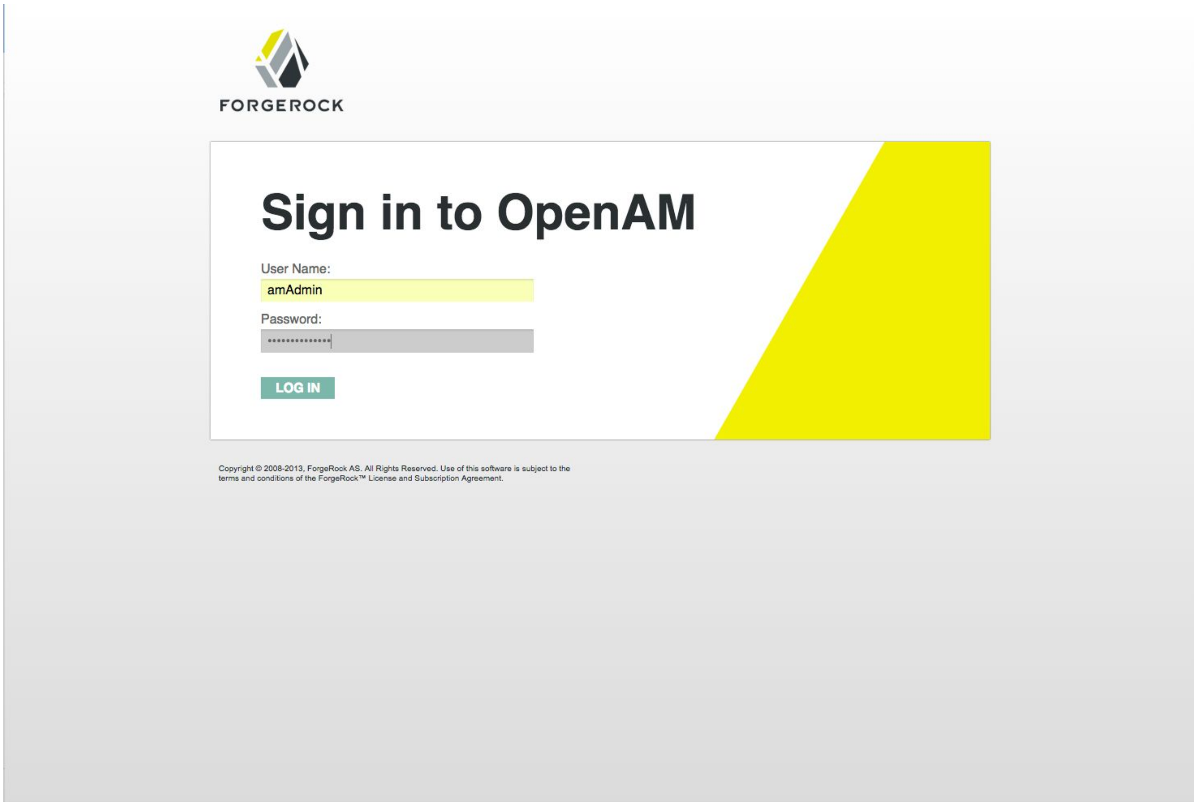
This document does not discuss the process of managing user accounts in Active Directory. The remainder of Section 7.1 describes how to add user accounts using the OpenAM software.

To access and configure user management, use the URL
http://edge-hostname.example.com:3000/openam/console
and enter OpenAm admin login credentials (configured in Section 2.7). See Figure 7-1 for an example login screen.

You must use the fully qualified domain name in the URL. If the hostname of the Edge Server is **edge-hostname.example.com**, you must use that full host name. Do not use only **edge-hostname** or an IP address.

- Username: `amAdmin`

The `amAdmin` user has full privileges, including the ability to create other users, change system configuration options, and view logs in OpenAM. Logging in as the `amAdmin` user takes you directly to the management interface (no other accounts have this access).



Sign in to OpenAM

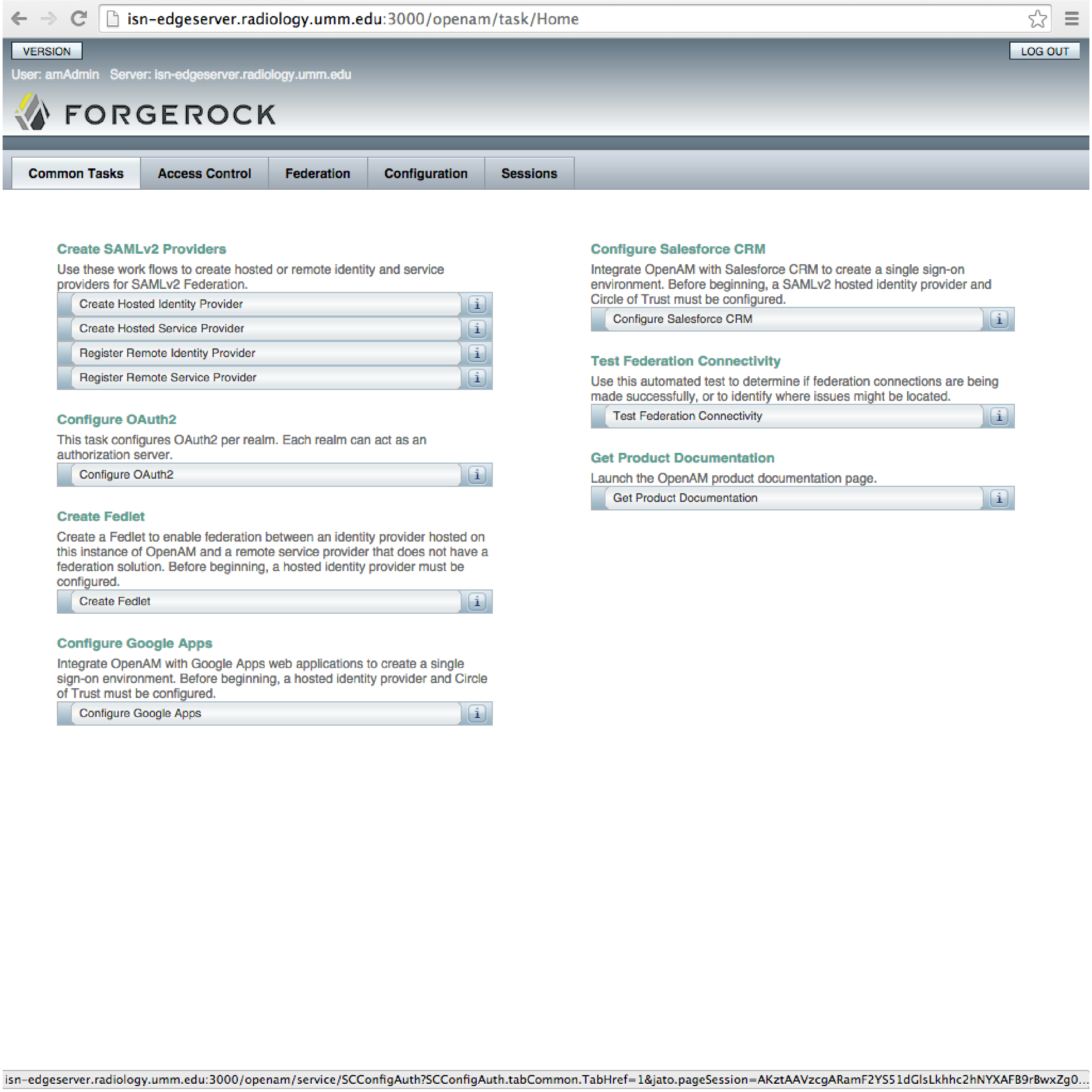
User Name: amAdmin

Password: ••••••••••••••

Copyright © 2008-2013, ForgeRock AS. All Rights Reserved. Use of this software is subject to the terms and conditions of the ForgeRock™ License and Subscription Agreement.

Figure 7-1: Open AM Login Screen

Once you are logged in (**Figure 7-2**), you will need to navigate to the account management interface. There are many other links available, but please avoid clicking them unless you are configuring advanced functionality (outside the scope of this document). Start by clicking the `Access Control` tab.



isn-edgeserver.radiology.umm.edu:3000/openam/task/Home
VERSION
LOG OUT
User: amAdmin Server: isn-edgeserver.radiology.umm.edu
FORGEROCK
Common Tasks
Access Control
Federation
Configuration
Sessions

Create SAMLv2 Providers

Use these work flows to create hosted or remote identity and service providers for SAMLv2 Federation.

Create Hosted Identity Provider
Create Hosted Service Provider
Register Remote Identity Provider
Register Remote Service Provider

Configure OAuth2

This task configures OAuth2 per realm. Each realm can act as an authorization server.

Create Fedlet

Create a Fedlet to enable federation between an identity provider hosted on this instance of OpenAM and a remote service provider that does not have a federation solution. Before beginning, a hosted identity provider must be configured.

Configure Google Apps

Integrate OpenAM with Google Apps web applications to create a single sign-on environment. Before beginning, a hosted identity provider and Circle of Trust must be configured.

Configure Salesforce CRM

Integrate OpenAM with Salesforce CRM to create a single sign-on environment. Before beginning, a SAMLv2 hosted identity provider and Circle of Trust must be configured.

Test Federation Connectivity

Use this automated test to determine if federation connections are being made successfully, or to identify where issues might be located.

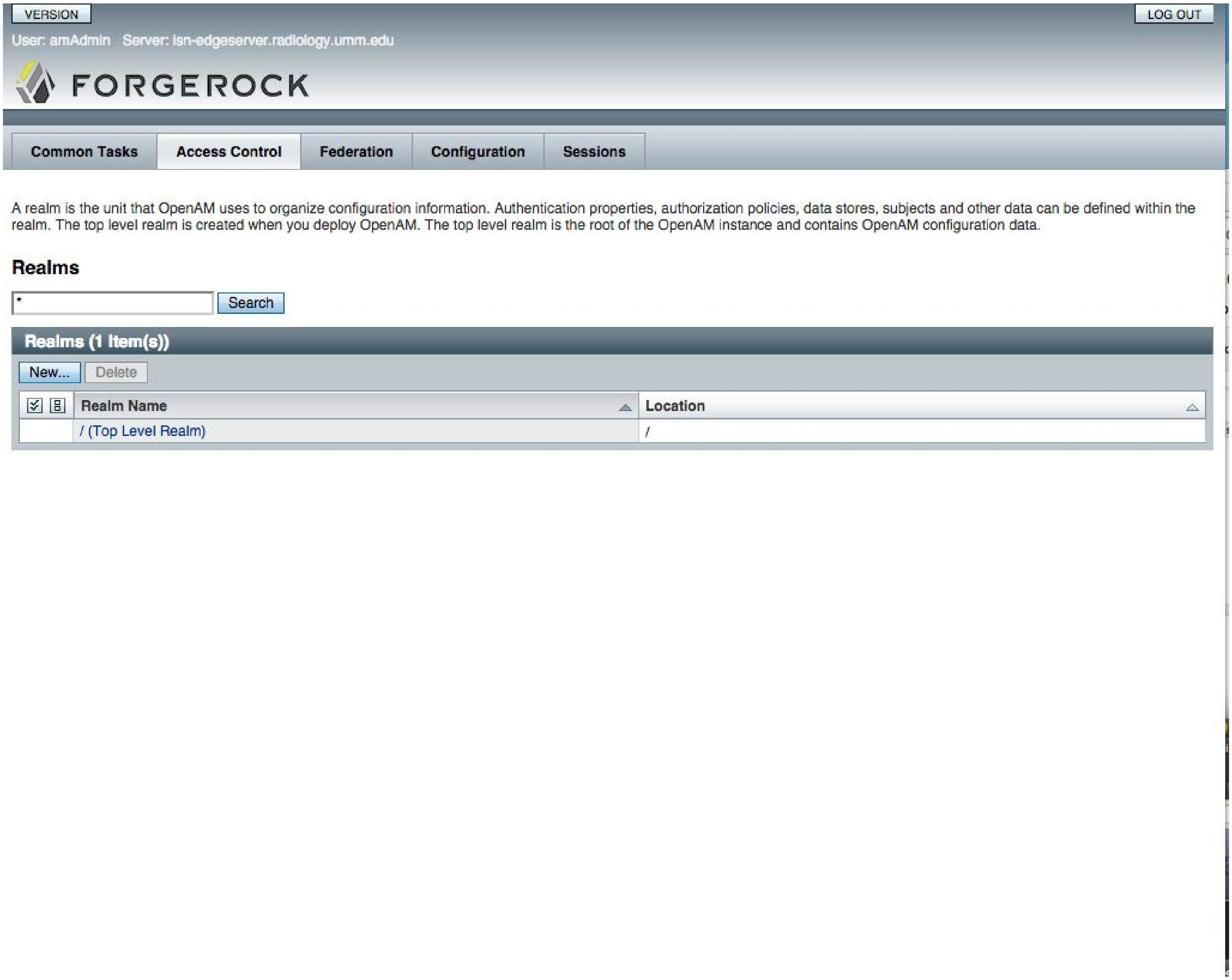
Get Product Documentation

Launch the OpenAM product documentation page.

