Navigator
User Manual

LAUREL BRIDGE

Providing DICOM Connectivity for the Medical Community

Laurel Bridge Software, Inc.
302-453-0222
www.laurelbridge.com

Document Version: 2.1.9
Document Number: LBDC-000089-0219
Last Saved: 7/18/2018 11:35:00 AM

Contents

1 What is Navigator?

Navigator is a collection of software applications that assist in the automation of fetching DICOM objects. Navigator applications focus on reliability, flexibility, and a simplified user experience.

Legacy archives often have features that present challenges for moving DICOM data, including:

- Merger of two or more archives
- Access to historical relevant priors
- Mismatched patient/study information
- Archive vendor proprietary issues
- Private DICOM tag handling
- Non-compliant/inconsistent DICOM data
- Unknown size of the job
- Uncertainty of completeness
- Inability to validate the data moved
- Excessive manual effort
- Inability to pre-fetch relevant priors
- Unresponsive support

Navigator allows the user to **automate the process** of collecting information from multiple medical image archives and fetching relevant priors based on that information.

Using built-in reporting systems, the user is able to **determine exactly what has moved** and what has not. Navigator ensures that exams are moved in a timely way and that they are available for use in their entirety on the target systems - all automatically.

From start to finish, the goal of Navigator is to provide a complete and transparent view of the issues related to moving DICOM studies, plus provide options to **automatically control and report the movement of the DICOM data** in a simple, high-level way, freeing the user to concentrate on other tasks.

1.1 Overview – Priors Fetching Basics

Priors fetching is defined as the process of locating relevant DICOM exams (studies) and transferring them from one location to another. This is typically done prior to the reading of a current exam so that that the reading radiologist has copies of any earlier exams available for comparison to the current exam. An automated priors fetcher makes a determination of what exams should be moved, a list of exams to move are collected, and then subsequently moved.

2 Installation

2.1 Recommended System Specification

The system may be dedicated hardware or may be a virtual machine. The suggested configuration is:

- Intel i5, 8GB RAM, 500GB HD or better
- Windows 10 or Windows Server 2008 R2, Server 2012/2014/2016 or newer

2.2 System Software Prerequisites

Standard Installation – Navigator utilizes several components that must be installed for it to work properly. The software prerequisites are:

- Microsoft .NET Framework 3.5 SP1
- Microsoft SQL Server 2008 R2 SP2 Express x64 or SQL Server 2008 R2 SP2 x64, or SQL Server 2012/2014/2016 x64 or newer
- ***SQL Management Studio for SQL Server 2008 Express*** or ***SQL Server 2008*** or newer
- A recent web browser – suggested: Google Chrome

Cluster Installation – If Navigator is being installed as part of a Windows Failover Cluster, then the Windows Server 2008 R2 operating system must be installed and the following prerequisites must be installed prior to installing Navigator:

- Microsoft .NET Framework 3.5 SP1
- Microsoft SQL Server 2008 R2 SP2 x64 or newer
- **SQL Management Studio for SQL Server 2008 x64** or newer

IMPORTANT NOTE ON SOFTWARE UPDATES:

For running this application we recommend that it be installed on a supported operating system and that there be a regular application of updates and security patches to that system.

Regular system backups are encouraged. A backup, especially of the application configuration data, including rules, scripts, and filters, should be made before applying any system updates. It may be "easy" to re-install the application, but it may not be easy to re-create your local configuration without a backup.

We also recommend that automatic updates be disabled on systems; while we encourage updates, especially security updates, we do recommend testing and manual application of such updates.

A system administrator should manage and be present for the application of any upgrades and for any system re-boot – for whatever reason. Be wary of unintended consequences like privileges, permissions, or firewalls that change as a side-effect of patches.

Handle these activities in a controlled and planned manner; always have a plan and methodology that will allow you to back out of changes. In the event that an update proves undesirable for any reason, the process should allow the changes to be rolled back to the previous state. Most of the time things will go well, but remember that there is always the possibility that bad things will happen when you make changes.

Your operating system vendor has likely published best practices for managing patches and updates. Take the time to read them as well as to read the documentation that may be provided with any patches or updates.

2.3 Installing and configuring SQL Server 2008 R2 SP2 Express x64

These are instructions for installing SQL Server Express in its most basic configuration for use by Navigator. These instructions are valid for Windows 7 and Windows Server 2008. If you have older versions of SQL Server installed or if you are installing the full version of SQL Server or if you are using SQL Server authentication mode, then your installation procedure may be different.

1. Log in to Windows as a user with administrative privileges
2. Run the **SQL Server 2008 R2 SP2 Express x64** installer
3. On the **Setup** screen, select **New installation or add features to an existing installation**
4. On the **License Terms** screen, Accept the license, click the **Next>** button
5. On the **Setup Support Files** screen make sure all of the checkboxes are checked for all of the **Instance Features**, click the **Next>** Button
6. On the **Instance Configuration** screen the defaults should be correct.
   The named instance should be **SQLExpress**. Allow it to install in the default location, which should be **C:\Program Files\Microsoft SQL Server**
7. On the **Server Configuration** screen the defaults should be fine for the **Service Accounts** tab and the **Collation** tab defaults.
8. On the **Database Engine Configuration** screen on the **Account Provisioning** tab, select **Mixed Mode** if you want to use **SQL Server Authentication**, or select **Windows Authentication Mode** to use **Windows Authentication**. The Current user (who ***must*** have Administrative Privileges) should be in the list under **Specify SQL Server Administrators**. If it is not, click the button to **Add Current User**. Leave the defaults on the other three tabs. If you are using **Mixed Mode**, specify the password for the (**sa**) account as **N@vigator1**. (See section 2.3.3 if you wish to use a non-administrative user.)
9. On the **Error Reporting** screen click the **Next>** button.
10. Installation should complete in several minutes.
11. **Reboot** the system.
12. From the Windows Start Menu: `Start → Microsoft SQL Server 2008 R2 → Configuration Tools → SQL Server Configuration Manager`
13. **Double-click** on SQL Server Network Configuration → Protocols for SQLEXPRESS → TCP/IP
14. On the IP Addresses tab, under the IPAll group, set the TCP Dynamic Ports to **9003**
15. Close the dialog.
16. **Right-click** on SQL Server Network Configuration → Protocols for SQLEXPRESS → TCP/IP and select **Enable**
17. **Right-click** on SQL Server Services → SQL Server(SQLEXPRESS) and select **Restart**.
18. SQL Server has now been configured for use by Navigator.

2.3.1 Reconfiguring SQL Server

If you are installing Navigator on a machine that already has SQL Server installed, you may need to reconfigure SQL Server so that Navigator can connect to it.

1. From the Windows Start Menu: `Start → Microsoft SQL Server 2008 R2 → Configuration Tools → SQL Server Configuration Manager`
2. **Double-click** on SQL Server Network Configuration → Protocols for SQLEXPRESS → TCP/IP
3. On the IP Addresses tab, under the IPAll group, set the TCP Dynamic Ports to **9003**
4. Close the dialog.
5. **Right-click** on SQL Server Network Configuration → Protocols for SQLEXPRESS → TCP/IP and select **Enable**
6. **Right-click** on SQL Server Services → SQL Server(SQLEXPRESS) and select **Restart**.
7. **Exit** SQL Server Configuration Manager.

8. From the Windows Start Menu: `Start → Microsoft SQL Server 2008 R2 → SQL Server Management Studio`
9. **Right-click** on the name of the SQL server and select **Properties**.
10. Select the **Security** page.
11. Under Server Authentication, click **Windows Authentication mode** to use only **Windows Authentication**, or click **SQL Server and Windows Authentication mode** to allow **SQL Server authentication**. Then click **OK**.
12. **Right-click** the name of the SQL Server and click **Restart**.

2.3.2 To enable the sa login

1. From the Windows Start Menu: `Start → Microsoft SQL Server 2008 R2 → SQL Server Management Studio`
2. In Object Explorer, expand **Security**, expand **Logins**, right-click **sa**, and then click **Properties**.
3. On the **General** page, you might have to create and confirm a password for the login.
4. On the Status page, in the Login section, click **Enabled**, and then click **OK**.

2.3.3 Using a non-administrator user

For security reasons, you may at times wish not to use the **sa** (administrator) user. If so, modify the SQL installation steps described above to avoid enabling the **sa** login. Instead, you should create a different database login that will act as the owner of the Navigator database, and you should create the Navigator database yourself.

1. Open SQL Management studio:
   `Start Menu → Microsoft SQL Server 2008 R2 → SQL Server Management Studio`
2. **Login** using SQL Server authentication as a database administrator.
3. Create the Navigator database. Remember the name you choose, since you will need it when you install Navigator.
   a. From the Object Explorer open the Databases subtree.
   b. **Right-click** and select **New Database…**
   c. Enter the database name and click **OK**
4. Create the new user and his password. Remember these values, since you will need them when you install Navigator.
   a. From the Object Explorer open the Security subtree.
   b. **Right-click** and select **New Login…**
   c. Enter the login name and password; select SQL Server authentication and uncheck "**enforce password expiration**" and "**user must change password at next login**". Set the default database to be the Navigator database you created in Step 3.
5. Assign the role of database owner of the new Navigator database to the user you created.

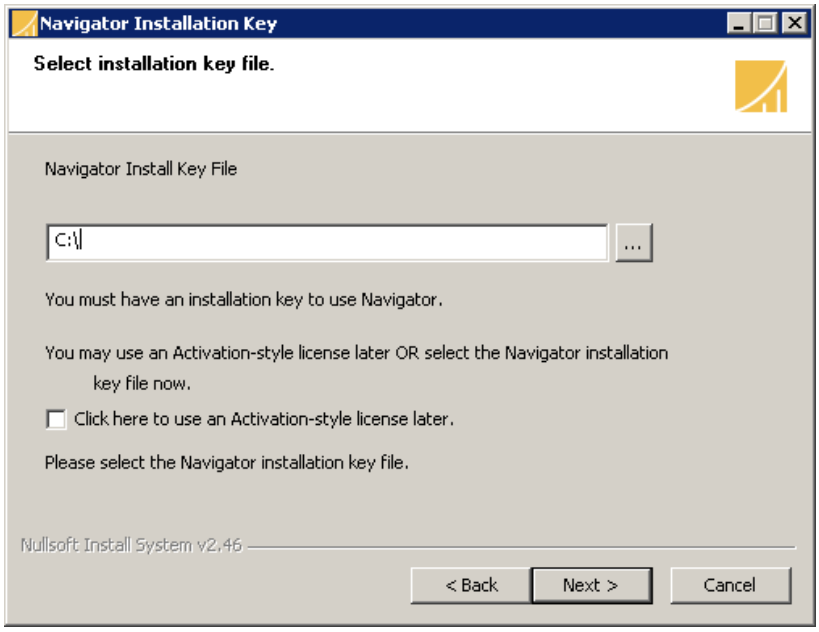
Note that you don't need to create the tables in the Navigator database – the Navigator software will do that itself when it accesses the database as the database owner.

2.4 Navigator Main Software Installation

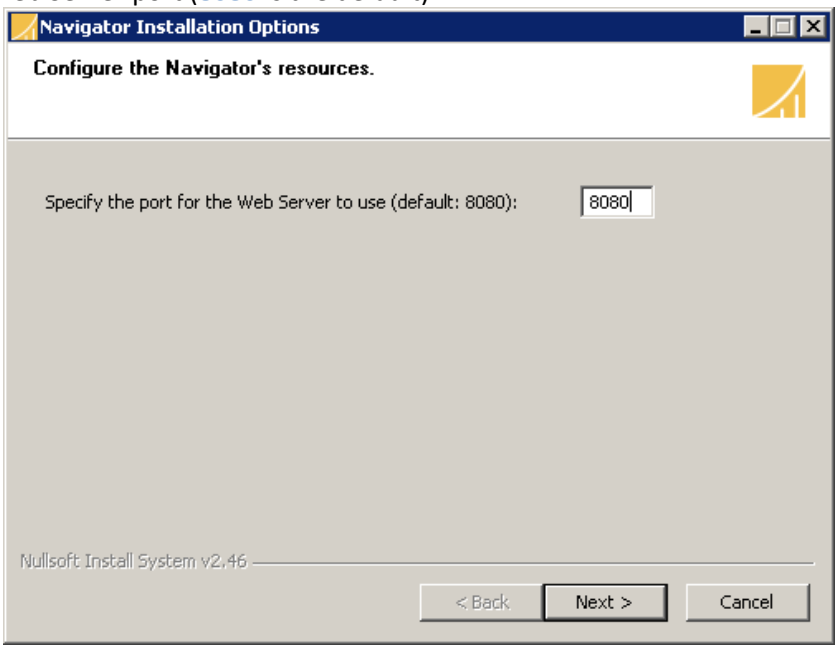
After installing the prerequisites, the Navigator application installer (**Install_Navigator.exe**) should be run. For machines with an older version installed, you may need to uninstall the old version, install the new version, and then copy the configuration data from the older version to the new version. **Note** also that you should be logged in as a user with administrative privileges in order to install/uninstall Navigator and to modify the system settings; you may need to right-click on the installer icon and select "**Run as administrator**".

1. **Accept** the license agreement.
2. Choose an installation directory; default is **C:\LB_Navigator**.
3. Select a Navigator license file. The license installation key is typically downloaded and is stored in a file with the ".key" extension, e.g.,
   `NAVIGATOR-2.1.x-DM-company-site-host-YYYYMMDD-xx.xx.xx.xx.xx.xx.key`
   Press the "…" button to select the license key file, and then press the "Next" button to continue with the installation.

   Alternatively, if you have a Product Serial Number for an Activation-style license, click the checkbox to activate it later in the installation, and then press the "Next" button to continue with the installation.

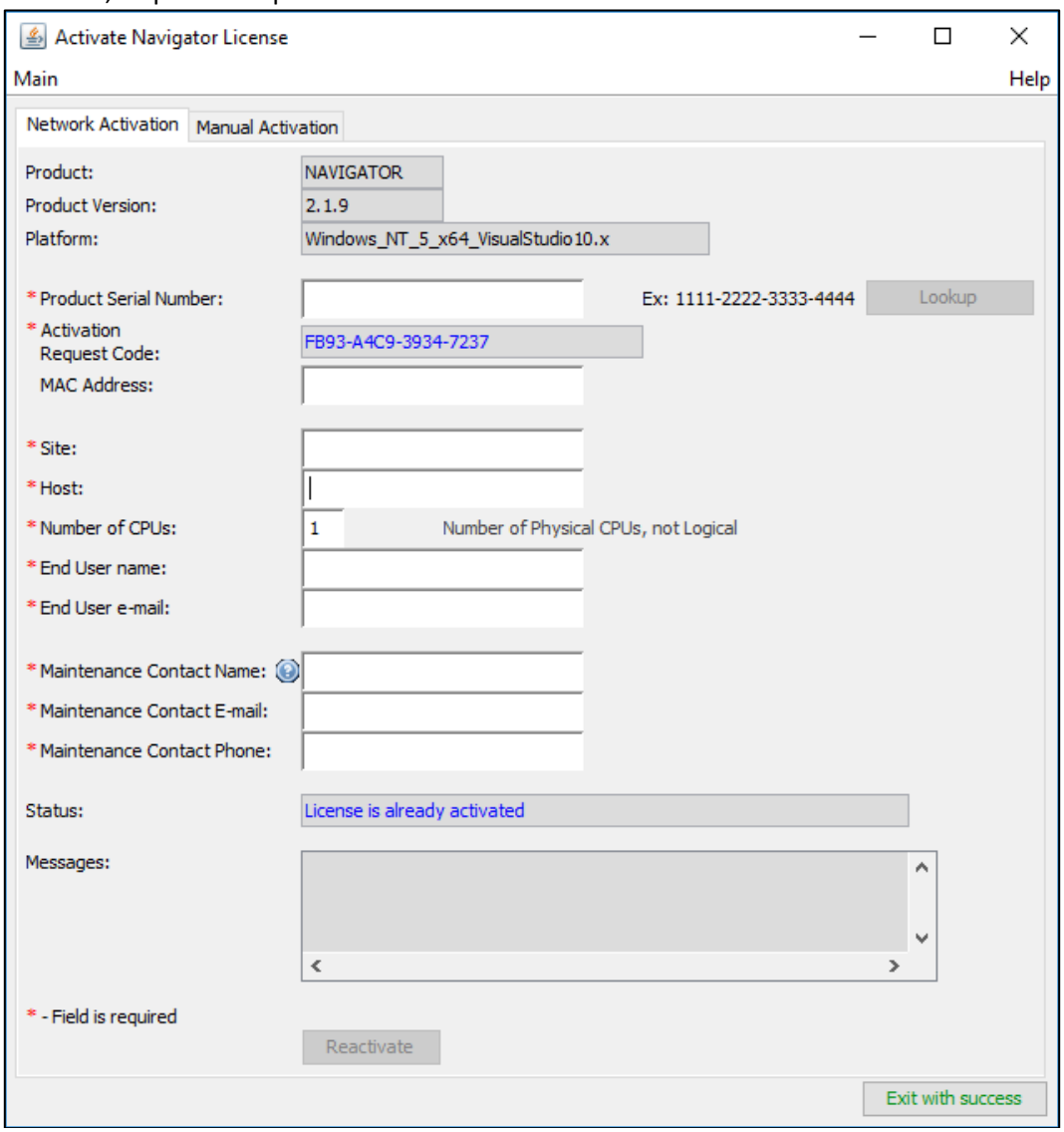


4. Specify the Web Server port (**8080** is the default).



5. The installer will copy the Navigator files to your system and then set up Navigator's environment.

6. If your license requires activation or you were given only a Product Serial Number, you must activate the license before you can use Navigator. If this is so, you will be given the option of activating the license during installation – you can also choose to activate it later, via the Windows Start menu. If you choose to activate it now (***which is recommended***), the installer will launch the License Activation Utility, shown below – note that it can take several seconds to start the first time that it is run, so please be patient.



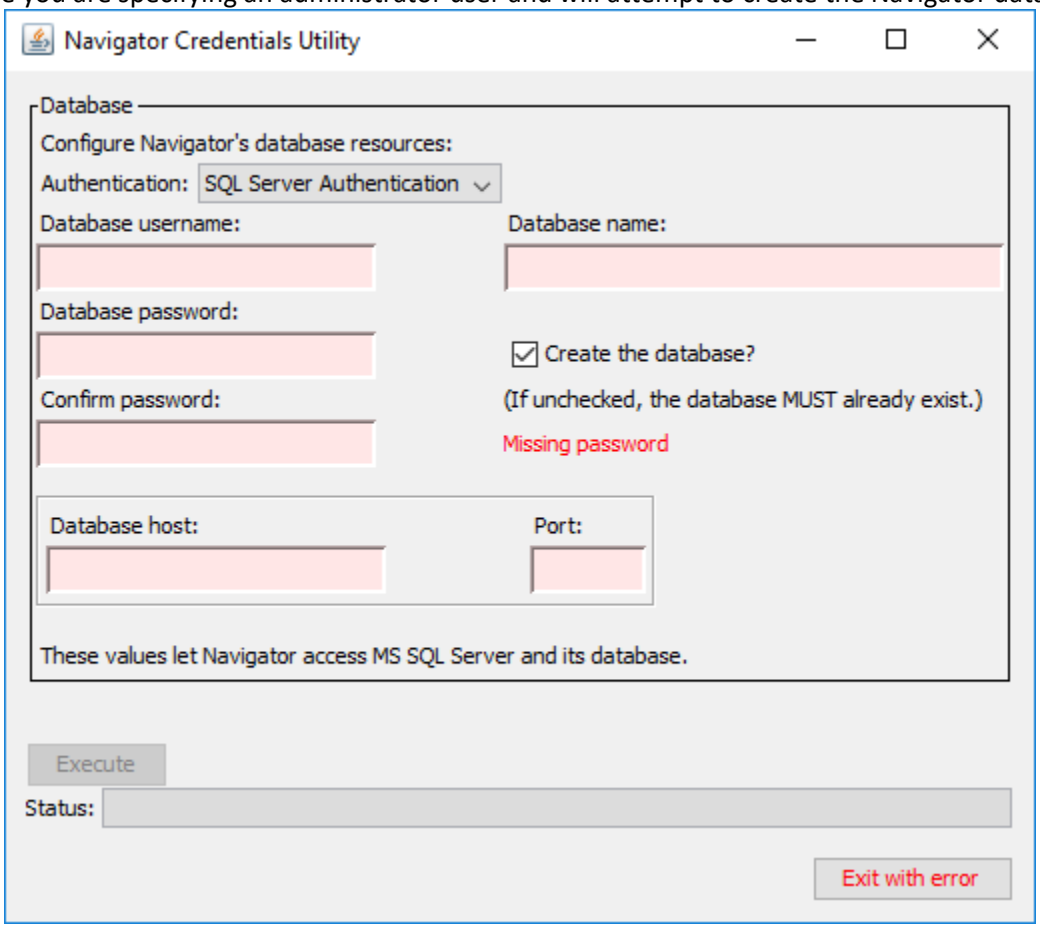
Fill out ***all*** the fields (only the MAC Address is optional) and press the "**Activate**" button. Once the license is successfully activated, exit the utility by pressing the "**Exit**" button. The installation will continue. (See section **7.5 Activate License** for more information on License Activation and its modes, including how to do **Manual Activation**.)

7. The installer will now launch the **Database Credentials Utility**. Enter the database credentials from installing SQL Server; alternatively you may use the values that you chose above if you are using a non-administrator user (see **2.3.3 Using a non-administrator user** above).
    - Select the Authentication mode – **SQL Server Authentication** or **Windows Authentication** – depending on how you configured your SQL Server above. Some of these fields are not required if you are using Windows Authentication.
    - Database username: **sa**

- Database password: **N@vigator1**
- Database name: **Navigator1**
- Database host: **localhost**
- Database port: **9003**

Once all the fields are filled in, click the Execute button. If the utility fails, correct the credentials and try again. Once the utility has successfully completed, click **Exit with Success**.

Note: If you are using a non-administrator user, you should have already created Navigator's database. In this case, uncheck the "**Create the database**" box; if the box is checked, the utility will assume you are specifying an administrator user and will attempt to create the Navigator database.



Note: you may need to modify your firewall's settings to allow communication on the Database port that you specify, as well as for the Web Server port.

8. If you receive an error message you will need to manually create the Navigator database.
   a. Open SQL Management studio:
      `Start Menu → Microsoft SQL Server 2008 R2 → SQL Server Management Studio`
   b. **Login** using SQL Server Authentication using the **sa:N@vigator1** login credentials (or your appropriate credentials).
   c. From the Object Explorer open the Databases subtree.
   d. **Right-click** and select **New Database…**
   e. Enter the name Navigator1 and click **OK**
9. **Reboot** your computer.
10. Navigator is ready to use.

2.4.1 Quiet Mode Installation

If you want to script the installation of Navigator, you will want to run the installer but without any user interaction. It is possible to run the Navigator installer from a command-line or batch script, passing the configuration options on the command line.

1. Install and configure SQL Server as described in **Section 2.3 Installing and configuring SQL Server 2008 R2 SP2 Express x64 above**.
2. Run the Navigator installer, specifying the Web Server Port and the Installation directory, like this:

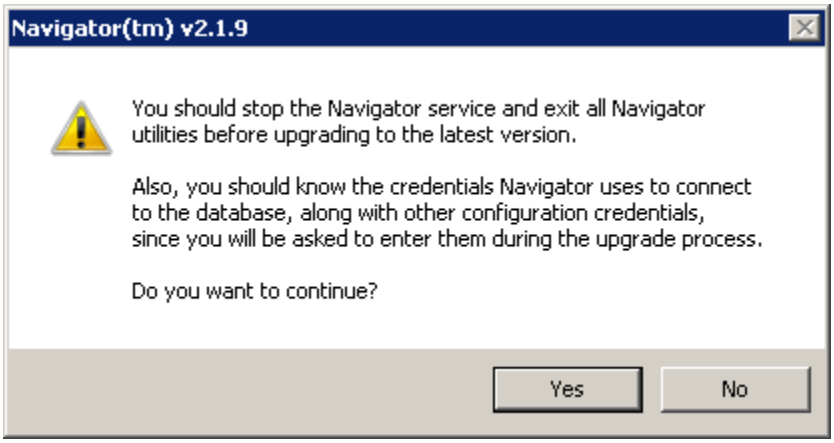
   ```
   Install_Navigator.exe /QUIET=true /WEBPORT=8080 "/INSTDIR=C:\LB Navigator"
   ```

   Note that the case of the options is important, as is the placement of the quotes around the **INSTDIR** option. You can choose different values for the port or for the installation directory. If the installation succeeds, the installer will exit quietly; however, messages may appear if an error occurs during installation.
3. **IMPORTANT:** Activate your license by running the **License Activation Utility** from the Windows Start menu – see **Step 6 above** and **Section 7.5 Activate License** for more information.
4. **IMPORTANT:** The database must still be created. From the Windows Start menu, run the **Database Credentials Utility**; enter the name of the database and the credentials to access it. See **Step 7 above** and **Section 7.1 Change Database Credentials** for more information.
5. **Reboot** your computer.
6. Navigator should now be ready to use.

