

Navigator User Manual



LAUREL BRIDGE

Providing DICOM Connectivity for the Medical Community

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

Document Version: 2.1.23
Document Number: LBDC-000089-02123
Last Saved: 4/5/2022 4:05:00 PM

Contents

1	What is Navigator?	1
1.1	Overview – Priors Fetching Basics	1
2	Installation	2
2.1	Recommended System Specification	2
2.2	System Software Prerequisites.....	2
2.3	Installing and configuring SQL Server 2012 Express x64	3
2.3.1	Reconfiguring SQL Server	3
2.3.2	To enable the sa login.....	4
2.3.3	Using a non-administrator user	4
2.3.4	Database Recovery Model.....	4
2.4	Navigator Main Software Installation.....	5
2.4.1	Quiet Mode Installation.....	9
2.5	Upgrading Navigator.....	9
2.6	Uninstalling Navigator	11
2.6.1	Removing PHI.....	12
3	Navigator Configuration Worksheet.....	14
3.1	DICOM Device Configuration Prerequisites	14
3.2	Configuration Worksheet	14
4	Configuring Navigator	16
4.1	Navigator’s Main Screen.....	16
4.2	Configuration	17
4.3	General Settings	18
4.4	Devices.....	24
4.5	Study Rules	27
4.6	Worklist Readers.....	32
4.7	Scripts	34
4.8	Contacts	37
4.9	Users	38
4.9.1	Creating a User	39
4.9.2	Editing a user	40
4.10	Advanced Configuration Options	41

4.10.1	Custom Tags.....	41
5	Logging.....	42
5.1	Audit Log.....	43
6	Worklist Entries	44
6.1	Manual Job Entry	49
7	Navigator Utilities	50
7.1	Change Database Credentials.....	50
7.2	Configure for TLS / SSL.....	51
7.2.1	Using the SSL Configuration Utility.....	52
7.2.2	Manual SSL configuration	53
7.2.3	Note on the HL7 Service	54
7.2.4	HTTP Strict Transport Security.....	54
7.3	Import a Script	55
7.4	Install New License	55
7.5	Activate License	56
7.5.1	Network Activation.....	56
7.5.2	Manual Activation.....	58
7.6	Navigator Service Manager	60
7.7	Change Web Ports	61
7.8	Reset Administrator Password	61
7.8.1	Alternate method to reset the administrator's password	62
8	HL7 Utilities.....	63
8.1	Configure HL7 Service.....	63
8.1.1	HL7 Template File	64
8.2	Configure HL7 Template	64
8.2.1	Configuration Page	64
8.2.2	Test Page.....	66
8.3	Send HL7 Test Messages.....	66
Appendix A: Navigator Privacy and Security Statement		68
1	Management of Private Data	68
1.1	Types of PHI Maintained	68
1.2	Persistence of Private Data.....	68

1.3	Transmission of Private Data	69
2	Security Capabilities	70
2.1	Automatic Logoff	70
2.2	Audit Controls	70
2.3	User Authorization.....	71
2.4	Security Configuration	71
2.5	Security Updates.....	71
2.6	De-Identification of PHI	71
2.7	Backup and Restore	71
2.8	Emergency Access	71
2.9	Data Integrity and Authenticity	71
2.10	Malware Protection	72
2.11	Node Authentication	72
2.12	Person Authentication.....	72
2.12.1	Local Web User Administration	72
2.12.2	Single Sign-On (LDAP/AD) Web User Administration	72
2.13	Physical Locks	72
2.14	Device Life Cycle Roadmap.....	72
2.15	System and Application Hardening	73
2.16	Security Guidance.....	73
2.17	Data Storage Confidentiality.....	73
2.18	Data Transmission Confidentiality.....	74
2.19	Data Transmission Integrity.....	74
2.20	Other Security Considerations.....	74
3	GDPR Notes	75
	Appendix B: Body Part Configuration File.....	76
1.	Adjacent Body Parts.....	77
	Appendix C: Backing up Navigator.....	78
	Appendix D: Start Menu Options on Different Windows.....	79
	Appendix E: Regular Expressions.....	81
1.	OR'ing Strings.....	81
2.	Odd or Even Load Balancing	81

3. Checking if a String Contains a Value	82
Appendix F: Changing Navigator's web port	83
1. Using the Change Web Ports utility:.....	83
2. Manual steps:	83
Appendix G: TLS Certificates	85
1 Self-Signed Certificate	85
2 Trusted Certificate	85
2.1 Using OpenSSL	85
2.2 Using Keytool	86
3 Convert PFX to PEM.....	86
Appendix H: User Chooses the Priors.....	88
Appendix I: Checking if a Study already exists on the Destination.....	90
1 Note on Storage Groups	90
Appendix J: Java Keystore	92
Appendix K: Navigator's CSV Reader	95
1 Configuration	95
2 Running the Reader	96
3 Using HTTPS Access	97

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 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 the exams are 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 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 4.8
- Microsoft SQL Server 2012/2014/2016 x64 or newer
- **SQL Management Studio for SQL Server 2012 Express** or **SQL Server 2012** or newer
- A recent web browser – suggested: Google Chrome (Internet Explorer is *not* recommended)

Cluster Installation – If Navigator is being installed as part of a Windows Failover Cluster, then the Windows Server 2012 operating system must be installed, and the following prerequisites must be installed prior to installing Navigator:

- Microsoft .NET Framework 4.8
- Microsoft SQL Server 2012 x64 or newer
- **SQL Management Studio for SQL Server 2012 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 2012 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 10 and Windows Server 2012. 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 2012 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.) If you plan to connect via **Windows Authentication**, the user should have the **dbcreator** server role.
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 2012 → 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 2012 → 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 2012 → 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**. Note that if you plan to connect via **Windows Authentication**, the user should have the **dbcreator** server role.
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 2012 → 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 2012 → 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.

2.3.4 Database Recovery Model

SQL Server backup and restore operations occur within the context of the recovery model of the database. Recovery models are designed to control transaction log maintenance. The Database Recovery Model controls how transactions are logged, whether the transaction log requires backing up, and the types of restore operations that are available. Navigator recommends using the **Simple** recovery model to keep the transaction logs from growing too large.

To set the recovery model:

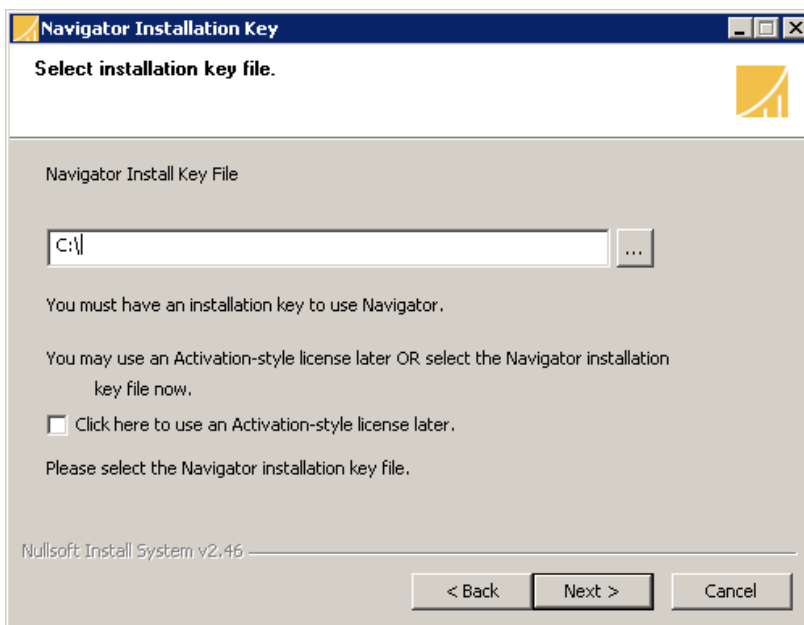
1. Start **SQL Server Management Studio** and login.
2. Open up the **Databases** subtree.
3. **Right-click** on the Navigator database and select **Properties**.
4. Click on the **Options** page
5. Set **Recovery model** to **Simple**.
6. Click **OK**.

2.4 Navigator Main Software Installation

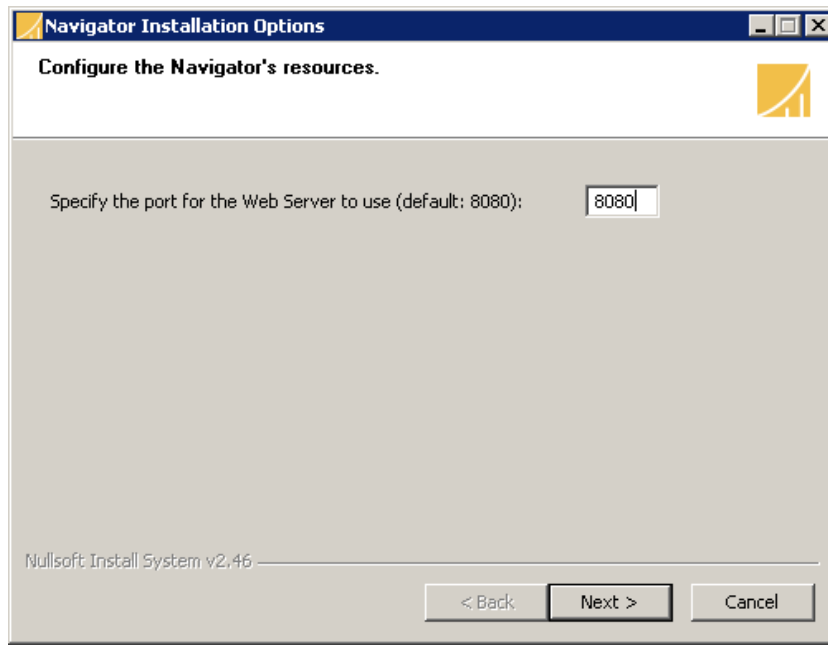
After installing the prerequisites and configuring SQL Server for access, the Navigator application installer (**Install_Navigator_2.1.22.exe**) should be run. For machines with an older version installed, you may need to uninstall the old version, install the new version, and then copy the configuration data from the older version to the new version (but see section **2.5 Upgrading Navigator** for more information). **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; **it is highly recommended** that you 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.

Activate Navigator License

Main Help

Network Activation **Manual Activation**

Product: NAVIGATOR

Product Version: 2.1.9

Platform: Windows_NT_5_x64_VisualStudio10.x

* Product Serial Number: Ex: 1111-2222-3333-4444 Lookup

* Activation Request Code: FB93-A4C9-3934-7237

* MAC Address:

* Site:

* Host:

* Number of CPUs: 1 Number of Physical CPUs, not Logical

* End User name:

* End User e-mail:

* Maintenance Contact Name:

* Maintenance Contact E-mail:

* Maintenance Contact Phone:

Status: License is already activated

Messages:

* - Field is required

Reactivate Exit with success

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; note that the user who is connecting should have [dbcreator](#) privileges.
 - Database username: [sa](#)
 - Database password: [N@vigator1](#)
 - Database name: [Navigator1](#)
 - Database host: [localhost](#)
 - Database port: [9003](#)