Get Product Documentation
isn-edgeserver.radiology.umm.edu:3000/openam/service/SCConfigAuth?SCConfigAuth.tabCommon.TabHref=1&jato.pageSession=AKztAAVzcgARamF2YS51dGlsLkhhc2hNYXAFB9rBwxZg0…

Figure 7-2: OpenAM Landing Page

This takes you to the `Access Control` page. Next, click the blue text link under the `Realm Name` heading labelled `/(Top Level Realm)`(Figure 7-3).



User: amAdmin Server: isn-edgeserver.radiology.umm.edu

A realm is the unit that OpenAM uses to organize configuration information. Authentication properties, authorization policies, data stores, subjects and other data can be defined within the realm. The top level realm is created when you deploy OpenAM. The top level realm is the root of the OpenAM instance and contains OpenAM configuration data.

Realms

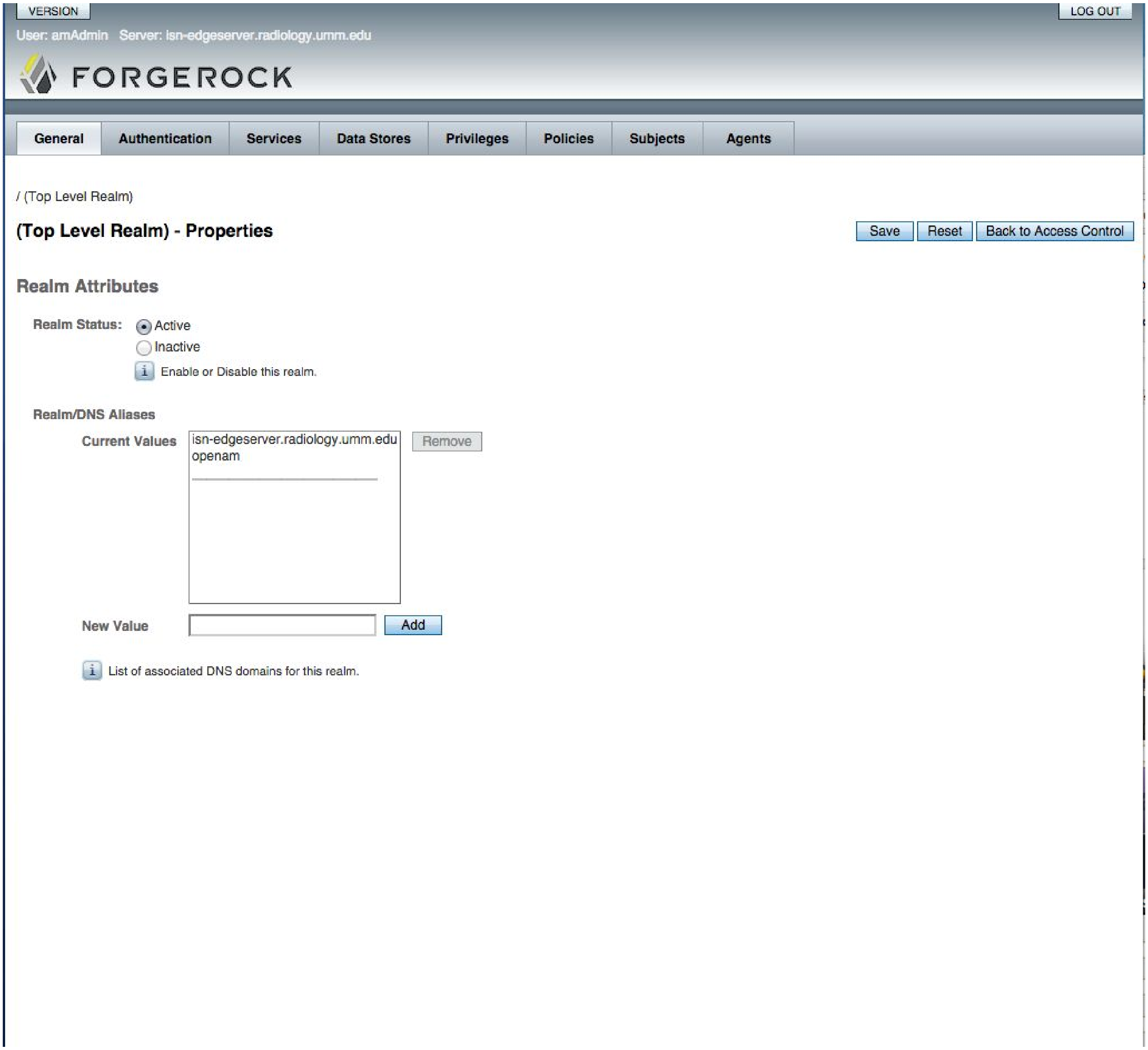
*

Realms (1 Item(s))

Realm Name	Location
/ (Top Level Realm)	/

Figure 7-3: OpenAM Access Control page

From the Top Level Realm page, click the Subjects tab (Figure 7-4).



User: amAdmin Server: isn-edgeserver.radiology.umm.edu

/ (Top Level Realm)

(Top Level Realm) - Properties

Realm Attributes

Realm Status: ● Active
○ Inactive
Enable or Disable this realm.

Realm/DNS Aliases

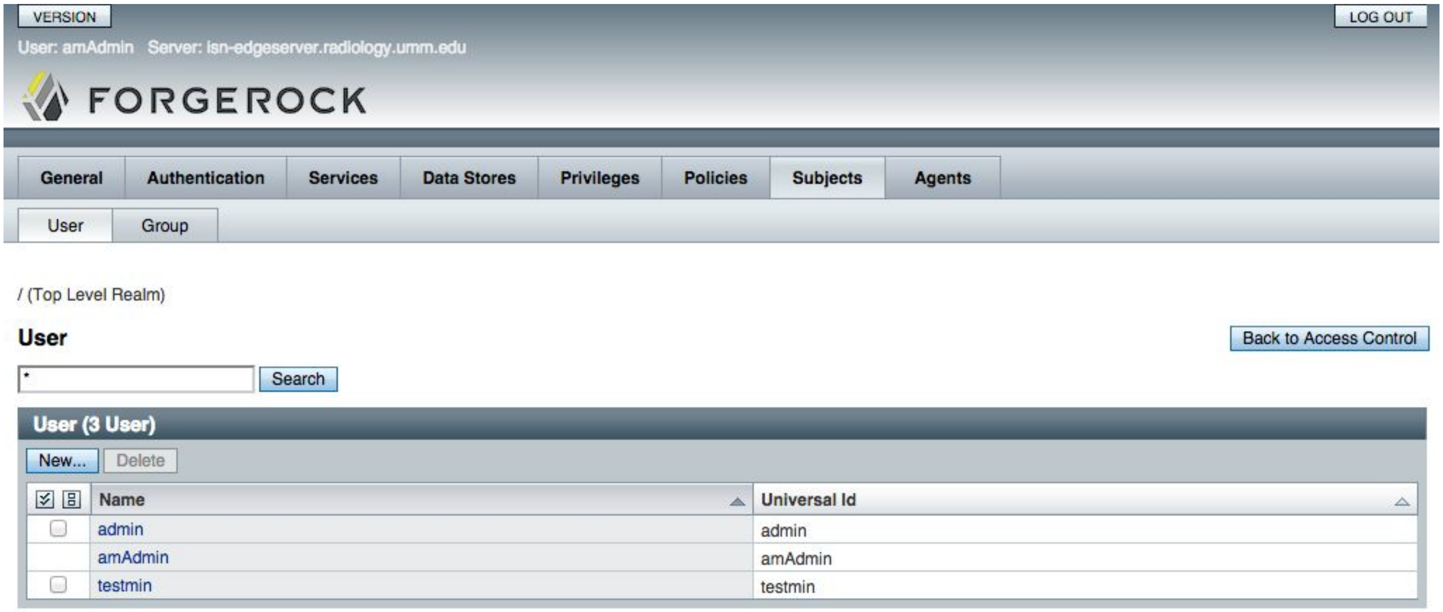
Current Values isn-edgeserver.radiology.umm.edu
openam

New Value

List of associated DNS domains for this realm.

Figure 7-4: OpenAM Top Level Realm page

The Subjects page lists all the user accounts on the Edge Server. This is the page where you can create new users, deactivate users, change user roles, and and reset passwords. Click the blue New button under the User table heading (**not** the User tab) (Figure 7-5).



User: amAdmin Server: isn-edgeserver.radiology.umm.edu

/ (Top Level Realm)

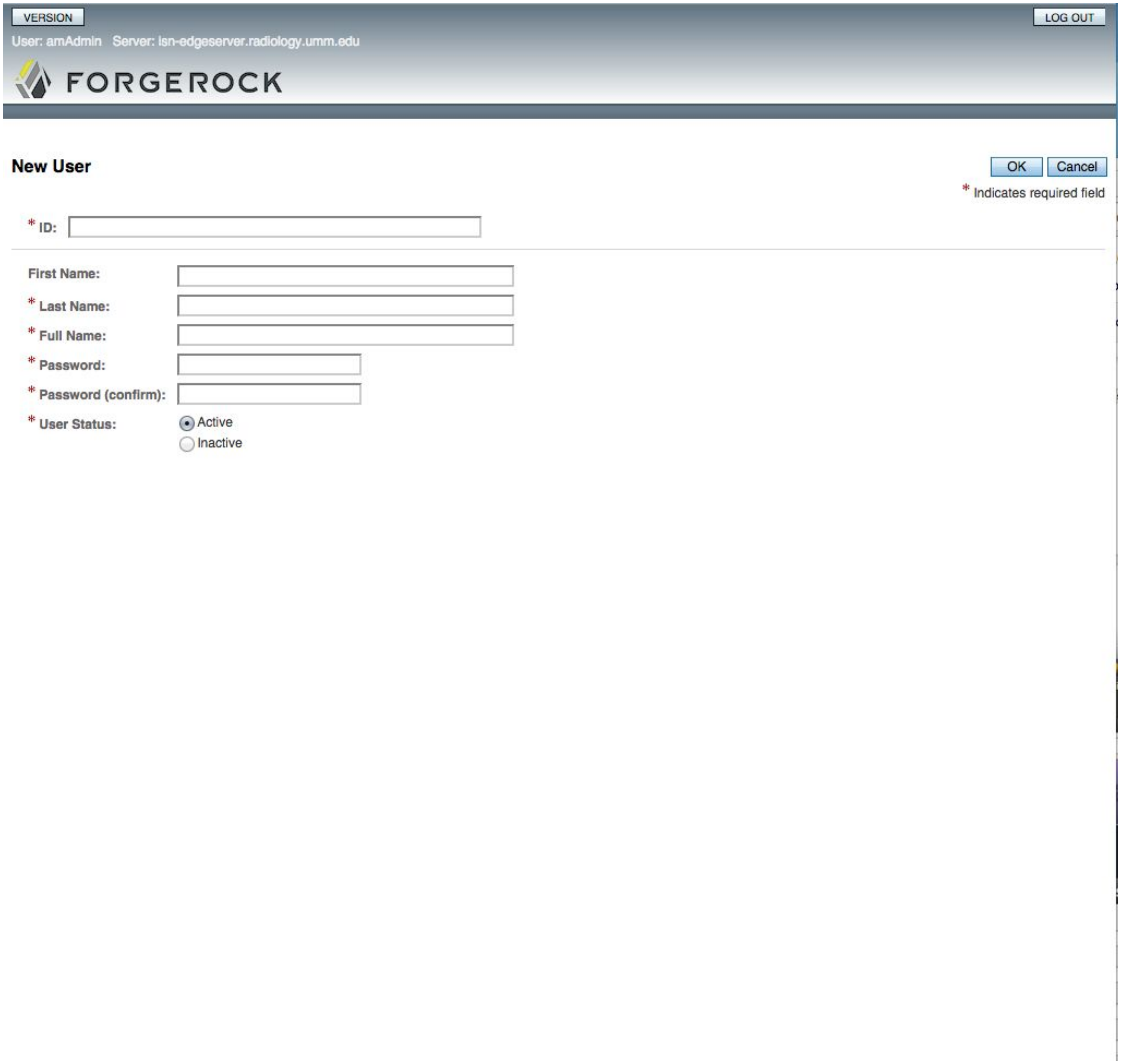
User

User (3 User)

	Name	Universal Id
□	admin	admin
	amAdmin	amAdmin
□	testmin	testmin

Figure 7-5: OpenAM Subjects page

To create a new account, **ALL** fields must be filled out, **INCLUDING** the **FIRST NAME** field. The field labeled **ID** will be the account **login name**. Click the blue `OK` button when all forms are filled in to create the account (Figure 7-6).