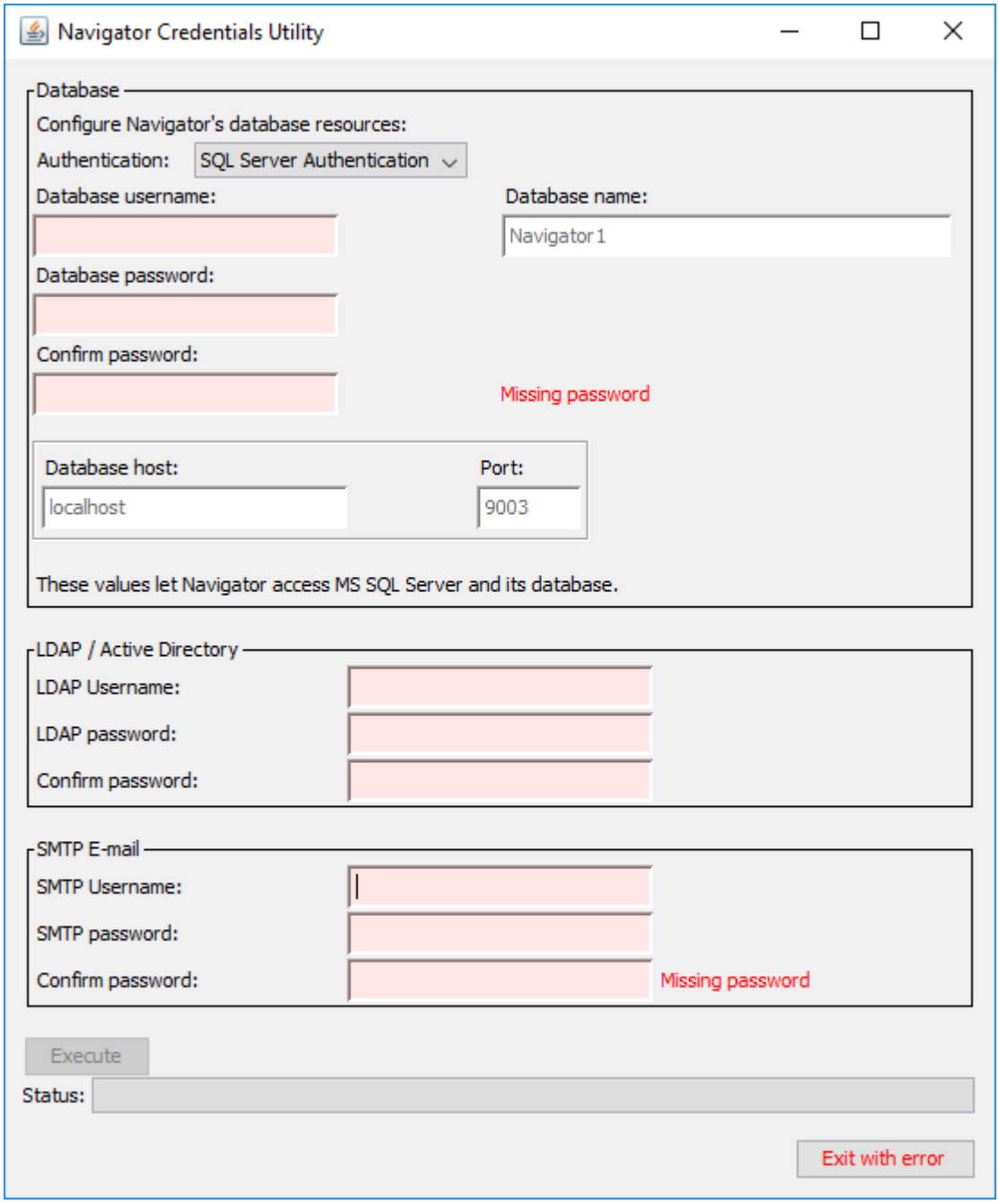
2.5 Upgrading Navigator

When upgrading from version 2.*, you do not need to uninstall Navigator first. As a precaution, make a backup of the existing configuration before installing – it is found in the directory `C:\ProgramData\Laurel Bridge Software\Navigator2`.
Note that you must be logged in as a user with administrative privileges in order to upgrade Navigator. **Also**, you should know your database access credentials – username and password – before upgrading, since you will have to enter them during the upgrade process.

1. Stop the Navigator services (see **Navigator Service Manager below** for an easy way; be sure to exit the Service Manager). Also exit from any of Navigator's utilities, as these will be upgraded, too.
2. Run the new Navigator installer.
3. Confirm that you are upgrading, and then that you know the database credentials to be used when upgrading. You may also have to reenter other configuration credentials when upgrading – see step 7 below.



4. Choose your license – if you are using an Activation license, click the checkbox to activate it later. (***Note*** that you will need to have a license appropriate to the version of Navigator you are upgrading to – you can request a new license by submitting a **License Transfer Form** to Laurel Bridge Software.)
5. The installer will upgrade your Navigator files – this may take a few minutes, so please be patient.
6. If you are using an Activation license, activate it now – see Step **6 above** for more information. (***Note*** that you will need to make sure you have a license appropriate to the version of Navigator you are upgrading to – if your maintenance support is up to date, reactivating the license may automatically provide you with the correct key.)
7. Enter your database credentials; some fields may not be required if SQL Server is configured to use Windows Authentication. If your Navigator was configured to use LDAP or SMTP (for e-mail notifications), you may need to reenter those credentials, too. Click **Execute,** and then click the Exit button once the utility has succeeded.



Reboot your computer.

8. Navigator is ready to use.

2.6 Uninstalling Navigator

Uninstalling Navigator requires deleting the files that were installed and removing its environment settings. You should be logged in as a user with administrative privileges in order to remove Navigator and its system settings.

Before uninstalling Navigator, you should make sure that its services are stopped. The easiest way to do this is via the **Navigator Service Manager**. Once both services are stopped, exit the Navigator Service Manager. Also, close any of Navigator's utilities that are in use.

To remove Navigator, open the `Control Panel`, go to `Programs and Features`, and choose `Laurel Bridge Navigator` and then `Uninstall`.

```
Start -> Control Panel -> Programs and Features -> Laurel Bridge Navigator
```

Then click "`Uninstall/Change`" or "`Uninstall`" (the exact wording may differ depending on the version of Windows OS).

2.6.1 Removing PHI

Note that uninstalling Navigator will not remove its configuration settings, its log files, or any information stored in the database, which may include patient Protected Health Information, or **PHI**. Navigator processes PHI transiently and may retain some traces of PHI in the associated database, log files, and audit trails. Generally, Navigator behaves as follows:

- Database records of studies are automatically purged on a configurable time interval. However, failed jobs may be retained until manually removed.
- Log files are managed as a rotating set of logs that overwrite old data at some configurable point. Logging may also be configured so that all data is retained until the system consumes all available storage.
- Audit trails are not deleted. Manual intervention is required to manage such data.

Since PHI may have been stored in the log files and in the database, it is up to you to delete those files and/or database records.

- Delete the log files in the `C:\ProgramData\Laurel Bridge Software\Navigator2\log` directory.
- Use SQL Server Management Studio to delete the database records that you do not want to keep.
    - **Login** using SQL Server Authentication using administrative login credentials.
    - From the Object Explorer open the Databases subtree.
    - Select the **Navigator1** database (or whatever name you specified when you installed Navigator).
    - To delete ***all*** the records in the database, the easiest way is to **right-click** on the **Navigator1** name and select **Delete**. This will remove the database from SQL Server. You should also use File Explorer to find the relevant MDF and LDF database files and delete those.
    - To delete only specific data records, open the **Tables** subtree.
        - To delete *all* Worklist Items, **right-click** on **dbo.worklist_item** and select **Delete** – this will delete the table and all its data. Alternatively, to delete only specific records, click **Edit Top 200 Rows**, then select the records you want to remove, **right-click**, and select **Delete**; repeat as needed.
        - To delete *all* Study Move Requests, **right-click** on **dbo.study_move_request** and select **Delete** – this will delete the table and all its data. Alternatively, to delete only specific records, click **Edit Top 200 Rows**, then select the records you want to remove, **right-click**, and select **Delete**; repeat as needed.
        - To delete *all* Audit records, **right-click** on **dbo.audit_record** and select **Delete** – this will delete the table and all its data. Alternatively, to delete only specific records,

click **Edit Top 200 Rows**, then select the records you want to remove, **right-click**, and select **Delete**; repeat as needed.

These are the only tables that may have PHI in them. You can use the above steps on the other tables if you want to delete the Contact Information (**dbo.contact_information**) or the users who have access to Navigator (**dbo.sec_user**).

These instructions apply if you are decommissioning the system that Navigator was installed on and wish to remove any PHI that may be on the system. These instructions should **not** be used if you plan to continue using Navigator but wish to remove old data.

3 Navigator Configuration Worksheet

3.1 DICOM Device Configuration Prerequisites

Both the Source PACS and the Destination PACS must be configured to communicate with each other and with Navigator. Enabling this may require configuring a new AE Title and hostname/port configuration on both the Source and/or Destination PACS. The typical configuration changes required are summarized below:

1. For any priors fetching configuration:
   a. The **Source PACS** should recognize **Navigator** as a DICOM Query/Retrieve SCU device.
   b. The **Destination PACS** must recognize **Navigator** as a DICOM Query/Retrieve SCU device.
   c. The **Source PACS** must be configured with the **Destination PACS** as a DICOM C-MOVE destination (C-STORE SCP).
   d. The **Destination PACS** must be configured with the **Source PACS** as a DICOM C-STORE client (C-STORE SCU).
2. For a C-FIND multiplexer configuration:
   a. The **Modalities** must be configured with **Navigator** as a DICOM MWL SCP to issue C-FINDS.
   b. The **MWL Servers** must be configured with **Navigator** as a DICOM MWL SCU to issue C-FIND responses.
3. For a C-MOVE multiplexer configuration:
   a. Requirements are not defined here at this time.
4. Navigator itself can be configured to use any AE title.
5. Navigator may be configured to use any available TCP/IP port as its DICOM port. The most common and standard DICOM ports used are 11112 and 104.

Configuration and setup of the Navigator software is covered in **Section 4 Configuring Navigator**.

3.2 Configuration Worksheet

A configuration worksheet like that below can help to summarize the devices that Navigator will need to communicate with and how those devices' configuration may change.

A shared configuration worksheet is usually made available via a shared Google Drive document. Typically the vendor and client discuss the information required for configuration and may actually fill out the sheet together during a conference call that includes all the stakeholders in the deployment effort. All parties being able to share the view of the information and update it concurrently facilitates accurate and timely completion of the configuration planning.

A sample view of a shared work sheet like that which is typically used is found on the next page. This sheet may be customized to meet the needs of a specific site and deployment.

Configuration Worksheet: Navigator Priors Fetching Workflow - Laurel Bridge Software

Today: 4/1/2014

Triggers *How Navigator finds newly scheduled studies.*
Triggers are either DICOM Modality WorkList (MWL) servers that Navigator queries, or HL7 message sources which send to Navigator

Item	Description	Type	host/ip (for type = MWL)	AE Title (for type=MWL)	Notes
1					
2					

Sources *What systems are queried to find relevant prior studies*

Item	Description	host/ip address	port	AE Title	Notes
1					
2					
3					

Destinations *What systems are priors sent to (C-Move sent to Source with this device as destination)*

Item	Description	host/ip address	port	AE Title	Notes
1					
2					
3					
4					
5					
6					
7					
8					

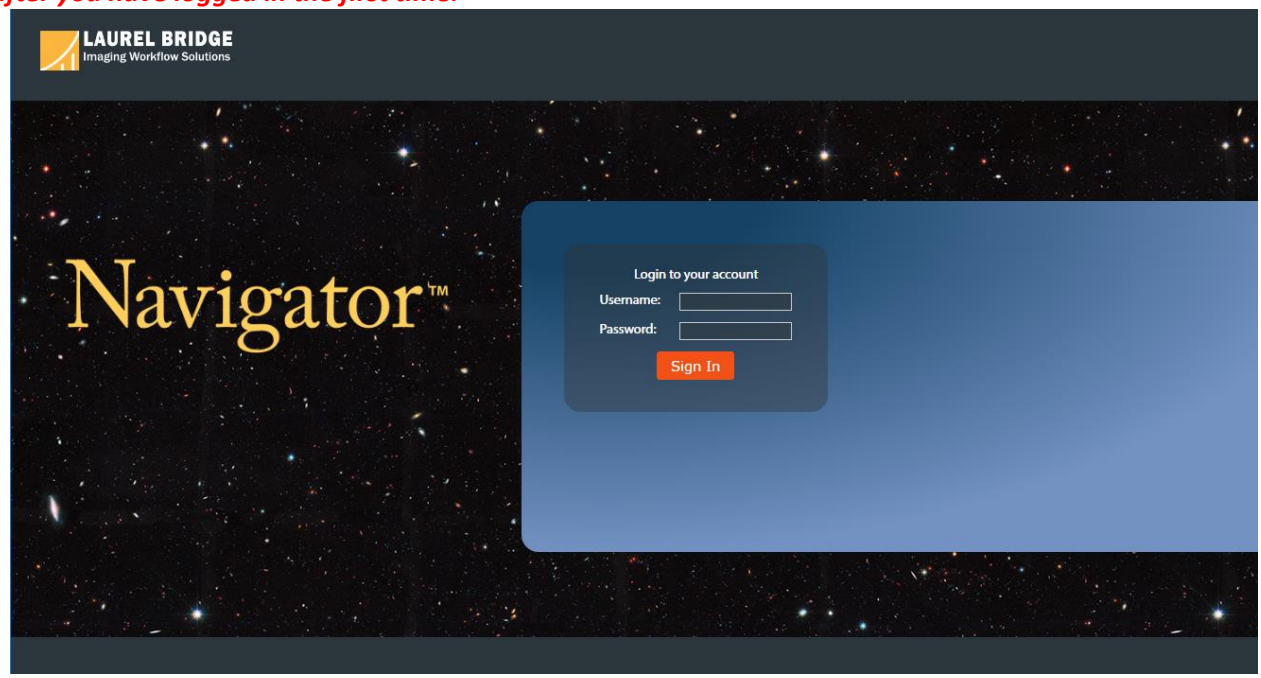
Study Rules Each Rule defines a particular workflow (type of new exams to process, sources to search for priors, destinations to send priors, relevancy rules)

Item	Description	Rule Selection	Sources	What to Query for	Which Priors Are Relevant	Destinations	Notes
		What information from the trigger causes this rule to be selected? Note: the first rule that matches is the only one selected.	Where does Navigator search for prior studies or series?	What DICOM elements are sent as "match" tags (M) and "return" tags (R)? Note any required processing of match tags (e.g. fuzzy name match).	Based on examining fields in the C-Find-Responses returned by the Sources	Where are priors sent?	
1							
2							
3							
4							
5							
6							
7							
8							

4 Configuring Navigator

Navigator is configured through a web interface – you can access the login page via the Windows Start menu: `Start → Laurel Bridge Software → Navigator → Access Navigator`. (See **Appendix D: Start Menu Options on Different Windows** for assistance on different versions of Windows.) On the Navigator's installation system, the URL will be something like **http://localhost:8080/Navigator**. Note that you can access Navigator from a web browser on any web-accessible machine on your network – just change "localhost" to be the name of Navigator's installation machine, e.g., **http://myNavigatorMachine:8080/Navigator**.

Your web browser will display the login page to access Navigator. The default username for administrative access is "administrator"; the default password is "LaurelBridge". ***You should change the default password after you have logged in the first time.***



4.1 Navigator's Main Screen

Once you have logged in, you will see Navigator's main screen – at the top are the buttons to **Start** and **Stop** Navigator's priors fetching processing, a button to log you out, Navigator's status, and counters showing the number of associations, worklist entries, and studies, along with other information. Below those is the menu of options: **Configuration**, **Logging**, and **Worklist Entries**. Taking up most of the screen is information on who should be contacted if a user has questions about Navigator's status (this information is configurable – see Section **4.8 Contacts**).

Important: You can return to this screen from any other screen by clicking the company logo in the upper-left corner or the Navigator link above the Start/Stop buttons.

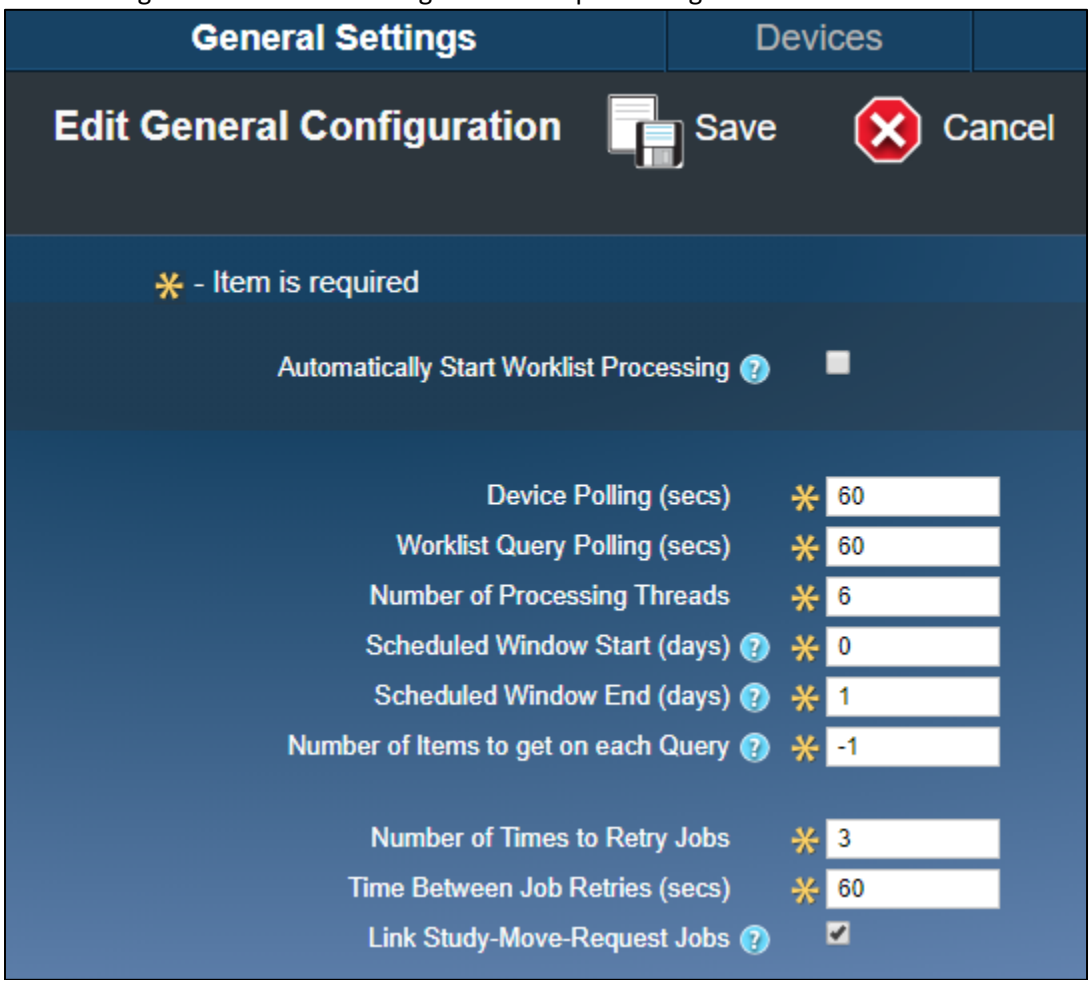
4.2 Configuration

When you click on the Configuration tab, you will see the options in Navigator that you can change: **General Settings**, **Devices**, **Study Rules**, **Worklist Readers**, **Scripts**, **Contacts**, and **Users**. From this page, you can also change your password. (Note that passwords should be at least 8 characters and have mixed case, unless you have enabled the **Require secure passwords** option on the **General Settings** page.)

You should first set the **General Settings** that affect Navigator's overall operation. Next you should define the **Devices** that Navigator will be querying and sending orders to. Third, you should define the **Study Rules** and how each Study Rule will decide which Worklist Entries to handle and how they should be processed; you may need to define **Custom Scripts** for specialized processing that is not defined in Navigator's user interface. Fourth, define the **Worklist Readers** and choose which Study Rules will be used by each Reader; this may also need a Custom Script for specialized processing of data. **Contacts** lets you declare the information that is shown when a user logs in. **Users** lets you add, delete, or modify the users and what each user can do in Navigator.

4.3 General Settings

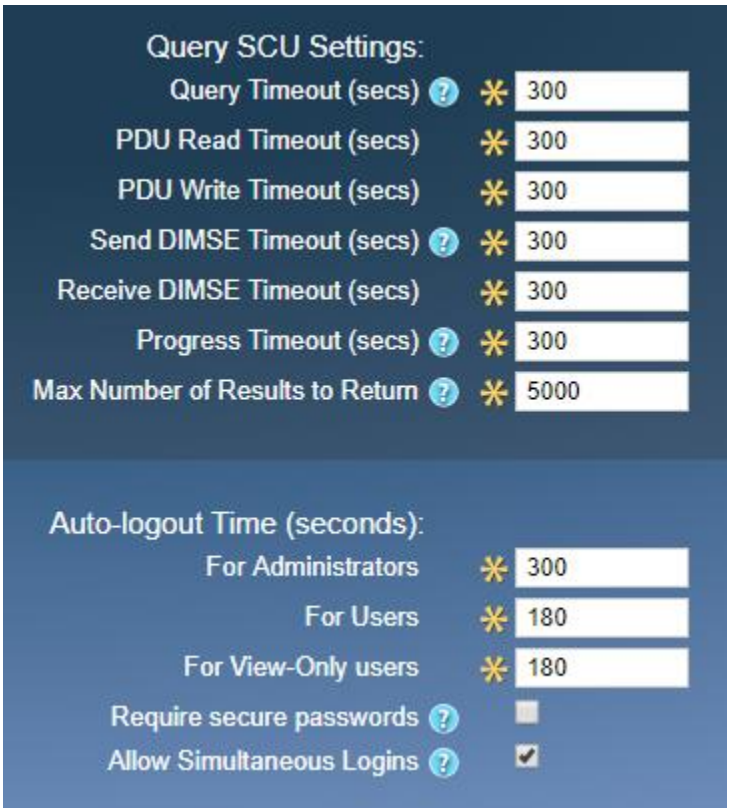
These are the settings that affect all of Navigator and its processing.



- **Automatically Start Worklist Processing** – If Navigator's host machine is rebooted, this setting affects if the priors fetching should start up automatically or if that must be started manually (via the Start/Stop buttons at the top).
- **Device Polling** – Devices are polled (sent a C-Echo) to check that they are "alive". This is how often they are polled.
- **Worklist Query Polling** – Worklist servers are polled to ask for new entries to be processed; this is how often those servers are polled. (Note that if the polling is too frequent, Navigator's processing of new items can be slowed down as it checks for duplicates.)
- **Number of Processing Threads** – Navigator can have several threads running simultaneously to speed up the processing of items. Since each thread is another connection to an SCP, this value should take into account how many connections your SCPs can handle.
- **Scheduled Window Start and End** – When querying a worklist server, these values tell how many days into the past and into the future to ask for items to process.
- **Number of Items to get on each Query** – How many items should be requested from the Worklist Server each time it is queried.

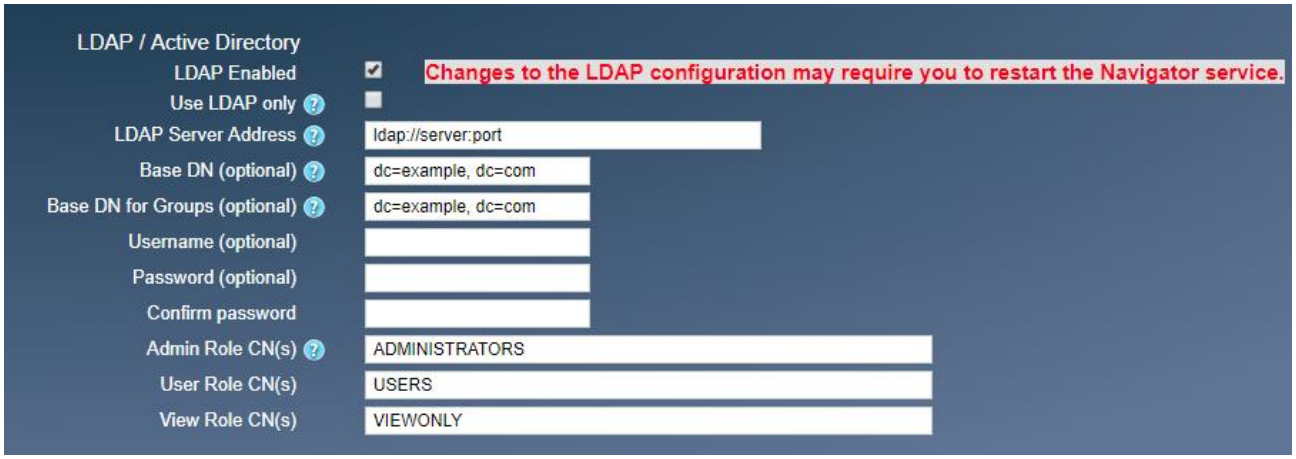
- **Number of Times to Retry Jobs** – How many times a job should be retried before it is marked as failed.
- **Time Between Job Retries** – How long to wait before retrying a job that has not yet succeeded.

- **Link Study-Move-Request Jobs** – Study Move Request Jobs will look for equivalent jobs that are running or have completed. If an equivalent one is found, then the current job will be marked as complete. This can reduce duplication of C-Move requests going from the same source to the same destination.



- **Query Timeout** – How long a query operation should be allowed to run before it is considered to have failed.
- **PDU Read / Write Timeout** – Maximum time to wait for a PDU to be read or written.
- **Send / Receive DIMSE Timeout** – Maximum time to wait for all results to be returned
- **Progress Timeout** – Timeout if no progress is being made on a Find or Move operation
- **Max Number of Results to Return** – Maximum number of Query results to return; this is used to prevent Navigator from being overwhelmed with data when searching for Priors.

- **Auto-logout Times** – You can adjust how long a user can be inactive before Navigator will log the user out. The three settings are for **Administrators**, **Users**, and **View-Only** users (see **Section 4.9 Users** for an explanation of each level).
- **Require secure passwords** – Passwords must be at least 8 characters in length and have both *UPPER* and *lower* case characters. Enable this option to require them to be at least 12 characters and to also have numbers or special characters. (This option does not apply if LDAP is exclusively used for authentication – see the LDAP configuration information below.)
- **Allow Simultaneous Logins** – By unchecking this box, you can prevent users from logging in to Navigator from different machines at the same time. Users will have to logout from Machine A before they can login from Machine B. Being auto-logged out due to inactivity is the same as if you manually logged out.