The **Encrypt Connection** checkbox can be used to enable encryption on the connection to SQL Server (this is only useful if the SQL Server instance is not on the local machine). (Note: some manual configuration steps may be required if you wish to use encrypted connections with SQLExpress – contact Laurel Bridge Software for assistance in this case.) 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 2012 → 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 2012 Express x64 above](#).
2. Run the Navigator installer, specifying the Web Server Port and the Installation directory, like this:

```
Install_Navigator_2.1.22.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

Note: Prior to upgrading Navigator, make sure that the license tied to the copy of Navigator being upgraded is covered under a valid maintenance contract that is not expired; licenses that don't have a valid maintenance contract cannot be upgraded. Contact Laurel Bridge for help if you are not sure if your maintenance contract is up to date.

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.

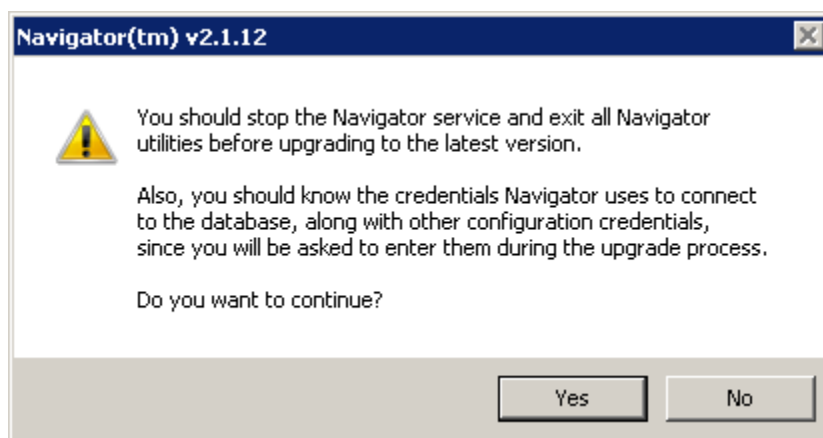
Also, you should know your database access credentials – username and password – before upgrading, since you will have to enter them during the upgrade process.

Note that if you have any custom code classes used by Navigator, you should back those up *before* you upgrade your Navigator. These are typically found in the directory `C:\LB Navigator\tomcat\webapps\Navigator\WEB-INF\classes\com` or a subdirectory of that directory. Once the upgrade is complete, it is up to you to *carefully* copy such custom classes back into the appropriate directory to continue using them.

To upgrade your Navigator:

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. (If you are using LDAPS, see [Appendix J:Java Keystore](#) for additional information about changes you may need to make once the installation has finished.) Click [Execute](#), and then click the Exit button once the utility has succeeded.

Navigator Credentials Utility

Database

Configure Navigator's database resources:

Authentication:

Database username:

Database password:

Confirm password:

Database name:

☐ Create the database if needed?
(If unchecked, the database MUST already exist.)

Missing password

Database host: Port: ☐ Encrypt Connection

These values let Navigator access MS SQL Server and its database.

LDAP / Active Directory

LDAP Username:

LDAP password:

Confirm password:

SMTP E-mail

SMTP Username:

SMTP password:

Confirm password: Missing password

Execute

Status:

Exit with error

8. If you had configured the older version of Navigator to use HTTPS for network security, most of those settings are migrated by the installer. However, if you manually configured Navigator to use [HTTP Strict Transport Security](#) (HSTS), you will need to reconfigure it manually again.
9. Reboot your computer.
10. If you had backed up any custom code classes, you should restore them now – carefully copy *only* the custom classes back into the original directories where they came from. The installer may make a backup directory with the contents of the directory, but your custom class files may be mingled in there with Navigator-specific files – you want to restore *only* your custom files, since the other files will not have the latest changes to Navigator. You may need to restart the Navigator service after the files have been restored in order for Navigator to use them.
11. Navigator is now 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. Navigator itself can be configured to use any AE title.

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.

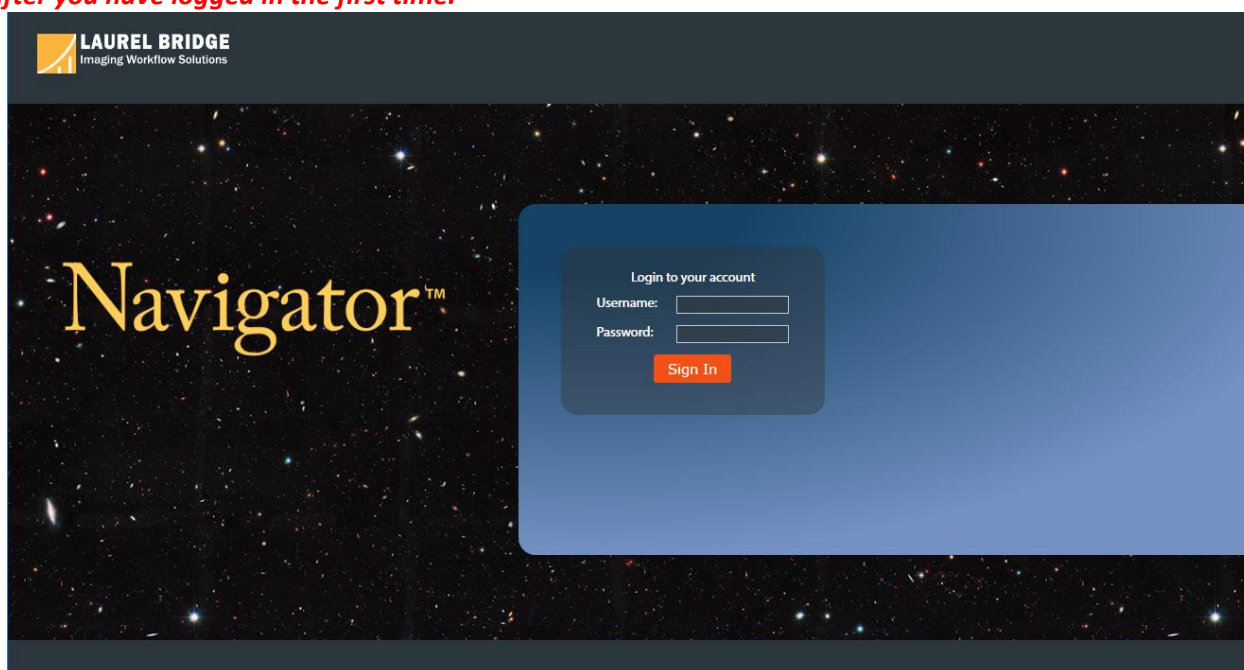
Configuration Worksheet: Navigator Priors Fetching Workflow - Laurel Bridge Software

						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.***



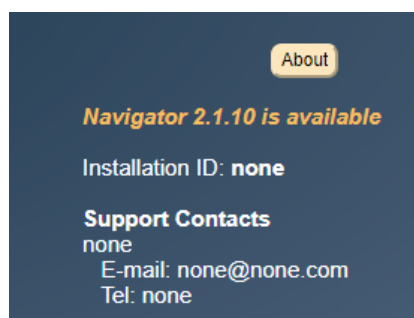
4.1 Navigator’s Main Screen

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](#)). The home screen also shows information about your license, including the anniversary date, how many moves per worklist item you are allowed, the count of items processed, and the number of items that your license allows.

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.

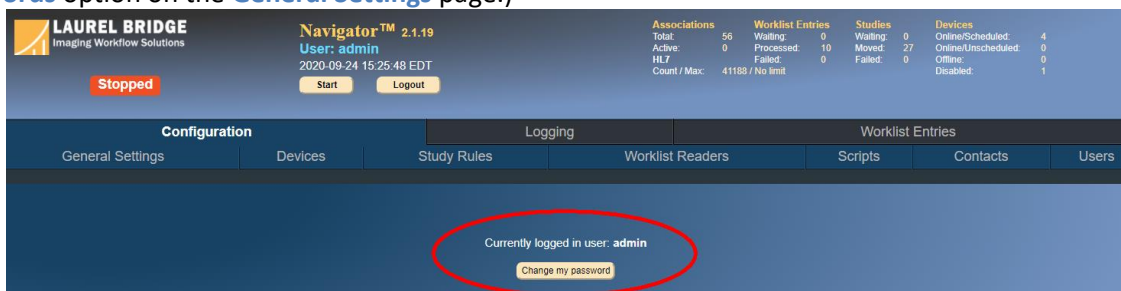


The main screen will also let you check for updates by clicking the **Check for Updates** button. If Navigator has already detected that a new release is available, the latest version will be displayed in place of the button, as shown below:



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, as shown in the red circle in the image below. (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 **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.

Setting	Value	Required
Automatically Start Worklist Processing	<input type="checkbox"/>	No
Device Polling (secs)	60	Yes
Worklist Query Polling (secs)	60	Yes
Number of Processing Threads	6	Yes
Scheduled Window Start (days)	0	Yes
Scheduled Window End (days)	1	Yes
Number of Times to Retry Jobs	0	Yes
Time Between Job Retries (secs)	60	Yes
Link Study-Move-Request Jobs	<input checked="" type="checkbox"/>	No
Worklist Purge Rate (secs)	30	Yes

- **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. (**Note** that Navigator has no DICOM listening ports and functions strictly in a DICOM initiator/SCU role. This means that it will not *respond* to DICOM C-Echo requests.)
- **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 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.
- **Worklist Purge Rate** – How frequently *completed* Worklist Item jobs are considered for deletion. Note that the deletion of completed jobs is affected by the retention time specified for each of the **Worklist Readers**. Only Completed jobs are considered for deletion; Failed jobs or Completed-Partial jobs must be manually deleted.

Query SCU Settings:		
Query Timeout (secs) ?	*	300
PDU Read Timeout (secs)	*	300
PDU Write Timeout (secs)	*	300
Send DIMSE Timeout (secs) ?	*	300
Receive DIMSE Timeout (secs)	*	300
Progress Timeout (secs) ?	*	300
Max Number of Results to Return ?	*	5000

Auto-logout Time (seconds):		
For Administrators	*	300
For Users	*	180
For View-Only users	*	180
Require secure passwords ?		<input type="checkbox"/>
Allow Simultaneous Logins ?		<input checked="" type="checkbox"/>

- **Query Timeout** – How long a query / move operation should be allowed to run before it is considered to have failed. Note that this may need to be increased if you expect large studies to be moved and think they will take a long time to move.
- **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. Note that this value may need to be increased if jobs are timing out, especially if the counters for sub-operations do not change until the job is actually done.
- **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.

LDAP / Active Directory

LDAP Enabled ☒ **Changes to the LDAP configuration may require you to restart the Navigator service.**

Use LDAP only ☐

LDAP Server Address

Base DN (optional)

Base DN for Groups (optional)

Username (optional)

Password (optional)

Confirm password

Admin Role CN(s)

User Role CN(s)

View Role CN(s)

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.) *Note that you should make sure that Navigator works with your LDAP settings before enabling this option.*
- **LDAP Server Address** – The URL of the LDAP server to use; note the value should be formatted as “`ldap://<server-name>:<port>`”. (See [Appendix J: Java Keystore](#) for Java keystore settings that may need to change if you are using LDAPS.)
- **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 Navigator uses to connect to the LDAP server – this is usually not the same as a username for logging in to Navigator. For some systems you may need to enter the full Distinguished Name for the Username in order to connect to the LDAP (or LDAPS) server; for example, `CN=john.doe,CN=Users,DC=bogustech,DC=com`. (You may find it useful to run the command “`whoami /fqdn`” from a Windows command prompt as you determine the username to use – this will show you the **Fully Qualified Distinguished Name** for the current user, as an example of what the format for the username may be.) 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

<https://grails-plugins.github.io/grails-spring-security-ldap/v2/guide/configuration.html>

The screenshot shows a configuration window with the following settings:

- Log Directory**: C:/USERS/patrick/DCF-3.3.63a/tmp/log
- Max number of log files**: 5
- Max size per log file (KB)**: 3000
- Parse log files for errors?**: ☐
- Don't parse files bigger than this (KB)**: 10000
- Delete per-job log files automatically**: ☐
- Enable DICOM Audit Log**: ☐
- Host**: [Empty text field]
- Port**: 514
- Protocol**: UDP (dropdown menu)
- Suppress PHI from logs**: ☐

- **Log Directory** – the directory where Navigator’s log files are stored. Note that since log files may grow quickly and become very large depending on the settings you choose, it may be advantageous to set the log directory to use a different disk volume; doing this will cause the logs to write to a different disk than the one that Navigator is installed on. For example, if you have Navigator installed on your C-drive, you may want the log files to be written to your D-drive.
- **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. **Note** that the default value for this changed from “unchecked” (False) to “checked” (True) in v2.1.15; it is **highly** recommended that this box be checked so that the log files are deleted when the corresponding job is removed, which will help to keep your hard disk from filling up.
- **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.
- **Suppress PHI from logs** – Check this if you do not want PHI to be written to Navigator’s log files at the same time that it is being sent to the SysLog server.

Enable E-mail Notifications

SMTP Server

SMTP Port

From

Use TLS or SSL

Auth Mode

Username

Password

Confirm password

Test recipient:

Send notification if the count exceeds a threshold

E-mail address of threshold recipient

Threshold %

Frequency of notifications Minutes

- **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
- **From** – The sender’s e-mail address
- **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; leave these blank if no authentication is required. 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.
- **Send notification if the count exceeds a threshold** – Navigator can be configured to send someone an e-mail when the count of items processed exceeds some threshold of the number of items allowed by your license.
- **E-mail address of threshold recipient** – who should get the notification
- **Threshold** – When the count of items processed reaches this percent of the total number of items allowed by the license, an e-mail will be sent.
- **Frequency of notifications** – how often (in minutes) the notification should be sent.

Enable Periodic Error Report ?	<input type="checkbox"/>
E-mail address of recipient ?	<input type="text"/>
Frequency (minutes) ?	<input type="text" value="120"/>
Report Contents:	
Job Summary	<input type="checkbox"/>
Summary for Device Pairs	<input type="checkbox"/>
Problem Job List ?	<input type="checkbox"/>

Enable Daily Report ?	<input type="checkbox"/>
E-mail address of recipient ?	<input type="text"/>
Time of day to generate report ?	<input type="text" value="1130"/>
Report Span Hours ?	<input type="text" value="24"/>
Report Contents:	
Job Summary	<input type="checkbox"/>
Summary for Device Pairs	<input type="checkbox"/>
Problem Job List ?	<input type="checkbox"/>
Success Job List ?	<input type="checkbox"/>

The system may need to be restarted to apply any changes you have made.

- **Enable Periodic Error Report** – Periodically generate and e-mail a report of all Worklist Item Jobs in the Navigator database with the status of **FAILED** or **COMPLETED_PARTIAL**. If no jobs have those states, then no e-mail message will be sent. Note that notifications are only sent if **E-mail Notifications** are enabled and the **SMTP Server** is configured correctly.
- **E-mail address of recipient** – Who should be sent the report. You can specify multiple e-mail addresses by separating them with commas.
- **Frequency** – The approximate number of minutes between e-mail notifications
- **Report Contents** – The data that should be in the report
 - **Job Summary** – Overall count of Worklist Item Jobs in each state
 - **Summary for Device Pairs** – Counts of completed and failed Study Move Request Jobs for each combination of source and destination devices. This can provide information about a particular device or network route that is having problems.
 - **Problem Job List** – List of all Worklist Item Jobs with status **FAILED** or **COMPLETED_PARTIAL**. **Note** that this will include confidential patient information.
- **Enable Daily Report** – Generate and e-mail a report at a specified time every day. The format of the report is similar to the **Periodic Report** above except that **COMPLETED** jobs may optionally be included and that the jobs listed are limited to those that have been modified within a specified time span.
- **E-mail address of recipient** – Who should be sent the report. You can specify multiple e-mail addresses by separating them with commas.

- **Time of day to generate report** – When the report should be generated each day; must be specified in 24-hour format (i.e., 0000-2359).
- **Report Span Hours** – How many hours to look back for jobs to report. Note that the purge time for **COMPLETED** orders may affect what is shown in reports.
- **Report Contents** – The data that should be in the report
 - **Job Summary** – Overall count of Worklist Item Jobs in each state
 - **Summary for Device Pairs** – Counts of completed and failed Study Move Request Jobs for each combination of source and destination devices. This can provide information about a particular device or network route that is having problems.
 - **Problem Job List** – List of all Worklist Item Jobs with status **FAILED** or **COMPLETED_PARTIAL**. **Note** that this will include confidential patient information.
 - **Success Job List** – List of all Worklist Item Jobs with status **COMPLETED**. **Note** that this will include confidential patient information.

When you change one of these settings, Navigator must be restarted to effect the changes.

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 reorder the devices and the order that they are displayed by clicking the up or down arrows at the left. This can be useful if you have many devices and want to have all the Sources grouped together, for example. Once you are done reordering the devices, press the **Save order** button to save your changes, or press **Cancel** to discard the changes.

Note that Navigator has no DICOM listening ports and functions strictly in a DICOM initiator/SCU role. This means that it will not respond to DICOM C-Echo requests.

You can create a new device by clicking **New DICOM Device** near the top. To view or edit an existing device, click on the description.

LAUREL BRIDGE Imaging Workflow Solutions

Navigator™ 2.1.13
User: admin
2019-10-03 16:36:35 EDT

Associations
Total: 47
Active: 0
HL7 Count / Max: 1142 / 15000

Worklist Entries
Waiting: 0
Processed: 10
Failed: 0

Studies
Waiting: 0
Moved: 25
Failed: 0

Devices
Online/Scheduled: 4
Online/Unscheduled: 0
Offline: 0
Disabled: 0

Configuration
General Settings | **Devices** | Study Rules | Worklist Readers | Scripts | Contacts | Users

DICOM Device List

+ New DICOM Device

Total number of DICOM Devices: 4
Device Polling (secs): 60

	Sources	Destinations	Triggers
Current:	2	1	1
Licensed:	6	5	3

Save order Cancel Disable All Enable All DICOM Ping All

ID	Description	Status	Last Echo	Role	Called AE Title	Called Address	Default Called Port	Calling AE Title	Calling Address	Storage Group Name
2	PACS Source_1	Online / Sched	2019-10-03 16:35:43 EDT	S -	DICOM_SCP_1	localhost	2002	LBS_Navigator_01	127.0.0.1	ALPHA
1	primary worklist server	Online / Sched	2019-10-03 16:35:43 EDT	- - T	MWLSCTP1	localhost	2001	LBS_Navigator_01	127.0.0.1	ALPHA
3	PACS Source_2	Online / Sched	2019-10-03 16:35:43 EDT	S -	DICOM_SCP_2	localhost	2003	LBS_Navigator_01	127.0.0.1	ALPHA
4	Reading Station_1	Online / Sched	2019-10-03 16:35:43 EDT	- D -	READING_STN_1	localhost	2025	LBS_Navigator_01	127.0.0.1	ALPHA

Total number of DICOM Devices: 4

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.

Edit DICOM Device Save Delete Copy Cancel

* - Item is required

ID: 2

Description: * PACS Source 1

Enabled: ☒ Last Echo: 2018-11-13 13:41:58 EST

Role: Source ☒ Destination ☐ Trigger ☐

Max Threads per Role: ? * 64

Send notifications: ? ☐ E-mail address:

Calling AE Title: ? * LBS_Navigator_01

Calling Address:

Called AE Title: ? * DICOM_SCP_1

Called Address: * localhost **DICOM Ping**

Default Called Port: * 2002 **Show Advanced Options**

Session Settings Config File:

☒ Device is always scheduled ?
☐ Use schedule

- **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”, and only enabled devices can be queried for priors or have priors moved to them.
- **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 to 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 Address** – The AE Title and hostname / IP address for Navigator
- **Called AE Title** and **Called Address** – The AE Title and hostname / IP Address of the device to contact
- **Default Called Port** – The port of the device to contact
 You can press the **DICOM Ping** button to test the connection to the device; any debugging data from the C-Echo-Request can be viewed in the Navigator log files on the **Logging** tab.
- **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.

☐ Device is always scheduled ?
☒ Use schedule

	12am	4am	8am	12pm	4pm	8pm
Sun	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Mon	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Tue	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Wed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Thu	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Fri	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sat	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Legend: ☒ Available ☐ Unavailable

Click the boxes above to adjust the schedule.

Presets: All

The schedules can be used for slightly different effects depending on the type of device:

- **Triggers** – For a Worklist device, the schedule determines when it can be queried for new Jobs to process. At times when the device is marked Unavailable, no Worklist Queries will be sent to it.
- **Sources** – The schedule determines when the Device can be queried for possible priors for an existing Worklist Entry Job, and Jobs referencing that Device will not be processed until the Device is available. For example, if you want Navigator to only move priors at night, you could configure all your devices to have a schedule that says they are available only at night; Jobs could come in at any time and be queued up, but the Jobs would not query for priors or move them until nighttime.
- **Destinations** – The schedule determines when priors can be moved to the Device. Similar to Sources, if the Schedule says that priors should be moved only at night, Jobs could come in at any time, but no priors would be moved until nighttime.

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

2025 Hide Advanced Options

Advanced Options

These port values are used if the device uses different ports for these operations. Set to "-1" to use the default port.

Called C-Echo Port: *	<input type="text" value="-1"/>	Called C-Find Port: *	<input type="text" value="-1"/>
Called C-Move Port: *	<input type="text" value="-1"/>	Called C-Store Port: *	<input type="text" value="-1"/>

Query for Series Information: ? ☐
 Request Relational Query Mode: ? ☐
 Storage Group Name: ?
 Q/R Find Data Model: ?
 Q/R Move Data Model: ?

Wait for Forwarding Confirmation: ? ☐
 Confirmation Timeout (secs): ?

- **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. This is related to **Step 4** in **Study Rules** in case you need to filter out priors by Modalities-in-Study.
- **Request Relational Query Mode** – Controls whether the Navigator Query/Retrieve client or SCU code will request the SOP class specific option to enable relational queries. Some PACS or archive devices make use of this information to determine what parameters are required for a C-Find or C-Move request.