User: amAdmin Server: lsn-edgeserver.radiology.umm.edu

New User

* Indicates required field

* ID:

First Name:

* Last Name:

* Full Name:

* Password:

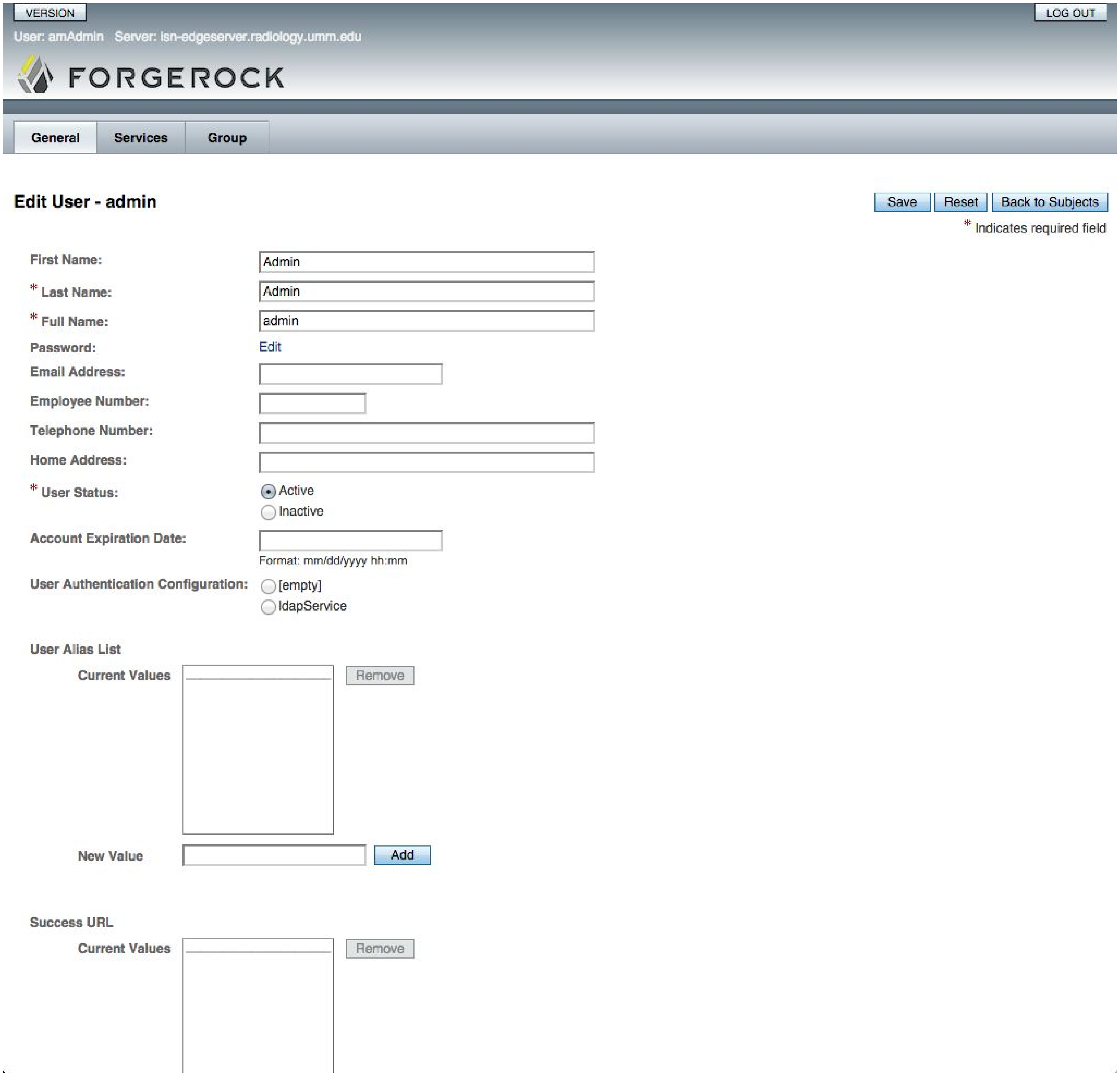
* Password (confirm):

* User Status: ● Active ○ Inactive

Figure 7-6: OpenAM Account Creation

Finishing user creation leaves you back at the `Subjects` page (Figure 5-5). Select the account name you just created (blue link under the `Name` column in the table). This will take you to the `Edit User` page (Figure 5-7).

Account properties like password, name, and active status can be edited by changing the properties, and hitting the blue `Save` button (Figure 7-7). Inactive accounts can no longer login.



Edit User - admin

* Indicates required field

First Name: Admin

* Last Name: Admin

* Full Name: admin

Password: Edit

Email Address:

Employee Number:

Telephone Number:

Home Address:

* User Status: ● Active ○ Inactive

Account Expiration Date:
Format: mm/dd/yyyy hh:mm

User Authentication Configuration: ○ [empty] ○ ldapService

User Alias List
Current Values
New Value

Success URL
Current Values

Figure 7-7: OpenAM editing user properties

7.2 User Privilege Management in OpenAM

User privileges are managed in OpenAM. This is true for user accounts that are authenticated through Active Directory.

As described in Section 7.1, login to the OpenAM console by using the URL
http://edge-hostname.example.com:3000/openam/console

The login name is **amAdmin**.

As described in Section 7.1,

1. Select the Access Control link.
2. Click the blue text link under the Realm Name heading labelled `/ (Top Level Realm)`
3. From the Top Level Realm page, click on the `Subjects` tab

When you select the Subjects tab, you will see the list of subjects that are known by OpenAM. This includes the amAdmin account and any users that have logged in as authenticated by Active Directory. A user account is not visible Active Directory until that user has logged in at least one time. Therefore, to assign a user to a group, you will first need to instruct that user to login to the Edge Server application and then logout. You can then complete the procedure described below for adding group privileges to individual users.

Click the `Group` tab on the `Edit Users` page to adjust user groups (Figure 5-8).

All users that are created have access to basic functionality of sending images to the clearinghouse. These users can look up patients and create RSNA IDs, reset PINs, submit jobs, and view their own job. There are five *additional* roles that can be added to an account for additional functionality:

- **Admin**: ability to access Administrative pages (view logs, view all jobs, set system configuration)
- **Export**: Access to the Research Send functionality (CTP only)
- **Import**: Access to the Retrieve functionality (CTP only)
- **Read:** Access to files on the server's local file system (CTP only)
- **Super:** a deprecated role with the same access as the **Admin** role**. Do not use this role.**

*Please note that the **Admin** role does not overlap or grant **Export** or **Import** privileges.* **These additional roles must be manually added at this time** for a user account to have CTP Export or Import privileges.

Click the blue `Save` button to finish role assignment for the user you created (Figure 7-8).

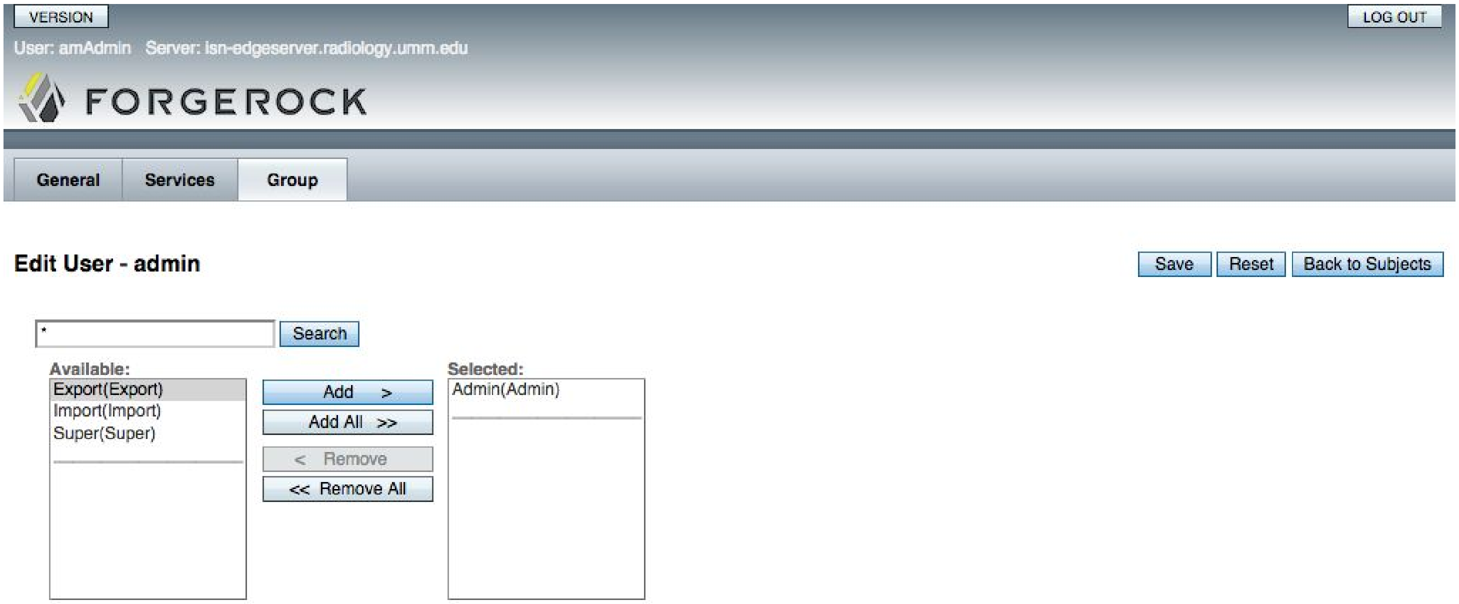


Figure 7-8: OpenAM editing user roles

Roles can always be adjusted by visiting the `Subjects` page, clicking a specific user account link, then clicking the `Group` tab to add or remove (a) role(s) and hitting the blue `Save` button as above (Figure 7-8).

Appendix A: Integrity of Downloaded Files

Large, binary files that are downloaded using the Internet may become corrupted during the process. A possible scenario is that the download did not fully complete and that the end of the file is just missing.

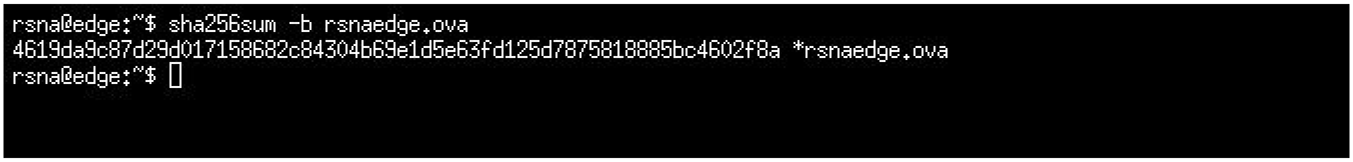
If you are downloading files such as a large VM image, you should test the integrity of the file. This is done by computing an SHA-256 hash of the file you just downloaded and comparing that value to the value computed and published by the RSNA.

A.1: Linux Integrity Checking

If you use a Linux system to download files, there is a program that is already included that will compute the SHA256 hash for you. From the command line:

```
sha256sum -b file
```

This will produce a result like this:



```
rsna@edge:~$ sha256sum -b rsnaedge.ova
4619da9c87d29d017158682c84304b69e1d5e63fd125d7875818885bc4602f8a *rsnaedge.ova
rsna@edge:~$ 
```

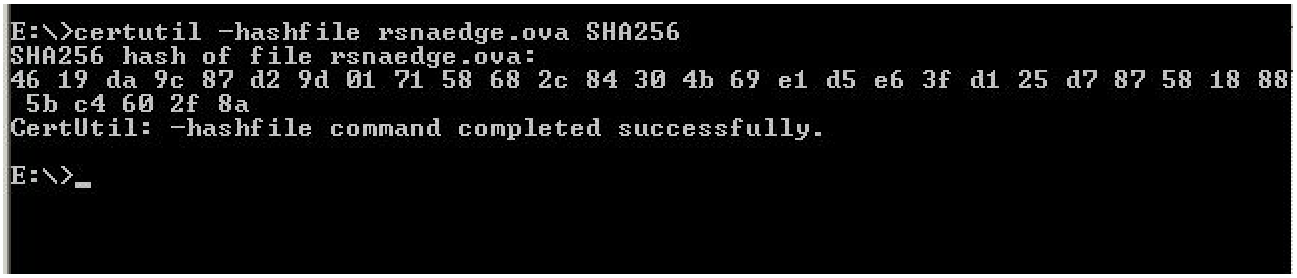
You would then compare the computed value to the value published for the file.

A.2: Windows Integrity Checking

You can compute the SHA256 hash of a file as follows:

```
certutil -hashfile file SHA256
```

This will produce a result such as:



```
E:\>certutil -hashfile rsnaedge.ova SHA256
SHA256 hash of file rsnaedge.ova:
46 19 da 9c 87 d2 9d 01 71 58 68 2c 84 30 4b 69 e1 d5 e6 3f d1 25 d7 87 58 18 88
 5b c4 60 2f 8a
CertUtil: -hashfile command completed successfully.

E:\>_
```

You would then compare the computed value to the value published for the file.

A.6 Installing pgAdmin (optional)

You may find it helpful to use the GUI tool pgAdmin to perform database operations on the Edge Server from a remote PC. pgAdmin is already installed by default on the VM.

If you are installing to a Windows PC you can obtain the installer at

http://pgadmin.org/download/windows.php

Figure F-10: Login page using Active Directory

Out of the box, PostgreSQL does not allow network based queries for a secure default environment. You need to modify the `postgresql.conf` and `pg_hba.conf` files to enable either remote network access directly to the database. In the Ubuntu configuration used by the Edge Server, these files are found in `/data`. **Updates to these files will require a PostgreSQL server restart for the change to take effect.**

The `pg_hba.conf` file will have a line like this.:

```
#IP4 Local Connections
host all  all  127.0.0.1/32    md5
```

At the empty line (following the line ending `md5`), add another line:

```
host all  all  192.168.0.1/32  trust
```

Substituting **the IP address of the remote computer** from which you desire to run pgAdmin from the example `192.168.0.1`. Be sure to investigate the security options (`md5, trust`, etc) before using them on your network.