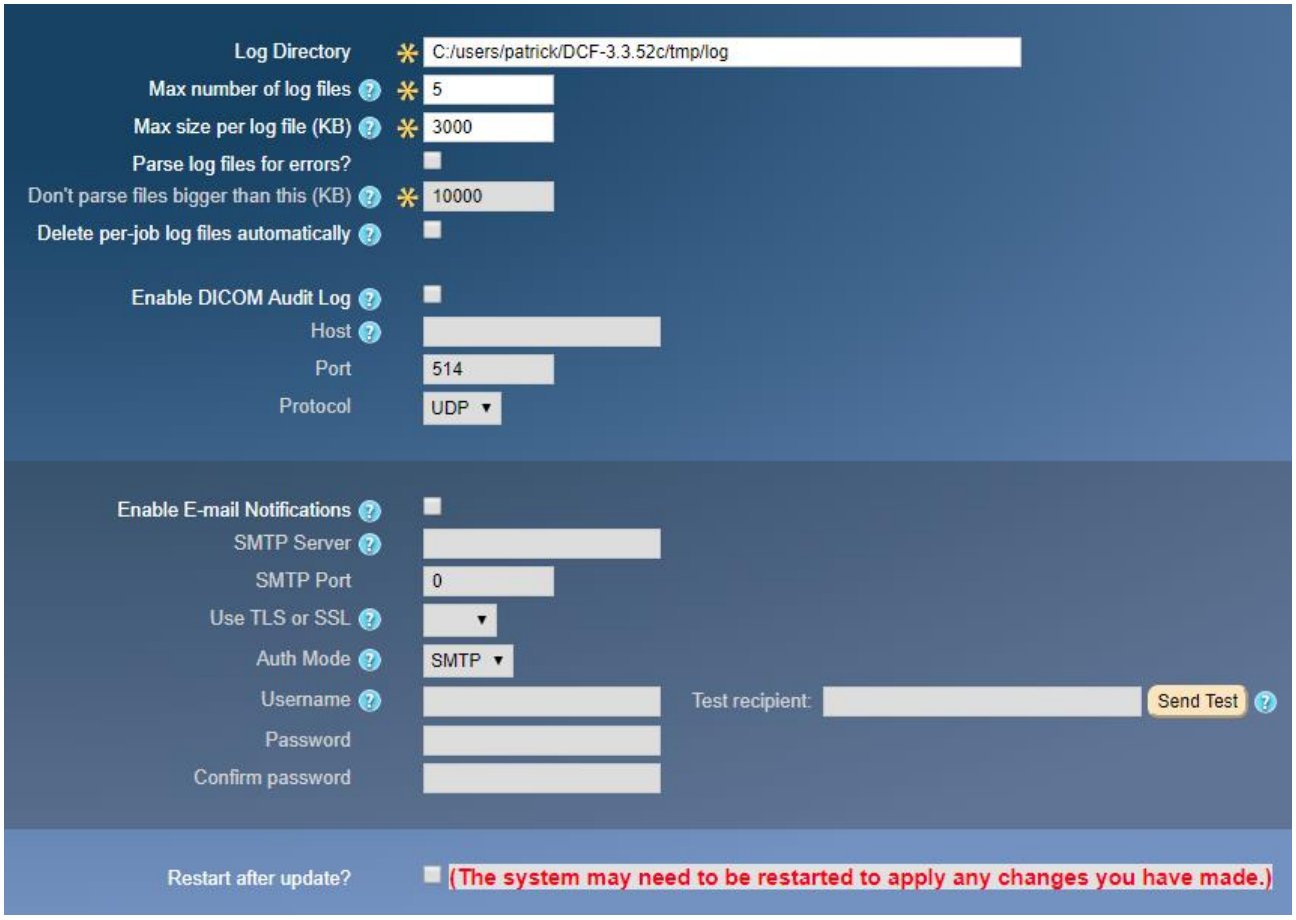


Navigator supports LDAP / Active Directory for user account login to its interface. Configure it with these settings:

- **LDAP Enabled** – Check this box to use LDAP / Active Directory to manage user logins.
- **Use LDAP only** – Check this to authenticate users using LDAP only. If this is unchecked, Navigator's locally administered users may also be used. (See **Section 4.9 Users** for more information on Navigator's users.)
- **LDAP Server Address** – The URL of the LDAP server to use; note the value should be formatted as "`ldap://<server-name>:<port>`".
- **Base DN** – The root from which all queries will be performed.
- **Base DN for Groups** – The base DN from which the search for group membership should be performed. (In some situations, this may have the same value as **Base DN**.)
- **Username** and **Password** – The credentials used to connect to the server. Note that you will have to confirm the password by entering it twice.
- **Admin Role CN(s)**, **User Role CN(s)**, and **View Role CN(s)** – These are the groups (LDAP Common Names [CN]) that will map to the **Administrator**, **User**, and **View-Only** permissions when accessing Navigator. The CNs are comma-separated to allow for specifying multiple values that map to a single role. (See **Section 4.9 Users** for more information on each permission level.)

Note that any changes to the LDAP configuration may require you to restart the Navigator *service* – the simplest way to do this is via the **Navigator Service Manager**.

See **Section 4.9 Users** for information on the users that are built in to Navigator and their permission levels. For more information on what each LDAP setting means, go to **http://grails-plugins.github.io/grails-spring-security-ldap/v2/guide/configuration.html**



- **Log Directory** – the directory where Navigator's log files are stored.
- **Max number of log files** – Navigator uses rotating log files to minimize the amount of disk space consumed by the logs. Set this value to be the maximum number of files that Navigator will rotate through.
- **Max size per log file** – When a log file is bigger than this value, Navigator will create a new log file and write to it; this is used with the above "max number of log files" as part of the rotating log files.
- **Parse log files for errors** – Check this if the log files should be automatically parsed for any errors when you click the Logging link. Note that this can take a lot of time as the number or size of the log files grow.
- **Don't parse log files bigger than this** – If log files should be parsed, you can specify that some files are too big and shouldn't be parsed.
- **Delete per-job log files automatically** – Automatically delete the log files associated with a job when the job is removed from the processing list. Otherwise, you should manually delete them.

- **Enable DICOM Audit Log** – Also send DICOM audit log messages to a SysLog server.
- **Host / Port** – The SysLog server's name (or IP Address) and port
- **Protocol** – The protocol to use when connecting to the SysLog server; choices are UDP, TCP, and TLS.

- **Enable E-mail Notifications** – You can configure Navigator to send an e-mail when certain events occur, such as a device going offline. Turn all e-mail notifications on or off via this checkbox.
- **SMTP Server / Port** – The SMTP Mail server and port to use for e-mail notifications
- **Use TLS or SSL** – Use TLS, Secure Sockets Layer, or none when connecting with the mail server.

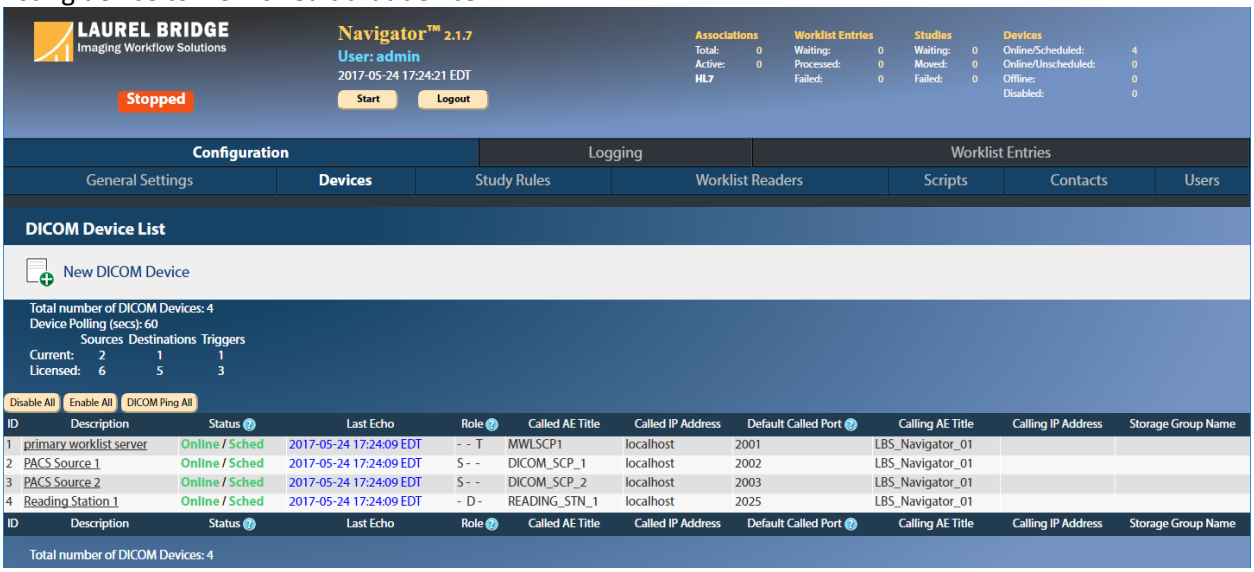
- **Auth Mode** – Mode for authenticating the connection to the Mail server. Use **POP3** to authenticate to a POP3 Server before sending e-mail via open SMTP; use **SMTP** to authenticate directly with the SMTP server.
- **Username** and **Password** – The credentials for authentication. Note that you will have to confirm the password by entering it twice.
- **Test recipient** – You can send a test message to an e-mail address as a way of verifying that the E-mail settings are correct.

- **Restart after update** – when you change one of these settings, Navigator must be restarted. Check this to restart the processing right away; otherwise, you will need to click the Start/Stop buttons at the top.

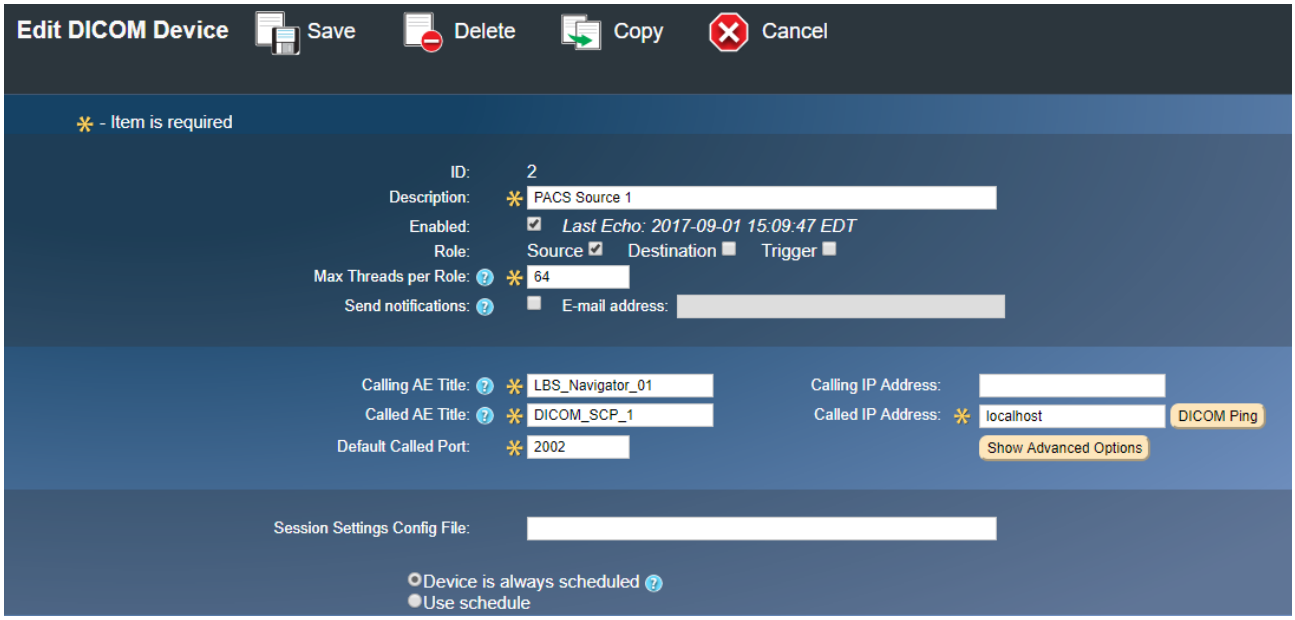
Once you have changed the settings, click the **Save** button near the top; if you don't want to save your changes, click **Cancel**.

4.4 Devices

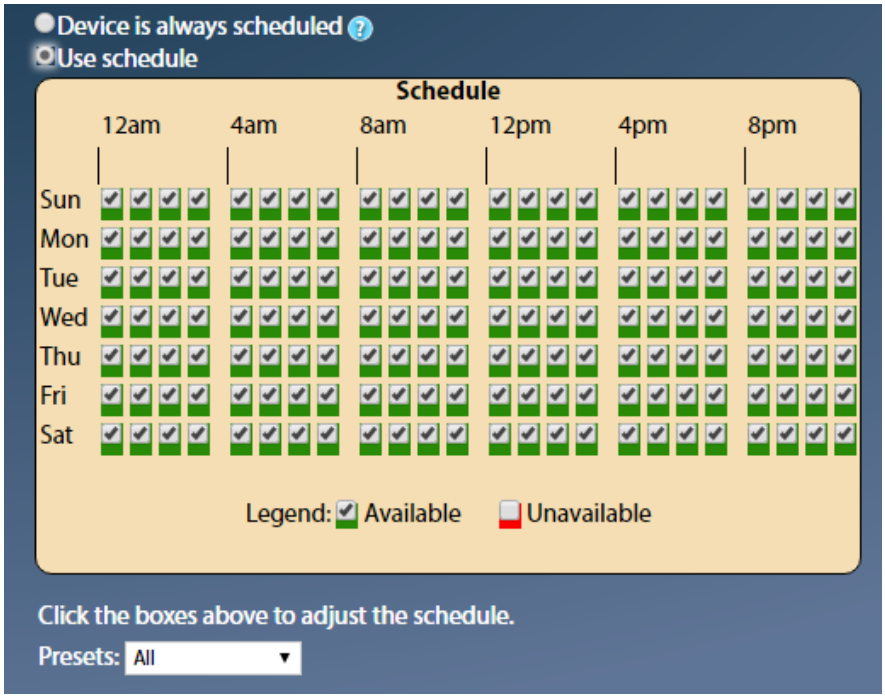
Click the **Devices** tab to see the devices that have been defined in Navigator and their status; you will also see a count of how many of each type of device you have and how many your license permits.
You can create a new device by clicking **New DICOM Device** near the top, or click on the description of an existing device to view or edit that device.



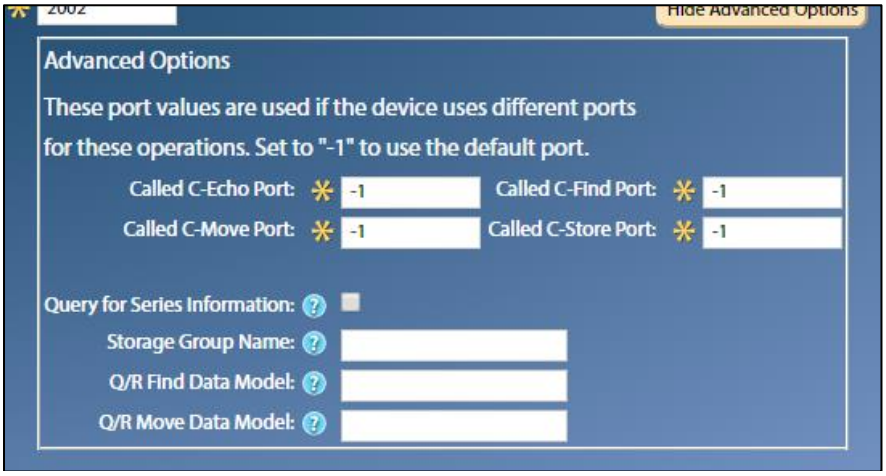
When you create or edit a device, you will see a page like that shown below, with fields that must be filled in to define the device fully.



- **Description** – Name or description for the device
- **Enabled** – Check this if the device is active and online; only enabled devices are polled to make sure they are "alive".
- **Role** – Click the checkboxes to indicate if the device is a **Source** for priors, a **Destination** for priors, or a worklist **Trigger**.
- **Max Threads per Role** – The maximum number of threads for each role that this device plays. This value will be constrained by the value for **Number of Processing Threads** in the **General Settings**.
- **Send notifications** – Check this box if an e-mail should be sent the specified **E-mail address** if the device goes offline or comes online; uncheck the box if no notification is desired. You can specify multiple e-mail addresses by separating them with commas. Note that notifications are only sent if **E-mail Notifications** are enabled on the **General Settings** page and the **SMTP Server** is configured correctly.
- **Calling AE Title** and **Calling IP Address** – The AE Title and IP address for Navigator
- **Called AE Title** and **Called IP Address** – The AE Title and IP Address of the device to contact
- **Default Called Port** – The port of the device to contact
- **Session Settings Config File** – This is unused right now.
- **Device is always scheduled** / **Use schedule** – By clicking the second radio button, you can set a schedule during which a device is unavailable – just click the boxes for each hour of a day that the device will be available. There are presets of commonly-used schedules below the Schedule Editor.



There are also advanced settings, available by clicking the "**Advanced Options**" button.

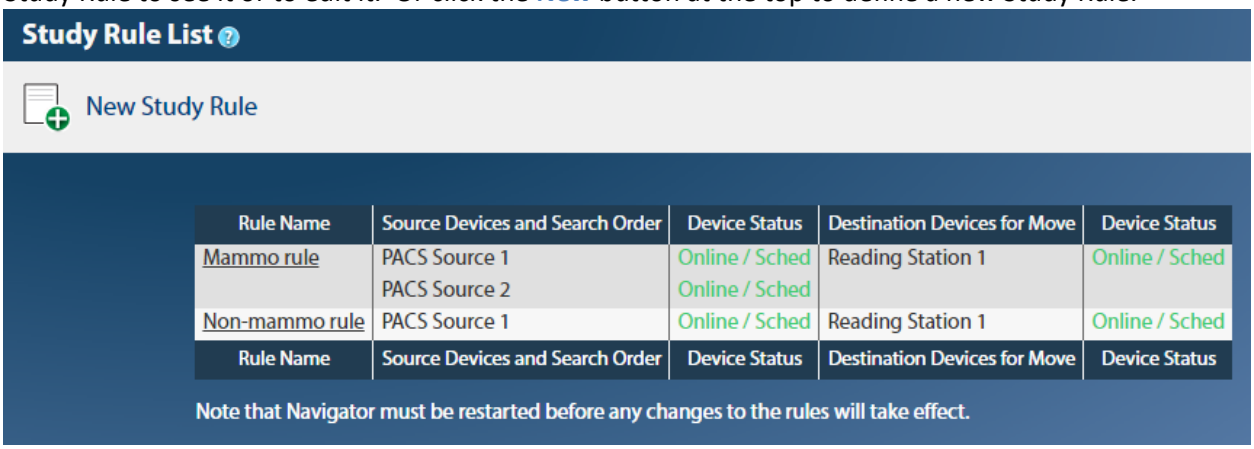


- **Called C-Echo Port, Called C-Find Port, Called C-Move Port, Called C-Store Port** – The port values to use if the device uses different ports for different operations.
- **Query for Series Information** – The Source device will be queried for Series information, which will be used to construct a value for Modalities-in-Study.
- **Storage Group Model** – Set the same Storage Group Model for a Source device and Destination device that share the same database backend (the value can be any string, it just needs to be the same for all the devices that have the same backend). If a Source and Destination have the same Storage Group Model, studies on the Source don't need to be moved to the Destination since they are already there, which can speed up the processing
- **Q/R Find Data Model** – Set this to P for Patient Query, S for Study Query, or PS for Patient Study Query.
- **Q/R Move Data Model** – P for Patient Root, S for Study Root, PS for Patient Study Root

Once the device's settings are as you desire, click the **Save** button at the top to keep the changes; otherwise click **Cancel** to discard the changes.
If you are editing an existing device, you can click **Delete** to delete the current device. You can click **Copy** to make a duplicate of the current device – *note that the copy will not have any changes you have made to the current data but have not yet saved*. When you click Copy, a copy will be made and the device will be opened for editing right away.

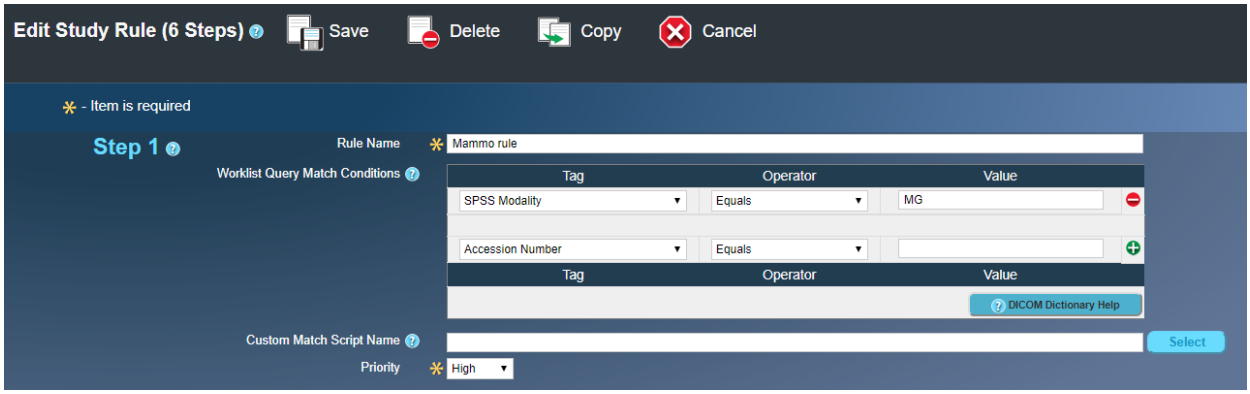
4.5 Study Rules

The Study Rules determine which Source Devices are queried for priors and to which Destination Devices the priors are sent. The responses from the **Worklist Readers** (MWL servers or incoming HL7 messages) are processed to find a Study Rule that matches certain criteria. The Study Rules associated with the particular Worklist Reader that received the Worklist Entry are searched in order; the *first* Study Rule that matches is used, and its operations are applied to the Worklist Entry data to determine what priors to move. (Note that a Worklist Entry will use only *one* Study Rule.)
When you click on the Study Rules tab, you will see a table of the existing Study Rules. Click on the name of a Study Rule to see it or to edit it. Or click the **New** button at the top to define a new Study Rule.

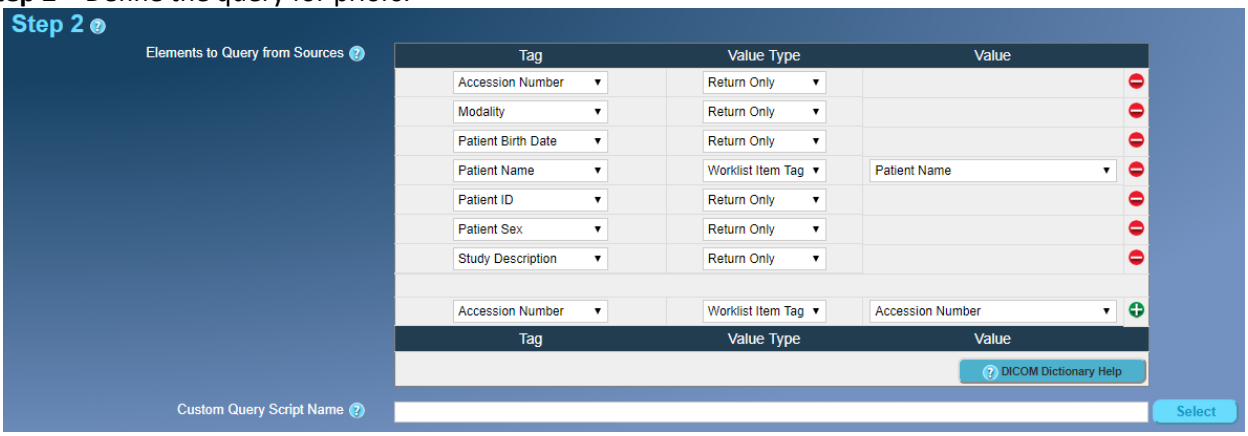


When you are configuring a Study Rule, there are steps in its processing to be configured: rule matching, query definition, selecting sources, response filtering, and selecting destinations.

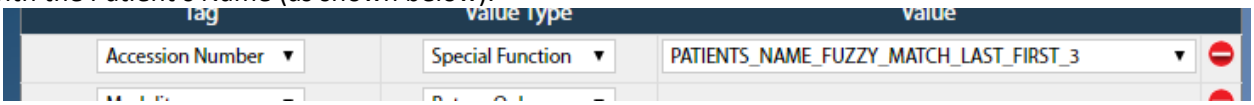
Step 1 – Here you give the Study Rule a name and define what conditions should be matched so that this rule is used. If you specify multiple conditions, *all* of them must be true in order for this Study Rule to be selected. You can specify a Custom Script for more complex matching conditions – for example, if you want Condition A *or* Condition B to match (see Section **4.7 Scripts** for more information). You can also choose the **Priority** – Low, Medium, or High – for the handling of Worklist Items matching this Study Rule.



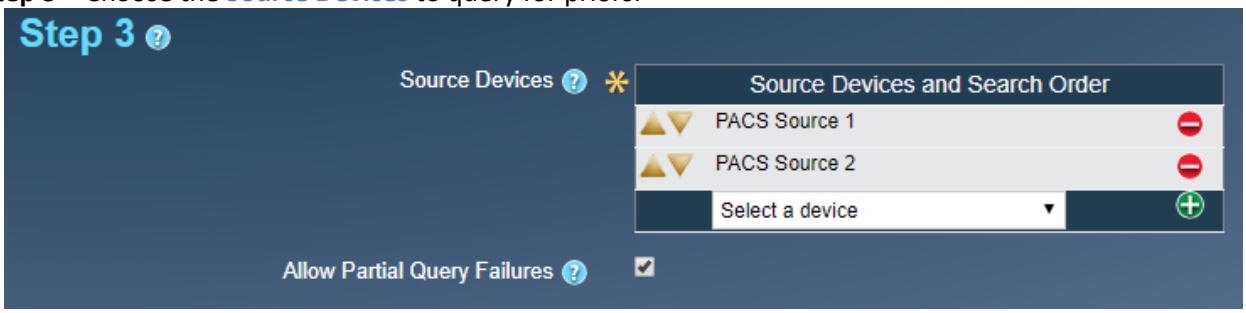
Step 2 – Define the query for priors.



You can define what elements should be included in the query, which ones should match a value from the Worklist Item or a constant, or tags whose value should be returned for processing in a later step. You can also specify a Custom Script to do complex operations on the query that will be sent. When selecting the elements to query, you can also select from a limited set of special functions to do "fuzzy name matching" with the Patient's Name (as shown below).



Step 3 – Choose the **Source Devices** to query for priors.