- **Storage Group Name** – Set the same Storage Group Name 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 Name, studies on the Source don't need to be moved to the Destination since they are already there, which can speed up the processing. See **Note on Storage Groups** for more information.
- **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
- **Wait for Forwarding Confirmation** and **Confirmation Timeout** – Destination devices can be configured so that a Study sent to this device is not marked as Completed until the destination sends back a confirmation message (via the web call to **Navigator/worklistItem/updateStudyMoveRequestForwardingStatus** – contact Laurel Bridge Software for assistance using this option). This is used in case the Destination device is actually forwarding the Study to another device and you want to know when the Study has reached its ultimate destination. The **Confirmation Timeout** indicates how many seconds to wait for the confirmation message to arrive from the time the Job actually starts to run; if the confirmation is not received in that time, the Job will be marked as Failed.

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 worklist item triggers received from the **Worklist Readers** (DICOM C-Find responses from MWL servers, incoming HL7 messages or other triggers received via the RESTful web API) are processed to find matching Study Rules. The Study Rules associated with the particular Worklist Reader that received the trigger are tested in the order that they are listed in the Worklist Reader configuration. A new WorklistItemJob object (and WorklistItem DB record) are created for each Study Rule that a worklist item trigger from a Worklist Reader matched.



In earlier versions of Navigator, only one Study Rule was ever matched when processing a worklist item trigger. Each Study Rule now has an attribute "Stop on Match" that can be set using a checkbox on the editor window. When processing worklist item triggers from a particular Worklist Reader, searching for a rule will stop if a matching Study Rule has the "Stop on Match" option set.

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.

Study Rule List 				
 New Study Rule				
Rule Name	Source Devices and Search Order	Device Status	Destination Devices for Move	Device Status
Mammo rule 	PACS Source 1 PACS Source 2	Online / Sched Online / Sched	Reading Station 1	Online / Sched
Non-mammo rule	PACS Source 1	Online / Sched	Reading Station 1	Online / Sched
Single DICOM Move Rule 	PACS Source 1 PACS Source 2	Online / Sched Online / Sched	Reading Station 1	Online / Sched
Rule Name	Source Devices and Search Order	Device Status	Destination Devices for Move	Device Status

Note that Navigator must be restarted before any changes to the rules will take effect.

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 for this Study Rule to be selected. Also note that any whitespace entered as part of a match condition value is significant (i.e., the string is not trimmed). Add additional matching conditions by filling in the bottom row of the table and pressing the green “plus” button ; remove matching conditions by pressing the red “minus” button  at the end of the row. 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). If you want to choose a Study Rule because a value contains *either* one string *or* another string, you may be able to use a regular expression to do that – see [Appendix E:Regular Expressions](#) for more detail.

This section is where you set the **Priority** – Low, Medium, or High – for the handling of WorklistItemJobs that are created for worklist item triggers that matched this Study Rule. Note that both the WorklistItemJob (which during typical pre-fetch workflows performs DICOM C-Find operations) and any subsequently created StudyMoveRequestJob objects (which perform DICOM C-Move operations) will be scheduled at this priority. The priorities assigned to the Jobs are up to you – for example, you could have one Study Rule for emergency jobs and give them high priority, while another Study Rule could exist for routine jobs and give them low priority. Low priority jobs will not run until nothing with a higher priority needs to run. Note that you cannot change priorities for Jobs after they are created.

The **Stop on Match** checkbox specifies whether additional Study Rules will be considered if this Study Rule meets the matching conditions. Note that if **Stop on Match** is not checked then a single worklist item trigger may result in more than one WorklistItemJob objects.

Edit Study Rule (6 Steps) Save Delete Copy Cancel

* - Item is required

Step 1

Rule Name * Mammo rule

Worklist Query Match Conditions

Tag	Operator	Value
SPSS Modality	Equals	MG
Accession Number	Equals	

Custom Match Script Name

Priority * High

Step on Match ☒

DICOM Dictionary Help

Select

Step 2 – Define the query for priors.

Step 2

Elements to Query from Sources

Tag	Value Type	Value
Accession Number	Return Only	
Modality	Return Only	
Patient Birth Date	Return Only	
Patient Name	Worklist Item Tag	Patient Name
Patient ID	Return Only	
Patient Sex	Return Only	
Study Description	Return Only	
Accession Number	Worklist Item Tag	Accession Number

Custom Query Script Name

DICOM Dictionary Help

Select

You can modify the query that is sent to the Sources to search for priors by selecting the tags you want in the **Tag** column and setting the **Value Type** and **Value** for each tag that is in the query. To add elements to the query, set the desired fields at the bottom of the table and press the green “plus” button . To remove elements from the query, press the red “minus” button at the end of the row you want to remove.

- Set the **Value Type** to **Return Only** if you want to match on anything and get that tag’s value back for processing in a later step.
- Set the **Value Type** to **Constant** if you want to match a specific value, which is then specified in the **Value** column.
- Set the **Value Type** to **Worklist Item Tag** if you want to query for priors which have the same value as an element in the Worklist Item, and then select the appropriate tag from the drop-down in the **Value** column. (Note that many systems are limited in what searching can be done by the elements in a query – typical limitations are to match by Accession Number, Patient ID, Patient Name, and Study Date.)
- You can also select from a limited set of **special functions** to do “fuzzy name matching” with the Patient’s Name (as shown below).

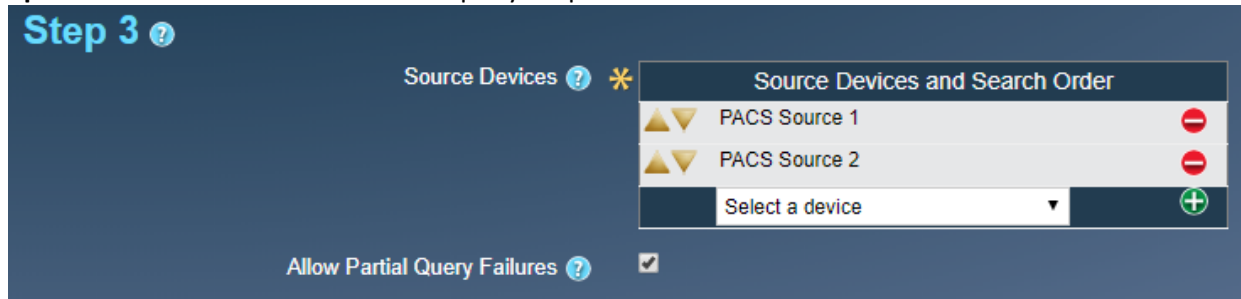
Tag	Value Type	Value
Accession Number	Special Function	PATIENTS_NAME_FUZZY_MATCH_LAST_FIRST_3



For example, to find priors for only women, you would select **Patient Sex** in the **Tag** column, set the **Value Type** to **Constant**, and then set the **Value** to **“F”**. To find priors with the same Patient Name as the Worklist Item, select **Patient Name** in the **Tag** column, set the **Value Type** to **Worklist Item Tag**, and select **Patient**

Name from the drop-down in the **Value** column. If you were to set the **Value Type** to **Constant** and entered “0010,0010” (the DICOM tag for Patient Name) in **Value**, you would find only those priors where the Patient Name is *literally* “0010,0010” – this is probably not what you want!

You can also specify a Custom Script to do complex operations on the query that will be sent. Note: if the Source needs to be configured to query for information to construct the **Modalities-in-Study** value, that is configured on the **Devices** page.

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. (See [Appendix I: Checking if a Study already exists on the Destination](#) for how to configure Navigator if it should check if an item exists on a Destination before trying to move it.)

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

Step 4

Source Response Processing

Priors Study Tag	Operator	Value Type	Value	
Patient Birth Date	Equals	Worklist Item Tag	Patient Birth Date	
Patient Sex	Equals	Worklist Item Tag	Patient Sex	
Accession Number	Equals	Worklist Item Tag	Accession Number	

DICOM Dictionary Help

Custom Response Processing Script Name Select

Remove duplicate Study Instance UIDs: ☒

Remove duplicate accession numbers: ☐

Filter by body part: ☐

Body Part Configuration filename: Select

Oldest Prior Study *

Don't move studies newer than this date

Max Number of Priors to Fetch *

Number of oldest priors to fetch

Custom Result List Processing Script Names Select

User Action Required: ☐

Send notification for User Action: ☐ E-mail address:

- 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.
Note: If you are comparing a tag against a string value via “Regex Match”, you may need to be explicit in your specification of the regular expression – see [Appendix E:Regular Expressions](#) for details.
- 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**”). (Note that these values can be affected by how many moves per worklist item your license allows.)
- 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.) See **Appendix H: User Chooses the Priors** for more details on how a user can choose the desired priors.

Step 5 – Choose the **destinations** for the priors. These are the devices where you want the priors to be sent. (See **Appendix I: Checking if a Study already exists on the Destination** for how to configure Navigator if it should check if an item exists on a Destination before trying to move it.)

Step 5 ?

Destination Devices * Destination Devices for Move

Reading Station 1	⊖
Select a device ▼	⊕

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.

Step 6 ?

Worklist Item Job start script ?		Select
Worklist Item Job stop script ?		Select
Study Move Request Job start script ?		Select
Study Move Request Job stop script ?		Select

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 it queries, and then choose which Study Rules are used by this Reader. **Note** that the order of the Study Rules is important, since typically only 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. Note that beginning with Navigator version 2.1.15, multiple Study Rules may be matched for a given worklist item trigger; this is possible if you un-check the “[Stop on Match](#)” option for a Study Rule. You should also set the number of days and hours that Completed jobs are held before deletion – Completed jobs may be deleted once they are not on the Worklist. (Failed jobs or Partially Completed jobs must be manually deleted.) You can also specify a custom script if you need to modify the MWL query.

* - Item is required

ID: 1

Description: * Check Primary Worklist

Worklist Server Device: * Worklist Server Device
primary worklist server

Custom Processing Script Name: ?

Time to Keep Completed Jobs: ? * Days: 2 Hours: 0

Study Rules

- Mammo rule
- Non-mammo rule
- Single_DICOM_Move_Rule

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. (Failed jobs or Partially Completed jobs must be manually deleted.) 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.) See section [8 HL7 Utilities](#) for how to configure the HL7 port that is being used.

* - Item is required

ID: 2

Description: * Receive Web Requests

Worklist Server Device: ? * HL7 Web Service

Enabled: ☒

Send notification: ? ☐ E-mail address:

Custom Processing Script Name: ?

Time to Keep Completed Jobs: ? * Days: 2 Hours: 0

Study Rules










- Single_DICOM_Move_Rule
- Mammo rule
- Non-mammo rule

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.

NOTE: The setting for **Time to Keep Completed Jobs** applies **only** to jobs that have *successfully completed*. Jobs are considered for deletion only according to the **Worklist Purge Rate** setting under **General Settings**. Once a job is off the Worklist and that amount of time has passed, the job will be automatically deleted; jobs received via the HL7 web interface may be automatically deleted after that time has passed. However, failed jobs or jobs that are partially completed must be deleted *manually*. Also, Completed jobs that are no longer associated with a Worklist Reader – “orphans”, if you will – may be deleted *before* the specified retention time on the Worklist Reader that they *originally* came from; a job can become an “orphan” if its Worklist Reader is deleted from the Navigator configuration; deletion of orphaned jobs is recorded in the **Audit Log**.

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.

Custom Script List 	
 New Custom Script	
Type: HL7 / MWL Processing 	
create study instance uid if missing.groovy	
sample hl7 copy accession number to study iuid.groovy	
sample hl7 copy patientid into studyInstanceUid.groovy	
sample hl7 split study date and time.groovy	
Type: Study Rule Match Conditions 	
sample study rule select script1.groovy	
Type: Study Rule Query Processing 	
sample priors query processing script1.groovy	
Type: Study Rule Response Processing 	
response filter test1.groovy	
sample result filter script1.groovy	
Type: Study Rule Result List Processing 	
body part equivalents 1.cfg	
fetch all but outside film.groovy	
new body part.cfg	
result list filter test1.groovy	
result list filter with per destination logic.groovy	
select studies based on relevance quality.groovy	
skip studies with similar accession numbers.groovy	
skip studies with specific terms in description.groovy	
test multi level body parts.cfg	
Type: Worklist Item Job Processing 	
example run exe.groovy	
test wij start.groovy	
test wij stop.groovy	
wij1.groovy	
worklist item job2.txt	
Type: Study Move Request Job Processing 	
study move request job.txt	
study move request job.txt.groovy	
study move request job2.txt	
test smrj start.groovy	
test smrj stop.groovy	

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

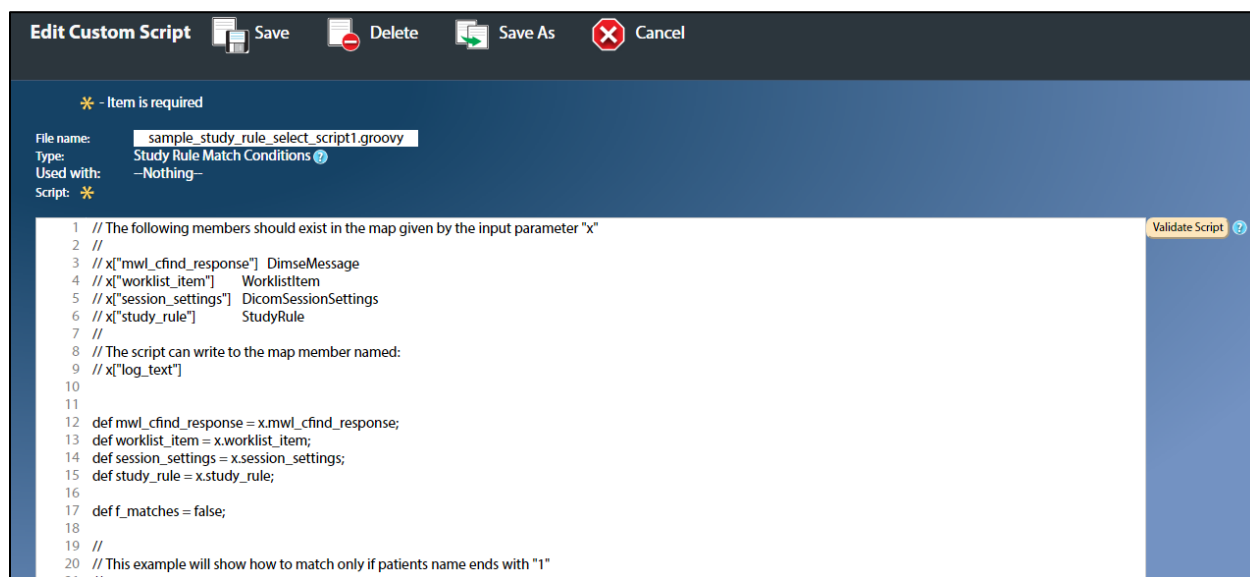
- **HL7 / MWL Processing** – These convert HL7 and web parameters into MWL-style data; these scripts are used by the HL7 Web Worklist Reader. They can also be used by MWL Worklist Readers if you need to modify the MWL query, such as adding parameters.
- **Study Rule Match Conditions** – These are for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

Edit Contact Information  Save

This contact information is displayed on Navigator's front page to inform users whom to contact regarding issues.

Installation ID:

Primary Contact:

E-mail:

Tel:

Secondary Contact:

E-mail:

Tel:

Login Warning Text:

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:


LAUREL BRIDGE
 Imaging Workflow Solutions

Navigator™ 2.1.11
 User: admin
 2019-02-04 14:39:36 EST

Associations	Worklist Entries	Studies	Devices
Total: 0	Waiting: 0	Waiting: 0	Online/Scheduled: 0
Active: 0	Processed: 0	Moved: 0	Online/Unscheduled: 0
HL7: 0	Failed: 0	Failed: 0	Offline: 4
Count / Max: 0 / 15000			Disabled: 0

Running
Stop
Logout

Configuration
 Logging
 Worklist Entries

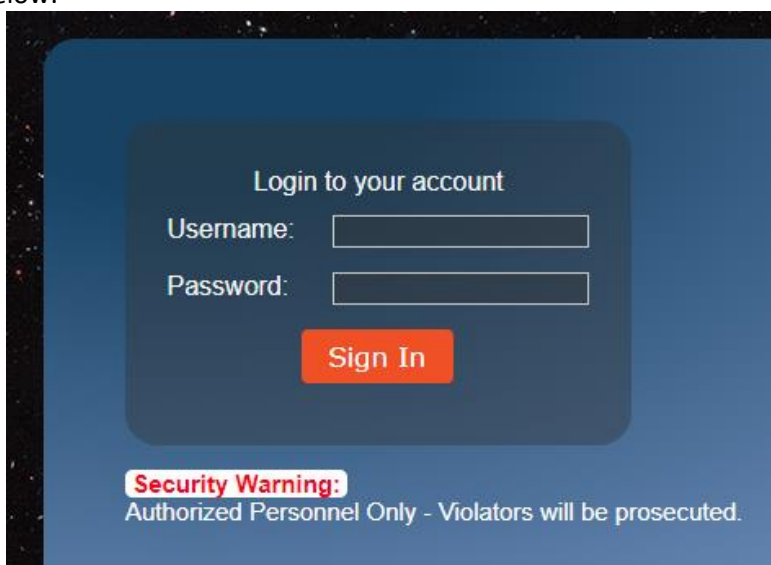
Navigator™

About
Check for Updates

Installation ID: none
Support Contacts
 none
 E-mail: none@none.com
 Tel: none
 none
 E-mail: none@none.com
 Tel: none
 Licensee: BCSI
 Product Serial Num: ABCD-ABCD-1234-5678
 License Anniversary Date: 20190704
 Max Moves per Worklist Item: 10
 Count / Max: 0 / 15000
 Expires: February 4, 2020
 Test - Expires in 365 Days
Check license

Copyright © Laurel Bridge Software, Inc. All Rights Reserved.

The **Login Warning Text** field is text that is displayed on the login screen to warn users of any legal ramifications of accessing Navigator; this text is optional. If this field is configured, the warning would appear like shown below:



Note: You should set the Contact 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.** See section **7.8 Reset Administrator Password** if you need to reset the password if you forgot it.

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.

LAUREL BRIDGE
Imaging Workflow Solutions

Navigator™ 2.1.11
User: admin
2019-02-04 15:22:50 EST

Associations
Total: 33
Active: 0
Count / Max: 10 / 15000

Worklist Entries
Waiting: 0
Processed: 10
Failed: 0

Studies
Waiting: 0
Moved: 0
Failed: 0

Devices
Online/Scheduled: 4
Online/Unscheduled: 0
Offline: 0
Disabled: 0

Configuration | **Logging** | **Worklist Entries**

General Settings | Devices | Study Rules | Worklist Readers | Scripts | Contacts | **Users**

Search Users | Create Users

Security Management Console

Show Search Form

Username	Enabled	Account Expired	Account Locked	Password Expired
admin	True	False	False	False
viewonly	True	False	False	False

Showing 1 through 2 out of 2.

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, use mixed case, and also have numbers or special characters – for example, “waterBottle1234” or “waterBottle!\$”.

Configuration | **Logging** | **Worklist Entries**

General Settings | Devices | Study Rules | Worklist Readers | Scripts | Contacts | **Users**

Search Users | Create Users

Security Management Console

Create User

User Details | **Roles**

Username:

Password:

Enabled: ☒

Account Expired: ☐

Account Locked: ☐

Password Expired: ☐

Save

Then click the [Roles](#) sub-tab and click the checkbox next to the role that the new user should have (see below) – **choose 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.

The screenshot shows the 'Create User' window within the 'Security Management Console'. The top navigation bar includes 'Configuration', 'Logging', and 'Worklist Entries'. Below this, a sub-navigation bar contains 'General Settings', 'Devices', 'Study Rules', 'Worklist Readers', 'Scripts', 'Contacts', and 'Users'. The main area is titled 'Create User' and features two tabs: 'User Details' (active) and 'Roles'. Under the 'Roles' tab, there is a list of roles with checkboxes: ☐ ROLE_ADMIN, ☐ ROLE_USER, and ☐ ROLE_VIEWONLY. A 'Save' button is located at the bottom left of the dialog.

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). (Note that the checkboxes for Account Expired, Account Locked, and Password Expired are for future enhancement and should not currently be used.)

The screenshot shows the 'Edit User' window. It has two tabs: 'User Details' (active) and 'Roles'. Under 'User Details', there are the following fields and options:

- Username:** A text field containing the value 'viewonly'.
- Password:** A text field with masked characters represented by dots.
- Enabled:** A checkbox that is checked.
- Account Expired:** An unchecked checkbox.
- Account Locked:** An unchecked checkbox.
- Password Expired:** An unchecked checkbox.

 At the bottom of the dialog are 'Save' and 'Delete' buttons.

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.

mw1_user001_tag, mw1_user001_label	smr_user001_tag, smr_user001_label
mw1_user002_tag, mw1_user002_label	smr_user002_tag, smr_user002_label
mw1_user003_tag, mw1_user003_label	smr_user003_tag, smr_user003_label
mw1_user004_tag, mw1_user004_label	smr_user004_tag, smr_user004_label
mw1_user005_tag, mw1_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.)

Configuration **Logging** Worklist Entries

Log Files Log Level Audit Log

Log Directory: C:\users\patrick\DCF-3.3.52c\tmp\log

Clear All Log Files Delete selected

Files are listed newest to oldest.

Filename	Size
<input type="checkbox"/> dcf_sysmgr.4408.log	0.00 KB
<input type="checkbox"/> DLOG_Server.001.0.log	0.00 KB
<input type="checkbox"/> DLOG_Server.001.out.log	0.00 KB
<input type="checkbox"/> DCDS_Server.001.0.log	0.00 KB
<input type="checkbox"/> DCDS_Server.001.out.log	0.00 KB
<input type="checkbox"/> NavigatorTestSCP-QR.003.0.log	0.00 KB
<input type="checkbox"/> NavigatorTestSCP-QR.003.out.log	0.10 KB
<input type="checkbox"/> ex_jstore_scp.002.0.log	0.00 KB
<input type="checkbox"/> ex_jstore_scp.002.out.log	0.09 KB
<input type="checkbox"/> ex_jstore_scp.003.0.log	0.00 KB
<input type="checkbox"/> ex_jstore_scp.003.out.log	0.09 KB
<input type="checkbox"/> ex_jstore_scp.004.0.log	0.00 KB
<input type="checkbox"/> ex_jstore_scp.004.out.log	0.09 KB
<input type="checkbox"/> ex_jstore_scp.005.0.log	0.00 KB
<input type="checkbox"/> ex_jstore_scp.005.out.log	0.09 KB
<input type="checkbox"/> error.0.log	0.00 KB
<input type="checkbox"/> system.38.log	56.95 KB
<input type="checkbox"/> Navigator.5448.0.log (process is active)	0.00 KB
<input type="checkbox"/> NavigatorTestSCP-QR.001.9.log	13.72 KB
<input type="checkbox"/> NavigatorTestSCP-QR.001.out.log	0.10 KB

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).

Logging

Log Level

Logging Level: Quiet ▼ Update logging level

- Quiet
- Warnings only
- Navigator tracing
- Navigator verbose tracing