The `postgresql.conf` will have a line like:

```
# listen_address = xxxx
```

Make sure this line is uncommented (remove the `#`) and change the xxxx to the value of **the IP address of the server**.

Appendix B: Extended DICOM Configuration

The following presentation contexts are supported by the Edge Server's SCP. Additional presentation contexts can be added using the procedure described in section 5.3.1

SOP Class	Description	Implicit VR Little Endian	Explicit VR Little Endian	JPEG Baseline (Process 1)	JPEG Lossless Non-Hierarchical (Process 14)	JPEG Lossless Non-Hierarchical First-Order Prediction	JPEG 2000 Image Compression (Lossless Only)	JPEG 2000 Image Compression	RLE Lossless
1.2.840.10008.5.1.4.1.1.1	Computed Radiography Image Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.1.1	Digital X-Ray Image Storage - For Presentation	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.1.1.1	Digital X-Ray Image Storage - For Processing	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.1.2	Digital Mammography X-Ray Image Storage - For Presentation	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.1.2.1	Digital Mammography X-Ray Image Storage - For Processing	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.1.3	Digital Intra-oral X-Ray Image Storage - For Presentation	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.1.3.1	Digital Intra-oral X-Ray Image Storage - For Processing	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.104.1	Encapsulated PDF Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.11.1	Grayscale Softcopy Presentation State Storage SOP Class	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.11.2	Color Softcopy Presentation State Storage SOP Class	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.11.3	Pseudo-Color Softcopy Presentation State Storage SOP Class	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.11.4	Blending Softcopy Presentation State Storage SOP Class	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.12.1	X-Ray Angiographic Image Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.12.1.1	Enhanced XA Image Storage	X	X	X	X	X	X	X	X

SOP Class	Description	Implicit VR Little Endian	Explicit VR Little Endian	JPEG Baseline (Process 1)	JPEG Lossless Non-Hierarchical (Process 14)	JPEG Lossless Non-Hierarchical First-Order Prediction	JPEG 2000 Image Compression (Lossless Only)	JPEG 2000 Image Compression	RLE Lossless
1.2.840.10008.5.1.4.1.1.12.2	X-Ray Radiofluoroscopic Image Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.12.2.1	Enhanced XRF Image Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.128	Positron Emission Tomography Image Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.2	CT Image Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.2.1	Enhanced CT Image Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.20	Nuclear Medicine Image Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.3.1	Ultrasound Multi-frame Image Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.4	MR Image Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.4.1	Enhanced MR Image Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.4.2	MR Spectroscopy Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.481.1	RT Image Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.481.2	RT Dose Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.481.3	RT Structure Set Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.481.4	RT Beams Treatment Record Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.481.5	RT Plan Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.481.6	RT Brachy Treatment Record Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.481.7	RT Treatment Summary Record Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.6.1	Ultrasound Image Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.66	Raw Data Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.66.1	Spatial Registration Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.66.2	Spatial Fiducials Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.67	Real World Value Mapping Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.7	Secondary Capture Image Storage	X	X	X	X	X	X	X	X

SOP Class	Description	Implicit VR Little Endian	Explicit VR Little Endian	JPEG Baseline (Process 1)	JPEG Lossless Non-Hierarchical (Process 14)	JPEG Lossless Non-Hierarchical First-Order Prediction	JPEG 2000 Image Compression (Lossless Only)	JPEG 2000 Image Compression	RLE Lossless
1.2.840.10008.5.1.4.1.1.7.1	Multi-frame Single Bit Secondary Capture Image Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.7.2	Multi-frame Grayscale Byte Secondary Capture Image Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.7.3	Multi-frame Grayscale Word Secondary Capture Image Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.7.4	Multi-frame True Color Secondary Capture Image Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.77.1.1	VL Endoscopic Image Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.77.1.1.1	Video Endoscopic Image Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.77.1.2	VL Microscopic Image Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.77.1.2.1	Video Microscopic Image Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.77.1.3	VL Slide-Coordinates Microscopic Image Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.77.1.4	VL Photographic Image Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.77.1.4.1	Video Photographic Image Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.77.1.5.1	Ophthalmic Photography 8 Bit Image Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.77.1.5.2	Ophthalmic Photography 16 Bit Image Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.77.1.5.3	Stereometric Relationship Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.88.11	Basic Text SR Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.88.22	Enhanced SR Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.88.33	Comprehensive SR Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.88.40	Procedure Log Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.88.50	Mammography CAD SR Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.88.59	Key Object Selection Document Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.88.65	Chest CAD SR Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.88.67	X-Ray Radiation Dose SR Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.104.1	Encapsulated PDF Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.104.2	Encapsulated CDA Storage	X	X	X	X	X	X	X	X

SOP Class	Description	Implicit VR Little Endian	Explicit VR Little Endian	JPEG Baseline (Process 1)	JPEG Lossless Non-Hierarchical (Process 14)	JPEG Lossless Non-Hierarchical First-Order Prediction	JPEG 2000 Image Compression (Lossless Only)	JPEG 2000 Image Compression	RLE Lossless
1.2.840.10008.5.1.4.1.1.9.1.1	12-lead ECG Waveform Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.9.1.2	General ECG Waveform Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.9.1.3	Ambulatory ECG Waveform Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.9.2.1	Hemodynamic Waveform Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.9.3.1	Cardiac Electrophysiology Waveform Storage	X	X	X	X	X	X	X	X
1.2.840.10008.5.1.4.1.1.9.4.1	Basic Voice Audio Waveform Storage	X	X	X	X	X	X	X	X

Appendix C: 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 9-20: 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 9-12)
-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 9-20: Audit Trail Interface) for specific error information.
-24	Exam has been canceled	Indicates the Edge Server was unable retrieve images because the exam was canceled.
-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 9-20: 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 LifeImage Support (support@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 lifeIMAGE Support (support@lifeimage.com)

Appendix D: 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 lifeIMAGE Support (support@lifeimage.com).

D.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

D.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 of 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 E: Unix Hints

E.1. 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.

E.2. 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*.

E.3. Remote Access to the Server Console via VNC

A physical server can have a monitor and keyboard attached. Remote access to servers located in a computer room is desirable. We recommend you use VNC (http://en.wikipedia.org/wiki/Virtual_Network_Computing) for this access. The VNC server is installed by default on the VM. If you have access to a physical console (or a virtual console using VMware or similar product). You will start the server from the command line:

```
     vncserver -geometry 1400x800
```

will start the server with a display that is 1400x800. By default, the VNC server runs on port 5900. When you launch the vncserver -geometry 1400x800, it will start up the first instance which runs on port 5901.   You can verify that you are running the first instance of vncserver by the response you receive after starting:

```
     New “rsna-isn;1 (root)’ desktop is rsna-isn:1
     Log file is /root/.vnc/rsna-isn:1.log
```

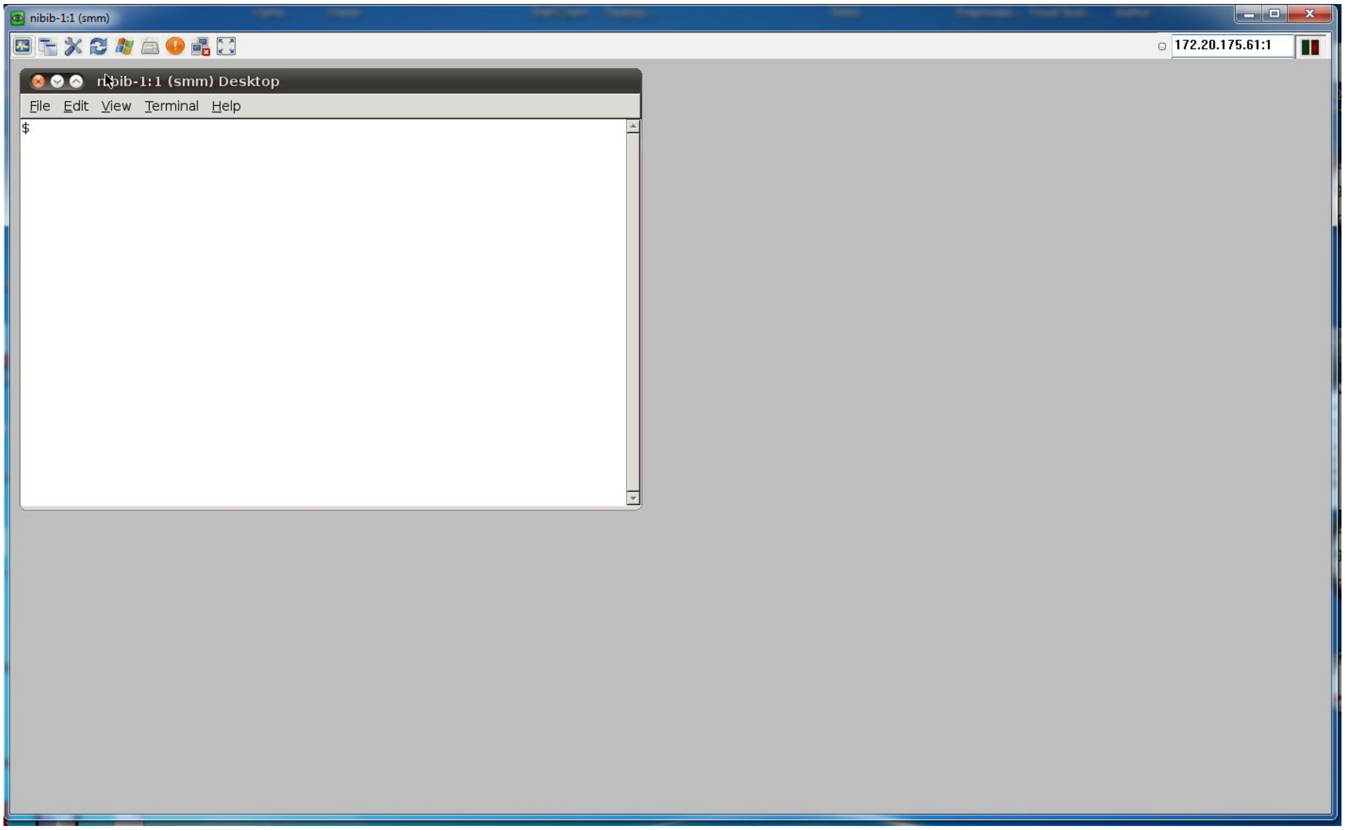
If you see you are starting desktop #2, you would need to connect on port 5902.

If you need to stop vncserver, you can do so by typing the following command:

```
     vncserver -kill:1
```

You can adjust the display parameters as appropriate for your laptop or desktop. If this is the first time you invoked the server, it will prompt you for a password to protect the display. You can choose to use the same password used for the unix account you are using or register a different password; they do not need to match.

Now that the VNC server application is running on the Edge Server system, you need to connect a client application to provide the remote access. For example, UltraVNC is a client you can download and install on your PC. When you use a VNC client to make a connection to the VNC server, you will be shown a screen like the one in the next figure.



```
$
```

Figure E-1: VNC Client Connected to a VNC Server Application

You have a basic X Window session without the extra Desktop Manager/Applications you expect to see. In the xterm that is presented, enter

```
gnome-session
```

This will create a desktop session with visual controls. Minimize the original xterm, and you will see the desktop shown in Figure E-2.

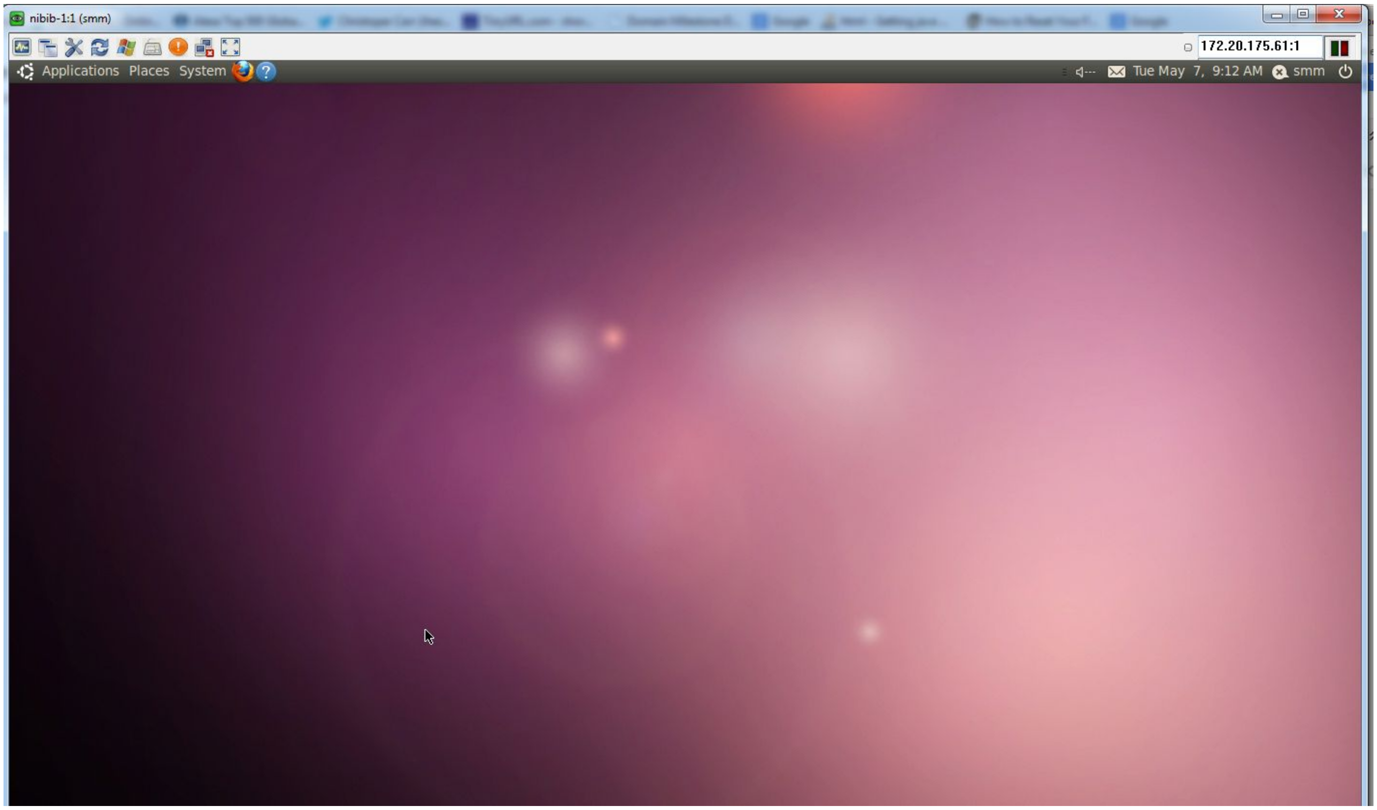


Figure E-2: Gnome Desktop Session

E.4. Keytool Command Line Hints

To list the external certificates (e.g., from lifeIMAGE)

```
keytool -list -storepass edge1234 -keystore $RSNA_ROOT/conf/truststore.jks
```