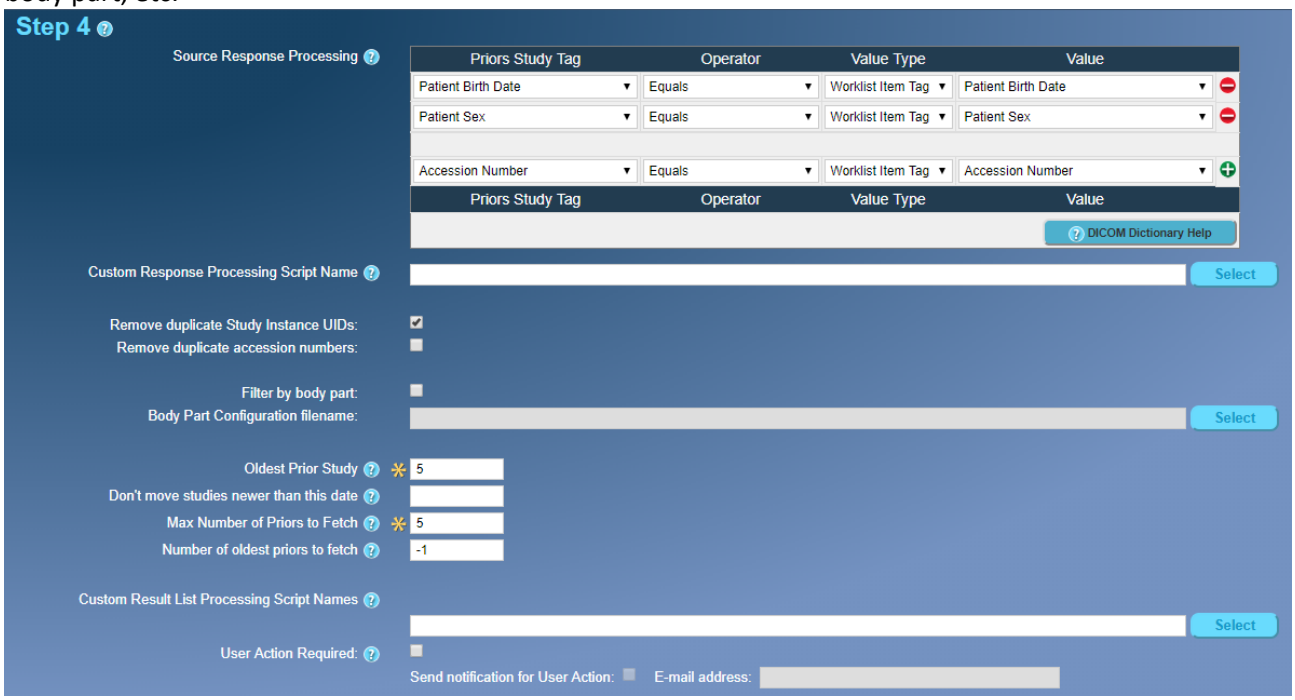


From the list at the bottom of the table, select a device and click the green "plus" button to add a device; click the red "minus" button next to a device to remove it from the list of sources. You can use the up and down arrows next to the names to reorder the list – order is important, since a study will be used from the first device where it is found, even if it exists on the other devices.

Check the box for **Allow Partial Query Failures** if at least *one* of the selected sources must be enabled and respond to the queries; uncheck the box if *all* the selected sources must be enabled and respond. For

example, you may have 3 source devices selected. If one does not respond to the queries, you may want the priors found on the other devices to be moved, and you will consider that sufficient – in that case, check the box. But if you must have the priors found on *all* 3 devices, uncheck the box.

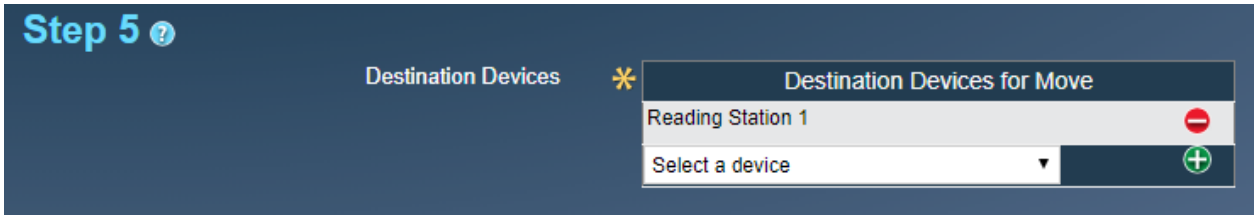
Step 4 – From the priors returned by the Sources, decide which ones should be moved, filtering on age, body part, etc.



- The **Source Response Processing** table at the top of Step 4 lets you decide which tags must match which constants or values from the Worklist Entry in order to be considered as a valid prior. Note that *all* the tags specified must match in order for the prior to receive further consideration. You can specify a **Custom Response Processing Script** for more complex processing on the values returned to decide which studies should be moved.
- Click the checkbox if you want to **Remove Duplicate Study Instance UIDs** (this is true by default).
- Click the checkbox if you want to **Remove Duplicate Accession Numbers**.
- If you want, you can check **Filter by body part** – you must then choose a **Body Part Configuration File**. This could be used, for example, to get all priors for the patient's leg if the Worklist Entry refers to his foot. (See **Appendix B: Body Part Configuration File** for an explanation of how the Body Part Filter works.)
- The **Oldest Prior Study** field tells Navigator how far back in time it should look for priors. You can set it to just a positive integer, such as "8", to go back to January 1st eight years ago – this is the default behavior. Or you can set it to "-1" for no limit; or specify a relative date as "-number" followed by D, M, or Y (for **D**ays, **M**onths, or **Y**ears); for example, "**-7M**" means "seven months ago from today".
- If you know that some priors were already moved, you can enter a date in **Don't move studies newer than this date**. The date can be absolute (e.g., "19760704") or relative (e.g., "-5D"). Specify relative dates as "-number" followed by D, M, or Y (for **D**ays, **M**onths, or **Y**ears); for example, "-5D" means "5 days ago".
- You should enter a number for the **Max Number of Priors to Fetch** – this is how many of the newest priors you want to be moved. You can also configure the Study Rule so that M of the newest priors are moved but also N of the oldest priors found ("**Number of oldest priors to fetch**").

- You can choose one or more **Custom Result List Processing Scripts** to do final processing on the list of priors after all of the previous filtering operations are done – these let you alter the list and request more priors or exclude some priors; you can also use a script to specify that some priors go to one destination and other priors go to a different destination.
- Lastly, you may let a user choose which priors should be moved and which should be rejected. If you check the **User Action Required** box, a user will have to view the **Worklist Entries** and mark which priors should be accepted for a specific **Worklist Item**. You can specify the **E-mail address** of a user (or multiple users by separating the addresses with commas) who should be notified when his assistance is required. (Note that notifications are only sent if **E-mail Notifications** are enabled on the **General Settings** page and the **SMTP Server** is configured correctly.)

Step 5 – Choose the **destinations** for the priors. These are the devices where you want the priors to be sent.



Step 6 – You can use **custom scripts** that run and will modify a Worklist Item Job or Study Move Request Job or perform some action with the Job when the Job starts or stops running – for example, a script could be used to send a notification when a Worklist Item Job has completed. Select the scripts to use in this step.

Save your changes – Once you are done configuring the Study Rule, click the **Save** button at the top to save your changes, or click **Cancel** to discard the changes and return to the list of Study Rules. Click **Delete** to delete the rule. Click **Copy** to make a copy of the current, unedited rule – the new rule will automatically be opened for editing.

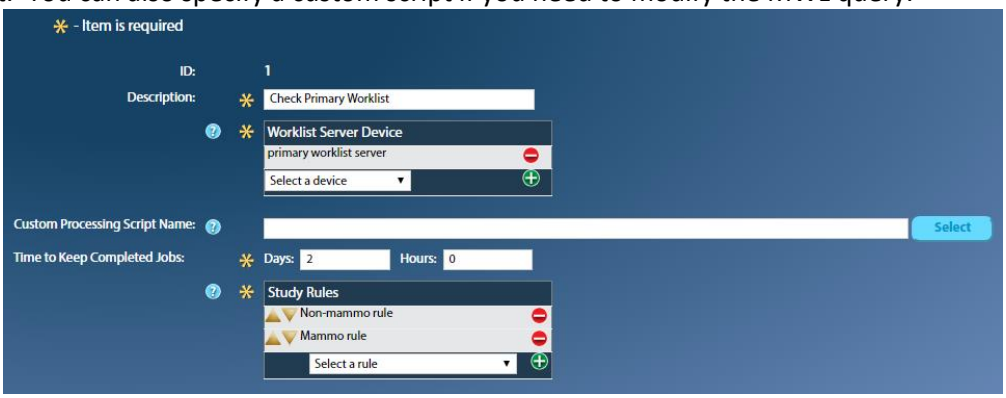
Note that a Study Rule must be associated with *at least* one Worklist Reader in order to process priors (see Section **4.6 Worklist Readers** below for associating a Study Rule with a Reader); a Study Rule can be used by multiple Readers. This lets you assign certain processing of some Worklist Items to one Reader, while a different Reader can process things differently, if you so desire.

4.6 Worklist Readers

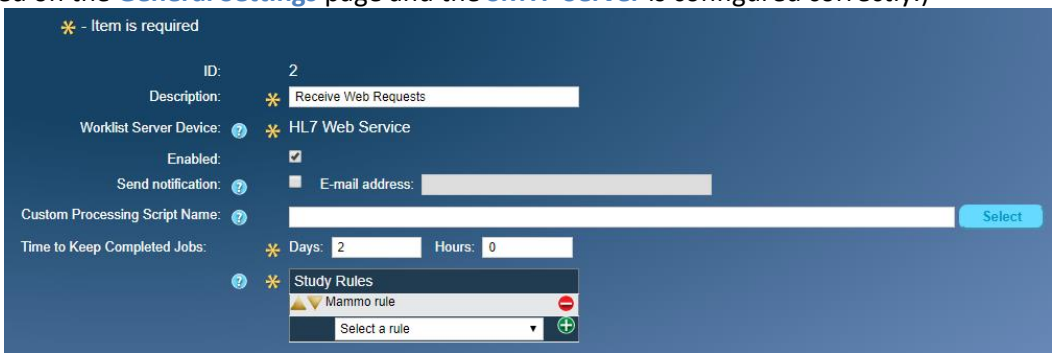
Navigator has to be told about the orders whose priors should be fetched. **Worklist Readers** are the Worklist Server Devices or the HL7 Web Service that tell Navigator about these orders. **Study Rules** are associated with each Worklist Reader to determine which Sources to query and to which Destinations the priors are sent and how the priors are filtered.

You can create new Worklist Readers that retrieve data from a DICOM Device that is a Worklist Trigger. However, you can have only *one* HL7 Web Service-based Worklist Reader.

If you are creating or editing a Reader that uses a **Worklist Server**, you specify a description, choose the Worklist Server Devices, and then choose which Study Rules are used by this Reader. **Note** that the order of the Study Rules is important, since the first rule that is matched will be used; you can reorder the Study Rules with the up and down arrows next to their names. You should also set the number of days and hours that completed jobs are held before deletion – completed jobs may also be deleted once they are not on the Worklist. You can also specify a custom script if you need to modify the MWL query.



If you are editing the **HL7 Web Service Reader**, you can change the description and then choose which Study Rules are used by this Reader; you can change the order of the Study Rules with the up and down arrows next to the names. You should also set the number of days and hours that completed jobs are held before deletion. You can also specify a custom script that is used to turn the HL7 parameters into MWL-style data to be processed by Navigator. If you are not using HL7, you can uncheck the **Enabled** box to ignore any HL7 Web requests that come in. You may also have an e-mail sent when the HL7 Reader goes offline or comes online – check the **Send Notification** box and specify an **E-mail address** (or multiple addresses by separating them with commas). (Note that notifications are only sent if **E-mail Notifications** are enabled on the **General Settings** page and the **SMTP Server** is configured correctly.)



Once you are done editing a Worklist Reader, click the **Save** button at the top to save your changes, or click **Cancel** to discard the changes and return to the list of Worklist Readers. Click **Delete** to delete it. Click **Copy** to make a copy of the current, unedited Reader – the new Reader will automatically be opened up for editing.

4.7 Scripts

Navigator can be configured via its user interface to do almost any processing that is required for the matching of worklist entries and the processing of priors. However, there are many special cases that require custom code to handle – for these situations, you can create Custom Scripts and tell Navigator to use them in its processing. You can edit the scripts and create new ones from the Scripts tab.

There are seven types of scripts you can create and use:

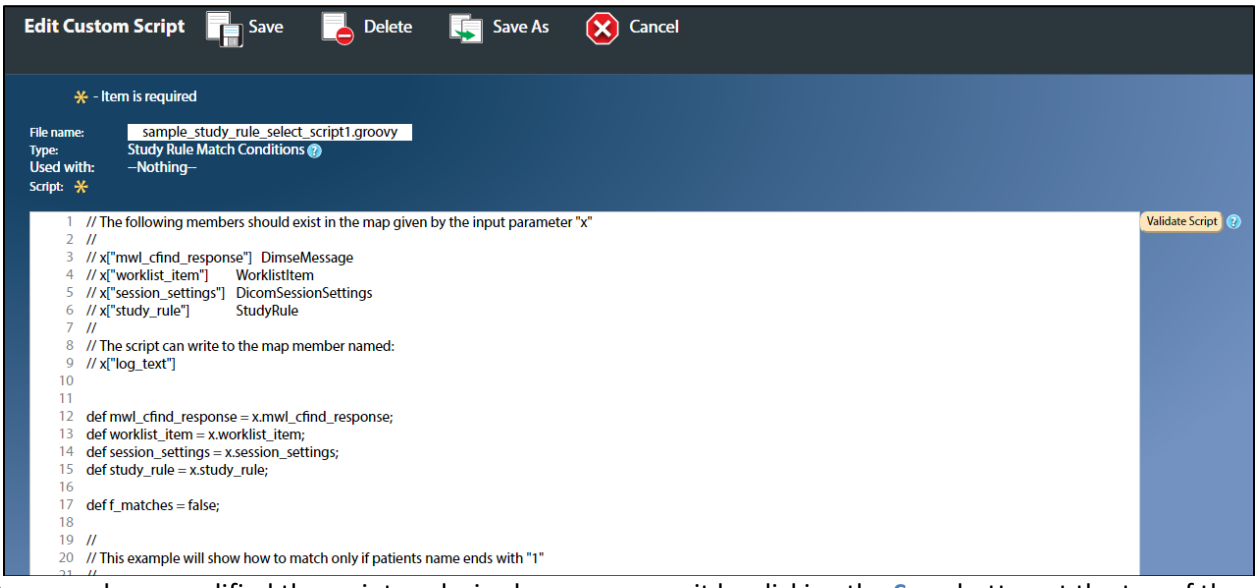
- **HL7 / MWL Processing** – These convert HL7 and web parameters into MWL-style data; these scripts are used by the HL7 Web Worklist Reader. They can also be used by MWL Worklist Readers if you need to modify the MWL query, such as adding parameters.
- **Study Rule Match Conditions** – These are for complex Boolean logic to determine if a given Study Rule should be used to process a Worklist Entry.

- **Study Rule Query Processing** – These are used to do complex processing on the conditions that decide which Priors to query for. For example, if you want to modify the Patient Name to match so that an exact match is not needed (a.k.a., "fuzzy matching"), this could be done here.
- **Study Rule Response Processing** – These scripts are used for complex filtering out of priors. For example, if you want a rule to handle all modalities but one, you would use this script to mark priors with that modality as "do not move".
- **Study Rule Result List Processing** – These are for final filtering operations on the list of results, allowing you to choose which priors to move and which to exclude. These can also be used if you want certain priors to go to one Destination Device and other priors should go to a different Destination Device.
- **Worklist Item Job Processing** – These are used to modify a Worklist Item Job or perform an action when the Job starts or stops running. For example, you could send a notification when the Job is completed.
- **Study Move Request Job Processing** – These are used to modify a Study Move Request Job or perform an action when the Job starts or stops running.

From the Scripts tab you can also choose to edit the default **Body Part Matching** configuration file (see **Appendix B: Body Part Configuration File** for an explanation of how the Body Part Filter works).

Navigator comes with several sample scripts – you can edit them and change them as necessary. You can also create new scripts from scratch. You can run a quick test of a script by clicking the "**Validate Script**" button to the right of the text area – this will let you know if the script has any syntax errors, and you can check the script's results against sample test data, which are shown below the script editing window.

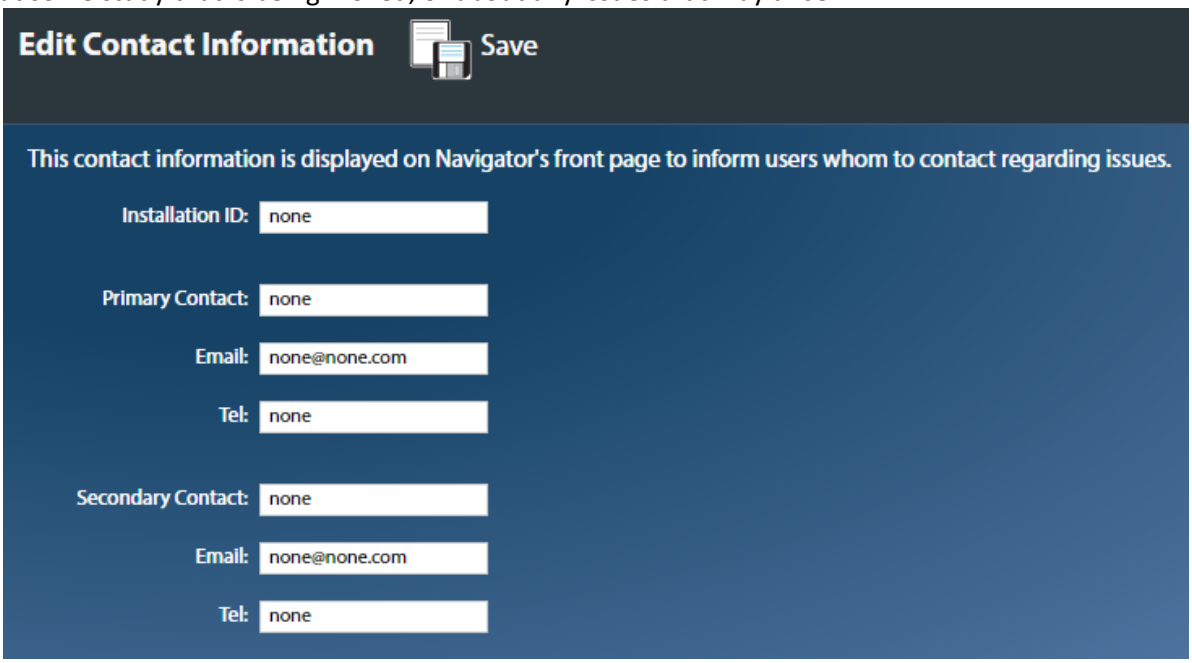
Tip: Make a copy of an existing sample script and change the copy to do what you need, and reference the copy in the Study Rules – this will let you preserve the original in case your script doesn't work right the first time, and you can compare the scripts to see the differences.



Once you have modified the script as desired, you can save it by clicking the **Save** button at the top of the page. You can save it under a new name by clicking "**Save As**", or you can delete the script via the **Delete** button. Click **Cancel** to discard any changes and return to the list of scripts.

4.8 Contacts

This page lets you configure the information that is displayed to users when they first login to Navigator. The **Installation ID** can be your site name, the name of the host machine, or anything that will let a user know where Navigator is running if they have a question. The **Primary** and **Secondary Contacts** are people in *your* organization who should be contacted if someone has a question about Navigator and its operation, about some study that is being moved, or about any issues that may arise.



The information that you entered on this page will be displayed on the first page when you login to Navigator, under the **Support Contacts** section of the page, as shown below:

Note: You should set this information when you are configuring Navigator the first time, as you will be repeatedly reminded to change the information until you have done so.

4.9 Users

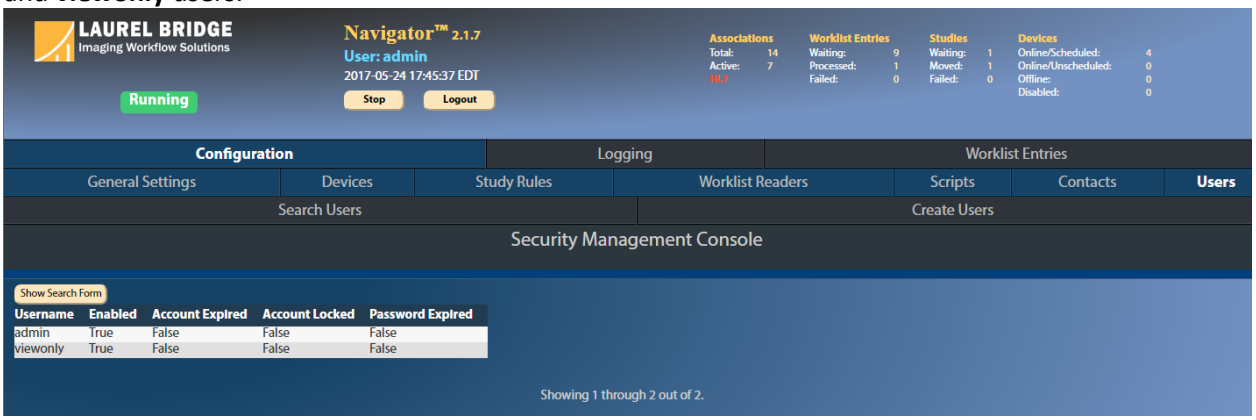
The Users page lets you define the users who can access Navigator and set each person's level of access. Navigator comes with three different permission levels: **Admin**, **User**, and **View-only**.

- **Admin** users can do anything in Navigator: start or stop its processing, reschedule or delete worklist items, view and delete log files, change the configuration, etc. These are the people who know how to use Navigator and configure it to do what is desired.
- **User** level, the middle set of permissions, can start or stop Navigator, view log files, and reschedule worklist items. The User level can view the configuration but cannot change it, and it cannot delete worklist items. This level might be used for technicians who need to start or stop Navigator's operation, for example if a server goes down.
- **View-only** is the lowest permission level. Such users can observe Navigator's operation and see the configuration but cannot change the configuration. Such people also cannot view the worklist items or the logs. This level might be used for people who want to ensure that Navigator is operating but who would only report any issues to someone else.

Navigator comes with two users built-in: an administrative user (username: "**administrator**"; password: "**LaurelBridge**"), and a view-only user (username: "**viewonly**"; password: "**viewOnly**"). You can add users for each person who is expected to have to use Navigator – this lets you see who logged in and what operations he did. ***You should change the administrator password after you have logged in the first time.***

Note that Navigator can be configured to use **LDAP / Active Directory** to manage the user accounts. The configuration should include mappings from your LDAP groups to these access levels. See **Section 4.3 General Settings** for more information on configuring LDAP.

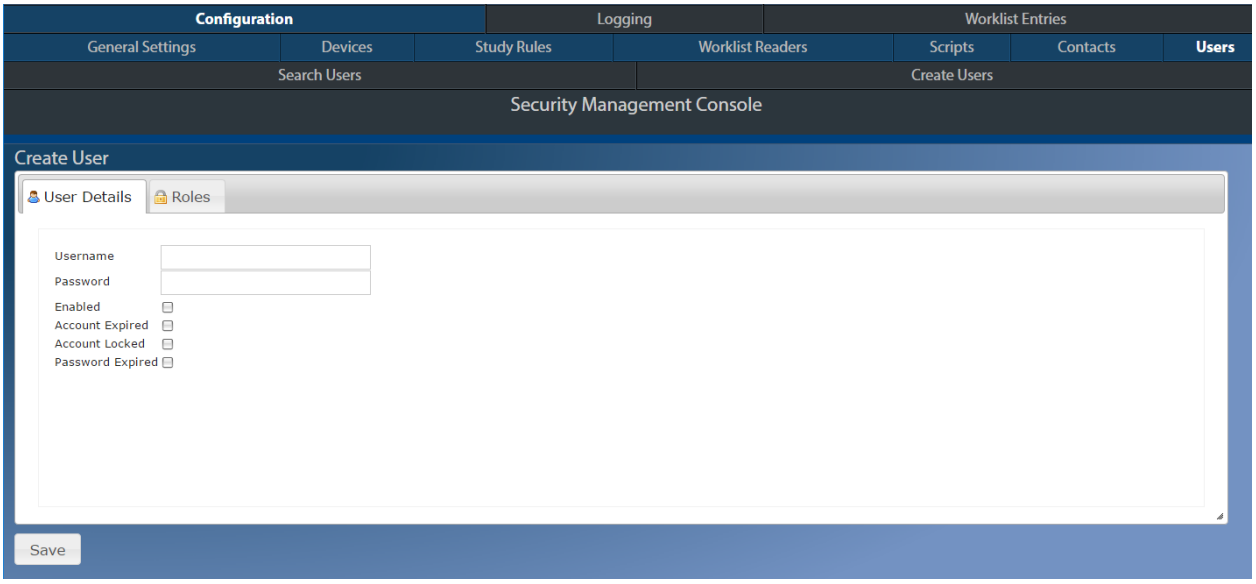
When you click on the **Users** tab or on **Search Users** at the next level down, you will see a list of the currently existing users in Navigator – for example, in the image below, there are only the **administrator** and **viewonly** users.