- DICOM tracing
- DICOM tracing and Navigator tracing
- DICOM verbose tracing
- DICOM verbose tracing and Navigator verbose tracing

5.1 Audit Log

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 by a user 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) or if an orphaned job was deleted (see section **4.6 Worklist Readers** above for more about orphaned jobs). 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). Note that you can Filter or Search the Audit records but not both simultaneously. Click the **Clear** button to clear both the filter and search parameters and to revert to the default values for sorting and ordering.

Configuration		Logging	Worklist Entries
Log Files		Log Level	Audit Log

Audit Log List			
Download			
Time Of Change	Username	Category	Changes Made
2019-07-23 17:20:47 EDT	admin	Access	User 'admin' logged in from IP: 0.0.0.0:0.0.1
2019-07-23 17:15:34 EDT	none	Access	User 'admin' logged out
2019-07-23 17:15:34 EDT	admin	Access	Session for user 'admin' ended
2019-07-23 17:15:14 EDT	admin	Access	User 'admin' logged in from IP: 0.0.0.0:0.0.1
2019-07-23 17:15:10 EDT	none	Access	User 'admin' logged out
2019-07-23 17:15:10 EDT	admin	Access	Session for user 'admin' ended
2019-07-23 17:15:03 EDT	admin	Logs	Clear all logs called: Deletion C:\USERS\patrick\DCF-3.3.64c\mpl\log\system.24...
2019-07-23 17:14:18 EDT	admin	Access	User 'admin' logged in from IP: 0.0.0.0:0.0.1
2019-07-23 17:08:59 EDT	none	Access	User 'admin' logged out
2019-07-23 17:08:59 EDT	admin	Access	Session for user 'admin' ended
2019-07-23 17:08:57 EDT	admin	Start/Stop	Stopping worklist processing services
2019-07-23 17:08:57 EDT	admin	Start/Stop	Starting teardown of Navigator services
2019-07-23 17:05:29 EDT	admin	Access	User 'admin' logged in from IP: 0.0.0.0:0.0.1
2019-07-23 17:05:19 EDT	admin	Access	User 'admin' logged in from IP: 0.0.0.0:0.0.1
2019-07-23 17:04:26 EDT	none	Access	User 'admin' logged out
2019-07-23 17:04:26 EDT	admin	Access	Session for user 'admin' ended
2019-07-23 16:57:24 EDT	admin	Start/Stop	Starting worklist processing services
2019-07-23 16:57:23 EDT	admin	Start/Stop	Starting startup of Navigator services
2019-07-23 16:57:19 EDT	admin	Access	User 'admin' logged in from IP: 0.0.0.0:0.0.1
2019-07-23 16:56:12 EDT	none	Start/Stop	Starting startup of Navigator services
Time Of Change	Username	Category	Changes Made

Filter by Category: None
Search:
Clear

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

Show Audit Log

Username	jdoe
Category	Access
Time Of Change	2017-05-24 17:55:31 EDT
Changes Made	User 'jdoe' logged in

Previous

6 Worklist Entries

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

ID	Patient's Name	Accession Number	SPSS Start Date	Scheduled Station AE Title	Modality	Study Rule	Priority	Status	Status Info	Log File
1	Doe^Jan01	0_123401_0	2019-02-04 15:09:47	MAMMO_STN_2	MG	Mammo rule	High	Completed		
2	Doe^Jan06	0_123406_0	2019-02-04 15:09:47	MAMMO_STN_3	MG	Mammo rule	High	Completed		
3	Doe^Jan11	0_123411_0	2019-02-04 15:09:47	ALT_MAMMO_1	MG	Mammo rule	High	Completed		
4	Doe^Jan16	0_123416_0	2019-02-04 15:09:47	MAMMO_STN_1	MG	Mammo rule	High	Completed		
5	Doe^Jan21	0_123421_0	2019-02-04 15:09:47	MAMMO_STN_2	MG	Mammo rule	High	Completed		
6	Doe^Jan26	0_123426_0	2019-02-04 15:09:47	MAMMO_STN_3	MG	Mammo rule	High	Completed		
7	Doe^Jan31	0_123431_0	2019-02-04 15:09:47	ALT_MAMMO_1	MG	Mammo rule	High	Completed		
8	Doe^Jan36	0_123436_0	2019-02-04 15:09:47	MAMMO_STN_1	MG	Mammo rule	High	Finding Priors		
9	Doe^Jan41	0_123441_0	2019-02-04 15:09:47	MAMMO_STN_2	MG	Mammo rule	High	Finding Priors		
10	Doe^Jan46	0_123446_0	2019-02-04 15:09:47	MAMMO_STN_3	MG	Mammo rule	High	Finding Priors		

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.

Worklist Entry List

Select allUnselect allReschedule Selected Worklist Entries?

Query MWL Server nowManually Add Job

100 Worklist Entries TotalDownload

ID	Patient's Name	Accession Number	SPSS Start Date	Scheduled Station	AE Title	Modality	Stu
<input type="checkbox"/> 101	Doe^Jan01	0_123401	2017-06-09 10:53:54	MAMMO STN 2		MG	Ma

An Admin-level user can click the checkboxes next to completed or failed entries and delete them by clicking the [Delete](#) button (shown below); note that non-Admin users cannot delete entries and are not shown the Delete button at all. 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 child Study Move Requests, 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 *active* Worklist Entries; only Entries that are finished can be deleted without stopping Navigator. In its normal processing routine, Navigator will automatically remove Worklist Items that have successfully completed and are no longer on the Worklist – when they are removed is affected by [Time to Keep Completed Jobs](#) under [Worklist Readers](#) and by [Worklist Purge Rate](#) under [General Settings](#). Failed jobs or jobs that were only partially successful must be deleted *manually*; you may wish to examine them to see why they failed and then retry them after fixing what didn’t work, or you can just delete them.

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.

Worklist Entry List

Select allUnselect allDelete Worklist Entries

100 Worklist Entries TotalDownload

ID	Patient's Name	Accession Number	S
<input type="checkbox"/> 101	Doe^Jan01	0_123401	2
<input type="checkbox"/> 102	Doe^Jan06	0_123406	2
<input type="checkbox"/> 103	Doe^Jan11	0_123411	2

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

Show Worklist Entry

ID 1
 Accession Number 0_123401_0
 Patient's Name Doe*Jan01
 Patient ID 123401
 Patient's Birth Date 1979-06-05
 Patient's Sex F
 SPSS Start Date 2020-01-22
 SPSS Start Time 14:36:15
 Scheduled Station AE Title MAMMO_STN_2
 Modality MG
 Requested Procedure BREAST SCREENING 4 VIEWS

Status Completed [Reschedule Worklist Item](#)
 Status Info Completed study move requests: 5
 Log File

Retry Count 0
 Date Added 2020-01-22 14:36:15 EST
 Date Modified 2020-01-22 14:36:21 EST
 Study Instance UID 2.1.0
 Study Date 20200122
 Study Time 143615

Worklist Reader 1 - Check Primary Worklist
 Study Rule 1 - Mammo rule
 Priority High

WLI User Tag 1
 WLI User Tag 2
 WLI User Tag 3
 WLI User Tag 4
 WLI User Tag 5
 WLI User Text 001 Tag
 WLI User Text 002 Tag

Study Move Requests Number of Studies: 5

ID	Study Instance UID	Accession #	Source	Destination	Priority	Status	Sub-Ops	Modality	Study Description
16	3.1.1	P_1234010	PACS Source 2 (DICOM_SCP_2)	Reading Station 1 (READING_STN_1)	High	Completed	0 / 4 / 0 / 0	MG	4 VIEW BREAST SCREENING
17	6.1.1	P_1234010	PACS Source 1 (DICOM_SCP_1)	Reading Station 1 (READING_STN_1)	High	Completed	0 / 3 / 0 / 0	CR	KNEE-RIGHT (QUAD KNEE/LG JOINT)
18	6.1.2	P_1234011	PACS Source 1 (DICOM_SCP_1)	Reading Station 1 (READING_STN_1)	High	Completed	0 / 3 / 0 / 0	CR	KNEE-RIGHT (QUAD KNEE/LG JOINT)

There may also be a table showing how the priors were filtered and which priors were rejected and why, along with which ones were accepted. They are shown in descending chronological order to make it easier to understand complex filtering setups. For instance, in the example below, several priors were rejected (highlighted in **pink**) because they didn't match the body part filtering, while others were accepted and moved (highlighted in **green**).

ID	Study Instance UID	Accession #	Source	Destination	Priority	Status	Sub-Ops	Modality	Study Description
Prior Studies Filtered									
Study Instance UID	Accession #	Name	Source	Study Description	Study Date	Move?	Reason		
6.6.1	P_1234060	Doe*Jan06	DICOM_SCP_1	KNEE-RIGHT (QUAD KNEE/LG JOINT)	20190605	No	BodyPartResultListFilter: no body part match		
3.6.1	P_1234060	Doe*Jan06	DICOM_SCP_1	4 VIEW BREAST SCREENING	20190605	Yes			
3.6.2	P_1234061	Doe*Jan06	DICOM_SCP_2	4 VIEW BREAST SCREENING	20180605	Yes			
6.6.2	P_1234061	Doe*Jan06	DICOM_SCP_1	KNEE-RIGHT (QUAD KNEE/LG JOINT)	20180605	No	BodyPartResultListFilter: no body part match		
6.6.3	P_1234062	Doe*Jan06	DICOM_SCP_1	KNEE-RIGHT (QUAD KNEE/LG JOINT)	20170605	No	BodyPartResultListFilter: no body part match		
3.6.3	P_1234062	Doe*Jan06	DICOM_SCP_1	4 VIEW BREAST SCREENING	20170605	Yes			
3.6.4	P_1234063	Doe*Jan06	DICOM_SCP_2	4 VIEW BREAST SCREENING	20160605	Yes			
6.6.4	P_1234063	Doe*Jan06	DICOM_SCP_1	KNEE-RIGHT (QUAD KNEE/LG JOINT)	20160605	No	BodyPartResultListFilter: no body part match		
6.6.5	P_1234064	Doe*Jan06	DICOM_SCP_1	KNEE-RIGHT (QUAD KNEE/LG JOINT)	20150605	No	BodyPartResultListFilter: no body part match		
3.6.5	P_1234064	Doe*Jan06	DICOM_SCP_1	4 VIEW BREAST SCREENING	20150605	Yes			
Study Instance UID	Accession #	Name	Source	Study Description	Study Date	Move?	Reason		

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. (For more detail on this process, see **Appendix H:User Chooses the Priors.**)

Accept All		Reject All		Study Move Requests		Number of Studies: 5		Approve Selected Priors			
Accept	Reject	ID	Study Instance UID	Accession #	Source	Destination	Priority	Status	Sub-Ops	Modality	Study Description
<input type="radio"/>	<input type="radio"/>	76	3.1.1	P_1234010	PACS Source 2 (DICOM_SCP_2)	Reading Station 1 (READING_STN_1)	High	Init	0 / 0 / 0 / 0	MG	4 VIEW BREAST SCREENING
<input type="radio"/>	<input type="radio"/>	77	6.1.1	P_1234010	PACS Source 1 (DICOM_SCP_1)	Reading Station 1 (READING_STN_1)	High	Init	0 / 0 / 0 / 0	CR	KNEE-RIGHT (QUAD KNEE/LG JOINT)
<input type="radio"/>	<input type="radio"/>	78	6.1.2	P_1234011	PACS Source 1 (DICOM_SCP_1)	Reading Station 1 (READING_STN_1)	High	Init	0 / 0 / 0 / 0	CR	KNEE-RIGHT (QUAD KNEE/LG JOINT)
<input type="radio"/>	<input type="radio"/>	79	3.1.2	P_1234011	PACS Source 1 (DICOM_SCP_1)	Reading Station 1 (READING_STN_1)	High	Init	0 / 0 / 0 / 0	MG	4 VIEW BREAST SCREENING
<input type="radio"/>	<input type="radio"/>	80	3.1.3	P_1234012	PACS Source 2 (DICOM_SCP_2)	Reading Station 1 (READING_STN_1)	High	Init	0 / 0 / 0 / 0	MG	4 VIEW BREAST SCREENING
Accept	Reject	ID	Study Instance UID	Accession #	Source	Destination	Priority	Status	Sub-Ops	Modality	Study Description

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 have 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.

[Return to Worklist Entry for Accession Number 0_123406_0](#)

Show Study Move Request for Accession Number 0_123406_0

Worklist Item ID	Accession Number 0_123406_0
Study Instance UID	60
Name of Device Where Found	6.6.3
Name of Device to Send to	PACS Source 1 (DICOM_SCP_1)
Retry Count	Reading Station 1 (READING_STN_1)
Date Added	0
Date Modified	2020-01-22 14:49:11 EST
Priority	2020-01-22 14:49:13 EST
Status	High
Status Info	Completed
Sub-Ops ?	id=60,DICOM C-Move successful
	0 / 3 / 0 / 0
Modality	CR
Study Description	KNEE-RIGHT (QUAD KNEE/LG JOINT)
Accession #	P_1234062
SMR User Tag 4	
SMR User Tag 5	

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. Nor can you retry only certain Study Move Requests – you can reschedule a parent Worklist Item Job, and that will force all its children Study Move Requests to be retried.)

LAUREL BRIDGE
Imaging Workflow Solutions

Navigator™ 2.1.15
User: admin
2020-01-22 14:49:11 EST

Running [Stop] [Logout]

Associations
Total: 121
Active: 5
HL7: 0
Count / Max: 4083 / 15000

Worklist Entries
Waiting: 6
Processed: 4
Failed: 0

Studies
Waiting: 5
Moved: 0
Failed: 0

Devices
Online/Scheduled: 4
Online/Unscheduled: 0
Offline: 0
Disabled: 1

Configuration **Logging** **Worklist Entries**

Worklist Jobs **Study Move Requests**

Study Move Request List
5 Study Move Requests Total

Show Display Options
Show: All

ID	Study Instance UID	Accession #	Source	Destination	Modality	Study Description	Priority	Status	Sub-Ops	Date Added
55	3.21.3	P_1234212	PACS Source 2 (DICOM_SCP_2)	Reading Station 1 (READING_STN_1)	MG	4 VIEW BREAST SCREENING	High	Completed	0 / 4 / 0 / 0	2020-01-22 14:49:10 EST
54	3.21.2	P_1234211	PACS Source 1 (DICOM_SCP_1)	Reading Station 1 (READING_STN_1)	MG	4 VIEW BREAST SCREENING	High	Running	0 / 0 / 0 / 0	2020-01-22 14:49:10 EST
53	3.21.2	P_1234211	PACS Source 1 (DICOM_SCP_1)	Reading Station 1 (READING_STN_1)	CR	KNEE-RIGHT (QUAD KNEE/LG JOINT)	High	Running	0 / 0 / 0 / 0	2020-01-22 14:49:10 EST
52	3.21.4	P_1234210	PACS Source 1 (DICOM_SCP_1)	Reading Station 1 (READING_STN_1)	CR	KNEE-RIGHT (QUAD KNEE/LG JOINT)	High	Running	0 / 0 / 0 / 0	2020-01-22 14:49:10 EST

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.
Wait for Fwd	The job is completed but is waiting for confirmation from the Destination device that the job was successfully forwarded to its ultimate destination. See Advanced Options under 4.4 Devices for more information.
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.

Manual Worklist Job Entry ?

Accession Number:	<input type="text"/>	Study Date: ?	<input type="text"/>
Study Instance UID:	<input type="text"/>	Study Time: ?	<input type="text"/>
Patient's Name:	<input type="text"/>	Requested Procedure:	<input type="text"/>
Patient ID:	<input type="text"/>	User defined field 1:	<input type="text"/>
Patient's Birth Date: ?	<input type="text"/>	User defined field 2:	<input type="text"/>
Patient's Sex:	<input type="text"/>	User defined field 3:	<input type="text"/>
Modality:	<input type="text"/>	User defined field 4:	<input type="text"/>
Scheduled Station AE Title:	<input type="text"/>	User defined field 5:	<input type="text"/>

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.

NOTE: This utility may have issues connecting to SQL Server if you have Navigator configured to use [Windows Authentication](#), since the Navigator service runs as a different user than the utility; this utility works best if Navigator is configured to use [SQL Server Authentication](#).

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 (but see the warning above). The **Encrypt Connection** checkbox can be used to enable encryption on the connection to SQL Server (this is only useful if the SQL Server instance is not on the local machine). (Note: some manual configuration steps may be required if you wish to use encrypted connections with SQLExpress – contact Laurel Bridge Software for assistance in this case.) 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.

Navigator Credentials Utility

Database

Configure Navigator's database resources:

Authentication:

Database username:

Database password:

Confirm password:

Database name:

☐ Create the database if needed?
(If unchecked, the database MUST already exist.)

Missing password

Database host: Port: ☐ Encrypt Connection

These values let Navigator access MS SQL Server and its database.

LDAP / Active Directory

LDAP Username:

LDAP password:

Confirm password:

SMTP E-mail

SMTP Username:

SMTP password:

Confirm password: **Missing password**

Status:

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

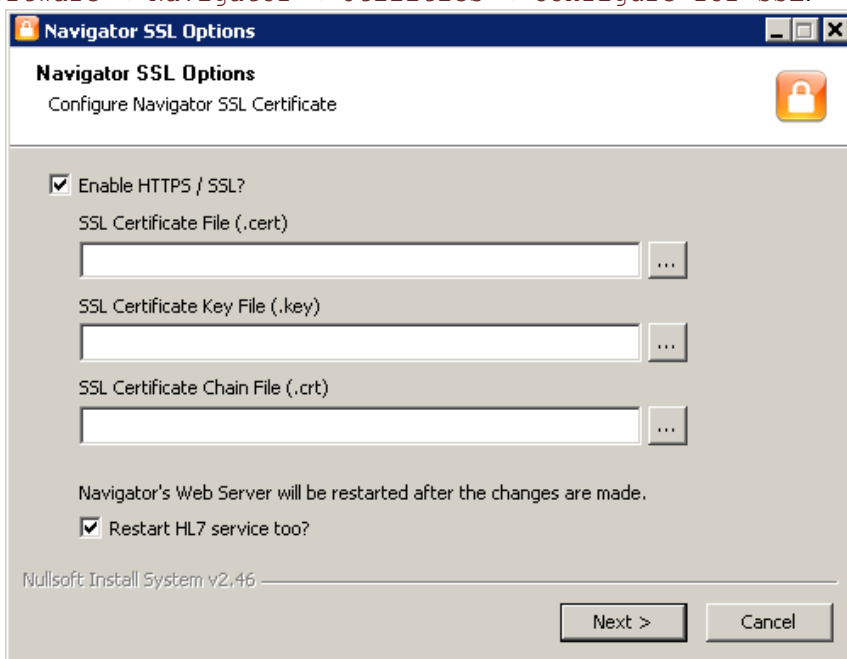
Control and configuration of Navigator is done through a web server via a web browser. Since it is possible for some users to view data on the priors being requested by Navigator, you may wish to require a secure connection to Navigator to view the data and the configuration. This can be done by changing 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. To minimize downtime while the configuration utility is running, you should login to Navigator and stop its processing of priors. The utility will restart Navigator once it is done, but Navigator can take a long time to stop and restart if it is processing priors at the time, so you can avoid this delay by stopping it beforehand.
2. 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 (<filename>.cert). (If you have PFX format instead of PEM format, Navigator has a script that might be able to help – see [Appendix G: TLS Certificates:3 Convert PFX to PEM](#). These pages have information on the files needed: <https://tomcat.apache.org/tomcat-7.0-doc/apr.html> or <https://tomcat.apache.org/tomcat-9.0-doc/ssl-howto.html>. You can obtain a sample self-signed certificate for testing at <https://www.selfsignedcertificate.com>. See [Appendix G: TLS Certificates](#) for more information on the files required.)
3. From the Windows Start menu, launch the SSL Configuration Utility – go to `Start → Laurel Bridge Software → Navigator → Utilities → Configure for SSL`.



4. Click the box if you want to enable HTTPS / SSL, and then follow the steps below. If you want to disable HTTPS / SSL – reverting to HTTP – uncheck the box and go to [Step 8 below](#).

5. Select the **SSL Certificate File** and enter its path in the first field. The file usually has a **.cert** or **.crt** file extension. You can browse your local file system by pressing the “...” button next to the field.
6. 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.
7. 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.
8. 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.
9. Once all the fields are filled in correctly, click the “**Next**” button. If you are enabling SSL, the certificate files will be copied to Navigator’s installation directory; no files will be copied if you are disabling SSL. In either case, 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 appropriate site. You should login to Navigator and restart the processing of priors by clicking the **Start** button.

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.

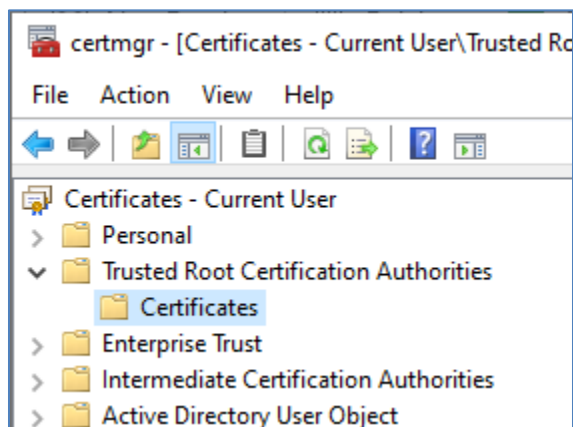
7.2.2 Manual SSL configuration

1. To minimize downtime you should login to Navigator and stop its processing of priors. Navigator can take a long time to stop and restart if it is processing priors at the time, so you can avoid this delay by stopping it beforehand.
2. 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 (**<filename>.cert**). (If you have PFX format instead of PEM format, Navigator has a script that might be able to help – see **Appendix G: TLS Certificates:3 Convert PFX to PEM**. These pages have information on the files needed: <https://tomcat.apache.org/tomcat-9.0-doc/apr.html> or <https://tomcat.apache.org/tomcat-9.0-doc/ssl-howto.html>. You can obtain a sample self-signed certificate for testing at <https://www.selfsignedcertificate.com>. See **Appendix G: TLS Certificates** for more information on the files required.)
3. Go to Navigator’s installation directory (default: C:\LB Navigator) and into the **tomcat/conf** subdirectory.
4. 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.
5. Edit the **web.xml** file.

- f. 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.
 - g. Save your changes to the web.xml file.
6. 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. Login to Navigator and restart the processing of priors by clicking the **Start** button.

7.2.3 Note on the HL7 Service

If you are using Navigator’s HL7 Service, when you change Navigator’s web configuration to use HTTPS (or to revert to HTTP), you will have to modify the HL7 Service’s configuration so that it uses the correct protocol (see [8.1 Configure HL7 Service](#) below). You may have to add the **PFX version** of your certificate to the Windows Certificate Store – it probably should go under **Trusted Root Certification Authorities / Certificates**, as shown below:



You will then have to restart the HL7 Service.

7.2.4 HTTP Strict Transport Security

As was mentioned above, Laurel Bridge Software recommends accessing the Navigator interface with the HTTPS protocol enabled for optimal security. Once you have enabled HTTPS, users who try to access the unsecured HTTP interface will automatically be redirected to the HTTPS address. You can add additional security by enabling **HTTP Strict Transport Security (HSTS)** and configuring the value for maximum age to be a reasonably large value.

HSTS works by notifying client web browsers that attempt to connect via HTTP that this website only supports HTTPS. It does this by sending a redirect response to the web browser which includes a special “Strict Transport Security” response header. The web browser then stores the redirect information in a special cache. The HSTS response header also includes a maximum age for the cache entry, after which time the entry is deleted from the cache. HSTS thus provides some protection against man-in-the-middle (MITM) attacks, where a malicious attacker is able to access the network, intercept traffic bound for the actual website, and trick the user into connecting to a dummy lookalike website via HTTP instead of HTTPS.

To enable HSTS, you should edit the **web.xml** file in the **tomcat/conf** subdirectory under the installation directory using Notepad, VIM, or some other text editor. Find the filter named **“httpHeaderSecurity”**. Add these parameters to the filter if they don’t already exist:

```

<init-param>
  <param-name>hstsEnabled</param-name>
  <param-value>true</param-value>
</init-param>
<init-param>
  <param-name>hstsMaxAgeSeconds</param-name>
  <param-value>60</param-value>
</init-param>

```

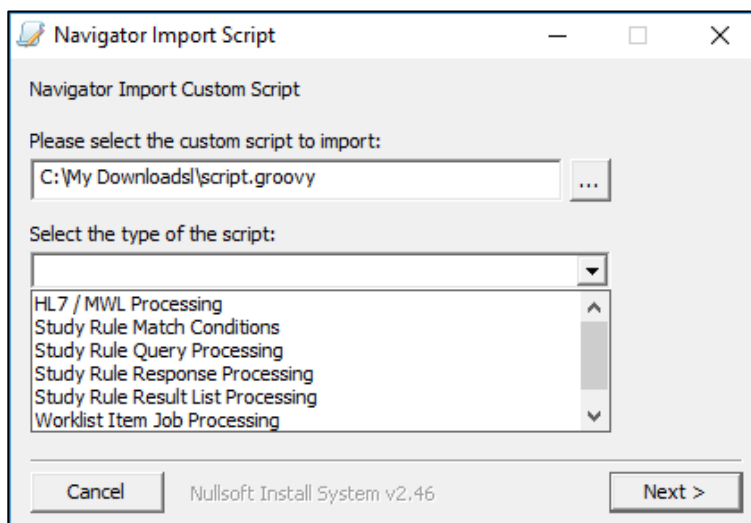
Save your changes to the file and then restart the Navigator service.

Note that the maximum age for the HSTS cache is set to 60 seconds in the sample shown above. This is to allow testing of the behavior with minimal cache impact prior to full implementation. Once testing is complete, the `web.xml` file should be edited to change `"hstsMaxAgeSeconds"` to a recommended value of at least two months (`"<param-value>5184000</param-value>"`, in seconds) up to one year (31536000, in seconds).

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**.

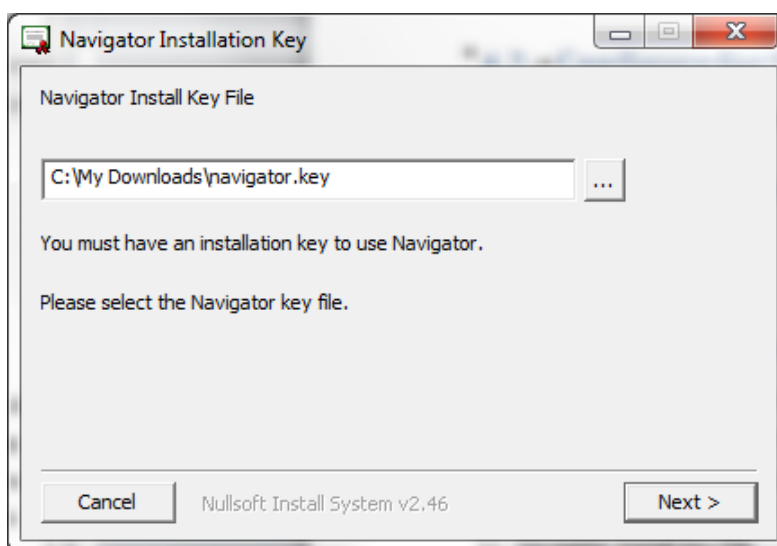


7.4 Install New License

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:

Activate Navigator License

Main Help

Network Activation Manual Activation

Product: NAVIGATOR

Product Version: 2.1.9

Platform: Windows_NT_5_x64_VisualStudio10.x

* Product Serial Number: Ex: 1111-2222-3333-4444 Lookup

* Activation Request Code: FB93-A4C9-3934-7237

MAC Address:

* Site:

* Host:

* Number of CPUs: 1 Number of Physical CPUs, not Logical

* End User name:

* End User e-mail:

* Maintenance Contact Name: ?

* Maintenance Contact E-mail:

* Maintenance Contact Phone:

Status: License is already activated

Messages:

* - Field is required

Reactivate

Exit with success

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:

Status: Success: AC=AD79-773D-B594-B376-E70D-99F9-9909-C429

Messages:

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.

Activate Navigator License

Main Help

Network Activation Manual Activation

Product: NAVIGATOR

Product Version: 2.1.9

Number of CPUs: 1 Number of Physical CPUs, not Logical

Platform: Windows_NT_5_x64_VisualStudio10.x

Activation Request Code: FB93-A4C9-3934-7237

Go to www.laurelbridge.com, click Support, and then click 'Manually Activate a Product License'.

Fill out the form completely using the values displayed above. Use the Product Serial Number that you were previously provided. Click Submit to activate your license.

Download your license file and copy it to this machine. Click 'Browse and install' below to install the new license.

Browse and install

Status: License is already activated

Messages:

Exit with success

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:



Manual Product Activation

This page should only be used when manual activation has been selected during product installation.

Please enter your license activation information below:

Product Serial Number:	<input type="text" value="XXXX-XXXX-XXXX-XXXX"/>	(use serial number you were provided)	<input type="button" value="I don't know my Product SN"/>
Product:	<input type="text"/>		
Version:	<input type="text"/>		
Activation Request Code (ARC):	<input type="text"/>	(displayed during installation)	
MAC Address (optional):	<input type="text"/>	Ex: 11.22.33.44.55.66	
Site:	<input type="text"/>		
Host:	<input type="text"/>		
Number of CPUs:	<input type="text"/>		
End User name:	<input type="text"/>		
End User e-mail:	<input type="text"/>		
Maintenance Contact name:	<input type="text"/>		
Maintenance Contact e-mail:	<input type="text"/>		
Maintenance Contact phone:	<input type="text"/>		
<input type="button" value="Submit"/> <input type="button" value="Start over"/>			

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

License information	
Product Serial Number:	F3AA-B529-3951-7006
Activation Request Code:	CF38-DB8F-DB10-7237
MAC Address:	
Expiration:	20160726
Site:	HQ
Host:	vtcmw7
Num CPUs:	2
End User:	John Doe
E-mail:	support@laurelbridge.com
Maintenance Contact:	
Name:	My Support Guy
E-mail:	support@laurelbridge.com
Phone:	111
<input type="button" value="Download your license"/> , then copy it to the target machine and install it.	

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:

Activate Navigator License

Main Help

Network Activation Manual Activation

Product: NAVIGATOR

Product Version: 2.1.9

Number of CPUs: 2 Number of Physical CPUs, not Logical

Platform: Windows_NT_5_x64_VisualStudio10.x

Activation Request Code: CF38-DB8F-DB10-7237

Go to www.laurelbridge.com, click Support, and then click 'Manually Activate a Product License'.

Fill out the form completely using the values displayed above. Use the Product Serial Number that you were previously provided. Click Submit to activate your license.

Download your license file and copy it to this machine. Click 'Browse and install' below to install the new license.

Browse and install

Status: Success!

Messages:

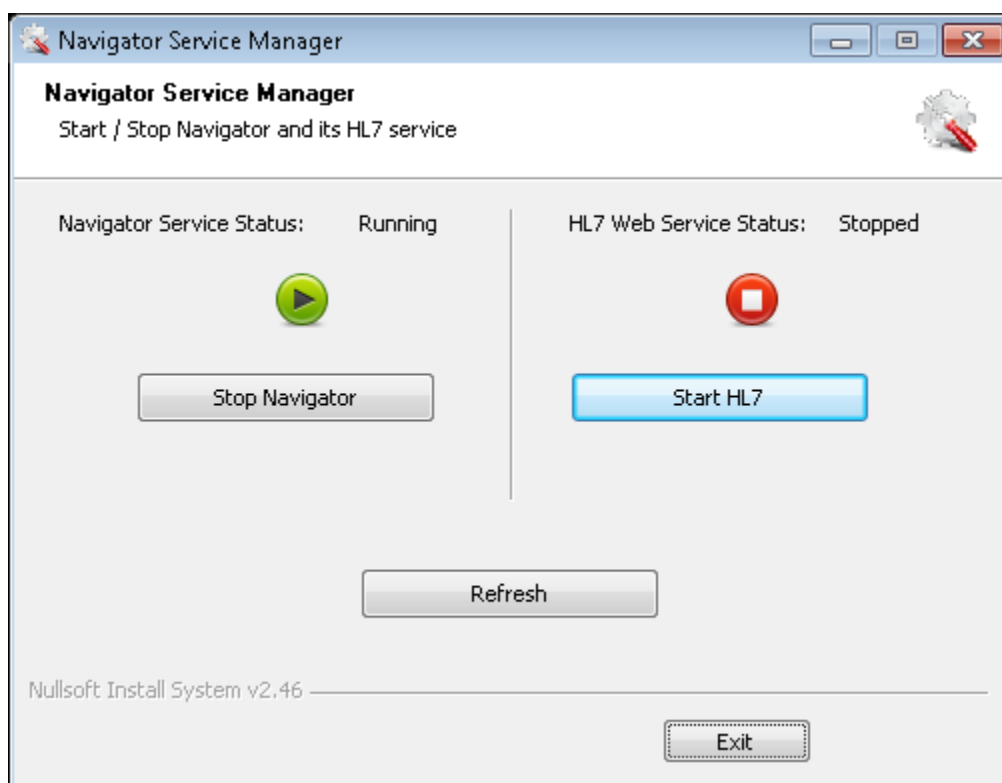
Exit with success

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.

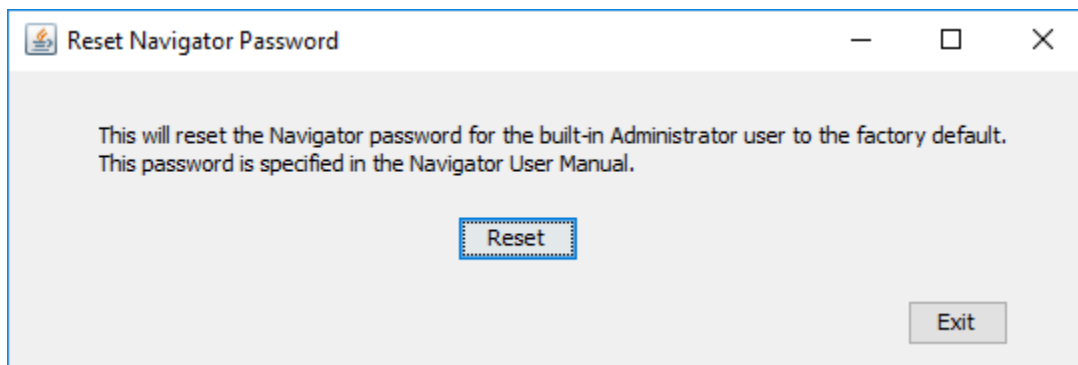
7.7 Change Web Ports

See [Appendix F: Changing Navigator's web port](#) for how to use this utility to change the web ports that Navigator uses.

7.8 Reset Administrator Password

If you changed the Administrator password and forgot it, you can use this utility to reset the password to the default – the password is mentioned in section [4.9 Users](#). This password should be immediately changed to a non-default, secure value (at least 8 characters in length and have both *UPPER* and *lower* case characters) after successfully logging in.

The utility is run from the Start menu: `Start → Laurel Bridge Software → Navigator → Utilities → Reset Navigator Password`



NOTE: This utility may not work if you have Navigator configured to use **Windows Authentication**, since the Navigator service runs as a different user than the utility; this utility works best if Navigator is configured to use **SQL Server Authentication**. There is an alternate method to reset the password described below.

7.8.1 Alternate method to reset the administrator's password

If the Reset utility does not work for you, you can use these steps to reset the password. Note that these steps apply *only* to the **administrator** user – it cannot be used to reset the passwords for other users.

1. Start **SQL Server Management Studio** and login – you may want to use the same credentials you used when you configured SQL Server during the installation process.
2. Go to **Databases**, open the Navigator database, and then select **Tables**.
3. Right-click on **dbo.sec_user** and select **Edit Top 200 Rows**.
4. Find the **administrator** user and delete his password – clear the data in the **password** column corresponding to the **administrator** username, and then press the Enter key. Your display of the data in the **dbo.sec_user** table should look similar to that below.
5. Restart the Navigator service – the easiest way may be to use the **Navigator Service Manager**.

Navigator will recognize that administrator has no password and will reset it to the default value. The next time you login as administrator, this password should be immediately changed to a non-default, secure value (at least 8 characters in length and have both *UPPER* and *lower* case characters).

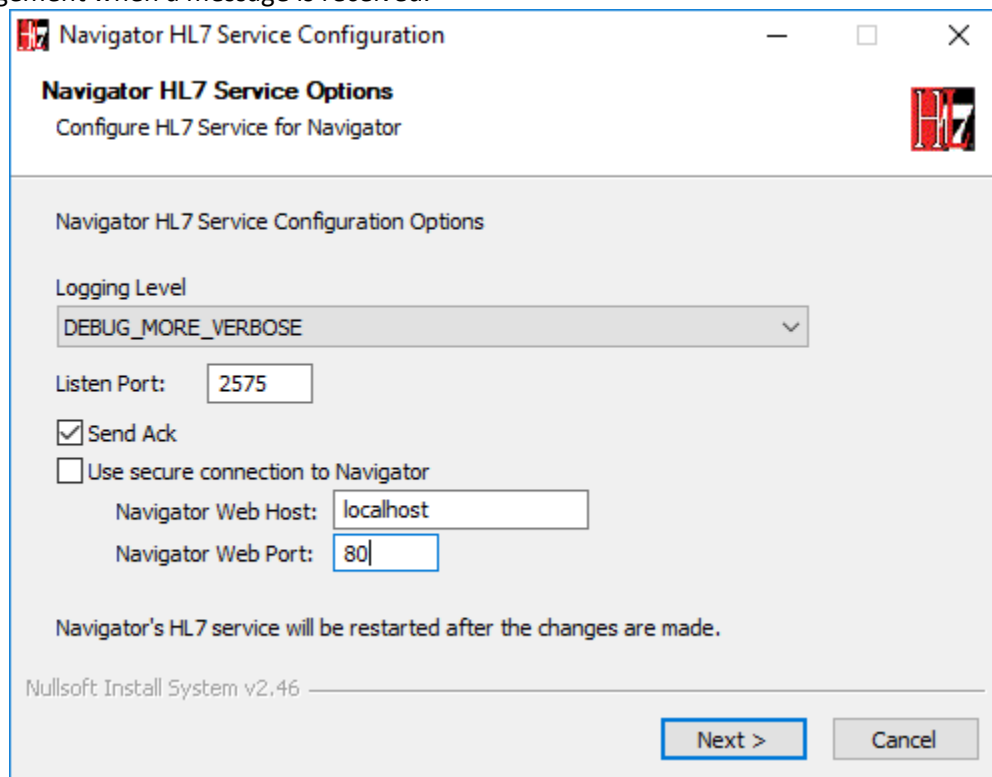
id	version	account_expired	account_locked	enabled	password	password_expiry	username
1	0	False	False	True	8c6976e5b5410...	False	admin
2	0	False	False	True	5e884898da280...	False	jdoe
3	0	False	False	True	847e7ca583b2a...	False	viewonly
4	0	False	False	True	5ef368722bf090...	False	testAdmin
5	16	False	False	True	NULL	False	administrator
..	NULL	NULL	NULL	NULL	NULL	NULL	NULL

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.

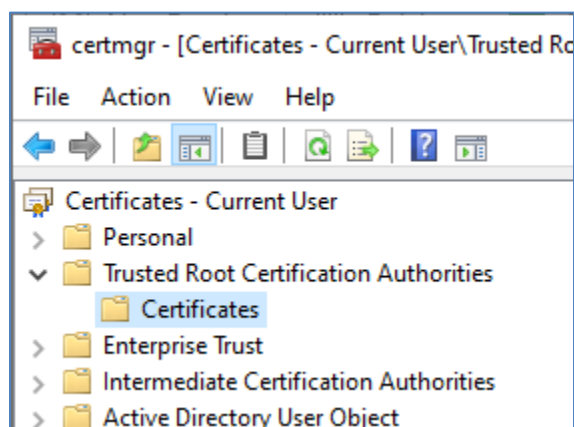


From the Start menu: Start → Laurel Bridge Software → Navigator → HL7 Configuration → Configure HL7 Service.

Note that if you have configured Navigator to require HTTPS for the web interface (see [7.2 Configure for TLS / SSL](#) above), you will have to select the box for “[Use secure connection to Navigator](#)” and then set the appropriate value for [Navigator Web Port](#) – the default HTTPS port is 8443.

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

You may have to add the **PFX version** of your certificate to the Windows Certificate Store – it probably should go under [Trusted Root Certification Authorities / Certificates](#), as shown below:



Note that Navigator’s HL7 Service currently does not support incoming TLS connections for HL7 messages – it only uses TLS for outgoing messages. If you need TLS for incoming HL7 messages, contact Laurel Bridge Software about using Compass with Navigator.

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

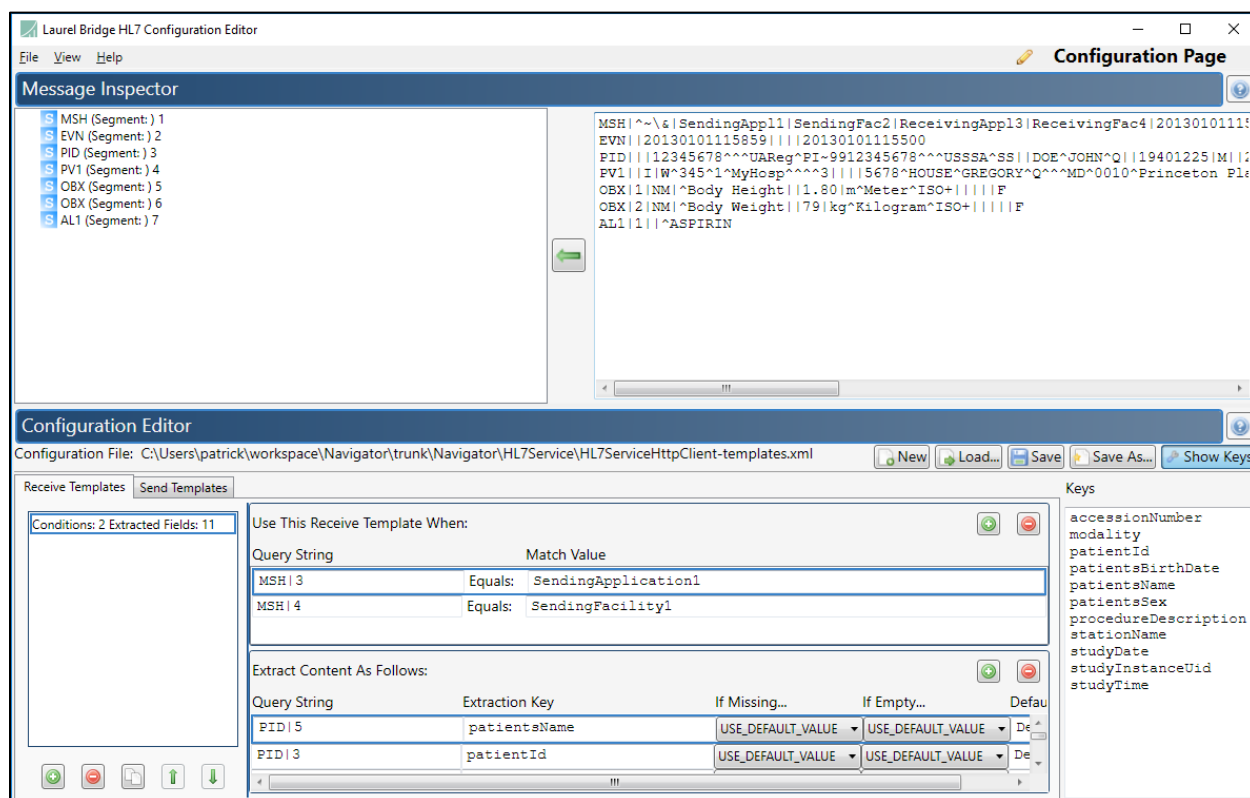
This utility lets you modify the template that parses the incoming HL7 messages and test that the message is parsed as you desire.

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:

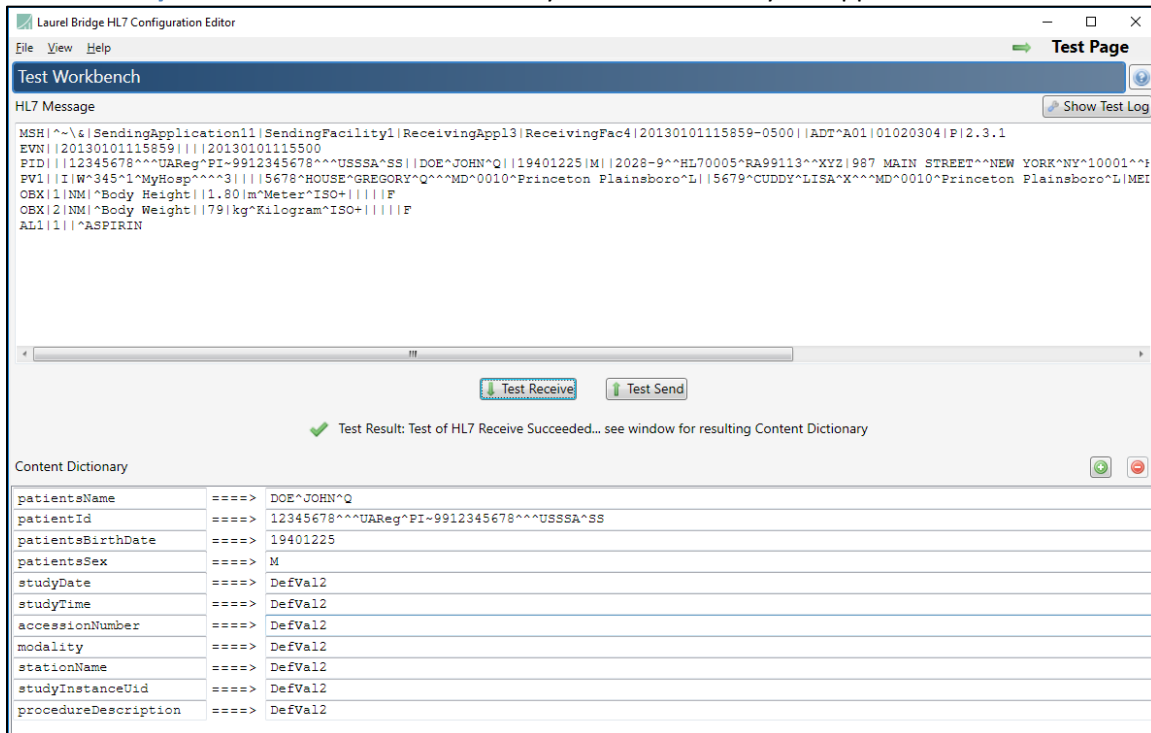
studyDate	patientsBirthDate
studyTime	patientsSex
modality	stationName
procedureDescription	user001
studyInstanceId	user002
accessionNumber	user003
patientsName	user004
patientId	user005

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.

HL7 Sender GUI

Message Template