To list the certificates for this Edge Server (the ones that we generated)

```
keytool -list -storepass edge1234 -keystore $RSNA_ROOT/conf/truststore.jks
```

Appendix F: Active Directory Authentication

F.1. Before you start

You will need to gather the following Active Directory parameters:

Parameters	Example
Active Directory server address and port number	10.242.100.41:3268
DN to Start User Search	CN=Users,DC=erl,DC=wustl,DC=edu
Bind user DN	CN=RSNA One, CN=Users, DC=erl, DC=wustl, DC=edu
Bind user password	1492blue
User search filter *(optional)*	(memberOf=CN=SomeGroup,CN=Groups,DC=example,DC=com) *see RFC 4515 for the syntax https://tools.ietf.org/html/rfc4515*

Your System Administrator should be able to provide these values. Some of them can be obtained by running dsquery from the console on the AD server

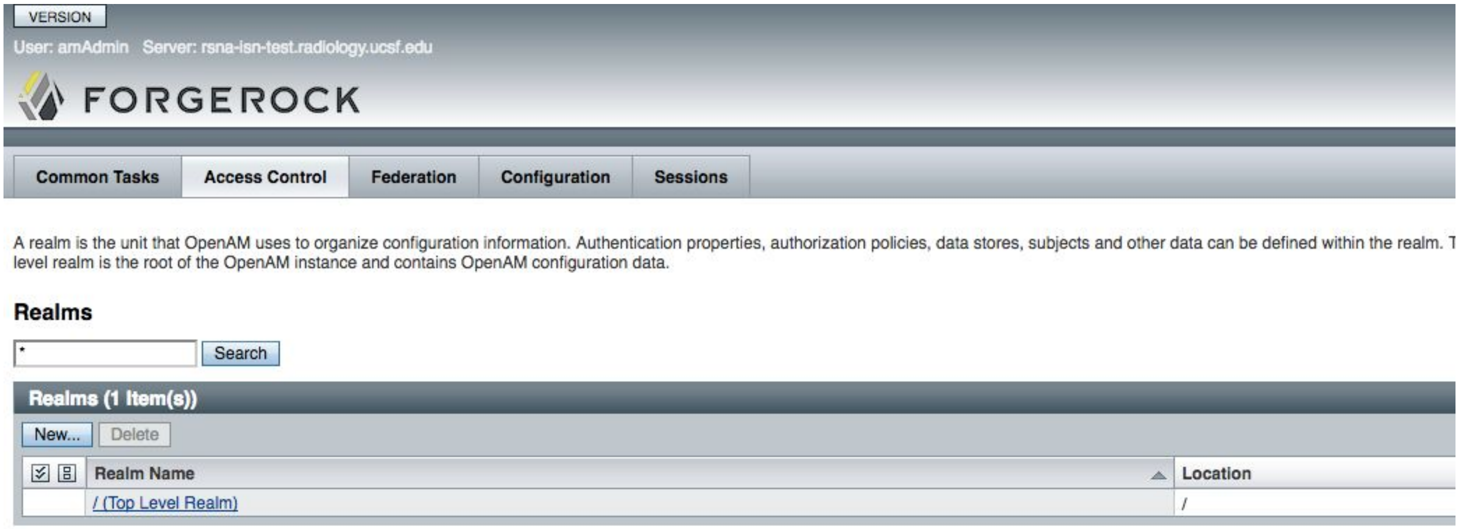
Run `dsquery users` to see the DNs of the users and `dsquery group` to list the DNs of the groups.

Before starting the configuration described below, you will need to configure the basic OpenAM setup as described above in Section 2.7. Follow the procedure as documented (command line script) and do not attempt to configure manually through a web interface.

F.2. Configuration

Sign onto the OpenAM admin console page **http://edge-hostname.example.com:3000/openam/console**. Use the account “amAdmin” and the password you selected when you originally configured user management in Section 2.7.

Click on the `Access Control` tab then `Top Level Realm` link.



User: amAdmin Server: rsna-isn-test.radiology.ucsf.edu

A realm is the unit that OpenAM uses to organize configuration information. Authentication properties, authorization policies, data stores, subjects and other data can be defined within the realm. T level realm is the root of the OpenAM instance and contains OpenAM configuration data.

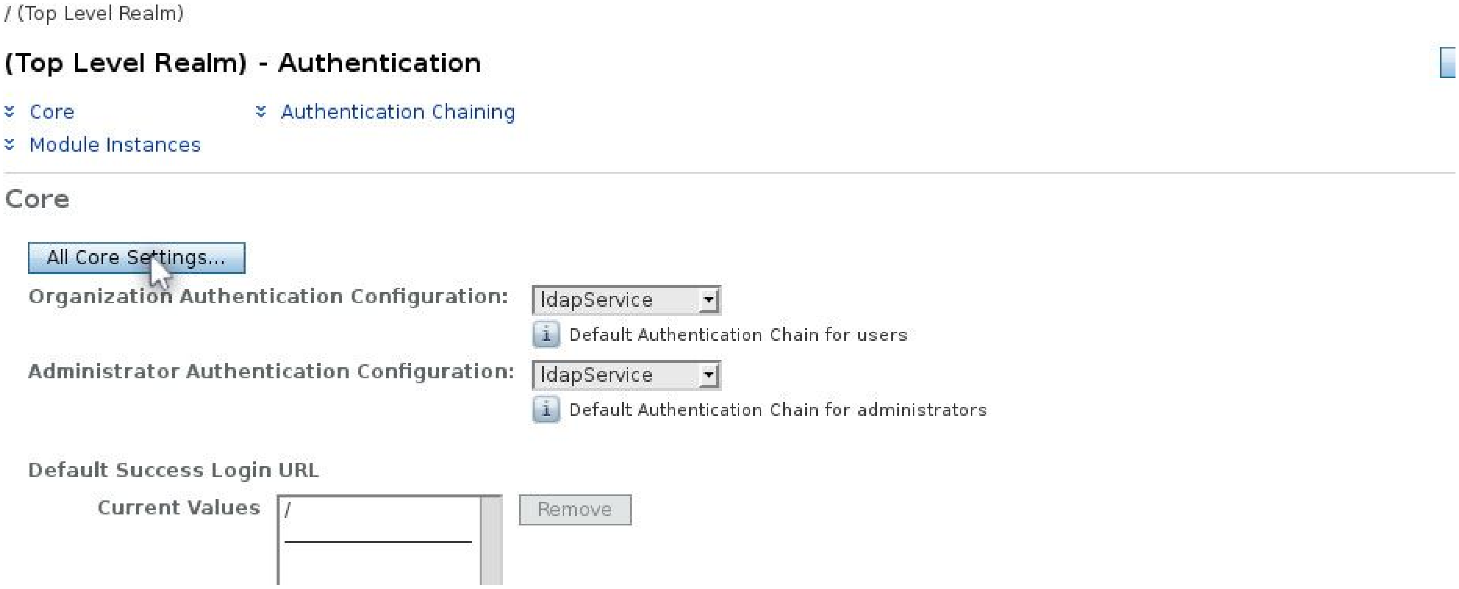
Realms

Realms (1 Item(s))

Realm Name	Location
/ (Top Level Realm)	/

Figure F-1

Click on the `Authentication` Tab, then click `All Core Settings`.



/ (Top Level Realm)

(Top Level Realm) - Authentication

Core

Organization Authentication Configuration: ldapService

Default Authentication Chain for users

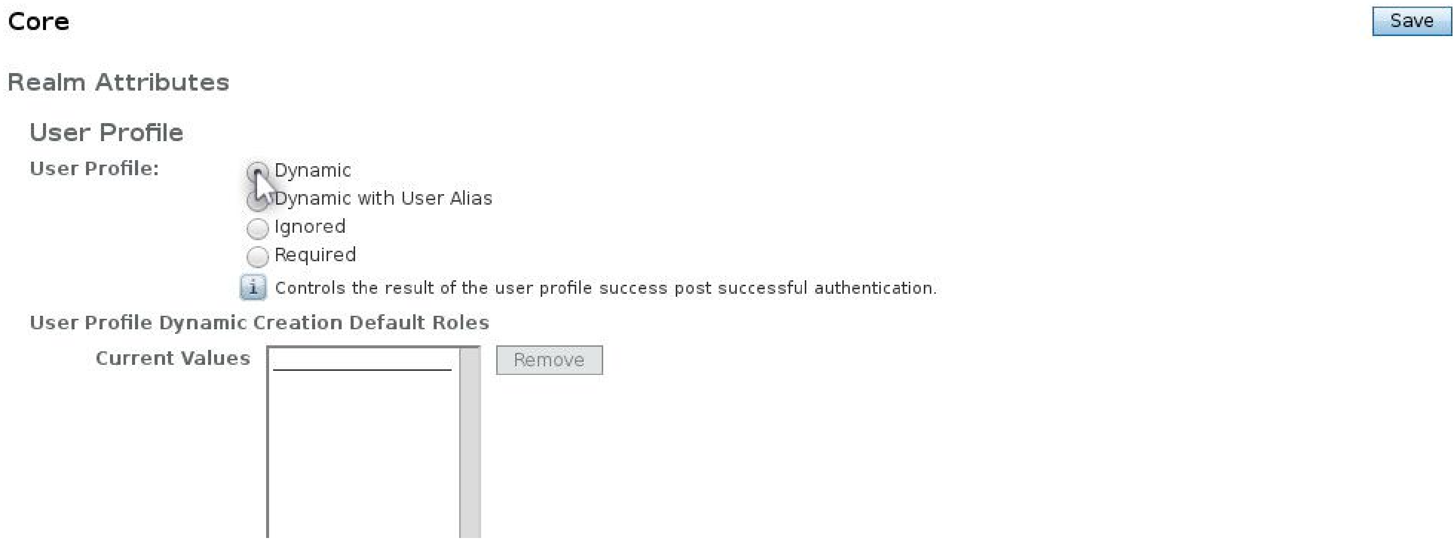
Administrator Authentication Configuration: ldapService

Default Authentication Chain for administrators

Default Success Login URL

Current Values /

Select `Dynamic`, then click `Save`. Next click `Back to Authentication`.



Core

Save

Realm Attributes

User Profile

User Profile:
● Dynamic
○ Dynamic with User Alias
○ Ignored
○ Required

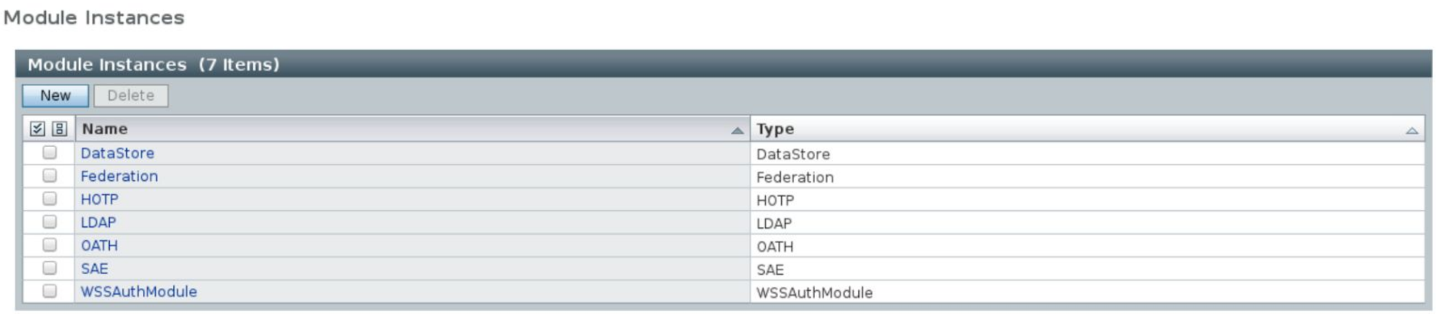
Controls the result of the user profile success post successful authentication.