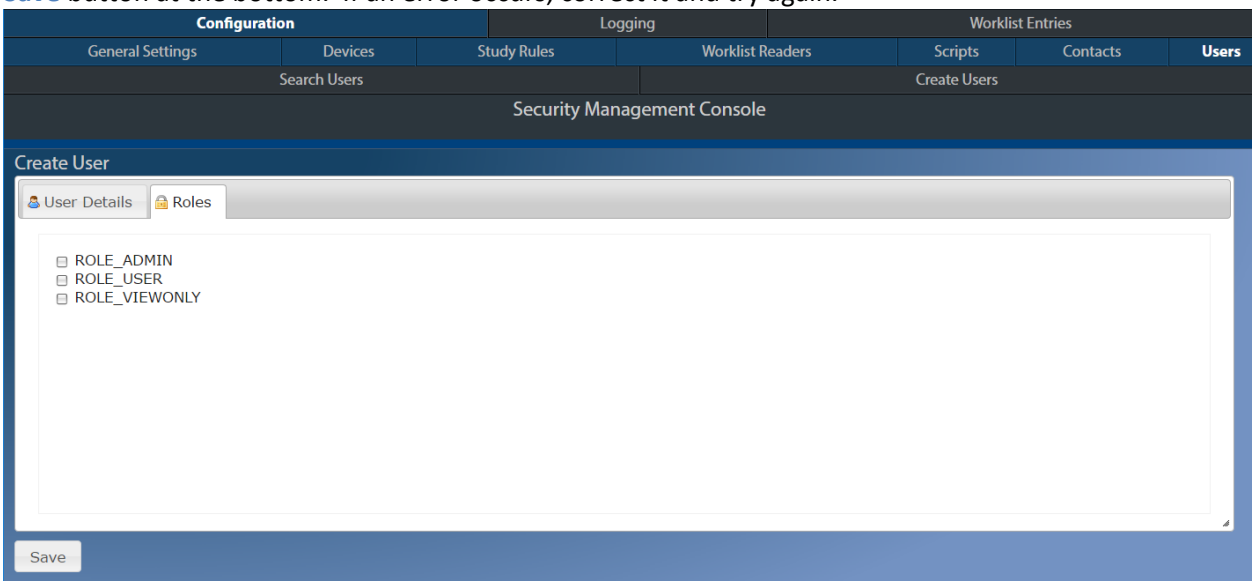
4.9.1 Creating a User

To create a new user, click on the **Create Users** tab. On the **User Details** sub-tab, enter the username for the new user and the initial password; click the **Enabled** checkbox. (For now, ignore the other checkboxes – these are for future enhancements.) Note that passwords should be at least 8 characters and have mixed case characters – for example, "waterBottle" (note the capital **B**) is valid, while "waterbottle" (all lower-case) is not valid; also, any leading or trailing spaces are ignored. If you enabled **Require secure passwords**

on **General Settings**, passwords must be at least 12 characters long and also have numbers or special characters – for example, “waterBottle1234”.



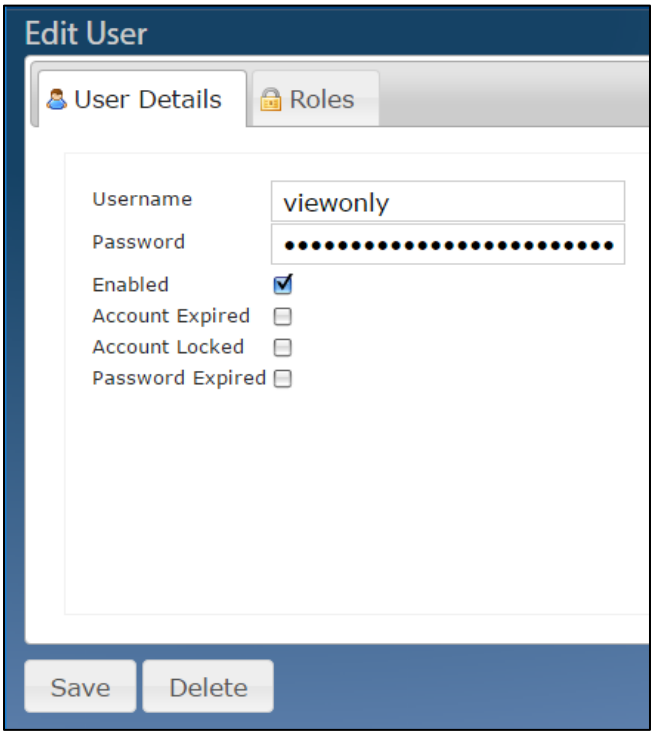
Then click the **Roles** sub-tab and click the checkbox next to the role that the new user should have (see below) – ***click only one***. (Look at the beginning of this section for what each role can do.) Then click the **Save** button at the bottom. If an error occurs, correct it and try again.



Please note that creating a user this way does not apply to LDAP – it is only for users administered locally by Navigator.

4.9.2 Editing a user

To edit a user, click on his username on the Search Users page. You can change his username, password, and his roles, and also disable his account (thus preventing him from logging in to Navigator).



Click **Save** after you are done making changes to the user. You can also **delete** the user by clicking the **Delete** button. (Note that you should **not** delete the administrator user. Also, this page does not apply to LDAP users.)

4.10 Advanced Configuration Options

Navigator has several configuration options that are not currently editable by the User Interface. These are for settings that require advanced knowledge to change and are rarely altered. These settings must be changed by manually editing the Navigator configuration file, a text file of settings usually stored in `C:\ProgramData\Laurel Bridge Software\Navigator2\cfg\apps\defaults\Navigator`. The file should be ***carefully*** edited with a standard text editor, such as Notepad or VIM, making sure that you do not alter the grouping of the data; after you save the changes, you should restart the Navigator service.

4.10.1 Custom Tags

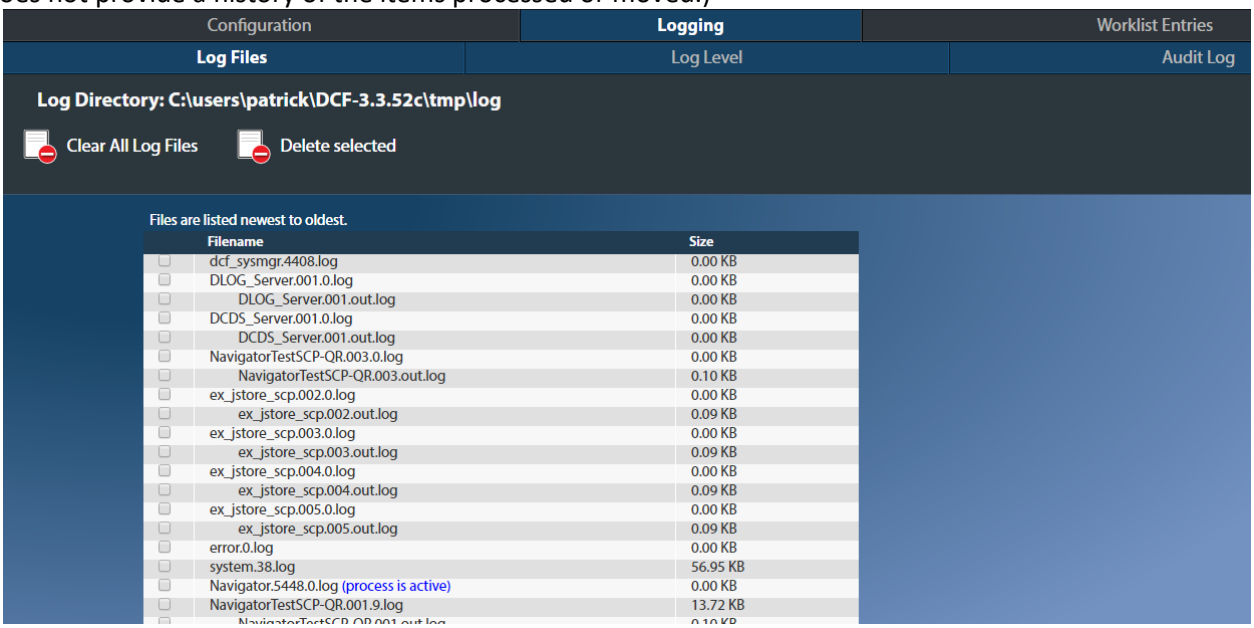
One of these settings is the **Custom Worklist Item and Study Move Request Tags**. These are tags whose data values will be used to populate Worklist Item Jobs and Study Move Request Jobs. You may specify different tags based on your needs, and you may also change the labels/text that will be displayed with these data elements.

The WorklistItem column user001(2,3,4,5) will be populated with data from the Modality Worklist Query Response with this tag. If the indicated element does not exist, an empty string will be stored for that column. Similarly, the StudyMoveRequest column user001(2,3,4,5) will be populated with the data from the prior study C-Find-Response data set at this tag, and an empty string will be used if the element does not exist.

mwl_user001_tag, mwl_user001_label	smr_user001_tag, smr_user001_label
mwl_user002_tag, mwl_user002_label	smr_user002_tag, smr_user002_label
mwl_user003_tag, mwl_user003_label	smr_user003_tag, smr_user003_label
mwl_user004_tag, mwl_user004_label	smr_user004_tag, smr_user004_label
mwl_user005_tag, mwl_user005_label	smr_user005_tag, smr_user005_label

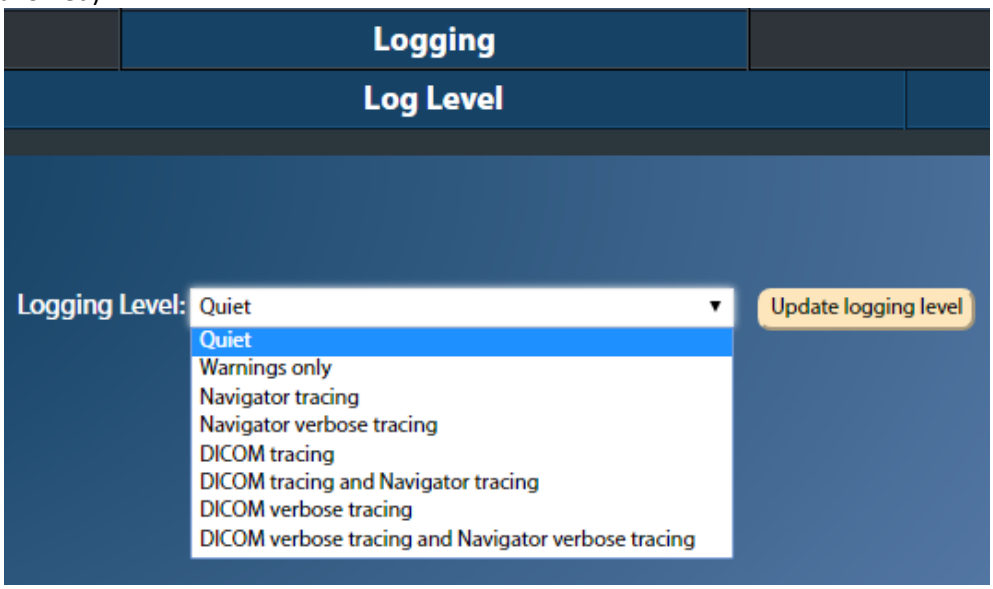
5 Logging

Click the Logging tab to see the **Log Files** used by Navigator or to adjust the **Logging Level**. Administrative users can also view the **Audit Log**, which records who logged in and what operations were performed to the configuration, as well as any changes made by a user to the list of Worklist Entries. (Note that the Audit Log does not provide a history of the items processed or moved.)



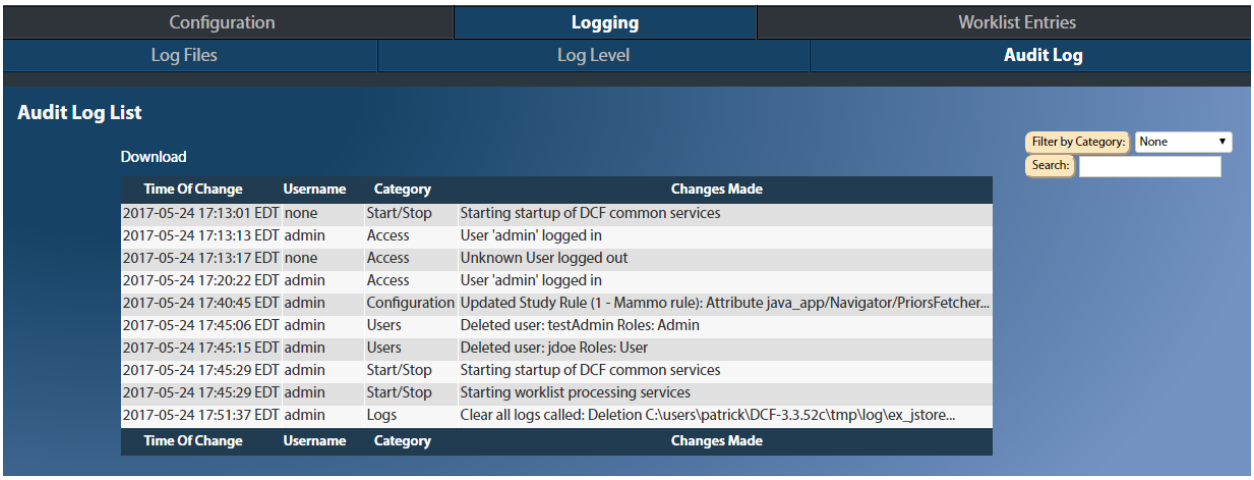
Click the **Log Files** tab to see a list of the files in the Log Directory. You can click on the name of a log file to view the contents of the file. Admin-level users can also delete or truncate log files with the **Clear All Log Files** button, or they can delete only a few files by clicking the boxes next to the filenames and pressing **Deleted selected**.

Click the **Log Level** tab to adjust the log level – this is useful for tracking Navigator's operations and determining why it does certain things. **Note** that you should *not* choose a high logging level for long periods of time, since the log files can grow very quickly (see **General Settings** for how to adjust the sizes of the log files allowed).



Click the **Audit Log** tab to see who has accessed Navigator, what changes have been made to its configuration, and what actions have been done to the Worklist Entries and the associated priors. The

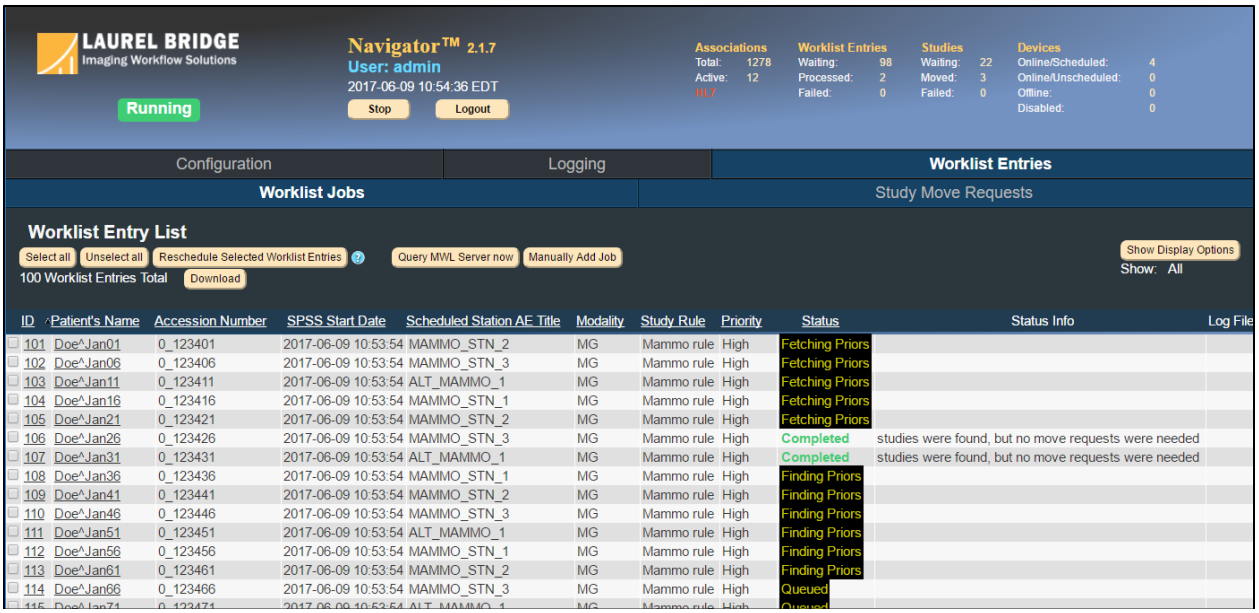
Audit Log may also have PHI in it if a Worklist Item is *manually* deleted (see Section 6 Worklist Entries below). You may use the **Filter by Category** button to see only audit records from a certain category (e.g., only Access records or only Configuration records). Or you can use the **Search** button to find records that have certain words in them (note that the Search may be case sensitive depending on your database's collation settings).



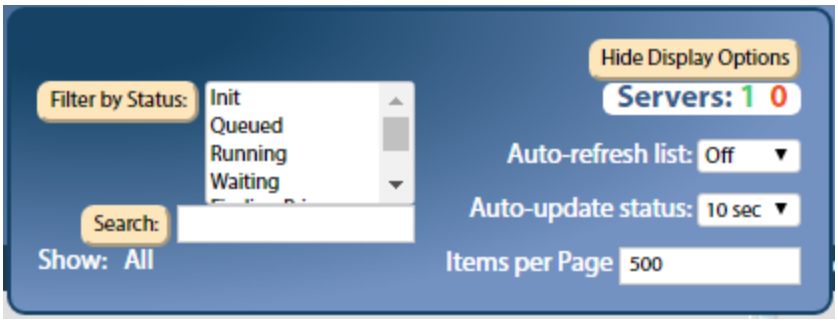
Click the date of a change for more information on that change.

6 Worklist Entries

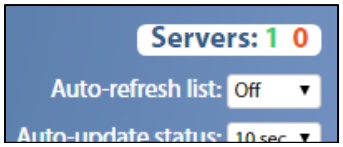
Click the **Worklist Entries** tab to view the items processed by Navigator.



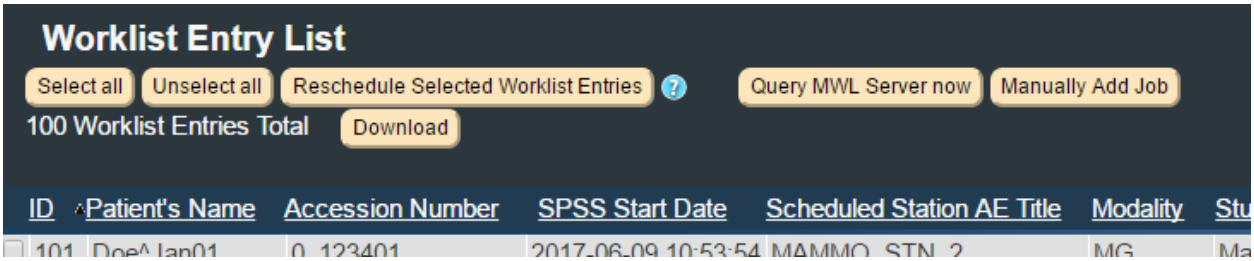
Click the **Show Display Options** button to view filters and other options for viewing the Worklist Jobs displayed.



The count of Servers at the right edge of the pop-up shows how many Worklist Servers are available in **green** and unavailable in **red** (see the image below for an example). Note that the servers only include those that are associated with a Worklist Reader – if you have 5 MWL Servers but only 1 is associated with a Worklist Reader, the counter will show only 1 is available; also, the HL7 Reader is not included in these counts. (See Section **4.6 Worklist Readers** above for associating a MWL Server with a Worklist Reader.)

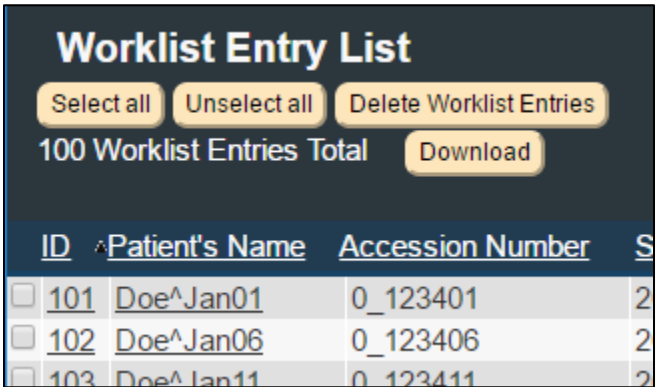


When Navigator is processing worklist items, certain users (**Admin** or **User** level) can click the checkboxes next to the entries and then click the **Reschedule** button (above the table; see the image below) to have those studies be reprocessed and moved again – this can be useful if you have modified a Study Rule, for example, and want to reprocess the item.



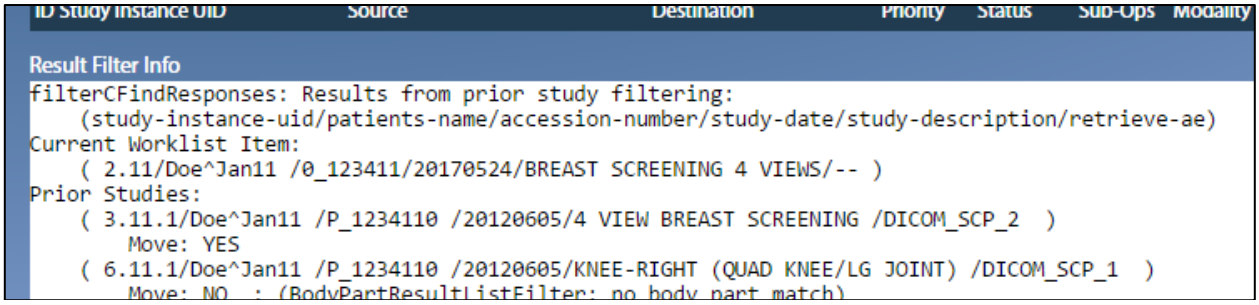
If Navigator is **stopped**, an Admin-level user can click the checkboxes next to the entries and delete them by clicking the **Delete** button (shown below). For example, if a worklist item no longer needs to be processed, an administrator could delete it and remove it, along with any of its Study Move Request children, from the list of items to handle. (The deletion of manually deleted Worklist Items is recorded in the Audit Log.) **Note** that Navigator's processing *must* be stopped to delete Worklist Entries.

The **Download** button lets you download the data in the table as a text file – this can be useful if you want a list of patients who have been processed, for example.

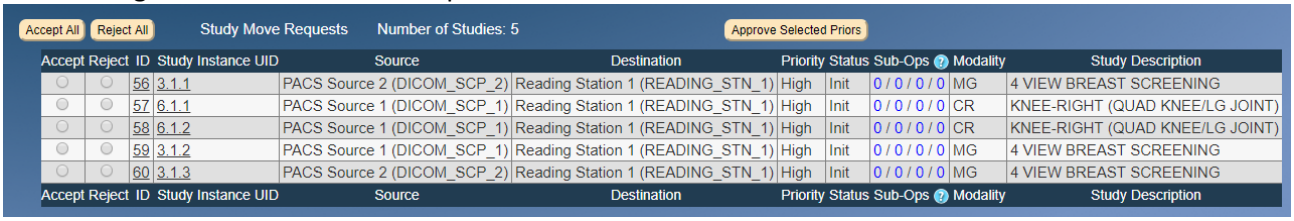


You can click the Job ID or the Patient's Name to see a detailed view of the Worklist Entry.

There may also be a field showing which priors were selected to be moved and which were rejected and why:



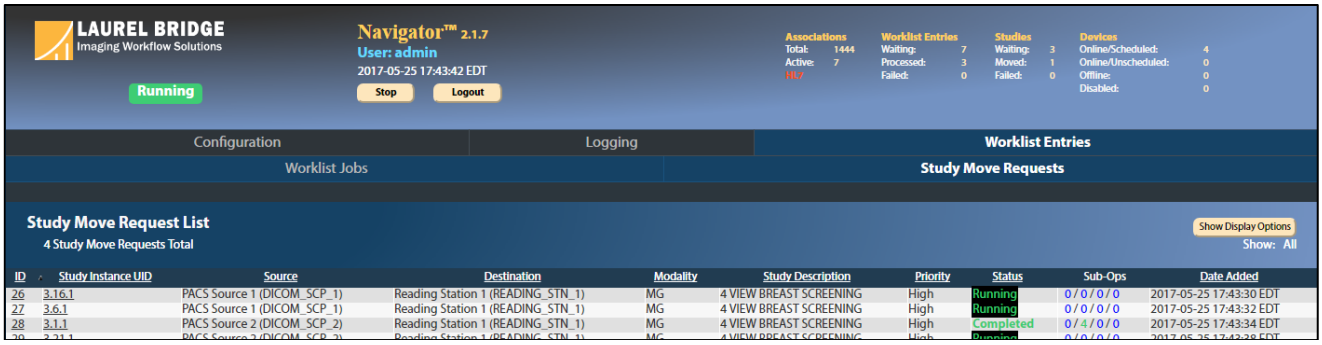
If the Study Rule specified **User Action Required**, the table of Study Move Requests will have **Accept** and **Reject** buttons next to each Study. For each Study you should mark whether it is accepted (and hence should be moved) or rejected. Once you have made your choices, click the **Approve Selected Priors** button to tell Navigator to move the chosen priors.



Worklist Item Job Statuses	
Init	Initial state; the job has been created but not yet queued for execution
Queued	The job is in one of the queues waiting for a thread from the thread pool to run it.
Running	A thread has begun running this job. For a worklist-item-job the **Running** and **Finding Priors** states both indicate that a thread is actually executing this job.
Waiting	The job is waiting for a timer to expire at which point it may re-queue itself – typically before a retry.
Waiting for User	The job is waiting for a user to choose which priors should be moved.
Finding Priors	The job has started to run and is now performing C-Find's to the source devices to find priors.
Fetching Priors	Priors have been found and evaluated. Now the job is not running, but it is waiting for Study-Move-Request Jobs that it has created to complete (or fail).
Completed	The job is completed and all Study-Move-Requests (if any) have been completed.
Completed Partial	The job is completed and 1 or more Study-Move-Requests have been completed, but 1 or more has failed.
Failed	The job is completed and all of the Study-Move-Requests have failed after the configured number of retries. A Worklist Item Job may also fail if the query or discovery of prior studies failed after the configured number of retries.

From this page, click a **Study Instance UID** in the table of Study Move Requests at the bottom to see detailed information on that Study Move Request – where it was found, where it was sent, its status, status of its Sub-Operations, and more. The **Sub-Ops** values show how many sub-operations are needed to complete moving the current Study; the numbers show how many remain, are completed, failed, or have warnings, in that order.

Click the **Study Move Requests** tab near the top of the page to view all the current Study Move Requests and their statuses. (Note that you cannot delete Study Move Requests by themselves; they are deleted only when their parent Worklist Item Job is deleted, as described further up.)