```
MSH|^~\|^SendingApplication|^SendingFacility|^|20140318171058BOGUSTECH|ORM^001|^2345|||||EPIC^RAD
PID|^I|^54321|^TEST^ONE|^19700704|^PL150 246 TEST REGISTRATION^^NEWARK^DE^19711^USA^^DOE||555|123-4567
P^PH|^I|^S|^111-11-1111|^Test^Mother
PV1|^I|^Z|^MAMMO^^ZZ^^^DEPO||387432^TESTER^JOE^R^^^ACHPROVID^^ACHPROVID^^
123456789012|||||20140318171058|||
ORCINW|^I|^9191|^EPC|^54321|^EPC|^Arrived|||RI|^20140318171058BOGUSTECH^ACH RIS^TECHNOLOGIST^^1987432
^TESTER^JOE^R^^^ACHPROVID^^ACHPROVID|^192837465^20070001^^ZZ^MAMMOGRAPHY|^555|967-5309|||||
OB|^I|^1923285|^EPC|^54321|^EPC|^54321^MAMMO DIGITAL SCREEN BILAT^SMSRADORD^^MAMMO DIGITAL SCREEN BILAT|^I|^
20140318171058|||Ancillary P||387432^TESTER^JOE^R^^^ACHPROVID^^ACHPROVID|^202456-1111|^54321|^54321|^4321
|||||MG|^Arrived||^R||^test^^No|||20140318171500|||||387432^MAMMO DIGITAL SCREEN BILAT^SMSRADORD^^MAMMO
DIGITAL SCREEN BILAT
```

Received Response

Name	Replace Value
*	

delay Seconds: 0

Repeat count: 0

host: localhost

port: 8080

Application Name:

Sending Facility:

☒ Wait For Ack

Ack Timeout: 0

Send

Cancel

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.

Section 3 - GDPR Notes found below contains comments regarding the European Union’s (EU’s) GDPR - General Data Protection Regulation.

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 <https://www.himss.org/resourcelibrary/MDS2> [NEMA Document ID: 100382]). The headers in the following sections map directly to the headers in the MDS2 document. The Navigator MDS2 document is included with the installation files; the MDS2 document for a particular release is available upon request from LBS.

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 logged:

- **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 login/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 not support the ability to configure de-identification of PHI.

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 8.1
- Windows 10
- Windows Server 2012 R2

- Windows Server 2016
- Windows Server 2019

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 2012 x64, SQL Server 2014 x64, or SQL Server 2016 x64, or newer)
- 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 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)

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 support encrypted SQL Server connections, and their use is highly recommended in the case of SQL Server instances accessed over a network.

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. 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 (8443 if using HTTPS)**

3 GDPR Notes

The European Union's (EU) General Data Protection Regulation (GDPR) is a refresh of Europe's data-protection laws that harmonizes statutes across the 28 EU member states; it became effective May 25, 2018. GDPR is a law that applies to any organization doing business in the EU or with EU-based clients. It is up to the Laurel Bridge application customer to ensure that they manage the Navigator application and the medical imaging data processed by it in a way that is conformant to their GDPR policies and practices.

The content in this appendix describes the relevant security and privacy information associated with this application. Relative to the GDPR some key points to remember are:

- The Laurel Bridge application is installed on virtual or physical systems that are provided, configured, and controlled by the customer, therefore Laurel Bridge Software (LBS) cannot make assertions about the privacy and security of a particular installation.
- It is up to the customer to ensure that the customer's host systems on which the application components are installed have been adequately secured.
- By virtue of using this application, Laurel Bridge Software receives no private data from the customer or the customer's clients; data remains with and under the control of the customer.
- The application does not maintain a designated record set and is not a primary repository of electronic health record (EHR) or electronic medical record (EMR) data. Data processed and tracked by the application is transient and purged after a user-configurable period of time.
- Section 1 in this appendix, Management of Private Data, describes private data that may be processed by the application and which may be relevant to the customer's GDPR compliance activities.
- Log files may possibly contain private data associated with the medical imaging data being processed. Such files should be handled in a way that is compliant with the customer's data retention and privacy policies.

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 ]
eq = brain
eq = cranium

[ chest ]
eq = heart
eq = lungs
eq = thorax

[ leg ]
eq = knee
eq = thigh

[ breast ]
eq = 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

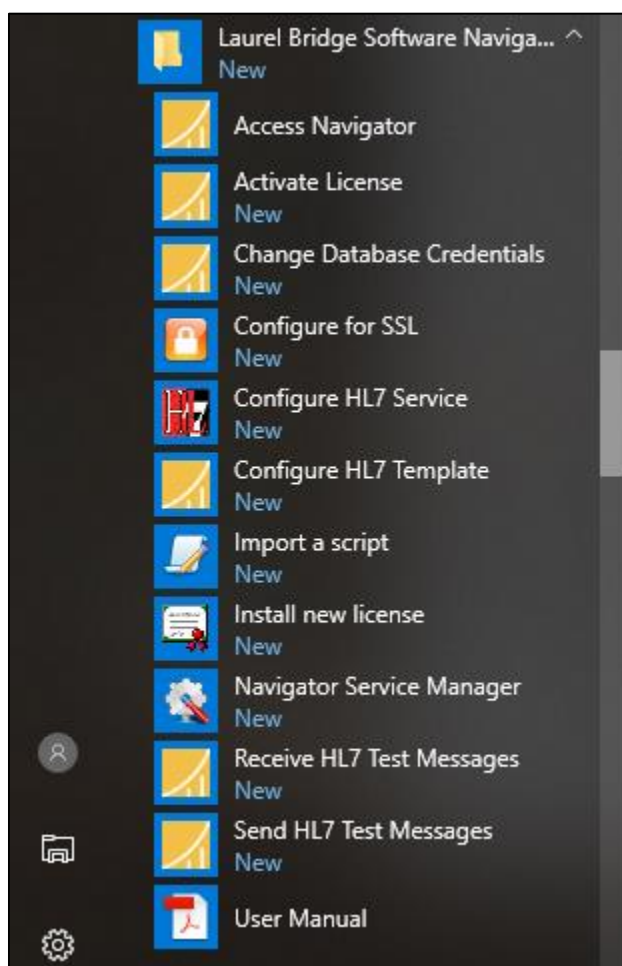
Navigator is controlled through a user interface accessible from your web browser. However, there are utilities (see section [7 Navigator Utilities above](#) for more information) that are run on the local computer. These are accessed via the Windows Start menu. On most Windows OSes, the Start menu and 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 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**

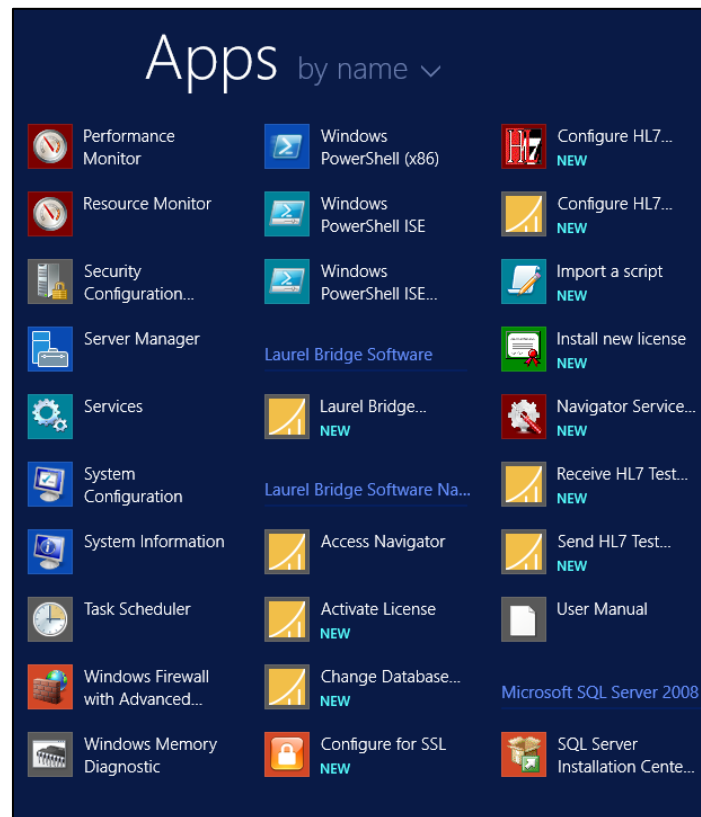
Click the **Start** button – it looks like a window with 4 panes.



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:

Tag	Operator	Value
SPSS Modality	Equals	MG
SPSS Scheduled Station AE Title	Regex Match	AAA BBB CCC

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. See the information in item [3 below](#) for more details.

Tag	Operator	Value
SPSS Modality	Equals	MG
SPSS Scheduled Station AE Title	Regex Match	.*AAA.* .*BBB.*

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.

Tag	Operator	Value
Accession Number	Regex Match	.*[13579]\$

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 (see item [3](#)

[below](#) for more details). 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.



3. Checking if a String Contains a Value

Note that care must be exercised when using a regular expression to check if a string contains a value. For example, if you wanted to match a prior only if the Study Description had “SCREENING” in it, you might think that all you need for the value to compare against is “SCREENING”. But Navigator may assume that that is *all* that is in the value, while in actuality, your Study Description is probably going to look more like “4 VIEW BREAST SCREENING”, not just the single word “SCREENING”.

What you should do is include the possibility of leading and trailing characters, via “. *” or “(. *)” in the value. For example:

```
( . *) SCREENING ( . *)
```

This indicates that there could be characters before or after the word. It can also be done for more complex regular expressions, like if you wanted it to match if the Study Description has TOMOSYN or SCREENING or ADD:

```
( . *) (TOMOSYN | SCREENING | ADD) ( . *)
```

This would check for any characters before any of the words “TOMOSYN”, “SCREENING”, or “ADD”, and allow for any characters after.

If the string should begin with the key word, you would omit the first “(. *)”, e.g.,

```
SCREENING ( . *)
```

If you want to make sure that the key word ends the value, you would omit the trailing “(. *)”, e.g.,

```
( . *) SCREENING
```

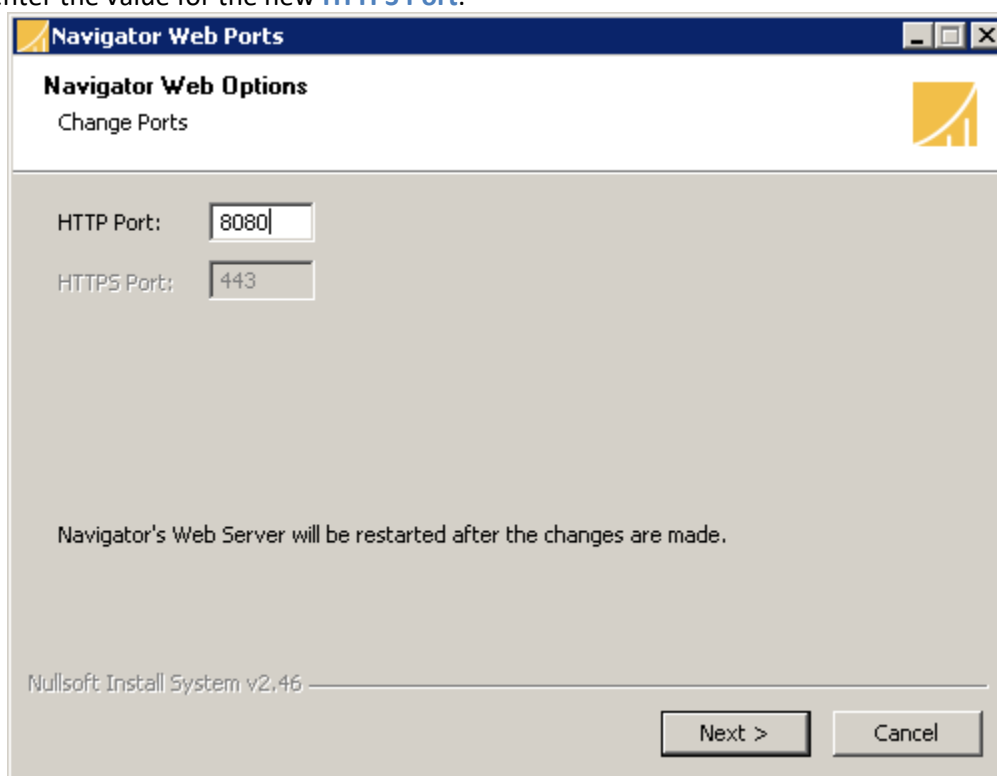
Keep these ideas in mind when you are building your regular expressions for **Step 1** and **Step 4** of your [Study Rules](#).

Appendix F: Changing Navigator's web port

When you installed Navigator, you selected the web server port that its Tomcat server would use. But later you may decide that you need to use a different port(s). These steps will guide you on how to change the ports to use – you can use the provided utilities, or do the steps manually. **Note** that you may need to be a user with Administrator permissions in order to edit the files; if you are using the utilities, you should run them as Administrator.

1. Using the Change Web Ports utility:

1. From the Windows Start menu, select `Start → Laurel Bridge Software → Navigator → Utilities → Configure Web Ports`.
2. Enter the **HTTP Port** that Navigator should use. If you have TLS/SSL enabled and are using HTTPS, also enter the value for the new **HTTPS Port**.



3. Click the **Next** button. The configuration changes will be saved, and the Navigator service restarted.
4. If you are using the HL7 Service, use the **HL7 Configuration Utility** and change the Navigator Web Port to match what you are now using and restart the HL7 Service. See Section **8.1 Configure HL7 Service** above for more information.

Note that Windows may take a while to update the **Access Navigator** link on the Windows Start menu, due to how Windows caches such data.

2. Manual steps:

1. Go to Navigator's installation directory, usually `C:\LB Navigator`. Go to the `tomcat\conf` directory.
2. Make a backup of the `server.xml` file – this is a precaution in case you make a mistake.
3. Edit the `server.xml` file.
4. Find the **Connector** node in the file that references your current web port. For example, if you are using port 8080, you are looking for text that looks like this:


```
<Connector port="8080" protocol="HTTP/1.1" connectionTimeout="20000"
redirectPort="8443" />
```

5. Replace the old **port** value with the new port value.

If you have HTTPS enabled and want to use a different port for TLS/SSL communication, do the following steps, too. If you are not changing the HTTPS port, skip down to Step 9.

6. In the same node as in Step 4 above, change the value for **redirectPort** to be a new value (which should not be the same as the value for "**port**").
7. Find the **Connector** node that looks like this:

```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
maxThreads="150" scheme="https" secure="true" sslProtocol="all" ... />
```

and change its **port** value. (This line is probably near the end of the file.)

8. Find the following line and change its **redirectPort** value:

```
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
```

9. After you have finished making all the changes, save the file.
10. Find the file **.install_cfg** in Navigator's installation directory; edit it and change the value for **web_port** to be the value used in Step 5. Save the file.
11. In Navigator's installation directory, find the file "**Navigator Web Site.URL**"; right-click on it and select **Properties**. Change the port in the **URL**. Click **Apply** and then **OK**. **Note** that Windows may take a while to update the **Access Navigator** link on the Windows Start menu, due to how Windows caches such data.
12. Restart the Navigator service.
13. If you are using the HL7 Service, use the **HL7 Configuration Utility** and change the Navigator Web Port to match what you are now using and restart the HL7 Service. See Section **8.1** for more information.

Appendix G: TLS Certificates

As noted above, Navigator can support HTTPS access for security. TLS authentication certificates should ideally be obtained from a trustworthy TLS certificate authority (CA). If this is not feasible, a self-signed certificate can be generated for a local computer, manually (and securely) copied to the computer, and installed into Navigator's Tomcat configuration. See [Appendix J: Java Keystore](#) if you are using the certificate for LDAPS.

NOTE: Navigator expects the certificate file to be **PEM** format, e.g., **<filename>.crt** or **<filename>.cert**. The SSL Certificate File that you get from a Certificate Authority often has a **.cert** file extension, while the SSL Certificate Key File that you get often has a **.key** file extension; the SSL Certificate Chain File often has a **.crt** file extension.

1 Self-Signed Certificate

For testing purposes, you can get a free self-signed certificate at <https://www.selfsignedcertificate.com/> - just enter the domain name and press the **Generate** button. Alternatively, if you have OpenSSL installed, you can create the key and certificate to use yourself.

To generate a key:

```
openssl genrsa -out <domain name>.key 2048
```

And then the certificate:

```
openssl req -new -x509 -key <domain name>.key -out <domain name>.cert -days 365 -subj /CN=<domain name>
```

Use the **SSL / TLS Utility** to install the certificates – see section [7.2 Configure for TLS / SSL](#) for details.

2 Trusted Certificate

In order to obtain a Certificate from the Certificate Authority of your choice, you have to create a so-called **Certificate Signing Request** (CSR). That CSR will be used by the Certificate Authority to create a Certificate that will identify your website as “secure”.

2.1 Using OpenSSL

1. First create a personal key for creating a Certificate Signing Request:

```
openssl genrsa -des3 -out <mykeyfile.key> 2048
```

This will create a personal key to be used for creating the certificate request and other necessary files. You will be prompted for a pass phrase.

2. Next run this command:

```
openssl rsa -in <mykeyfile.key> -out <mykeyfile.key.insecure>
```

This creates a slightly less secure version of the key file to be used with the Tomcat web server – the advantage is that you don't need to specify the pass phrase when the web server needs to be restarted.

3. Create your Certificate Request:

```
openssl req -new -key <mykeyfile.key> -out <my_request.csr>
```

You will be prompted for several values:

- the pass phrase from the first step
- the country code
- state
- Locality
- Organization Name
- Organizational Unit
- Common name (your domain name)
- Email address (usually something like “webadmin@<domain name>”)
- Challenge password (the value that you specified in Step 1)
- Company name (optional)

Now you have a file called `my_request.csr` that you can submit to the Certificate Authority (look at the documentation of the Certificate Authority website on how to do this). In return you get a Certificate.

4. Submit to the CA and get your certificates.
5. Use the SSL / TLS Utility to install the certificates – see section [7.2 Configure for TLS / SSL](#) for details.

2.2 Using Keytool

1. Create a key store


```
keytool -genkey -alias server -keyalg RSA -keysize 2048 -keystore yourdomain.jks
```

‘yourdomain’ is the name of the domain you are securing.
 You will be prompted for the DN information. Please note: when it asks for first and last name, this is not YOUR first and last name, but rather your domain name and extension (i.e., `www.yourdomain.com`).
 Confirm that the information is correct by entering 'y' or 'yes' when prompted. Next you will be asked for your password to confirm. Make sure to remember the password you choose.
2. Generate your Certificate Signing Request with your new keystore.


```
keytool -certreq -alias server -keyalg RSA -file yourdomain.csr -keystore yourdomain.jks
```

Enter the keystore password.
3. A SSL Certificate CSR file is created. Submit this to the CA and get your certificates. (Look at the documentation of the Certificate Authority website on how to do this.)
4. Use the SSL / TLS Utility to install the certificates – see section [7.2 Configure for TLS / SSL](#) for details.

3 Convert PFX to PEM

If you have only a PFX file but want to use HTTPS, Navigator includes a batch script that *might* be able to convert your PFX file to the various PEM files that Navigator uses for HTTPS. It uses [openssl](#), which must already be installed and in the PATH.

To run the script:

1. Open a Windows command prompt and change to Navigator’s installation directory.

2. Run this command: **convert_pfx_to_pem.bat PFXFILE PASSWORD**

Replace PFXFILE with the name of your PFX certificate file; replace PASSWORD with the password you used when creating the file.

If the script worked, you will now have 5 new files – 3 of these are used to configure HTTPS for Navigator. See Section [7.2 Configure for TLS / SSL](#) for details.

For example, if you run **convert_pfx_to_pem.bat MyCertificate.pfx AbcDefg**, you might end up with these files

- MyCertificate_encrypted.key
- MyCertificate_certificate.crt – use this for the SSL Certificate File
- MyCertificate_encrypted_pem.key – use this for the SSL Certificate Key File
- MyCertificate_decrypted.key
- MyCertificate_cert_chain.crt – use this for the SSL Certificate Chain File

Appendix H: User Chooses the Priors

Most users will configure Navigator so that it automatically chooses the priors to move. But some users may have special cases where they want Navigator to narrow down the possible priors but have a user choose which ones should actually be moved.

The first thing you need to do is to modify a Study Rule so Navigator knows that user interaction is required for these priors. Create the Study Rule so that it chooses priors from the Sources you want and sends them to the desired Destinations – see section [4.5 Study Rules](#) for more details about how to configure a Study Rule. Configure it so that it will narrow down the possible priors based on body part matching, age, and other filtering criteria related to the Worklist Item or HL7 “trigger”.

Then at the end of **Step 4** of the Study Rule, check the box next to **User Action Required**, as shown below – this tells Navigator that a user must choose which priors should be moved. If you want, you can have an e-mail sent to someone whenever this is needed – check the box for **Send notification for User Action** and enter an e-mail address in the field. Save your changes to the Study Rule and start Navigator.

st Processing Script Names ?

User Action Required: ? ☒

Send notification for User Action: ☒ E-mail address:

When this Study Rule processes data, it will query for priors and filter the list of possibilities for you, but then it will wait for someone to choose which priors should be moved. A user needs to login to Navigator, go to the Worklist Entries page, and find the Worklist Item Job marked with the status “**Waiting for User**”, as shown at the right edge of the image below.

<input type="checkbox"/>	1224	Doe^Jan01	0_123401_0	2020-08-06 15:33:53	MAMMO_STN_2	MG	Mammo rule	High	Waiting for User
	ID	▼ Patient's Name	Accession Number	SPSS Start Date	Scheduled Station AE Title	Modality	Study Rule	Priority	Status

Clicking on the record ID or the Patient’s Name will take you to a page displaying the details of the Worklist Item Job. Near the bottom of the page is a table listing the priors in question (the light gray table), followed by a table showing the priors that have been filtered by the Study Rule (the green and pink table).

WLI User Text 001 Tag
WLI User Text 002 Tag

Accept AllReject All

Study Move Requests

Number of Studies: 5

Approve Selected Priors

Accept	Reject	ID	Study Instance UID	Accession #	Source	Destination	Priority	Status	Sub-Ops	Modality	Study Description
<input type="radio"/>	<input type="radio"/>	4891	3.1.1	P_1234010	PACS Source 2 (DICOM_SCP_2)	Reading Station 1 (READING_STN_1)	High	Init	0 / 0 / 0 / 0	MG	4 VIEW BREAST SCREENING
<input type="radio"/>	<input type="radio"/>	4892	6.1.1	P_1234010	PACS Source 1 (DICOM_SCP_1)	Reading Station 1 (READING_STN_1)	High	Init	0 / 0 / 0 / 0	CR	KNEE-RIGHT (QUAD KNEE/LG JOINT)
<input type="radio"/>	<input type="radio"/>	4893	6.1.2	P_1234011	PACS Source 1 (DICOM_SCP_1)	Reading Station 1 (READING_STN_1)	High	Init	0 / 0 / 0 / 0	CR	KNEE-RIGHT (QUAD KNEE/LG JOINT)
<input type="radio"/>	<input type="radio"/>	4894	3.1.2	P_1234011	PACS Source 1 (DICOM_SCP_1)	Reading Station 1 (READING_STN_1)	High	Init	0 / 0 / 0 / 0	MG	4 VIEW BREAST SCREENING
<input type="radio"/>	<input type="radio"/>	4895	3.1.3	P_1234012	PACS Source 2 (DICOM_SCP_2)	Reading Station 1 (READING_STN_1)	High	Init	0 / 0 / 0 / 0	MG	4 VIEW BREAST SCREENING
Accept	Reject	ID	Study Instance UID	Accession #	Source	Destination	Priority	Status	Sub-Ops	Modality	Study Description

Prior Studies Filtered

Study Instance UID	Accession #	Name	Source	Study Description	Study Date	Move?	Reason
3.1.1	P_1234010	Doe^Jan01	DICOM_SCP_2	4 VIEW BREAST SCREENING	20190605	Yes	
6.1.1	P_1234010	Doe^Jan01	DICOM_SCP_1	KNEE-RIGHT (QUAD KNEE/LG JOINT)	20190605	Yes	
6.1.2	P_1234011	Doe^Jan01	DICOM_SCP_1	KNEE-RIGHT (QUAD KNEE/LG JOINT)	20180605	Yes	
3.1.2	P_1234011	Doe^Jan01	DICOM_SCP_1	4 VIEW BREAST SCREENING	20180605	Yes	
3.1.3	P_1234012	Doe^Jan01	DICOM_SCP_2	4 VIEW BREAST SCREENING	20170605	Yes	
6.1.3	P_1234012	Doe^Jan01	DICOM_SCP_1	KNEE-RIGHT (QUAD KNEE/LG JOINT)	20170605	No	CalendarResultListFilter: Count of studies to move exceeded or StudyDate not in range
6.1.4	P_1234013	Doe^Jan01	DICOM_SCP_1	KNEE-RIGHT (QUAD KNEE/LG JOINT)	20160605	No	CalendarResultListFilter: Count of studies to move exceeded or StudyDate not in range

You must choose to Accept or Reject each of the priors in the upper table by clicking a button at the left end of the table. Each button will change color to indicate whether it was accepted (**green**) or rejected (**red**). For example, the picture below shows that three priors have been accepted, one has been rejected, and one hasn't been chosen yet. There are buttons to **Accept All** or **Reject All** to make selecting them easier if there are many priors to be chosen.

The screenshot shows a software interface titled "Study Move Rec". At the top, there are two buttons: "Accept All" and "Reject All". Below them is a table with columns: "Accept", "Reject", "ID", "Study Instance", "UID", and "A". The "Accept" and "Reject" columns contain radio buttons. The "Accept" buttons for rows 3396, 3398, and 3399 are green and have a blue dot in the center. The "Reject" button for row 3397 is red and has a blue dot in the center. The other "Reject" buttons (for rows 3396, 3398, 3399, and 3400) are white with a blue outline. The "ID" column contains values 3396, 3397, 3398, 3399, and 3400. The "Study Instance" column contains values 3.1.1, 6.1.1, 6.1.2, 3.1.2, and 3.1.3. The "UID" column contains values F, F, F, F, and F. Below the table, there are labels "Accept", "Reject", "ID", "Study Instance", "UID", and "A".

Accept	Reject	ID	Study Instance	UID	A
<input checked="" type="radio"/>	<input type="radio"/>	3396	3.1.1		F
<input type="radio"/>	<input checked="" type="radio"/>	3397	6.1.1		F
<input checked="" type="radio"/>	<input type="radio"/>	3398	6.1.2		F
<input checked="" type="radio"/>	<input type="radio"/>	3399	3.1.2		F
<input type="radio"/>	<input type="radio"/>	3400	3.1.3		F

Once you have selected the priors you want, you must click the **Approve Selected Priors** button, just above the table. You will be warned if you have not made a choice for every one of the priors, and then you must confirm that you are done making your choices.

The screenshot shows a software interface with a button labeled "Approve Selected Priors" at the top. Below the button is a table with columns: "Destination" and "Priority". The "Destination" column contains values "p_2) Reading Station 1 (READING_STN_1)" and "p_4) Reading Station 1 (READING_STN_1)". The "Priority" column contains values "High" and "High".

Destination	Priority
p_2) Reading Station 1 (READING_STN_1)	High
p_4) Reading Station 1 (READING_STN_1)	High

Once you are done and have approved the priors you want, Navigator will move the chosen priors in time. When they are done, you can refresh the page and see the ones that were completed (in **green**) and the ones that were rejected by you (in **orange**).

The screenshot shows a software interface with a table. The table has columns: "Priority", "Status", "Sub-Ops", and "Moda". The "Status" column contains values "Completed" (in green) and "Rejected" (in orange). The "Sub-Ops" column contains values "0 / 4 / 0 / 0" and "0 / 0 / 0 / 0". The "Moda" column contains values "MG" and "CR".

Priority	Status	Sub-Ops	Moda
ING_STN_1) High	Completed	0 / 4 / 0 / 0	MG
ING_STN_1) High	Completed	0 / 3 / 0 / 0	CR
ING_STN_1) High	Rejected	0 / 0 / 0 / 0	CR
ING_STN_1) High	Completed	0 / 4 / 0 / 0	MG
ING_STN_1) High	Rejected	0 / 0 / 0 / 0	MG

Appendix I: Checking if a Study already exists on the Destination

Often you may want Navigator to check if a prefetch candidate already exists on a Destination and not issue a C-Move request in that case. This is actually fairly easy to configure in Navigator.

When you set up your [Devices](#), configure the Destination device in question as *both* a Source and a Destination – note that both Source and Destination are checked for the device shown below.

Edit DICOM Device [Save] [Delete] [Copy] [Cancel]

* - Item is required

ID: 4

Description: * Reading Station 1

Enabled: ☒ *Last Echo:*

Role: ☒ Source ☒ Destination ☐ Trigger

Max Threads per Role: ? 64

Send notifications: ? ☐ E-mail address:

Then in the [Study Rules](#), in Step 3, add this device to the Sources to query and make it the first one in the list of Sources – note in the image below that “Reading Station 1” is the first Source device to query.

Step 3 ?

Source Devices ? *

Source Devices and Search Order	
▲▼	Reading Station 1
▲▼	PACS Source 1
▲▼	PACS Source 2
Select a device ▼	

Allow Partial Query Failures ? ☐

Sources are queried in the order that they are listed, so when Navigator tries to move the study, it will note that the Source and Destination are the same and won't issue a C-Move request. The study will show as moved successfully but no instances will have actually transferred.

1 Note on Storage Groups

Defining a device's Storage Group is another way that can be used to prevent studies that already exist on a Destination device from being moved. The Storage Group Name should be the same for any Source and Destination devices that share the same database backend. When Navigator processes the priors and sees that a study is going from a Source to a Destination with the same Storage Group, Navigator won't move the study because it is already there.

This can be used in cases where the Destination cannot be queried as a Source. For example, if the Destination is a Compass (typically not queryable) that will forward the data to its ultimate destination and if the final destination shares the same database backend as the source, you could give both the Source and

the (Compass) Destination the same Storage Group Name. Then when Navigator wants to move a prior to Compass, it will see that the Storage Groups are the same and it won't move the study because it is already there. But if the prior comes from a different Source that does not share the same database backend, Navigator will move the job to Compass, which will then forward it to its ultimate destination.

Appendix J: Java Keystore

Java's keystore file is used by Navigator for operations that may require a certificate or key to ensure secure communication – for example, this would include if you are configuring Navigator to use LDAPS.

Starting in Navigator version 2.1.15 the Java keystore file has been changed from:

`C:\LB Navigator\java\lib\security\cacerts`
to
`C:\ProgramData\Laurel Bridge Software\Navigator2\cfg\nav_cacerts`

Any changes to the keystore file itself should be preserved during an install or upgrade. However, the settings to use the correct keystore may have changed during an upgrade. In a typical situation, the keystore's password might need to be specified in the settings in order to enable its correct usage.

The options for the Java VM for Navigator are in the Windows registry under the key named:

`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun
2.0\Navigator\Parameters\Java`

After a typical install, the default values for these are:

- Dcatalina.home=C:\LB Navigator\tomcat
- Dcatalina.base=C:\LB Navigator\tomcat
- Dignore.endorsed.dirs=C:\LB Navigator\tomcat\endorsed
- Djava.io.tmpdir=C:\LB Navigator\tomcat\temp
- Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager
- Djava.util.logging.config.file=C:\LB Navigator\tomcat\conf\logging.properties
- Djavax.net.ssl.keyStore=C:\ProgramData\Laurel Bridge Software\Navigator2\cfg\nav_cacerts
- Djavax.net.ssl.keyStorePassword=changeit
- Djavax.net.ssl.trustStore=C:\ProgramData\Laurel Bridge Software\Navigator2\cfg\nav_cacerts
- Djavax.net.ssl.trustStorePassword=changeit
- Dcom.sun.jndi.ldap.object.disableEndpointIdentification=true
- XX:+CMSClassUnloadingEnabled
- XX:+UseConcMarkSweepGC

Note that the path to the keystore and the password to access it are specified in these settings. You should use **extreme care** when editing these fields in the registry!

Also note the option `com.sun.jndi.ldap.object.disableEndpointIdentification`. This must be set to TRUE to allow use of self-signed certificates. If you are connecting to an LDAPS server using a certificate signed by a Certificate Authority, you may want to change this setting to FALSE.

Java's `keytool` utility should be used if you need to install or remove certificates from the keystore.

Navigator includes two sample batch files – in the installation directory root – that use `keytool` to list the contents of the keystore in either the old or the new location. The scripts should be run from a command prompt if you wish to use them.

- **list_keys_jre.bat** displays the contents of the keystore in the old location, `C:\LB Navigator\java\lib\security\cacerts`
- **list_keys_nav.bat** displays the contents of the keystore in the new location, `C:\ProgramData\Laurel Bridge Software\Navigator2\cfg\nav_cacerts`

Note that the scripts assume that the original password for the keystore, “changeit”, is in use; you will need to modify the scripts if you have changed the password.

Occasionally you may need to add a certificate to the keystore. For example, if you have added a certificate in the past, you will need to add a new one when that one expires, probably annually.

To install the certificate, use the following command from a command prompt:

```
keytool -importcert -file <Path to Certificate> -keystore "C:\ProgramData\Laurel Bridge Software\Navigator2\cfg\nav_cacerts" -alias <alias name>
```

where

- <Path to Certificate> is the complete path to the .cer, .der, or .crt file
- <alias name> is any short name to refer the certificate (this can be whatever you want).

When asked for a password, use "changeit" and answer "yes" to trust the certificate.

You can list the certificates installed with

```
keytool -list -keystore "C:\ProgramData\Laurel Bridge Software\Navigator2\cfg\nav_cacerts"
```

Note that you may need to specify the entire path to the keytool executable each time you use it; on a standard Navigator installation, it is found as C:\LB Navigator\java\bin\keytool.exe. (It is *not* recommended to add that directory to the PATH environment variable.)

When creating a certificate to use, the certificate should prove your identity to a remote computer and ensure the identify of the remote computer. If you were to look at the certificate through the Windows Certificate Manager, part of it might look like this:



Once the certificate is added to the keystore, you will probably need to restart the Navigator service in order for Navigator to use the updated keystore – one way to do this is via the [Navigator Service Manager](#).

Useful keytool commands:

- To add a certificate:

```
keytool -importcert -file <Path to Certificate> -keystore  
"C:\ProgramData\Laurel Bridge Software\Navigator2\cfg\nav_cacerts" -alias  
<alias name>
```

- To list the certificates in the keystore:

```
keytool -list -keystore "C:\ProgramData\Laurel Bridge  
Software\Navigator2\cfg\nav_cacerts"
```

- To display details about a certificate:

```
keytool -printcert -file <Path to Certificate>
```

Appendix K: Navigator's CSV Reader

Most jobs come into Navigator via Modality Worklist (MWL) [Devices](#) or via HL7 messages, and they are configured via the [Devices](#) and [Worklist Readers](#). Navigator also offers an application that can read CSV (Comma-Separated Values) files and enter those values as jobs to be processed. Jobs that are ingested in this way are treated as if they have come via the HL7 Reader – this means that any [Study Rules](#) for processing CSV file data should be associated with the HL7 Web Requests Worklist Reader.

There are example files for the CSV Reader in the installation directory:

- [Example_worklist_items.csv](#) – shows a typical CSV file and what values are expected in each column
- [Example_run_csv_reader.bat](#) – this batch script shows how to set the environment variables needed for the CSV Reader and will run the Reader to ingest the data from a CSV file.
- [Example_worklist_items.trigger](#) – an example of the file to tell the CSV Reader application that the CSV file is no longer being written and is ready for processing.

The batch script will launch the CSV Reader. The Reader will look for a “trigger file” – if the trigger file is not present, the Reader will just exit and do nothing. If the trigger file does exist, the Reader will read the contents of the data file and then submit each line as a job to Navigator. When all the lines in the file have been processed, the trigger file is deleted. (Note that the trigger file does not need any data in it – its very existence is all that is needed for the CSV Reader to know that it is safe to run now.)



```

set JAVA_BIN="C:\LB Navigator\java\bin\java.exe"
set NAV_INST_DIR=C:\LB Navigator
set DCF_CFG=C:\ProgramData\Laurel Bridge Software\Navigator2\cfg
set NAV_WEBAPP_DIR=C:\LB Navigator\tomcat\webapps\Navigator\WEB-INF
set CLASSPATH=%NAV_INST_DIR%\LaurelBridge.jar;%NAV_INST_DIR%\NavigatorClasses.jar;%NAV_WEBAPP_DIR%\lib\javax.json-1.0.4.jar;%NAV_WEBAPP_DIR%\lib\javax.json-api-1.0.jar;
set PATH=%PATH%;%NAV_INST_DIR%;%NAV_WEBAPP_DIR%\lib

copy "%NAV_INST_DIR%\MBI_worklist_items.csv" "%NAV_INST_DIR%\worklist_items.csv"
copy "%NAV_INST_DIR%\MBI_worklist_items.trigger" "%NAV_INST_DIR%\worklist_items_trigger.txt"

echo "Starting custom worklist reader"
::java com.LaurelBridge.NavigatorCSVReader.NavigatorCSVWorklistReader C:\temp\java.out.txt 2>&1
%JAVA_BIN% com.LaurelBridge.NavigatorCSVReader.NavigatorCSVWorklistReader
echo "Custom worklist reader completed"

```

The trigger file is used so that you can configure a Scheduled Task to run the batch script - if no data is present (i.e., no trigger file), then nothing needs to be done or possibly the data file is not yet ready to be processed, e.g., changes are still being made to the CSV file.

Note that the example batch script makes a copy of the example CSV file and renames it to what the Reader expects by default. Obviously, when using the Reader in a production environment, you don't need those copy commands. (You may want to make a copy of the example batch script to use in a Scheduled Task, after you delete those copy commands.)

1 Configuration

The CSV Reader can be configured by editing the file [NavigatorCSVReader](#) in the [C:\ProgramData\Laurel Bridge Software\Navigator2\cfg\apps\defaults](#) directory. Usually you will just need to change these attributes in the [[java_app/NavigatorCSVReader](#)] configuration group:

- **navigator_add_worklist_item_url_base** – set it to the URL to use for creating new jobs; default is `http://localhost:8080/Navigator/WorklistItem/addWorklistItem`
- **worklist_item_data_file_name** - the complete PATH of the file with the data to be inserted into Navigator; default is `C:/LB Navigator/worklist_items.csv`
- **worklist_item_trigger_file_name** - the complete PATH of the file that must be present for the CSV Reader to recognize that there is data to process; default is `C:/LB Navigator/worklist_items_trigger.txt`

The CSV file expects the first line to be column headers, so any data should begin on line number 2.

```
MRN,FIRST,LAST,BEG_DT_TM,BIRTH,GENDER,LOCATION,ORDER_ID,ORDER_NAME
111-22-3333,Elliott,Lord, 04/24/2020 09:00,05/17/1961,M,STN1,AC12345, CT Head, code 54321: XYZ; Check for missing brain,,
222-33-4444,TEST,PATIENT1,04/24/2020 09:00,06/06/1993,F,STN3,AC4567,Mammo Screening, 4 Views
```

The columns must be specified in the order given:

0	1	2	3	4	5	6	7	8
MRN,	FIRST,	LAST,	BEG_DT_TM,	BIRTH,	GENDER,	LOCATION,	ORDER_ID,	ORDER_NAME

Note that the modality is not specified in the CSV file and that the Reader hard-codes the value to “MG” – this must be accounted for in the [Study Rules](#) handling these jobs and the appropriate matching conditions.

All columns except 3 and 4 can contain most characters except comma “,”.

Column 3: Study Begin Date/Time **MUST** be in the format “M/d/yyyy H:m” OR “M/d/yyyy H:m:s”, i.e., date and time separated by space, seconds optional for the time.

Examples: “3/8/2019 13:10” or “12/31/2020 9:30:01”

Column 4: Birth date **MUST** be in the format “M/d/yyyy”.

Example: “5/17/1961”

Do not include quotes or other non-comma characters unless you want them in the values.

2 Running the Reader

To run the CSV Reader, you should open a Command Prompt and then change to the installation directory. Then run the batch script with the command “`Example_run_csv_reader.bat`” – this will send all worklist items in the data file to Navigator.

```
C:\LB Navigator>example_run_csv_reader.bat
C:\LB Navigator>set JAVA_BIN="C:\LB Navigator\java\bin\java.exe"
C:\LB Navigator>set NAV_INST_DIR=C:\LB Navigator
C:\LB Navigator>set DCF_CFG=C:\ProgramData\Laurel Bridge Software\Navigator2\cfg
C:\LB Navigator>set NAV_WEBAPP_DIR=C:\LB Navigator\tomcat\webapps\Navigator\WEB-INF
C:\LB Navigator>set CLASSPATH=C:\LB Navigator\LaurelBridge.jar;C:\LB Navigator\NavigatorClasses.jar;C:\LB Navigator\tomcat\webapps\Navigator\WEB-INF\lib\javax.json-1.0.4.jar;C:\LB Navigator\tomcat\webapps\Navigator\WEB-INF\lib\javax.json-api-1.0.jar;
C:\LB Navigator>set PATH=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Program Files (x86)\Microsoft SQL Server\150\Tools\Binn\;C:\Program Files\Azure Data Studio\bin\;C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\170\Tools\Binn\;C:\Program Files (x86)\Microsoft SQL Server\150\Tools\Binn\;C:\Program Files\Microsoft SQL Server\150\Tools\Binn\;C:\Program Files\Microsoft SQL Server\150\Tools\Binn\;C:\Users\Jody.Wilson.CTR\AppData\Local\Microsoft\WindowsApps;C:\LB Navigator;C:\LB Navigator\tomcat\webapps\Navigator\WEB-INF\lib
C:\LB Navigator>copy "C:\LB Navigator\WBI_worklist_items.csv" "C:\LB Navigator\worklist_items.csv"
1 file(s) copied.
C:\LB Navigator>copy "C:\LB Navigator\WBI_worklist_items.trigger" "C:\LB Navigator\worklist_items_trigger.txt"
1 file(s) copied.
C:\LB Navigator>echo "Starting custom worklist reader"
"Starting custom worklist reader"
C:\LB Navigator>"C:\LB Navigator\java\bin\java.exe" com.LaurelBridge.NavigatorCSVReader.NavigatorCSVWorklistReader
NavigatorCSVWorklistReader: Start
[ INFO 2021/08/30 16:42:00.025 ??/java_app/NavigatorCSVReader thrd=main ]
NavigatorCSVWorklistReader: Common services initialized
[ INFO 2021/08/30 16:42:00.025 ??/java_app/NavigatorCSVReader thrd=main ]
NavigatorCSVWorklistReader: read worklist items
[ INFO 2021/08/30 16:42:00.040 ??/java_app/NavigatorCSVReader thrd=main ]
NavigatorCSVWorklistReader: Start send items to server
[ INFO 2021/08/30 16:42:00.212 ??/java_app/NavigatorCSVReader thrd=main ]
NavigatorCSVWorklistReader: End send items to server (size of list = 14)
C:\LB Navigator>echo "Custom worklist reader completed"
"Custom worklist reader completed"
```

3 Using HTTPS Access

If you change Navigator to use HTTPS for access (see section [7.2 Configure for TLS / SSL](#)), you will have to adjust how the CSV Reader runs in order to continue to use it. In the configuration file, change `navigator_add_worklist_item_url_base` to have the correct port and hostname for Navigator under HTTPS. This might be just changing the port to 8443 (or whatever port you choose), but you may need to change the hostname from `localhost` to the name of the host, e.g., "`myMachine.myCompany.com`".

Example: `navigator_add_worklist_item_url_base = https://myMachine:8443/Navigator/WorklistItem/addWorklistItem`

If you are using a self-signed certificate for HTTPS, you will need to add the certificate to the `nav_cacerts` file, like this:

```
keytool -importcert -file <file.crt> -keystore "C:\ProgramData\Laurel Bridge
Software\Navigator2\cfg\nav_cacerts" -alias <some alias>
```

If you are using a purchased certificate from a Certificate Authority, this may also need to be added to the `nav_cacerts` file.

Then modify the batch script so that the Java command to run the application has the necessary options to specify the `KeyStore` and `TrustStore` files (note that "changeit" is the default password for the Java KeyStore, which you may want to change):

```
java -Djavax.net.ssl.keyStore="C:\ProgramData\Laurel Bridge
Software\Navigator2\cfg\nav_cacerts"
-Djavax.net.ssl.keyStorePassword=changeit
-Djavax.net.ssl.trustStore="C:\ProgramData\Laurel Bridge
Software\Navigator2\cfg\nav_cacerts"
-Djavax.net.ssl.trustStorePassword=changeit
com.LaurelBridge.NavigatorCSVReader.NavigatorCSVWorklistReader
```

If you have configured Navigator to restrict unsecure web calls, you may need to manually adjust Navigator's configuration file to allow the CSV Reader to send the jobs to Navigator. Contact Laurel Bridge Software for assistance.

== end of document ==