User Profile Dynamic Creation Default Roles

Current Values

Remove

Then click on `New` to create a new module instance.



Module Instances

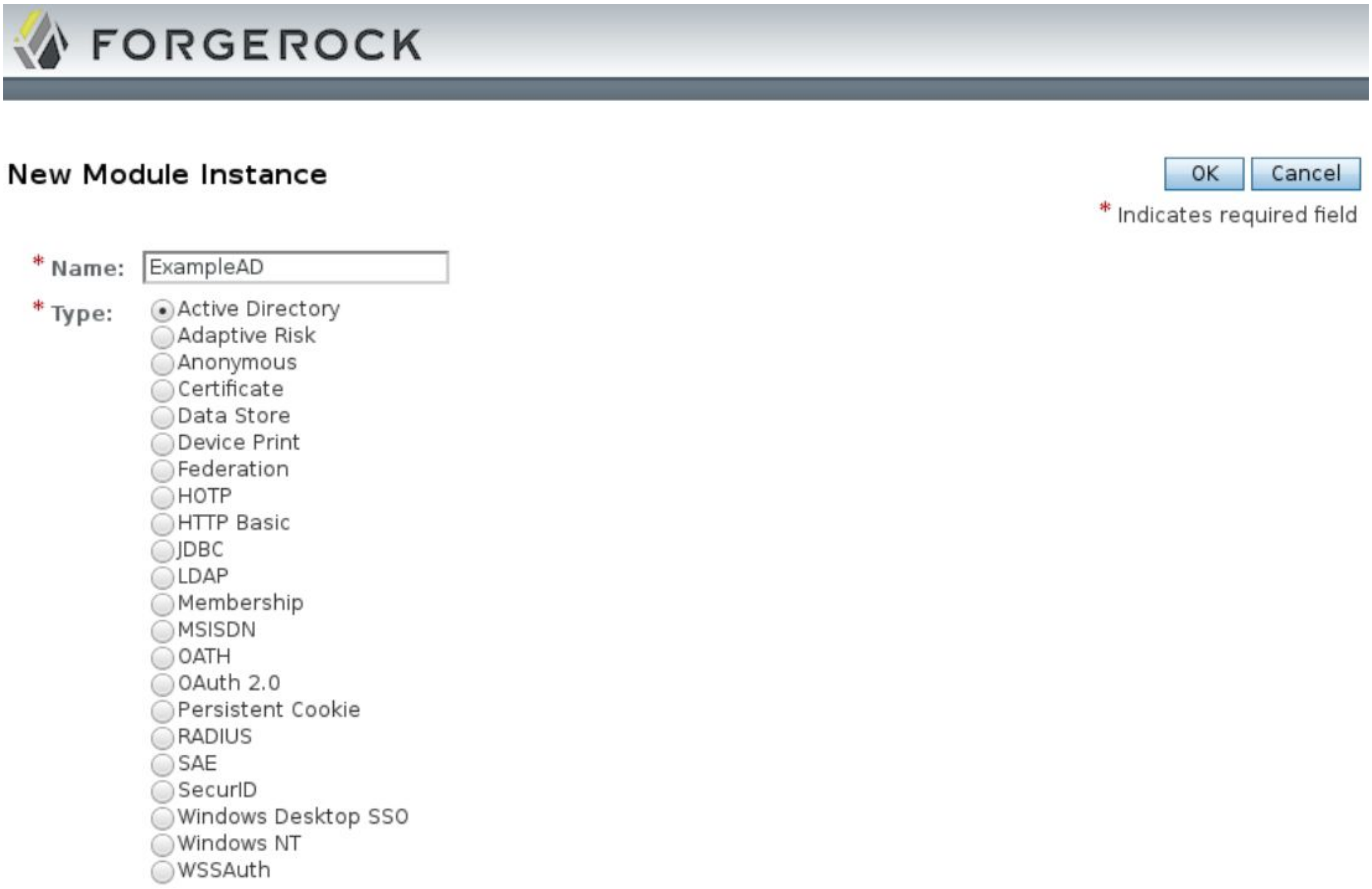
Module Instances (7 Items)

New Delete

□	Name	Type
□	DataStore	DataStore
□	Federation	Federation
□	HOTP	HOTP
□	LDAP	LDAP
□	OATH	OATH
□	SAE	SAE
□	WSSAuthModule	WSSAuthModule

Figure F-2

Enter a name for a new `Module Instance` and select `Active Directory` Type. Next click on `OK` on the upper right corner to save.



New Module Instance

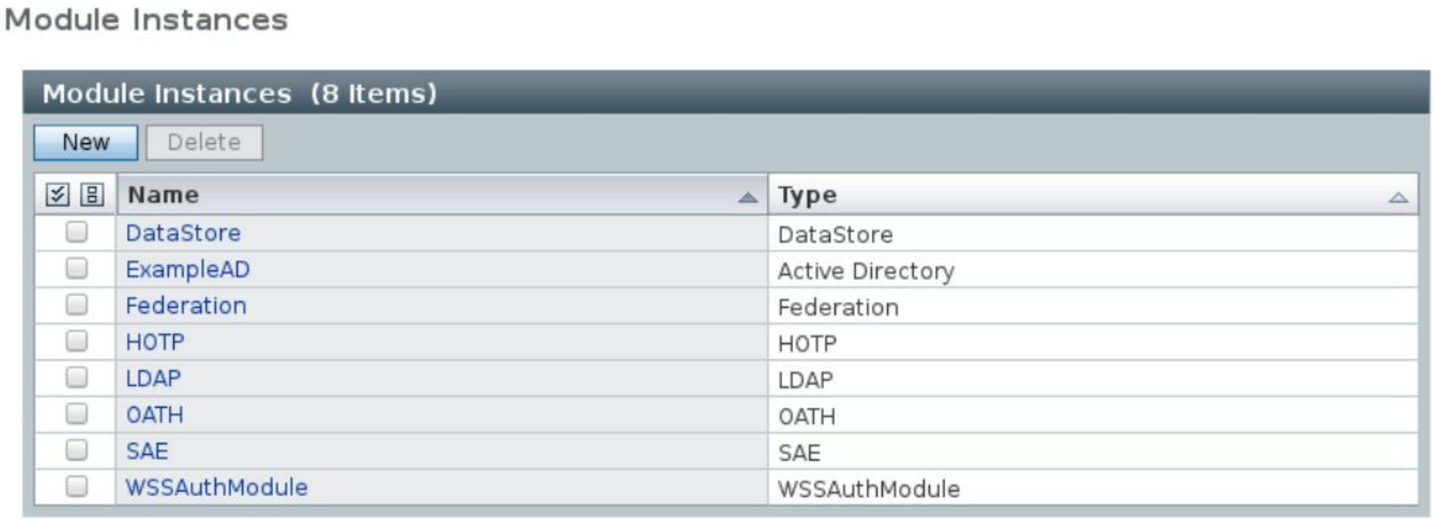
* Indicates required field

* Name: ExampleAD

* Type:
- ● Active Directory
- ○ Adaptive Risk
- ○ Anonymous
- ○ Certificate
- ○ Data Store
- ○ Device Print
- ○ Federation
- ○ HOTP
- ○ HTTP Basic
- ○ JDBC
- ○ LDAP
- ○ Membership
- ○ MSISDN
- ○ OATH
- ○ OAuth 2.0
- ○ Persistent Cookie
- ○ RADIUS
- ○ SAE
- ○ SecurID
- ○ Windows Desktop SSO
- ○ Windows NT
- ○ WSSAuth

Figure F-3

Scroll down to the `Module Instance` section, select the module that was created.



Module Instances

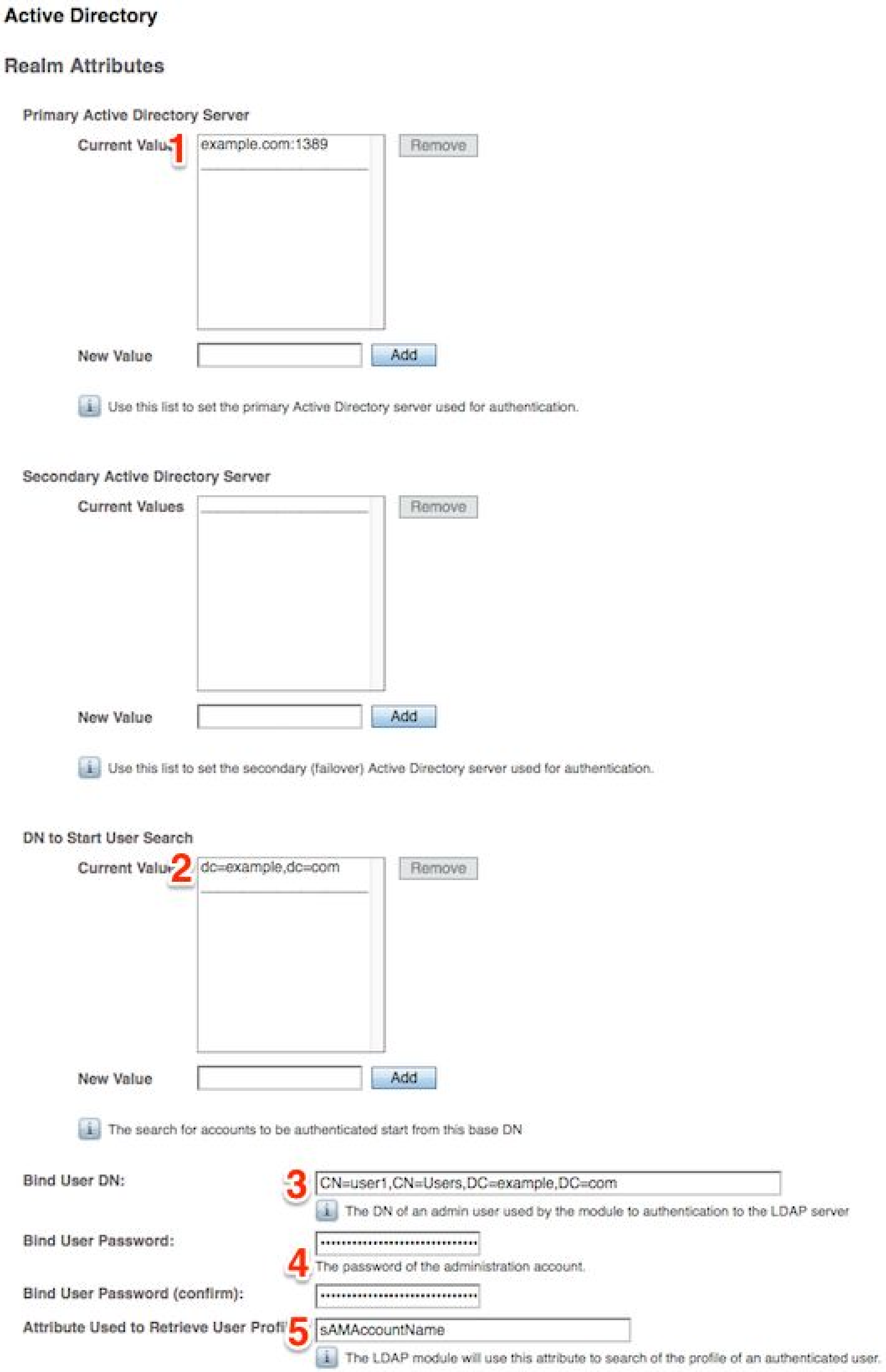
Module Instances (8 Items)

☐	Name	Type
☐	DataStore	DataStore
☐	ExampleAD	Active Directory
☐	Federation	Federation
☐	HOTP	HOTP
☐	LDAP	LDAP
☐	OATH	OATH
☐	SAE	SAE
☐	WSSAuthModule	WSSAuthModule

Figure F-4

Use the parameters in G.1., to fill out the relevant information. The numbered list below corresponds to the annotated screenshot in Figure F-5. Examples for 1.b, 2.b, 3.b 7 are found above in Section F.1

1. Active Directory Server
    a. Remove `localhost:1389`
    b. Add `SERVERNAME:PORT` (Port 3268 is default; 3269 is default for SSL/TLS)
2. DN to Start User Search (Search Base)
    a. Remove `dc=isn,dc=rsna,dc=org`
    b. Add DN to Start User Search
3. Add Bind User DN
    a. Remove `cn=amldapuser,ou=DSAME Users,dc=isn,dc=rsna,dc=org`
    b. Bind User DN
4. Enter Bind User Password
5. Attribute Used to Retrieve User Profile
    a. Add `sAMAccountName`
6. Attributes Used to Search for a User to be Authenticated
    a. Remove `uid`
    b. Add `sAMAccountName`
7. Add User Search Filter (optional)
8. SSL/TLS Access to Active Directory Server
    a. Check `Enabled` if using SSL. See Section F.3 below if the signing CA of the certificate is not already trusted.
9. Return User DN to DataStore:
    a. Uncheck `Enabled`
10. User Creation Attributes. Add each on its own line.
    a. `sn`
    b. `fullName|displayName`
    c. `givenName`
    d. `cn|sAMAccountName`
    e. `uid|sAMAccountName`
    f. `sAMAccountName`



Active Directory

Realm Attributes

Primary Active Directory Server

Current Valu: example.com:1389 — Remove

New Value: Add

Use this list to set the primary Active Directory server used for authentication.