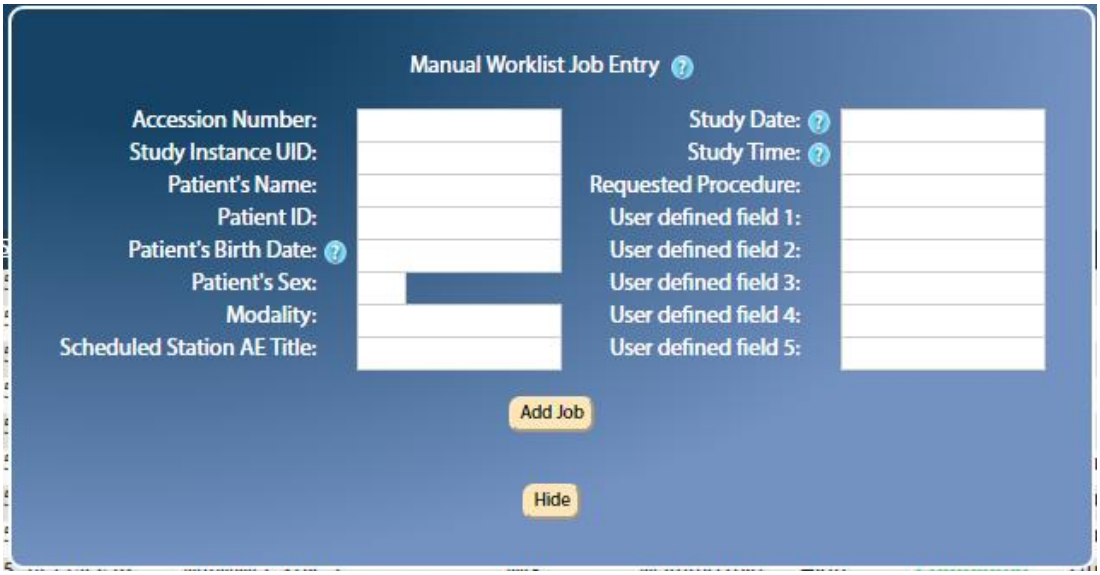


Clicking a **Study Instance UID** will take you to the detailed information on that Study Move Request.

Study Move Request Job Status Values	
Init	Initial state; the job has been created but not yet queued for execution
Queued	The job is in one of the queues waiting for a thread from the thread pool to run it
Running	A thread has begun running this job. For a **Study-Move-Request-Job**, most of the time spent in this state is when the C-Move operation is in progress.
Waiting	The job is waiting for a timer to expire at which point it may re-queue itself – typically before a retry.
Rejected	A user decided that this job does not need to be moved.
Completed	The job is completed, i.e., the requested study has been C-Move'd from the specified source to the specified destination.
Failed	The C-Move operation has failed after the configured number of retries

6.1 Manual Job Entry

Certain users – **Admin** or **User** level – can manually add jobs to be processed. When Navigator is running, clicking the "**Manually Add Job**" button (on the main Worklist Jobs page, below the menu bar) will open a form where the user can specify the job to process.



Enter the information on the job to process and then click "**Add Job**". Jobs entered this way will be processed as if they were received through the HL7 Web interface and its associated Worklist Reader, including any HL7 / MWL Processing scripts and the Reader's accompanying Study Rules.

7 Navigator Utilities

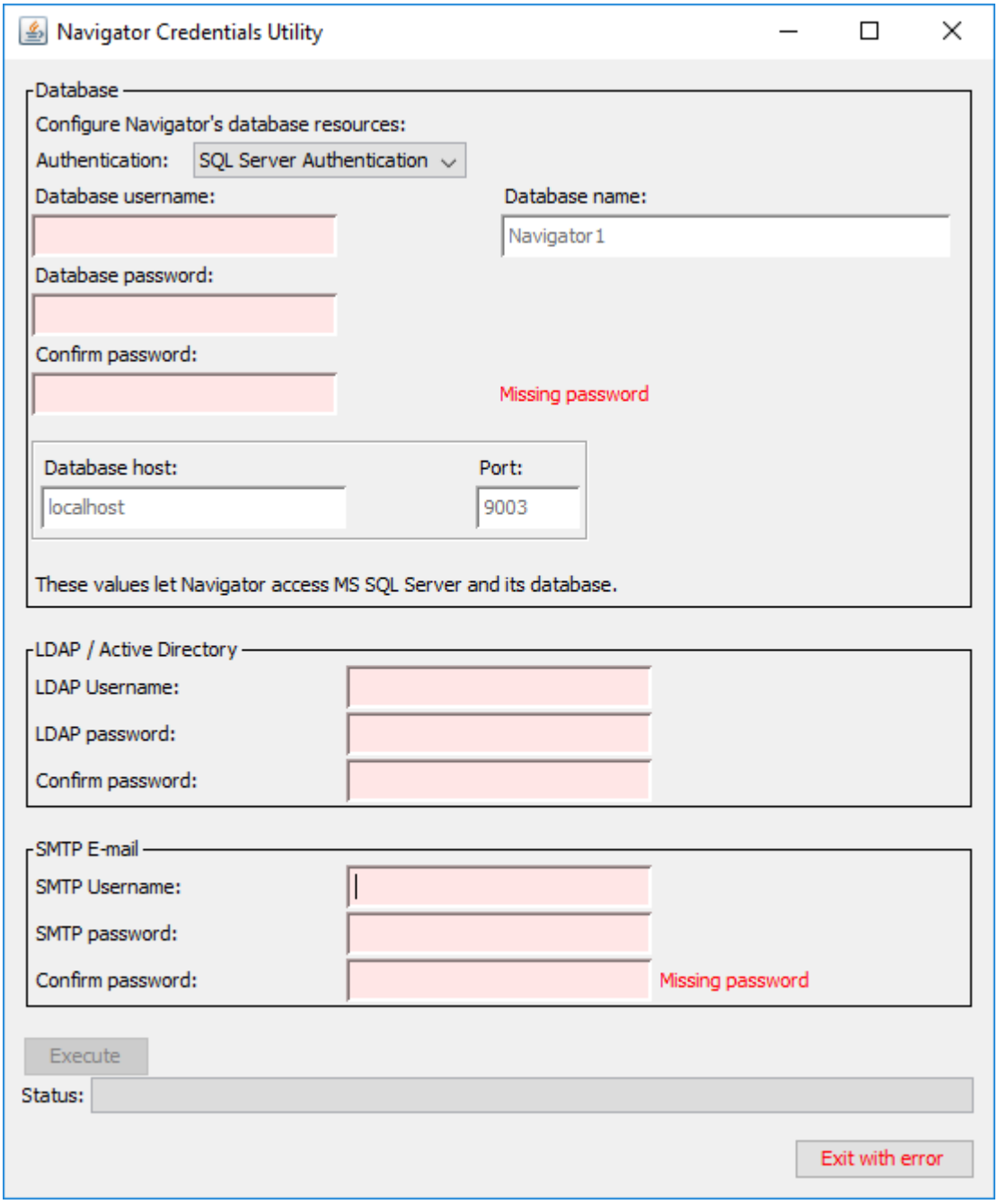
Navigator comes with several utilities designed to make it easy to add new options or to change existing options. The utilities are accessed from the Windows Start menu (see **Appendix D: Start Menu Options on Different Windows** for assistance on different versions of Windows).

7.1 Change Database Credentials

When you installed Navigator, you had to specify the username and password that Navigator would use to connect to SQL Server. If you change those credentials in SQL Server, you will need to change them for Navigator, too. You can also use this utility to change the credentials used for LDAP or SMTP.

Note that this utility will not change the credentials in SQL Server – you must do this manually via SQL Server Configuration Manager and / or SQL Server Management Studio; this utility will only change how Navigator accesses SQL.

1. Run the utility from the Windows Start menu: `Start → Laurel Bridge Software → Navigator → Utilities → Change Database Credentials`.
2. Enter the **username** and **password** that Navigator should use to access SQL – this is not needed if SQL Server is configured to use Windows Authentication. If Navigator is configured for LDAP or SMTP, you can update their credentials, too. Note that you will have to enter the passwords twice to confirm their spelling.



3. The utility will attempt to connect to SQL with the new credentials. If an error occurs, enter the correct credentials and try again.
4. Once the credentials are accepted, exit the utility.
5. You will have to restart Navigator's Web Server to apply the changes. One way to do this is via the **Navigator Service Manager**.

7.2 Configure for TLS / SSL

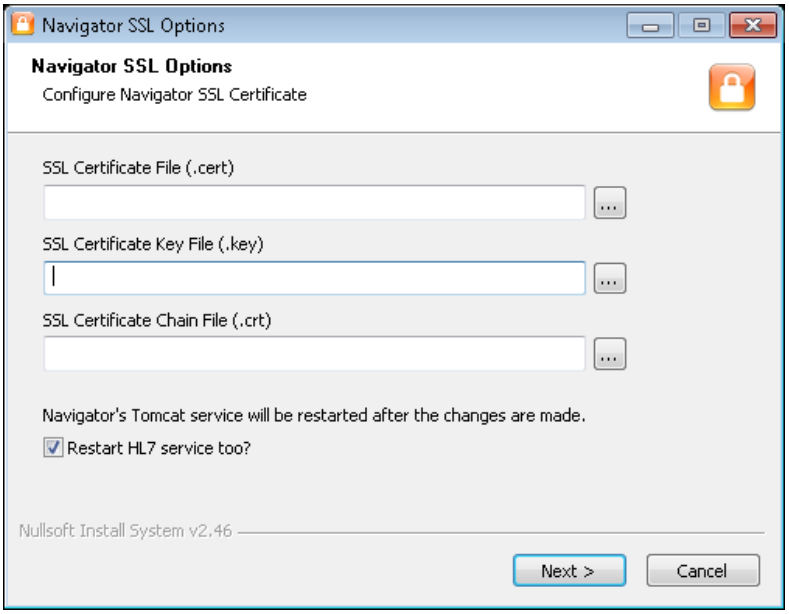
Control and configuration of Navigator is done through a web server via a web browser. Since it is possible for some users to view data on the priors being requested by Navigator, you may wish to require a secure connection to Navigator to view the data and the configuration. This can be done by changing the configuration to require TLS/SSL in your web browser.

Navigator provides a utility to help you modify the configuration, or you can do it manually.

Important Note on PHI and Security: Because the user interface can display patient protected health information (PHI) when accessed, users must follow appropriate procedures to preserve the security of such information. It is recommended that the HTTPS interface be used (in favor of the HTTP interface). If the HTTP interface is in use, it is strongly recommended that it only be accessible from within your LAN or VPN. Furthermore, it is recommended that the **Auto-logout Time** functionality (discussed in **Section 4.3 General Settings above**) be used to ensure that PHI does not stay visible on unattended screens (unless other similar security policies such as Windows auto-screen-lock policies are in place). Security of PHI is the responsibility of the organization using this software. Specific policies and practices to safeguard PHI are beyond the scope of this document.

7.2.1 Using the SSL Configuration Utility

1. 1. Get an SSL certificate for your host machine. This should include the Certificate File, the Certificate Key file, and optionally the Certificate Chain file. Note that the certificate file should be in PEM format. (This page has information on the files needed: **http://tomcat.apache.org/tomcat-7.0-doc/apr.html**. You can obtain a sample self-signed certificate for testing at http://www.selfsignedcertificate.com.)
2. From the Windows Start menu, launch the SSL Configuration Utility – go to `Start → Laurel Bridge Software → Navigator → Utilities → Configure for SSL`.



3. Select the **SSL Certificate File** and enter its path in the first field. The file usually has a **.cert** file extension. You can browse your local file system by pressing the "…" button next to the field.
4. Select the **SSL Certificate Key File** and enter its path in the second field. The file usually has a **.key** extension; it could also be the same as the SSL Certificate File.
5. Optionally, select the **SSL Certificate Chain File** and enter its path in the third field. This file is necessary if you do not want to be warned that the certificate is not trusted. If this is not a concern for you (for example, if Navigator will be accessed only from a secured internal network), you can leave this blank.

6. Navigator's Web Server service will be restarted after the configuration changes are made. You can choose to restart the HL7 Service too by checking the checkbox next to that option; uncheck the box if you don't want to restart the HL7 Service.
7. Once all the fields are filled in correctly, click the "**Next**" button. The certificate files will be copied to Navigator's installation directory, the configuration files will be updated, and the services will be restarted.

The next time you access Navigator's web site, you will be automatically redirected to the secure site.

If you want to change the certificates that are being used, the SSL Configuration Utility can do that, too – follow the same steps as described above.

Note that the utility can *not* be used to undo the SSL configuration changes – if you want to return to using HTTP instead of HTTPS to connect to Navigator, you will have to edit the configuration files *manually*. Please consult the Tomcat 7 documentation for how to do this.

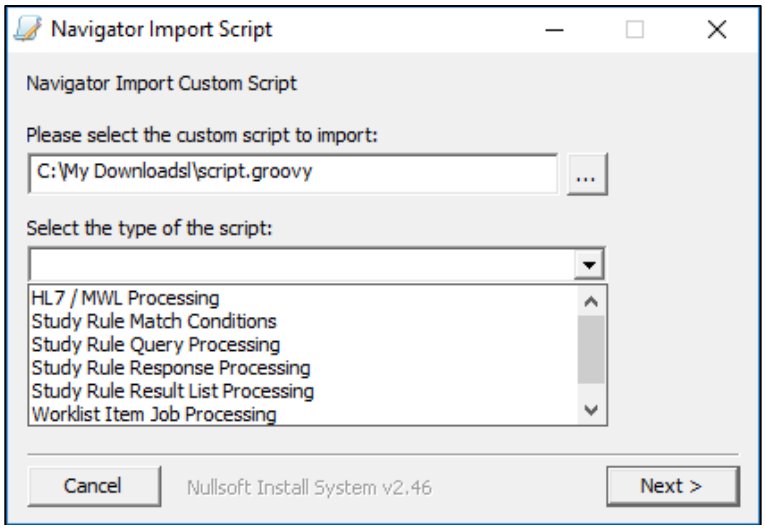
7.2.2 Manual SSL configuration

1. Get an SSL certificate for your host machine. This should include the **Certificate File**, the **Certificate Key file**, and optionally the **Certificate Chain file**. Note that the certificate file should be in PEM format. (This page has information on the files needed: **http://tomcat.apache.org/tomcat-7.0-doc/apr.html**. You can obtain a sample self-signed certificate for testing at http://www.selfsignedcertificate.com.)
2. Go to Navigator's installation directory (default: C:\LB Navigator) and into the **tomcat/conf** subdirectory.
3. Edit the **server.xml** file
    a. Near the middle of the file is a commented section of code marked "**TO ENABLE SSL**". Uncomment the "**Connector**" section directly below this by deleting the "**<!—**" and "**-->**" text at the beginning of the lines before and after the "Connector" section.
    b. Replace the text "**PATH_TO_CERTIFICATE_FILE.cert**" with the path to the SSL Certificate file that you got back in Step 1.
    c. Replace the text "**PATH_TO_KEY_FILE.key**" with the path to the SSL Key file.
    d. Optionally, you can replace "**PATH_TO_CHAIN_FILE.crt**" with the path to the SSL Certificate Chain file. This file is necessary if you do not want to be warned that the certificate is not trusted. If this is not a concern for you (for example, if Navigator will be accessed only from a secured internal network), you should just change the text to be blank.
    e. Save your changes to the **server.xml** file.
4. Edit the **web.xml** file.
    a. Near the bottom of the file is a commented section of code marked "**TO ENABLE SSL**". Uncomment the "**security-constraint**" section directly below this by deleting the "**<!—**" and "**-->**" text at the beginning of the lines before and after the "security-constraint" section.
    b. Save your changes to the web.xml file.
5. Restart the Navigator service (the easiest way is via the **Navigator Service Manager**, which can be accessed via the Windows Start menu: `Start → Laurel Bridge Software → Navigator → Navigator Service Manager`). The next time you access Navigator's web site, you will be automatically redirected to the secure site.

7.3 Import a Script

Navigator can use custom Groovy scripts to modify data and to affect the priors that are moved. You may have a custom script of your own or that was provided to you by Laurel Bridge Software – this utility will install it in the correct location for you.

1. Run the utility from the Windows Start menu: `Start → Laurel Bridge Software→ Navigator → Utilities → Import a script`
2. Enter the path to the script to be imported.
3. From the list, select the type of script that this is.
4. Click **Next**.

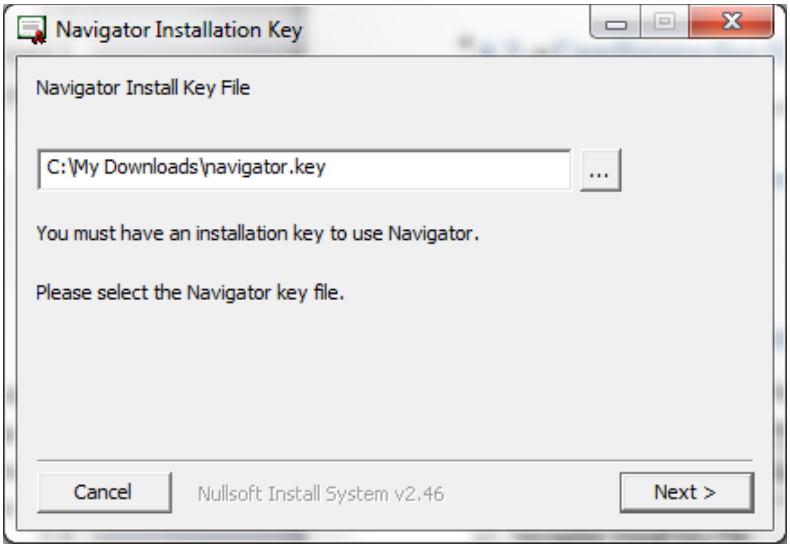


7.4 Install New License

If your Navigator license has expired, you may request a new one from Laurel Bridge Software. This utility is used to install your new license for you.

Run the utility from the Windows Start menu:

`Start → Laurel Bridge Software → Navigator → Utilities → Install New License`



On the Navigator web interface, you can click "Check license" to load the new license after it has been installed. Note that under some circumstances, you may need to restart the Navigator service to load the license – see Section **7.6 Navigator Service Manager** for the easiest way to restart the service.

7.5 Activate License

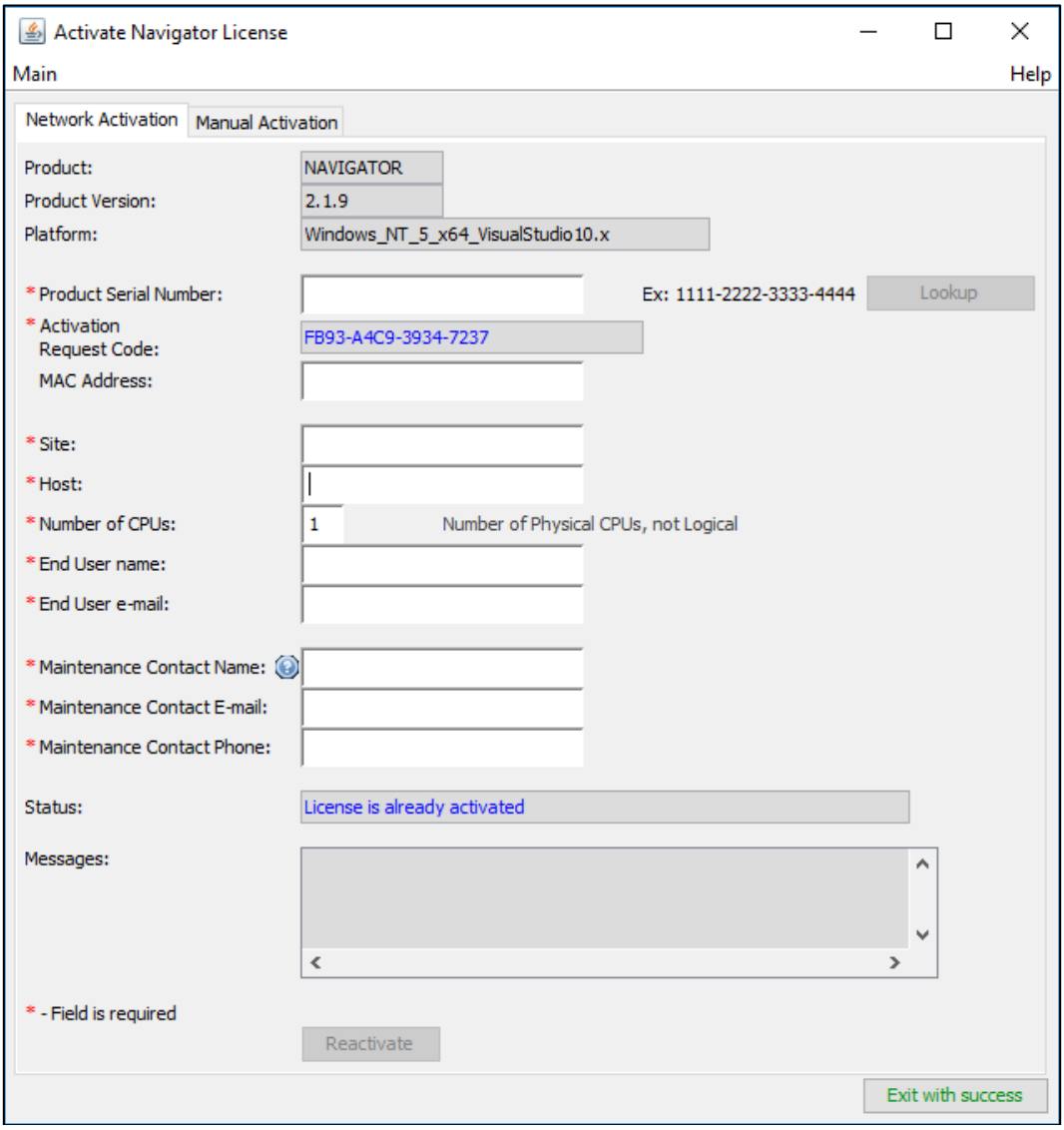
If your license needs activation, you can launch the License Activation Utility from the Start menu:

`Start → All Programs → Laurel Bridge Software → Navigator → Utilities → Activate License`

The License Activation Utility will let you activate your license in either Network mode or in Manual mode; each is described below. (Note that due to UAC restrictions, you may have to launch the utility with administrative privileges – right-click on the Start menu shortcut and click "*Run as administrator*".)

7.5.1 Network Activation

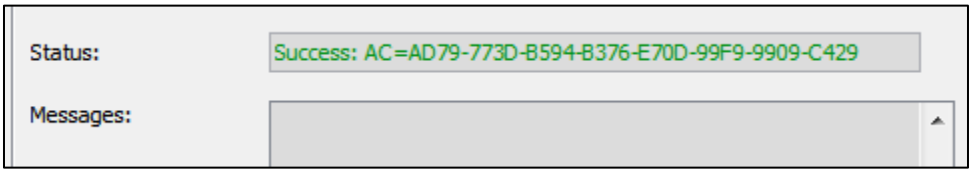
If you have Internet connectivity, you will want to activate the license via the Network – you will see a screen like that shown below:



Fill in all the fields – only the MAC Address is optional. The Product Serial Number was given to you when you purchased Navigator, or it can be found on the LBS licensing web site as you view your keys. (Once you have entered the Product Serial Number, you can use the **Lookup** button to query the Laurel Bridge Software website for any existing data for the key.) The Maintenance Contact is the person who Laurel Bridge Software should contact at ***your company*** when the application is due for renewal of its software

maintenance contract; it is ***not*** tech support. Note that the fields in blue do not need to be entered by you – the Activation Request Code is a system identifier that is generated on your computer by Navigator.