Secondary Active Directory Server

Current Values: Remove

New Value: Add

Use this list to set the secondary (failover) Active Directory server used for authentication.

DN to Start User Search

Current Valu: dc=example,dc=com — Remove

New Value: Add

The search for accounts to be authenticated start from this base DN

Bind User DN: CN=user1,CN=Users,DC=example,DC=com

The DN of an admin user used by the module to authentication to the LDAP server

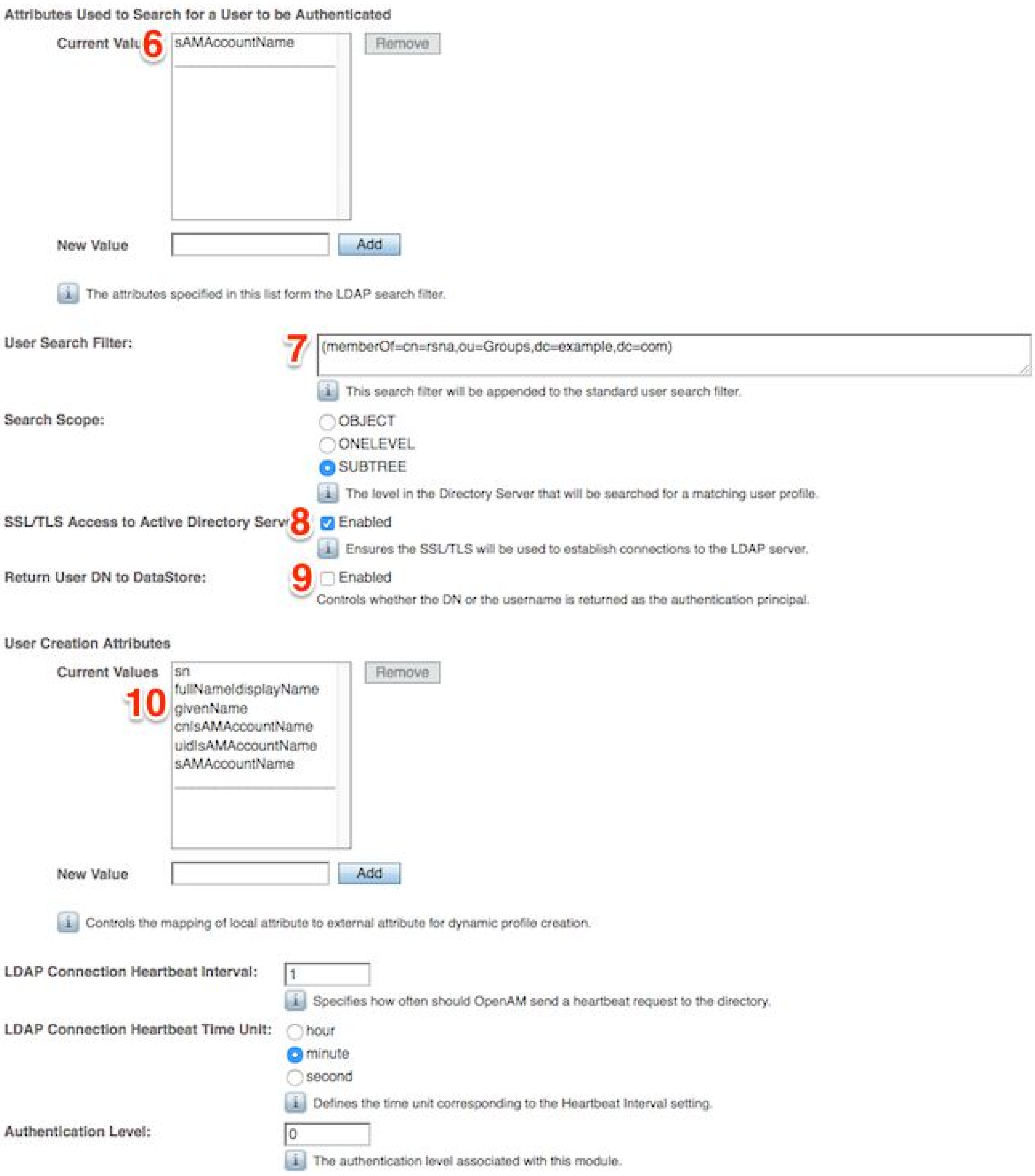
Bind User Password: ································

The password of the administration account.

Bind User Password (confirm): ································

Attribute Used to Retrieve User Profi sAMAccountName

The LDAP module will use this attribute to search of the profile of an authenticated user.



Attributes Used to Search for a User to be Authenticated

Current Valu sAMAccountName

New Value

The attributes specified in this list form the LDAP search filter.

User Search Filter: (memberOf=cn=rsna,ou=Groups,dc=example,dc=com)

This search filter will be appended to the standard user search filter.

Search Scope:
○ OBJECT
○ ONELEVEL
● SUBTREE

The level in the Directory Server that will be searched for a matching user profile.

SSL/TLS Access to Active Directory Serv ☑ Enabled

Ensures the SSL/TLS will be used to establish connections to the LDAP server.

Return User DN to DataStore: □ Enabled

Controls whether the DN or the username is returned as the authentication principal.

User Creation Attributes

Current Values
sn
fullName|displayName
givenName
cn|sAMAccountName
uid|sAMAccountName
sAMAccountName

New Value

Controls the mapping of local attribute to external attribute for dynamic profile creation.

LDAP Connection Heartbeat Interval: 1

Specifies how often should OpenAM send a heartbeat request to the directory.

LDAP Connection Heartbeat Time Unit:
○ hour
● minute
○ second

Defines the time unit corresponding to the Heartbeat Interval setting.

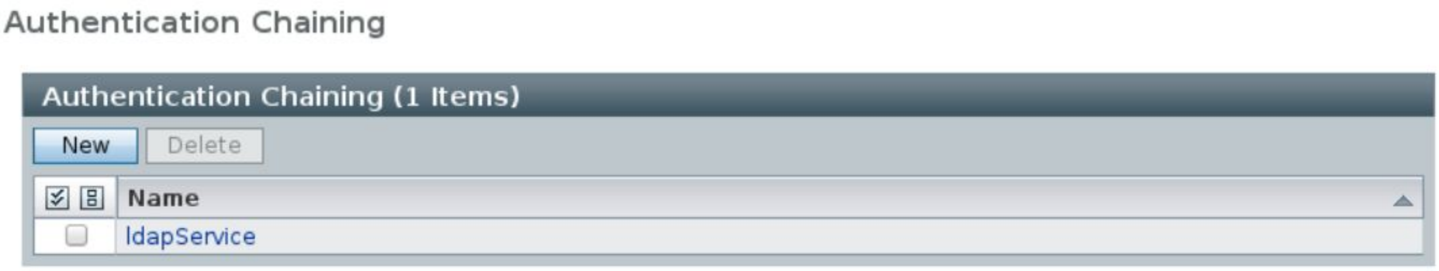
Authentication Level: 0

The authentication level associated with this module.

Figure F-5

Then click on `Save`, then `Back to Authentication`.

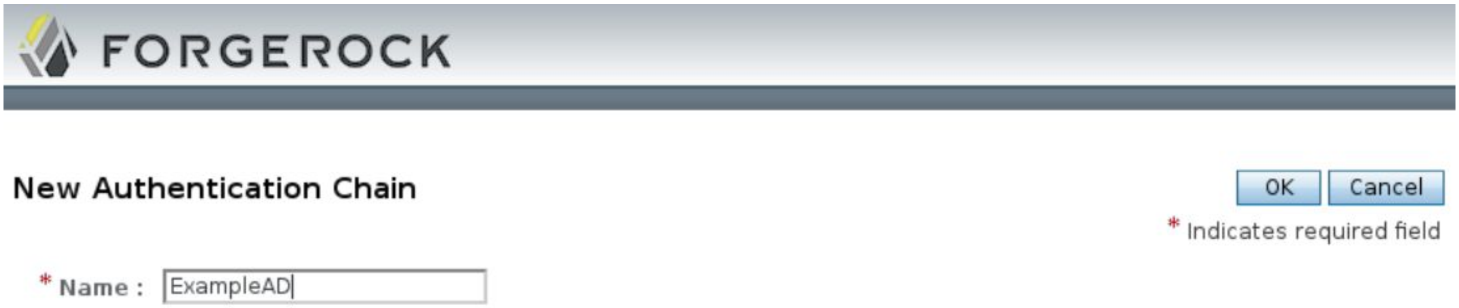
Under the Authentication Chaining section , click on `New`.



☐	Name
☐	ldapService

Figure F-6: Authentication Chaining

Enter a name for `Authentication Chain`, then click on `OK` to save.

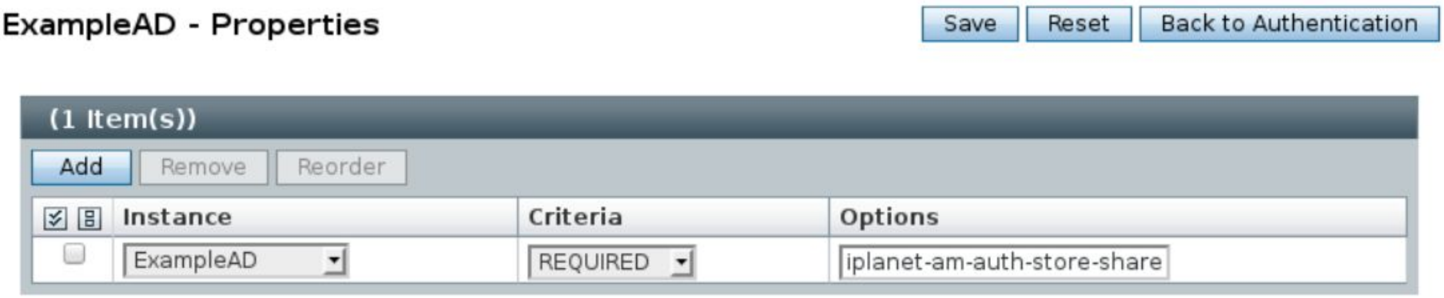


* Name : ExampleAD

Figure F-7: Creating a new authentication chain

Click on `Add`, then select for the module you created earlier. Choose `REQUIRED` in the `Criteria` field. Next, enter `iplanet-am-auth-store-shared-state-enabled=true` in the `Options` field. See Figure F-8.

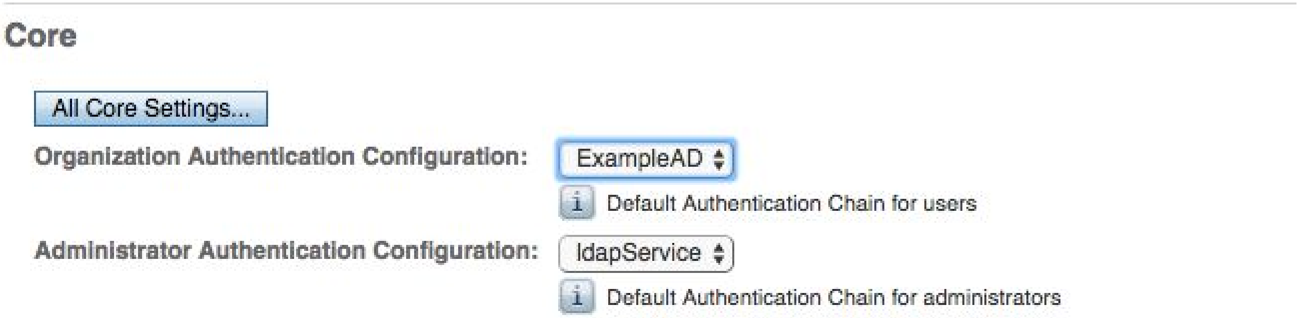
Click `Save`, then `Back to Authentication`



☐	Instance	Criteria	Options
☐	ExampleAD	REQUIRED	iplanet-am-auth-store-share

Figure F-8: Properties

In the Core section, select the authentication chain that was created from the previous step. See Figure F-9. Only set the `Organization Authentication Configuration`



Core

Organization Authentication Configuration: ExampleAD

Default Authentication Chain for users

Administrator Authentication Configuration: ldapService

Default Authentication Chain for administrators

Figure F-9: Core Settings

Click `Save` then `LOG OUT` on the top right of the page.

Browse to **http://edge-hostname.example.com:3000/** and login with the Active Directory user that will be the administration user. When the edge server page is loaded, logout of the edge server web interface.

Browse to **http://edge-hostname.example.com:3000/**openam/console
Login with the amAdmin user. Add the administrator user to the Admin group using the method in the user management section. Then `LOG OUT.`

F.3. Adding a Trust Store to OpenAM

If the Active Directory server is using SSL certificate not trusted by the default. The signing CA can be added to the trust store.

Add the certificate to truststore:

Copy certificate to the `/etc/pki/ca-trust/source/anchors` directory. The certificate should be in PEM or DER format.