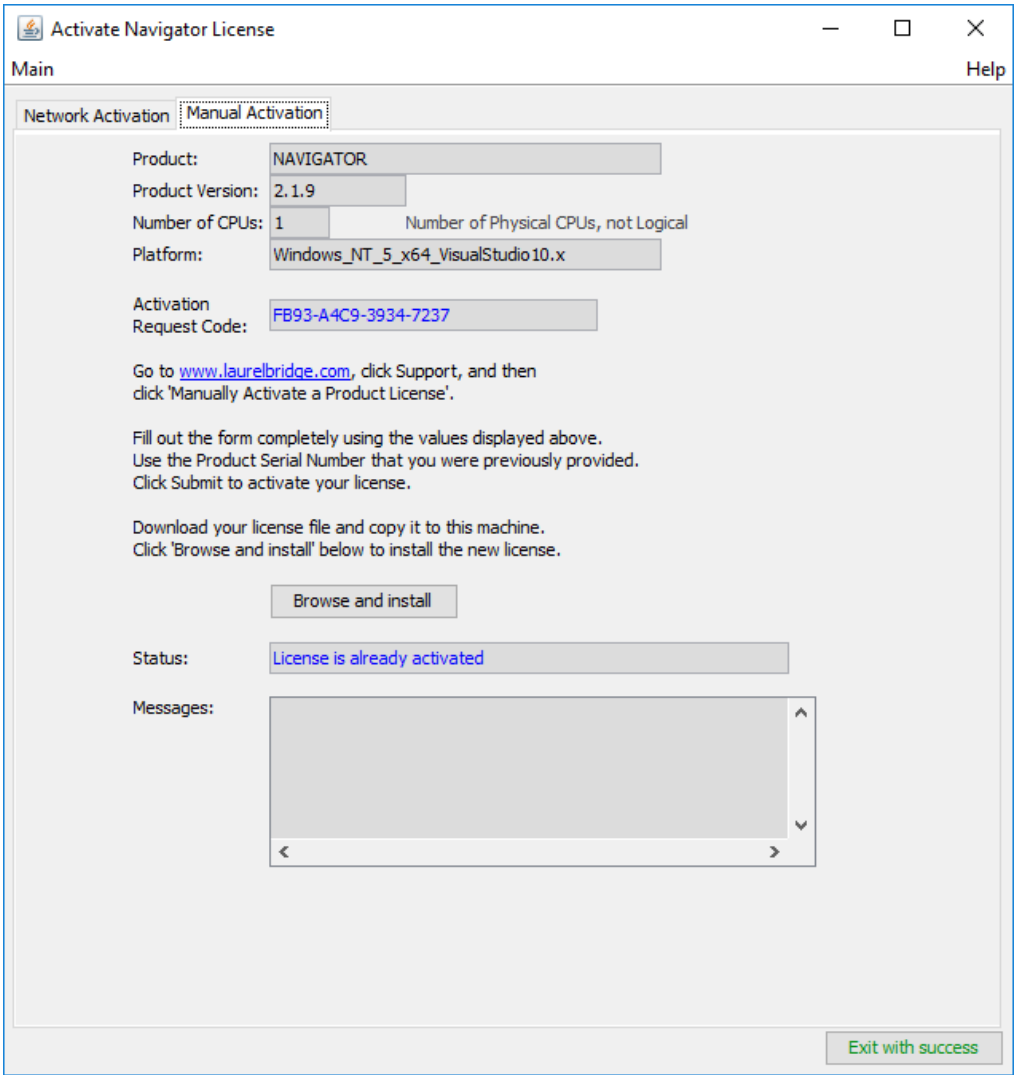
Once all the fields are filled in correctly, press the **Activate** button. The utility will communicate with the Laurel Bridge Software licensing web site and receive an Activation Code and other information back from the web site. Upon success, the status fields will look something like this:



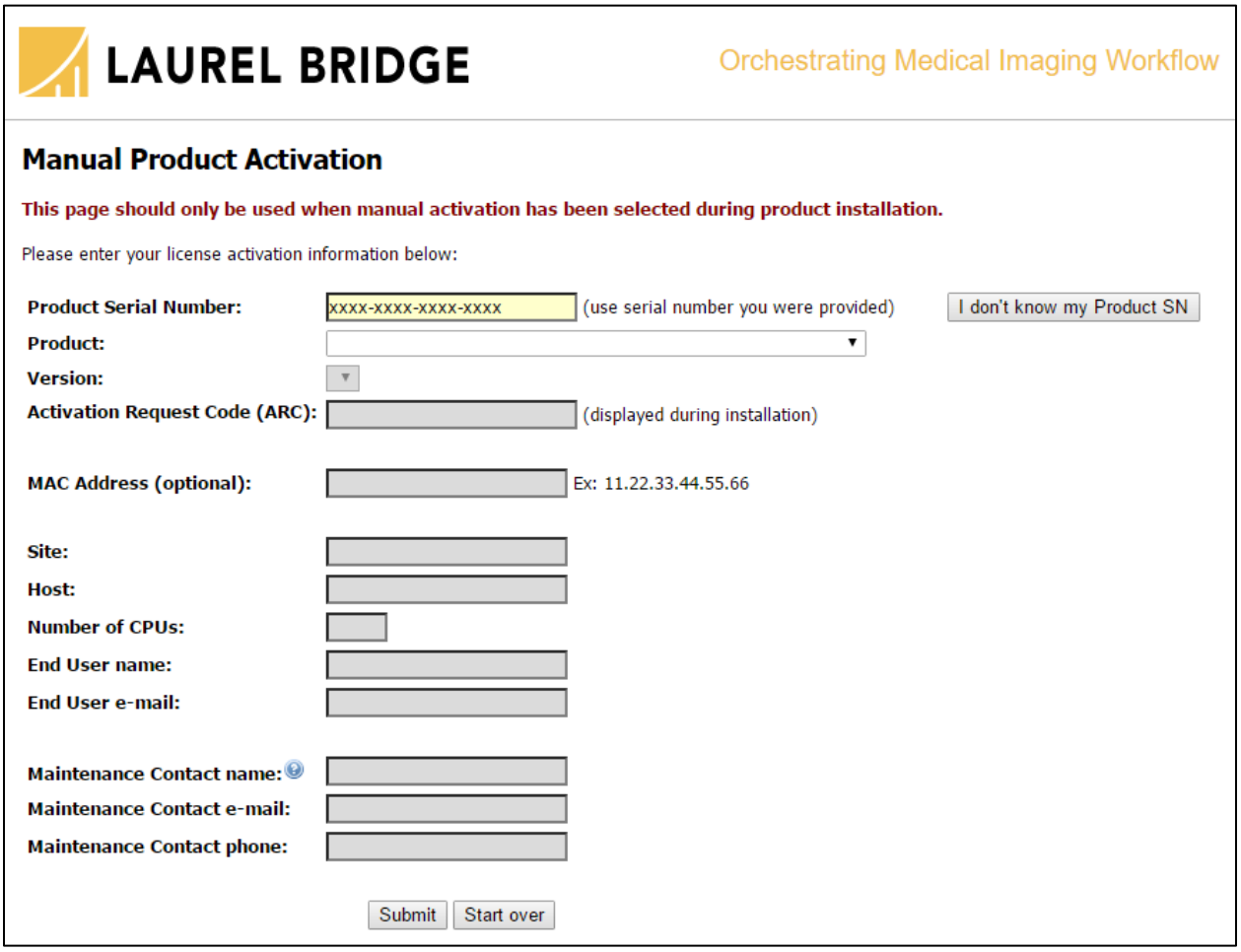
The Navigator license should now be activated, allowing you to use Navigator. Note that you may need to restart the Navigator service if you are installing a new license, in order for the license to take effect. If activation failed, you will see error messages explaining why. Resolve the errors if possible and try activating again.

7.5.2 Manual Activation

Manual Activation is used when the computer with Navigator does not have access to the Internet or to the Laurel Bridge Software licensing website – note that Network Activation is the *preferred* mode.
After you launch the License Activation Utility, you should select the Manual tab if it is not already selected.

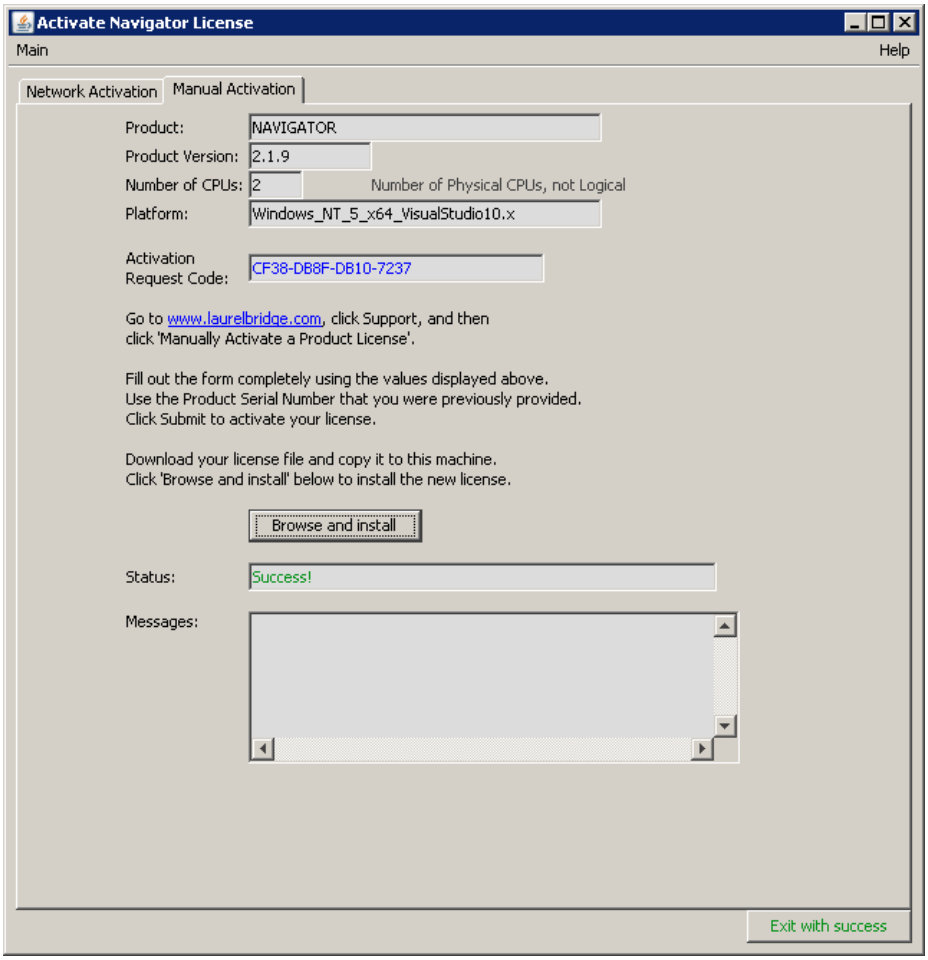


Using a web browser on a different system, proceed to the Laurel Bridge Software customer web site, select “Support”, and then select “Manually Activate a Product License” (or click this link: **https://www.laurelbridge.com/product_activation.php**). Enter the Product Serial Number that was obtained and then the Activation Request Code displayed by the utility (in the example above, it is CF38-DB8F-DB10-7237). Choose the version of software that you are activating. Also enter the site and contact information, and the number of CPUs for the system that is being activated, as well as the Maintenance Contact information. See the following screenshot:



After you click Submit, you will see a screen like that below.

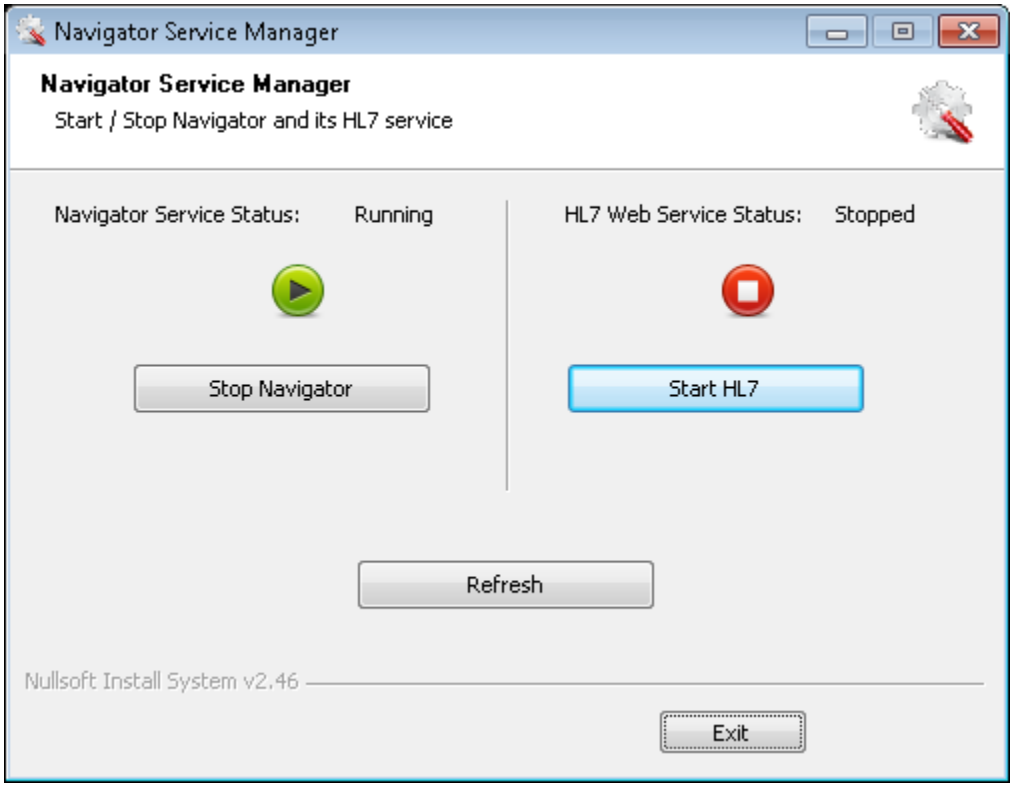
Click the **Download** button and save the license file, and copy it to the target machine. Then click "**Browse and Install**" on the License Activation Utility – search for the license file and select it. The utility will install it and verify that the license is valid. When it is done, the utility should look similar to this:



The Navigator license should now be activated, allowing you to use Navigator. Note that you may need to restart the Navigator service if you are installing a new license, in order for the license to take effect. If activation failed, you will see error messages explaining why. Resolve the errors if possible and try activating again.

7.6 Navigator Service Manager

If you need to check the status of the Navigator service or of its HL7 service, the Navigator Service Manager provides a simple user interface for this and for starting or stopping the services.
It is run from the Start menu: `Start → Laurel Bridge Software → Navigator → Navigator Service Manager`



From this interface, you can start or stop Navigator and the HL7 service independently. If you start or stop the service via some other mechanism (for example, via the Windows Control Panel), you can click Refresh to see what the current state of those services is. Since the HL7 service requires the Navigator service to be running, this utility will make sure that the HL7 service is stopped if the Navigator service is stopped. It will allow you to start Navigator without running HL7.

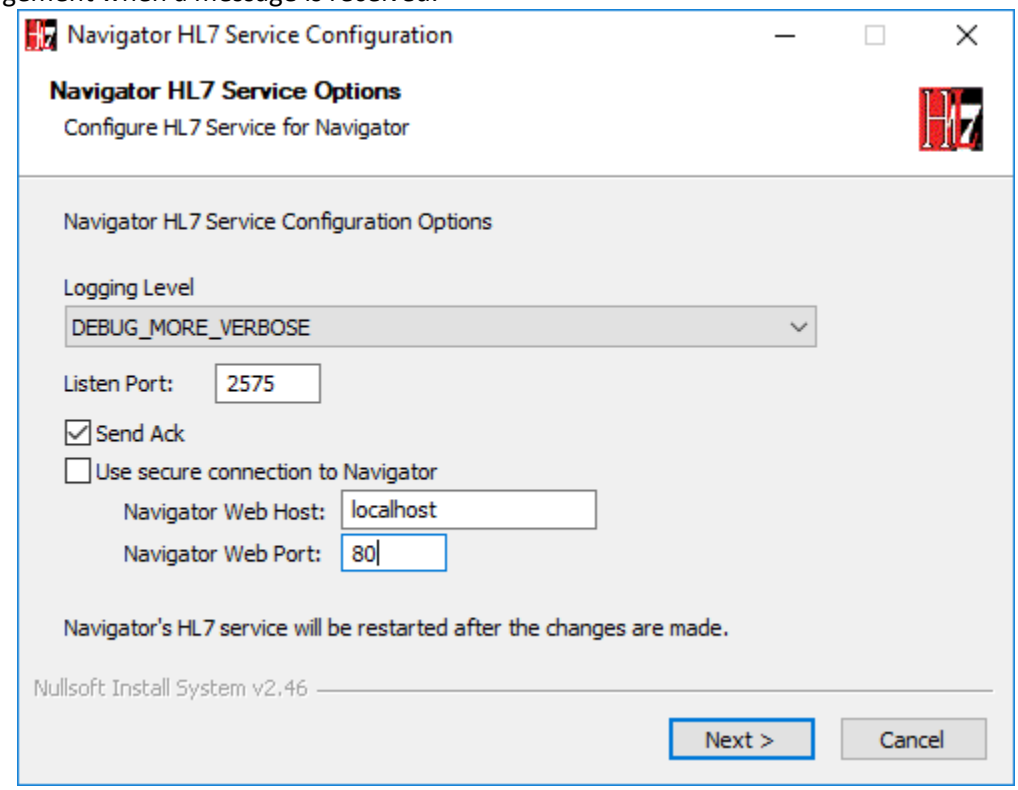
Note that it can take several moments – up to a few minutes – to do some operations, so please be patient.

8 HL7 Utilities

Navigator can be configured to process items that are received via HL7, not just via Worklist Server. Navigator includes some utilities to help you use and configure HL7. The HL7 utilities are accessed via the Windows Start menu (see **Appendix D: Start Menu Options on Different Windows** for assistance on different versions of Windows).

8.1 Configure HL7 Service

This utility provides an easy interface for changing the logging level of messages that the HL7 Service reports, changing the port that listens for HL7 messages, and whether the HL7 Service should send an acknowledgement when a message is received.



From the Start menu: `Start → Laurel Bridge Software → Navigator → HL7 Configuration → Configure HL7 Service`.

Modify the configuration as desired, and then click the Next button.

8.1.1 HL7 Template File

Navigator's HL7 Service uses a template file to parse HL7 messages and decide how the data should be sent to Navigator. The file is `HL7ServiceHttpClient-templates.xml`, usually located in the `C:\ProgramData\Laurel Bridge Software\HL7ServiceHttpClient` directory. If you are substituting your own template file, you should replace the existing one with your new one, making sure that the name is `HL7ServiceHttpClient-templates.xml`. (You can use the other HL7 utilities, described below, to configure and test your template file.)

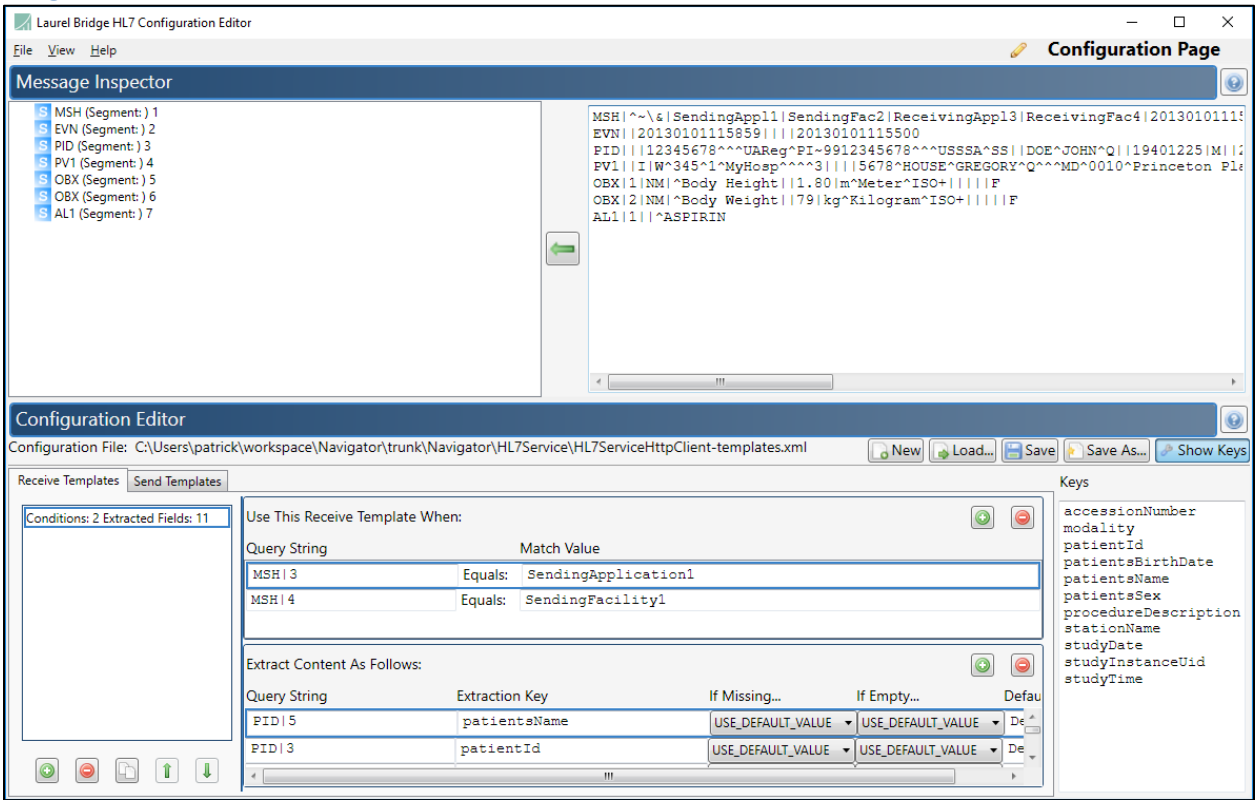
8.2 Configure HL7 Template

This utility lets you modify the template that parses the incoming HL7 messages and test that the message is parsed as you desire.

From the Start menu: `Start → Laurel Bridge Software → Navigator → HL7 Configuration → Configure HL7 Template`.
The Template Editor has a view for editing the template (**Configuration Page**), and a view for testing the parsing of a template (**Test Page**) – you can switch between the views using the View menu at the top.

8.2.1 Configuration Page

The Configuration Page is a place to author and publish configuration files that control the behavior for sending / receiving HL7 messages. There are two sections in this page: **Message Inspector** and **Configuration Editor**.



The **Message Inspector** provides an area to assist with authorship of Configuration files. Simply copy (or type) any HL7 Message string (e.g., one from a log file) into the "HL7 Message" window on the right. Then press the left arrow button, which will cause that message to be parsed into a hierarchical "tree view" in the left panel. In the tree view, you can right-click on any node to add a "*Content Extractor*" for that field to the currently selected Receive Template.
The **Configuration Editor** is where you author HL7 Configuration Files. Each template has Receive Templates and Send Templates. These templates contain **Conditions** (which indicate whether the templates will be used) and **Behaviors** (which indicates how they will be used). The Condition and Behavior fields are largely self-explanatory. These are used to define when a template is used and how the content is extracted from the message and into what fields the content is placed.

When you are modifying the Template to match your HL7 messages, keep in mind the terms that Navigator uses and expects to find when it is parsing an HL7 message into a Worklist Entry:

```
studyDate                    patientsBirthDate
studyTime                    patientsSex
modality                     stationName
procedureDescription         user001
studyInstanceUid             user002
```

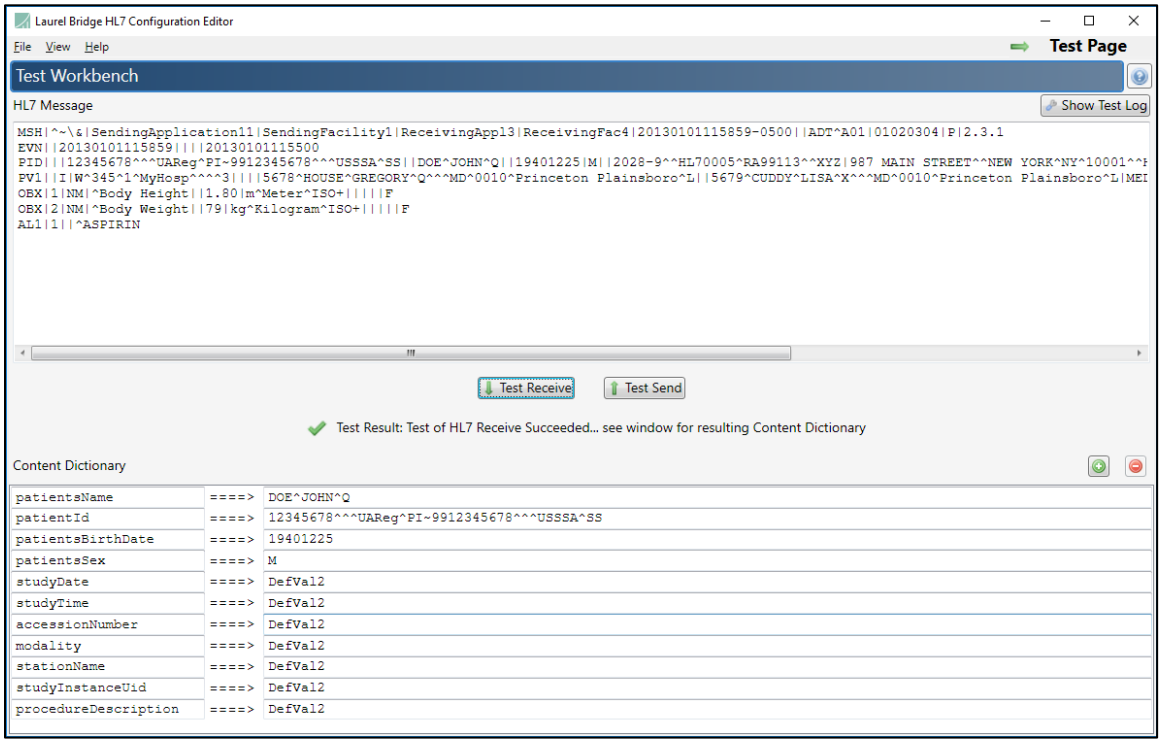


```
accessionNumber                 user003
patientsName                    user004
patientId                       user005
```

Note on HL7 and Study Dates: In most HL7 messages, a Study Date will include the date and time, while Navigator's DICOM processing expects the Study Date and Study Time to be separate fields. Navigator provides a sample HL7 Processing script – `Example_hl7_split_study_date_and_time.groovy` – that can be used with the **HL7 Web Service Reader** to split the HL7 Study Date field into separate Date and Time fields. See **Section 4.6 Worklist Readers** for more information on using a script with the HL7 Web Service Reader.

8.2.2 Test Page

The Test Page is a place to test both Send and Receipt of HL7 Messages using the currently loaded HL7 Configuration (from the **Configuration Page**).
There are two visible Input / Output panels – which one is Input and which one is Output depends on which button you use. The **HL7 Message** area contains the string version of a received / sent HL7 Message. The **Content Dictionary** area contains a collection of keys and values that your application knows about.



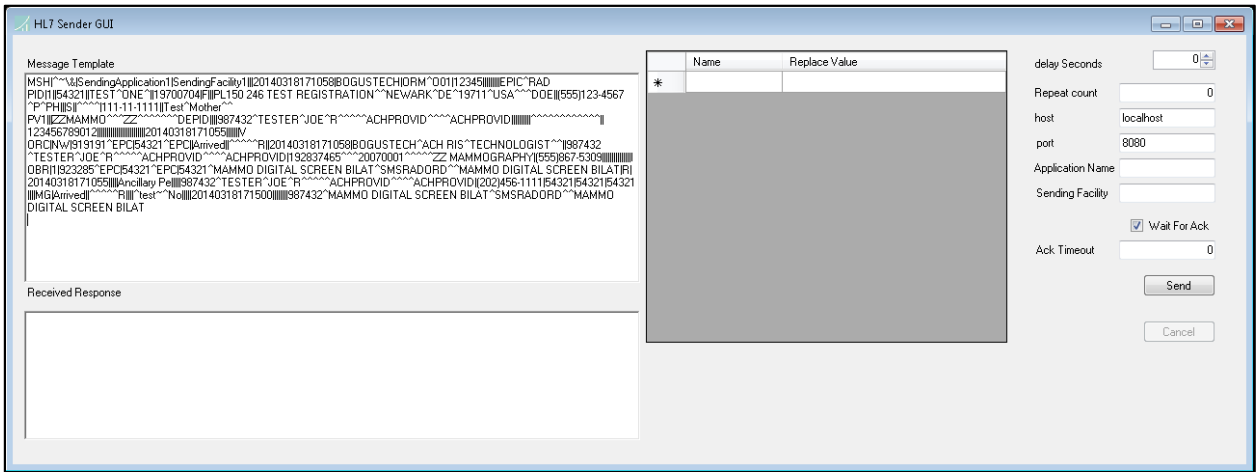
- To test **receipt** of an HL7 Message:
  Copy (or type) the HL7 Message into the "**HL7 Message**" panel and press the "**Test Receive**" button. The program will attempt to extract information from this message as if it were just received from the network. The fields that it successfully extracts will be populated into the "**Content Dictionary**" panel below it, and the results of the test will be displayed.
- To test **send** of an HL7 Message:
  Type the known "information" into the "**Content Dictionary**" panel and press the "**Test Send**" button. The program will compare this information to the Send Templates of the loaded configuration, find a match if possible, and then populate the Template String of the selected

template using the "**Content Dictionary**" information. The resulting HL7 Message will appear in the "**HL7 Message**" panel, and the result of the test will be displayed.