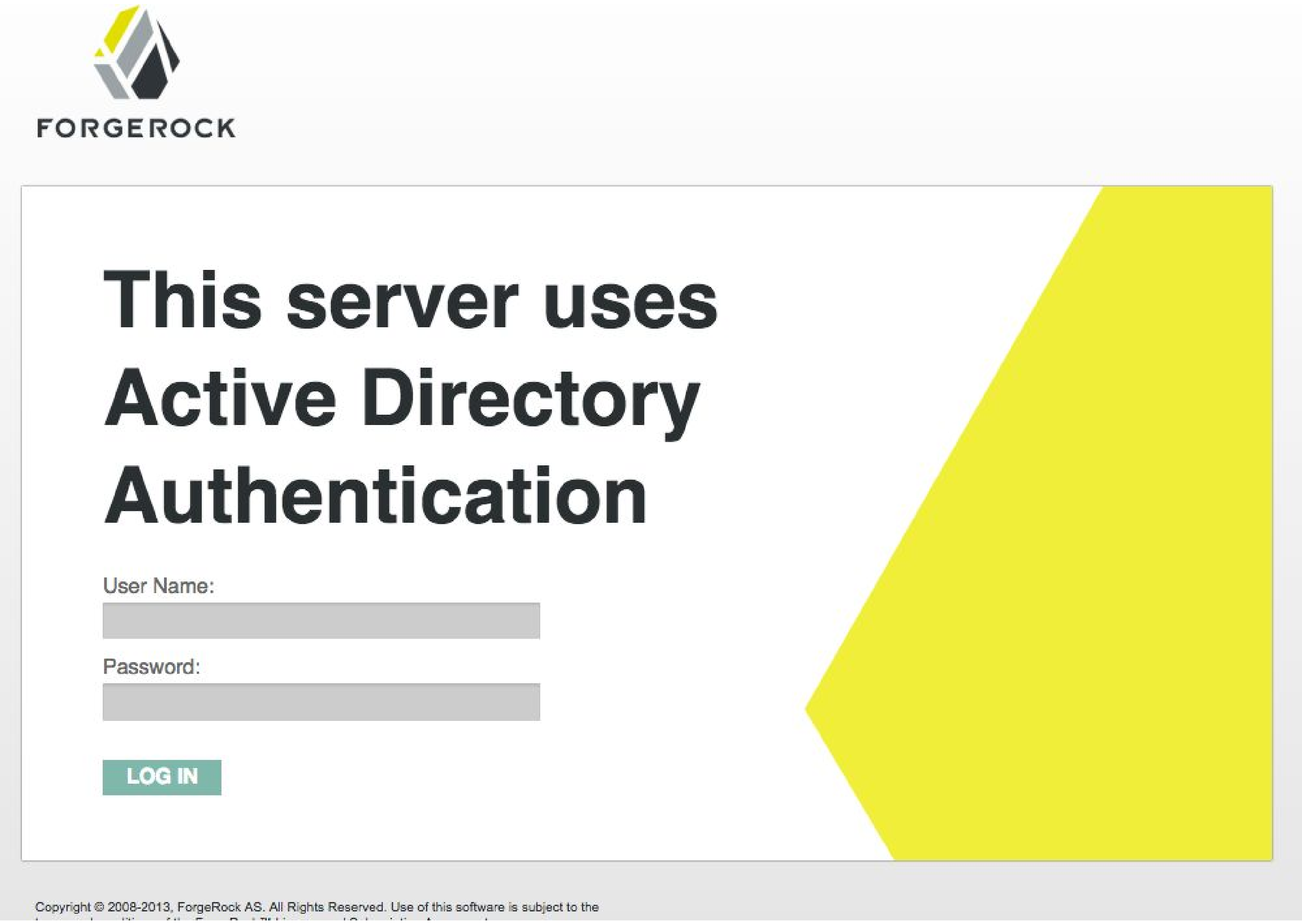
Run:

```
update-ca-trust extract
```

Restart torquebox:

```
sudo systemctl torquebox restart
```

Point your browser to http://edge-hostname.example.com:3000. The login page will now say `This server uses Active Directory Authentication.`



This server uses Active Directory Authentication

User Name:

Password:

Appendix G: Security Considerations and Password Management

G.1 Account Management

The Edge Server is built on the CentOS Linux distribution and has accounts with passwords at multiple levels that should be managed by the system administrator.

Application Accounts are provided to end users to perform web based access to the Edge Server user interface. These accounts do not allow access to the operating system. They are managed by OpenAM. In turn, OpenAM can be configured to use your enterprise Active Directory server (see Appendix F) to support single sign on within your organization.

The Edge Server is distributed with an admin account that uses the value “password” as the password. OpenAM has a default administrator account with the name amAdmin. As part of your configuration, you will set a password for that account.

Linux User Accounts are included on the Edge Server. In addition to the standard accounts created by the operating system, the Edge Server contains these accounts:

- rsna: A user account intended for an administrator to login to the system and perform administrative and maintenance operations.
- edge: A user account not intended for user login. This account is used by the system to run the Edge Server applications. The account is not enabled for user login. Do not enable this account for user login; do not set a password for this account.

The Edge Server is shipped using the standard CentOS username/password system. We do not document the procedure, but CentOS supports user account management using Active Directory (or other LDAP implementation). This means that you can add enterprise user accounts to your Edge Server by managing your user accounts with Active Directory.

Postgres Accounts are maintained by the Postgres database with the Postgres password based authentication system. These accounts are included with the Edge Server:

● postgres:	Standard postgres administrative account
● edge:	This account owns the database tables which are directly accessed by the Edge Server.
● mirth:	This account owns database tables in the Mirth HL7 interface.

Mirth Administrative Account: A single administrative account is used for the Mirth HL7 interface. The account name is admin and is managed directly by the Mirth software.

G.2 File Security

The Edge Server software is stored in these folders:

```
/usr/local/edge-server
/usr/local/mirthconnect
```

These folders are owned by the edge Linux user account and are generally world readable. Data files that might contain PHI or database passwords are protected so that only the edge account (or the root account) can view the contents of those files.

G.3 Postgres Security

The Postgres database system supports different mechanisms (local sockets, network connection to localhost, network connection from a remote host) to access the database that are configured in the Postgres file pg_hba.conf. The Edge Server is configured so that all methods require a password to access data within the database. Even the standard database account with the postgres name requires a password. The administrator may change that configuration to fit local needs. We do not recommend using the “trust” method in the Postgres pg_hba.conf file as that has the potential to allow unauthorized users to have access to the patient records in your database.

G.4 Changing Passwords

Because the default passwords of the Edge Server are included in this documentation and in other public locations, we recommend that you change the passwords listed in this document to more secure values that are known to your administrative staff. Passwords at the application level for end users are obviously known only to those end users.

Application Accounts:
Passwords are managed using Active Directory (if so configured) or through the OpenAM application. See Section 7 of this document. The overall

Linux User Accounts:
Linux user accounts are not needed by end users. You manage Linux user accounts using standard Linux tools that are not described here.

Postgres Accounts
You need to change passwords for the Postgres accounts in both the database and in Edge Server configuration files.

To change the passwords in the Postgres database, use this command:

```
psql -d postgres -U ACCOUNTNAME -c “\password”
```

Where ACCOUNTNAME is postgres, edge or mirth. You will be prompted for the existing password and then have the opportunity to change the password per your local requirements.

If you change the postgres passwords for any of the accounts, you will need to change values in the following files (depending on the actual postgres account).

Postgres Account	File to Update
postgres	
edge	Prep & Transfer Content Apps: Update the `rsnadb.password` property in the `$RSNA_ROOT/conf/database.properties` file. Token App (Torquebox Web Server): Update the web server configuration file found here: `$RSNA_ROOT/torquebox-3.1.2/jboss/standalone/configuration/standalone.xml`. The password property is easily located by searching for the string "edge" in this file. Mirth Connect: If you have not yet configured your Mirth Connect HL7 channels and you intend to start with the "Mirth Backup.xml" file supplied with the edge server, update that file with the new password for the edge account. The file is "`$RSNA_ROOT/Mirth\ Backup.xml`". If you have already configured your Mirth Connect software, you will need to update the "Get Database Connection" code template as described in section 2.10.2 Configuration and Management. Please note that we are referring to the postgres password for the edge account and not the mirth account. This is sometimes referred to as a setting for rsnadb. Monitoring Software: There are two instance of the rsnadb password in the file `$RSNA_ROOT/monitor-scripts/edgeserver_monitor.sh`. Find and update both instances. Once instance is a comment, but update the comment for consistency.
mirth	First ensure that Mirth is configured to use PostgreSQL (see 2.4.1 Configure Mirth to Use Postgres). Next update the `database.password` property in the `/usr/local/mirthconnect/conf/mirth.properties` file. Monitoring Software: There are two instance of the mirthdb password in the file `$RSNA_ROOT/monitor-scripts/edgeserver_monitor.sh`. Find and update both instances. Once instance is a comment, but update the comment for consistency.

After you have changed the passwords in these files, reboot the Edge Server. This will force all of the applications to read the updated passwords from the configuration files and will be synchronized with your database updates.

Mirth Administrative Account

When you first configure the Mirth software, you will be prompted for the admin account and password. You will use the values admin/admin. At that point, you will be prompted to enter a new password. You can enter a more secure password at this point.

If you need to update the Mirth admin password, refer to Section 2.10 of this document for logging in to the Mirth administrative system.

You do not need to update any files nor do you need to reboot the Edge Server if you change this password.

Appendix H: Changing Hostname/FQDN for a Configured Edge Server

You may find it necessary to change the hostname/FQDN (fully qualified domain name) for an already-configured edge server. For example, your IT staff may require the name of the host to change from edge.xyz.org to edge-01.xyz.org due to new network/naming policies. This appendix outlines the steps needed to properly configure the OpenAM software to recognize the modified hostname.

Here are the steps you can follow to do the hostname/FQDN change:

Step 0. Read All Instructions First

1. Please read all steps below before starting.
2. You will change the hostname entries for the computer in a later step.

Step 1. Add the New FQDN as an Alias

1. Login to OpenAM console as administrator: amAdmin.
2. Under **Access Control > / (Top Level Realm)**, add the new FQDN to the Realm/DNS Aliases list, and then save your work.
   Note: Do not remove the old FQDN at this point; you will change the configuration file to point to your new FQDN in Step 2, Item 4 below.

Step 2. Export, Edit, and Import the Service Configuration

1. Create a file /tmp/pwd.txt, insert it with the password for the user amAdmin (which you set in the first-time OpenAM configuration), and change the file's attribute to "readonly to owner":
   ```
   vi /tmp/pwd.txt
   ```
   <put the password of amAdmin in to the file, save and quit>
   ```
   chmod 400 /tmp/pwd.txt
   ```
2. Extract the Password Encryption key field for your server. You will need it for the export step below. You find this using the OpenAM console: **Configuration > Servers and Sites > Server Name > Security**
3. Export the service configuration. In the command below, $encrypted is the password encryption key you extracted in the step above.
   ```
   sudo $RSNA_ROOT/ssoadm/openam/ssoadm export-svc-cfg -u amAdmin -e
   $encrypted -f /tmp/pwd.txt -o config.xml
   ```
   OpenAM should respond with the message:
   ```
   Service Configuration was exported.
   ```
4. Edit the generated service configuration file config.xml
   a. Change all instances of the original FQDN to the new FQDN.
   b. If you also plan to change the domain name (say from .westmr-imaging.com to .consolidated-imaging.org, you will also need to change the value of that domain name in config.xml.
      i. This is just the domain name (full host name less the host part). For example, if the new host name is bay3.consolidated-imaging.org, the domain name is consolidated-imaging.com.

   ii. Also note the domain name in the value is preceded by a single period character: **<Value>.consolidated-imaging.com</Value>**.
   iii. After changing the FQDN (e.g., mr.westmr.com) to the new name, you should be able to search for the domain name (westmr.com) in the configuration file. Change all occurrences to the new value (e.g., consolidated-imaging.org).

5. Import the updated service configuration.

```
sudo $RSNA_ROOT/ssoadm/openam/ssoadm import-svc-cfg -u amAdmin -e
$encrypted -f /tmp/pwd.txt -X config.xml
```

   You will be prompted as follows:

```
Directory Service contains existing data. Do you want to delete it?
[y|N] y
Please wait while we import the service configuration...
Service Configuration was imported.
```

Step 3. Edit OpenAM Configuration Files for the New Hostname

1. Edit the bootstrap file, `$RSNA_ROOT/openam-cfg/bootstrap`, changing the FQDN, port, and deployment descriptor for OpenAM as necessary.
2. Edit the configuration file `/etc/rsna.conf`. Change the OPENAM_URL to use the new FQDN for your system.

Step 4. Change the hostname for VM

1. Edit `/etc/hosts`; change the old host name to new one;
2. Edit `/etc/hostname`; change the old host name to new one.
3. If needed, also change to use new IP address (see Section 2.6 of this manual).
4. Reboot the edge server to ensure that the new hostname is recognized by the operating system and all services.

Step 5. Check if the New Hostname Works

1. Open your web browser to http://<new FQDN>:3000 and verify that you can still login with different accounts:
   a. amAdmin
   b. admin
   c. At least one user account without import/export rights
   d. At least one user account with Retrieve and Research Send rights (if you are using that feature).