8.3 Send HL7 Test Messages

This utility lets you copy in an HL7 message template and send it to the HL7 Service. You can use this to test your HL7 configuration and Navigator's configuration. You can specify macros and values to substitute in the messages that are sent.

From the Start menu: `Start → Laurel Bridge Software → Navigator → HL7 Configuration → Send HL7 Test messages`.



Appendix A: Navigator Privacy and Security Statement

Because the Laurel Bridge Navigator application is installed on hardware that is provided, configured, and controlled by the Navigator customer, Laurel Bridge Software (LBS) cannot make assertions about the privacy and security of a particular Navigator installation. It is up to the customer to ensure that the host Windows system onto which Navigator is installed has been adequately secured and locked down. However, LBS does provide technology, tools, and guidance to assist customers in locking down their Navigator installations. In the context of this appendix, the term "Navigator customer" refers to the administrators for the host hardware system and for the Navigator application.

An overview of the Navigator application privacy and security features is given in the sections below, roughly following the format given in the HIMSS/NEMA Standard HN 1-2013, "Manufacturer Disclosure Statement for Medical Device Security", or MDS2 for short. (For more details about this form or to download it, see http://www.himss.org/resourcelibrary/MDS2 [NEMA Document ID: 100382]). The headers in the following sections map directly to the headers in the MDS2 document.

1 Management of Private Data

The Laurel Bridge Navigator application acts as an enterprise image fetcher for DICOM images, which may contain protected health information (PHI). Navigator can fetch these images from one or more sources and send them to one or more destinations. Consequently, Navigator can ingest, store, display, and transmit PHI. However, since the PHI only resides in Navigator temporarily, Navigator is not considered a primary repository of electronic health record (EHR) or electronic medical record (EMR) data, and thus is not maintaining part of the designated record set (as defined by HIPAA). Also, the Navigator application and the data it stores and manages is entirely resident within the customer premises (i.e., no part of the application or its data is cloud-hosted or hosted by LBS).

1.1 Types of PHI Maintained

Because Navigator is able to handle both DICOM and HL7 messages, it potentially transports and caches the following types of PHI:

- Patient demographic information
- Patient medical record information
- Patient diagnostic and therapeutic information (including diagnostic images)
- Patient financial information

1.2 Persistence of Private Data

Navigator maintains PHI both temporarily in memory (while running) and on disk (persistent storage). PHI may be found in data transmitted or cached by the application, and in log files generated during use of the application. Available security features to protect PHI when at rest are described below and in more detail elsewhere in this Navigator User Manual.

Note: Due to the sensitive nature of the PHI that Navigator handles, the only non-destructive and completely safe way to decommission a (non-virtual) computer system on which a production Navigator application has been running is to wipe the hard drive clean using a suitable hard drive wiping application. For self-encrypting drives, changing or overwriting the encryption key(s) should be sufficient.

1.3 Transmission of Private Data

PHI can be transmitted or received over the network via DICOM, HL7, or other messages. The ability to configure and control the behavior of this functionality is under the full control of the Navigator customer, and the use of these features remains under the full control of the customer. Available security features to protect PHI when in transit are described below and in more detail elsewhere in this Navigator User Manual.

Because Navigator does not process any patient billing transactions, it is not subject to the requirements of the Payment Card Industry (PCI) Data Security Standard.

2 Security Capabilities

The Laurel Bridge Navigator application is comprised of two parts:

1) **Navigator Service**, which runs as a Windows Service
2) **Navigator Web**, a web interface that allows configured web users to configure the system and to monitor and manage jobs

The following sections briefly describe available security features of the Navigator application. For more details, see the Navigator User Manual.

2.1 Automatic Logoff

The Navigator Web interface can be configured to automatically log off Navigator users in a configurable number of minutes. The default timeout is 5 minutes for admin users and 3 minutes for all other users, and the timeout can be configured to any value from 1 minute to 60 minutes.

2.2 Audit Controls

Navigator can be configured to send DICOM PS3.15 Appendix A.5 (“Audit Trail Message Format Profile”) audit messages to a syslog server (such as **syslog-ng** or **nsyslog)**. Messages can be sent via the TLS (recommended), UDP, or TCP protocols, and all messages include the user ID of the user performing the action as well as a date/time stamp.

The following types of audit trail messages can be enabled/disabled independently:

- **Application Start/Stop** – Logs when an application is started/stopped.
- **Software Configuration** – Logs when changes are made to the software configuration.
- **DICOM Instance Network Transfer** – Logs when DICOM instances are transmitted via the network.
- **User/Security Alerts** – Logs when web user or security alerts occur.
  These include events such as web user logon/logoff, web user addition/removal, web user password/role changes, and manual modifications of DICOM or HL7 jobs.

The following DICOM PS3.15 Appendix A.5 audit trail message types are supported by Navigator:

- **Application Activity**
  - Application Start
  - Application Stop
- **Audit Log Used**
- **Begin Transferring DICOM Instances**
- **DICOM Instances Accessed**

- **DICOM Instances Transferred**
- **Query**
- **Security Alert**
    - Security Configuration
    - Software Configuration
    - Use of Restricted Function
    - User Security Attributes Changed
- **User Authentication**
    - Login
    - Logout

2.3 User Authorization

The Navigator Web users can either be locally administered (by the Navigator Web module), or they can be administered using LDAP / Active Directory. This is done by the Navigator customer configuring one or more Active Directory groups for each of following built-in web user roles:

- Admin user
- Regular user
- View-only user

2.4 Security Configuration

The Navigator customer has full control over and responsibility for the security of Navigator, both through the ability to lock down the Windows system on which Navigator is installed, as well as through the ability to configure the security features built into the Navigator application. Extensive information about how to do this is found in this Navigator User Manual.

2.5 Security Updates

The Navigator customer has full control over the installation of Windows security updates, as well as over the installation of any Navigator application updates.

2.6 De-Identification of PHI

Navigator does support the ability to configure de-identification of PHI. However, due to the consequences this can have on the usability of the DICOM and HL7 messages, this is typically only configured when sending images containing PHI to external organizations (such as organizations which may use the images for academic or publication purposes). When sending PHI over the public internet to / from satellite locations, the use of TLS encryption or an encrypted VLAN is the way recommended by the DICOM Standard to protect the confidentiality of PHI in transit.

2.7 Backup and Restore

The Navigator customer has full responsibility to both install and maintain the SQL Server database which provides the backing store for the Navigator jobs. As such, the customer is also responsible for providing backup and restore capabilities for the SQL Server database. Microsoft provides an extensive set of SQL Server backup, restore, and replication technologies.

2.8 Emergency Access

Since the Navigator customer has full control over the installation and configuration of both the host system and the Navigator application itself, it is up to the customer to provide a means of emergency

access (“break-glass” feature) by maintaining alternate access to administrative credentials for the systems involved.

2.9 Data Integrity and Authenticity

Since one of the primary functions of Navigator is to modify DICOM messages, it is simply not practical to implement a mechanism whereby alteration of data can be detected. Instead, the following techniques can be used to control and track data modifications:

- Use Audit Trail logging to record any access to or modification of data.
- Use Navigator Web authentication (either locally-administered or based on Windows Authentication) to ensure that unauthorized web users cannot access the Navigator data remotely.
- Use TLS encryption on the web connections used by the system to ensure privacy, node authentication, and protection against man-in-the-middle (MITM) attacks.

Navigator does not currently use explicit error detection on data at rest, but rather depends on the built-in ECC error detection and correction technology provided by modern hard drives (as supported by Windows). If data redundancy is desired, LBS recommends the use of RAID data storage technology for both the SQL Server database repository and for the DICOM image cache.

2.10 Malware Protection

Since the Navigator customer has full control over the installation and configuration of both the host Windows system and the Navigator application itself, it is up to the customer to install and maintain malware protection technology. Navigator itself should be unaffected by the use of such technology (beyond the obvious potential impact to system performance that can occur when using anti-virus software). For performance reasons, it is generally recommended that antivirus checking be turned off for the SQL data directories used by Navigator.

2.11 Node Authentication

Node authentication (the ability to confirm the identity of sender of web data) can be implemented using TLS protocols on all web connections. Navigator supports TLS versions 1.0, 1.1, and 1.2 as a client . More details about how to do this and further security details can be found elsewhere in this Navigator User Manual.

2.12 Person Authentication

User authentication for web interface users can also be controlled either locally or using LDAP/AD.

2.12.1 Local Web User Administration

If you elect to administer web users locally, then there are no limits placed on the number of user accounts that can be created. Customers can and should immediately change default passwords during the installation process (there are two default accounts, an admin-level “administrator” account and a view-only-level “viewonly” account). Passwords must be a minimum of 8 characters long and must contain both uppercase and lowercase letters. Optionally, a high-security password mode can be enabled, which requires that passwords be a minimum of 12 characters long and must contain numeric digits, in addition to uppercase and lowercase letters. Shared user IDs can be used, but Navigator can also be configured to disallow simultaneous logins from different computers. Local users’ passwords cannot currently be configured to expire.

2.12.2 Single Sign-On (LDAP/AD) Web User Administration

When web users are administered via a single sign-on technology such as LDAP/AD (recommended), the rules regarding users and passwords are up to the single sign-on technology. Active Directory allows for the configuration of password complexity and expiration rules, account locking, centralized account administration, etc.

2.13 Physical Locks

Since the Navigator customer owns and has full control over the host Windows system on which Navigator is installed, it is up to the customer to maintain the physical security of the host system.

2.14 Device Life Cycle Roadmap

The Navigator application currently supports the following Windows operating systems:

- Windows 7
- Windows 8.1
- Windows 10
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016

LBS intends to support each of these operating systems up until their respective end-of-extended-support dates.

In addition, the Navigator application has the following software dependencies:

- SQL Server (can be SQL Server 2008 R2 x64, SQL Server 2012 x64, SQL Server 2014 x64, or SQL Server 2016 x64)
- SQL Server Management Studio
- .NET Framework 3.5 (or later)

2.15 System and Application Hardening

Since the Navigator customer provides, configures, owns, and has full control over the host system on which Navigator is installed, it is up to the customer to perform system hardening, as well as to configure the Navigator application for the desired level of application hardening. More details about hardening of the host Windows system and the Navigator application can be found elsewhere in this Navigator User Manual.

Some specific application hardening techniques that are supported by and/or implemented in Navigator include:

- Use of Authenticode digital signatures (currently SHA256) for all LBS executables, DLLs, and jars
- Support for TLS encryption for web data in transit
- Provision of instructions for how to lock down the TLS protocols and ciphers, which affects the Navigator Web interface
- Support for single sign on (Windows Authentication / Active Directory)
- Support for PHI anonymization for exported data (non-reversible)

The implementation of the following lockdown techniques on the host Windows system is the responsibility of the Navigator customer:

- Disabling of unnecessary Windows accounts
- Disabling of unnecessary open network ports (e.g., telnet, ftp, etc.)
- Removal of any unnecessary off-the-shelf applications
- Disabling of the ability to boot from removable media (if physical access to the host Windows system cannot be controlled)
- Enabling of BitLocker or other at-rest, full-disk encryption technologies (if desired)
- Enabling of SQL Server encryption (especially if the database resides on a different, unencrypted system)

2.16 Security Guidance

The security-related features of the Navigator application are described in detail in this Navigator User Manual.

2.17 Data Storage Confidentiality

Navigator does not encrypt data while at rest on the hard drive(s). PHI is mainly stored in the SQL Server database. If at-rest encryption of PHI is deemed necessary (e.g., if physical access to the host Windows system cannot be controlled), we recommend the use of a full disk encryption technology such as BitLocker or the use of self-encrypting drives. SQL Server at-rest encryption technologies such as Transparent Data Encryption (TDE) may also be necessary if the SQL Server database is resident on a different (unencrypted) system. Navigator does not currently support encrypted SQL Server connections.

2.18 Data Transmission Confidentiality

Navigator can be configured to encrypt web data in transit (using TLS), which will protect the data against interception by unauthorized parties. It can also be configured to use irreversible de-identification, which will remove any PHI from the data. And as mentioned above, Navigator supports encrypted SQL Server connections, and LBS highly recommends using them in the case of SQL Server instances accessed over a network.

2.19 Data Transmission Integrity

TLS encryption also protects the data against any attempt to modify the data during transmission (i.e., MITM attacks). Navigator will only transmit data to destinations that have been explicitly configured within the application by the customer.

2.20 Other Security Considerations

Navigator can be serviced remotely by LBS only with the express permission of the Navigator customer, as access to the host system onto which Navigator is installed is completely controlled by the customer. Navigator does not contain any service backdoors, nor does it contain any secret service accounts. All LBS access to an installed Navigator application must be explicitly enabled/allowed by the customer using standard Windows secure remote access technologies.

The following port numbers are the defaults used by the Navigator application. Note that these can all be changed by the Navigator customer, if so desired.

- HL7 input port = **2575**
- HTTP port = **8080** (8**443** if using HTTPS)

Appendix B: Body Part Configuration File

The **Body Part Configuration File** can be used in a **Study Rule** to filter out priors that do not have a matching body part. The original Worklist Entry's **Requested Procedure Description** is checked to find the body parts that match it by comparing the groups of related terms in the configuration file against the Procedure Description. When a matching term is found, the group is remembered. Then the **Study Description** in each prior is tested against the groups of terms in the remembered groups. If one of the terms in a remembered group matches a word in the Study Description, that prior is considered to be relevant because of a matching body part.
An example may make this clearer. Consider the following Body Part Configuration:

```
[ head ]
brain
cranium

[ chest ]
heart
lungs
thorax

[ leg ]
knee
thigh

[ breast ]
mammo
```

A Worklist Entry comes in with a Requested Procedure Description of **"CT of cranium and thorax",** and we want to find any priors that match. The terms in the groups are checked against the Requested Procedure Description – the relevant body part groups are **head** and **chest** (because "cranium" in the "head" group matches the Description, and "thorax" in the "chest" group also matches the Description).
Now several priors are received, with these Study Descriptions:

prior 1: "US of lungs"
prior 2: "MR knee"
prior 3: "Mammo 4 view"
prior 4: "XA heart"

Prior 1 is checked against the groups and is found to belong to the **chest** group (because "lungs", in the "chest" group, matches the prior's Description of "US of lungs"). Prior 2 belongs to the **leg** group ("knee" is in the "leg" group). Prior 3 belongs to the **breast** group ("mammo" is in the "breast" group). Prior 4 belongs to the **chest** group ("heart" is in the "chest" group).

prior 1: "US of lungs" → **chest**
prior 2: "MR knee" → leg
prior 3: "Mammo 4 view" → breast
prior 4: "XA heart" → **chest**

The original Worklist Entry used the groups **head** and **chest** – this means that prior 1 and prior 4 are relevant, and these will be moved as relevant priors based on the body part.

Note that the names of the groups don't matter – they are purely descriptive for ease of reference in finding related terms.

The Body Part Configuration file is a text file. This means it can be edited in any normal text editor, such as VI or Notepad. It can also be edited via Navigator's GUI under **Configuration → Custom Scripts**. You can customize the Body Part Configuration file to suit the terms and groupings used at your location. You can also have multiple configuration files, with different ones used in different Study Rules.

Note that if the **Requested Procedure Description** is "ALL", the body part matching will be ignored and all priors will be regarded as relevant. This can be useful if you want to get all priors for a patient regardless of body part, especially in Manual Entry Mode. Other filtering of priors will still occur – age of prior, maximum number to fetch, etc. – but no filtering will be done based on body part.

1. Adjacent Body Parts

Navigator's Body Part Matching can also be configured to allow priors for body parts that are *near* to the body part in the **Requested Procedure Description**. For example, if a patient is having a study done on his wrist, you may want priors that include his hand or his forearm but not those for his abdomen or legs. Each group in the body part configuration file may be modified to have "includes" – these are groups in the configuration file that may be relevant to the items in the current group. An example is shown below:

```
[ WRIST ]
eq = WRIST
eq = WRISTS
include = FOREARM
include = HAND
```

This means that priors that match the terms in either the FOREARM group or the HAND group will be included for processing.

You can modify the includes in the file to match your own relevancy requirements – just make sure that each group that is listed as an include is the valid name of a body part group in the file.

See the example file **Example_body_part_equivalents_with_includes.cfg** for more detail.

Appendix C: Backing up Navigator

As with any piece of software, you should regularly back up Navigator and its configuration data, as well as its database files. (Consult your SQL Server manual for how to back up your databases.) Backing up Navigator's configuration files is necessary in case of a system failure, but it can also be helpful if you are creating a secondary server with the same configuration.

Navigator's configuration files are stored under the `C:\ProgramData\Laurel Bridge Software\Navigator2` directory.

Files to backup:

- `cfg\apps\defaults\Navigator`
- `cfg\systeminfo`
- `cfg\datasrc_external.properties`
- Any files in `cfg\dicom\filter_sets`
- All the files in the `scripts` directory

If you are using HL7, you should also backup the XML configuration files in `C:\ProgramData\Laurel Bridge Software\HL7ServiceHttpClient`.

If you are creating a backup server, you should install Navigator with the license for the backup server – use the same installation directory and install settings as you used for the primary server. Then copy over these files to the same locations:

- `cfg\apps\defaults\Navigator`
- Any files in `cfg\dicom\filter_sets`
- All the files in the `scripts` directory
- The HL7 XML configuration files in `C:\ProgramData\Laurel Bridge Software\HL7ServiceHttpClient`

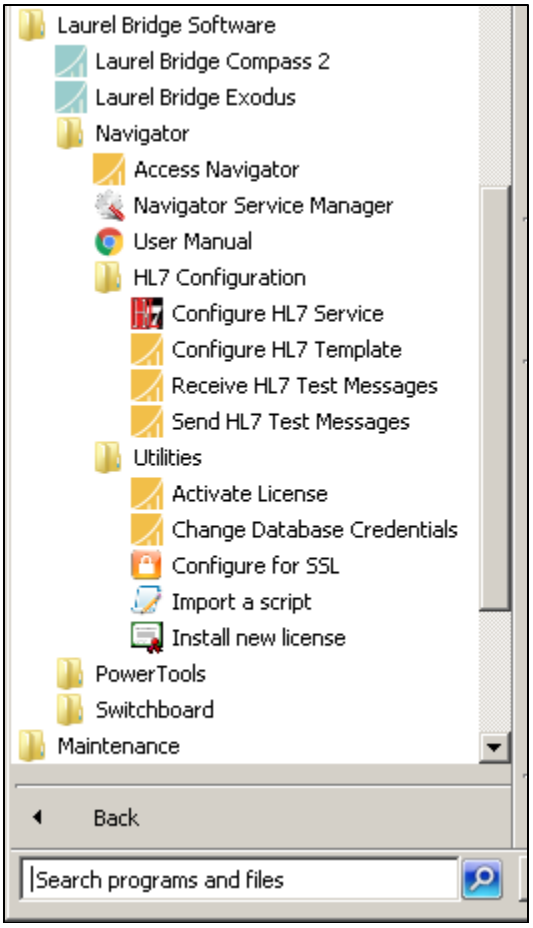
Appendix D: Start Menu Options on Different Windows

Navigator is controlled through a user interface accessible from your web browser. However, there are utilities (see section **7 Navigator Utilities above** for more information) that are run on the local computer. These are accessed via the Windows Start menu. On most Windows OSes, the Start menu and the options are easy to find, but it can be more difficult on Windows Server 2012 and similar OSes, and the style can vary as new updates are issued. Below are some samples of how to find the utilities.

- ## Windows 7

Click the **Start** button in the lower-left corner of the screen.

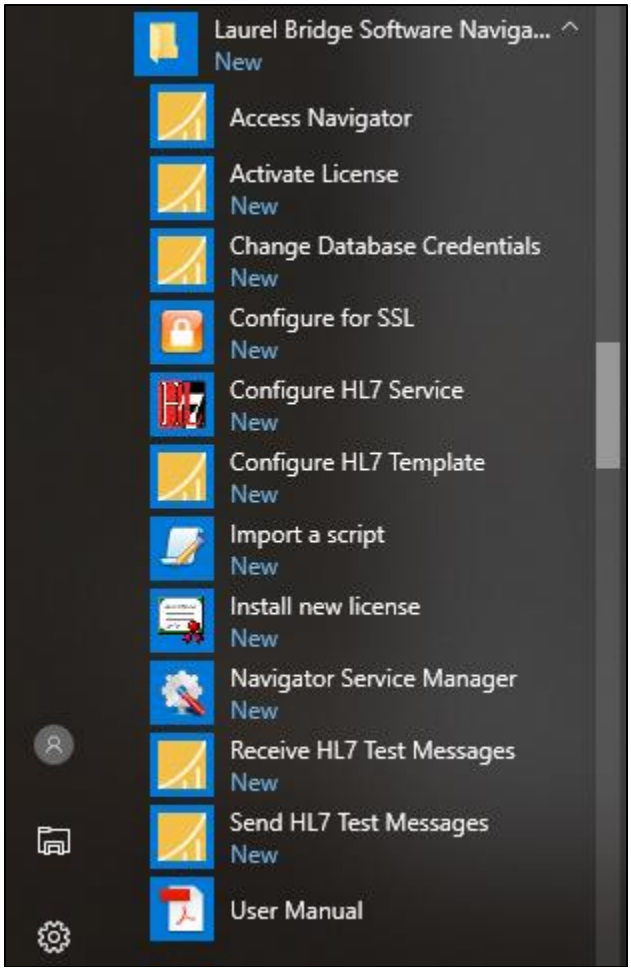
Then select **All Programs**, then **Navigator**, then **Utilities**.



- ## Windows 10

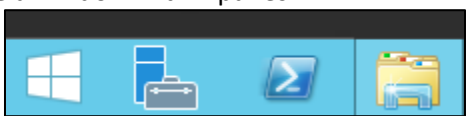
Click the **Start** button in the lower-left corner of the screen – it looks like a window with 4 panes.

Then scroll down the list of menu options to **Laurel Bridge Software Navigator**. The utilities are listed there along with other Navigator tools and links.



- ## Server 2012 and similar

Click the **Start** button – it looks like a window with 4 panes.



Then click the **Down** arrow button on the screen,

And scroll down or to the right until you find **Laurel Bridge Software Navigator**. The utilities are listed there along with other Navigator tools and links.

Appendix E: Regular Expressions

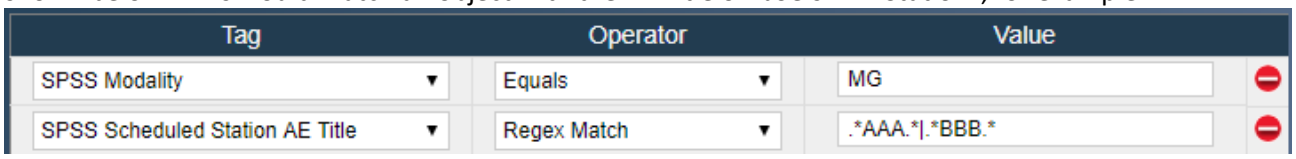
1. OR'ing Strings

If you know how to use regular expressions, you can reduce the complexity and number of your Study Rules. For example, if you have several different AE Titles to match on, you would probably create one Study Rule for each AE Title – the Matching Conditions for Study Rule One would match AE Title One, the Matching Conditions for Study Rule Two would match AE Title Two, and so forth. But if the Study Rules are the same except for that one Match Condition, you can use a regular expression (or "regex") to check if AE Title is One or Two or Three, etc.

You would set one of the Match Conditions (Step 1 for a Study Rule) like this:

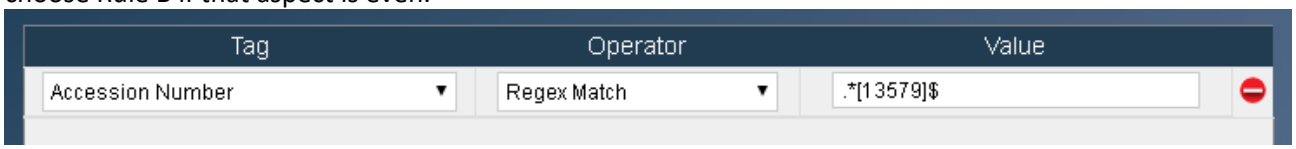
If the Scheduled Station AE Title *exactly* matches "`AAA|BBB|CCC`" – e.g., the AE Title is "AAA" – and the Modality is "MG", this Study Rule would be used. (Note that we only used AE Title and "AAA", "BBB", etc., for this example – you would use your own values for AE Titles, along with whatever Worklist Item Tag you desire.) You could then have a different Study Rule that used a similar regex for AE Titles NNN, OOO, and PPP.

The above regular expression example matches the *exact* strings "AAA" or "BBB" or "CCC". If you wanted the rule to match if the AE Title *contains* either "AAA" or "BBB", you would specify the regex as "`.*AAA.*|.*BBB.*`" – this means "any number of characters followed by AAA followed by any number of characters **OR** any number of characters followed by BBB followed by any number of characters". This is shown below. This would match an object with the AE Title of "Joe's BBB Station", for example.



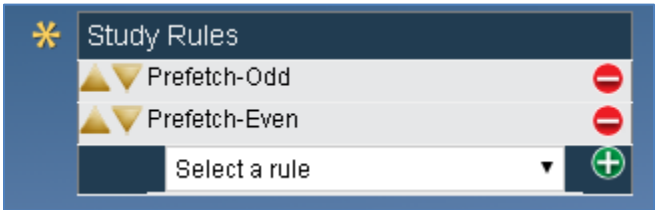
2. Odd or Even Load Balancing

Let's say you are moving a lot of studies to two different PACS systems – the same processing needs to be done, but you want to balance the load by moving some studies to PACS #1 and some to PACS #2. You could create two identical Study Rules and then choose Rule A if some aspect of the Worklist Item is odd, or choose Rule B if that aspect is even.



Here, we are saying to use this rule if the Accession Number matches "`.*[13579]$`", which means any number of characters, followed by one of the odd digits, followed by the end of the string. In this example, if the Accession Number is odd, this Study Rule would be chosen. You would create a similar Study Rule with a check for the even numbers.

Alternatively, you could not check for the even digits, but just make sure that the Prefetch-Odd rule is listed before the Prefetch-Even rule in the Worklist Reader configuration, as shown below.



== end of document ==

