

Lighthouse User Manual



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

Document Version: 3.0.0
Last Saved: 11/14/2023 4:09:00 PM

Table of Contents

1	Overview.....	1
1.1	Which remote applications can be monitored?	1
2	Installation	1
2.1	Upgrading from a Previous Version	1
2.2	Minimum System Specification.....	1
2.3	Prerequisites	1
2.3.1	Installing SQL Server 2016 Express x64.....	2
2.4	Installation: Lighthouse Application	2
2.5	Configuring Lighthouse	6
3	Workflow Definitions.....	6
3.1	Nodes	6
3.2	Users	7
4	Configuration QuickStart.....	7
4.1	Access Lighthouse’s Website	7
4.2	Log In.....	7
4.3	Click “Configuration”	8
4.4	Click “System”	8
4.4.1	Click “Database” under the “System->Administration” tab	8
4.5	Click “Nodes”	9
4.6	Click “Dashboard”	10
5	Web Client: Lighthouse Web Interface Details	10
5.1	Dashboard.....	10
5.1.1	Dashboard List View.....	10
5.1.2	Dashboard Details View	11
5.2	Login.....	13
5.3	Search.....	14
5.3.1	Compass	14
5.3.2	Navigator.....	17
5.3.3	Waypoint.....	20
5.4	Configuration	21
5.4.1	System Configuration.....	21
5.5	Users	25
Appendix A:	Lighthouse Privacy and Security Statement.....	26
1	Management of Private Data	26
1.1	Types of PHI Maintained.....	26
1.2	Persistence of Private Data	26
1.3	Transmission of Private Data	27
2	Security Capabilities	28
2.1	Automatic Logoff.....	28
2.2	Audit Controls	28

2.3	User Authorization	28
2.4	Security Configuration	29
2.5	Security Updates	29
2.6	De-Identification of PHI.....	29
2.7	Backup and Restore	29
2.8	Emergency Access	29
2.9	Data Integrity and Authenticity	29
2.10	Malware Protection	30
2.11	Node Authentication.....	30
2.12	Person Authentication	30
2.12.1	Local Web User Administration	30
2.12.2	LDAP Enabled Web User Administration	31
2.13	Physical Locks.....	31
2.14	Device Life Cycle Roadmap	31
2.15	System and Application Hardening.....	31
2.16	Security Guidance	32
2.17	Data Storage Confidentiality	32
2.18	Data Transmission Confidentiality	32
2.19	Data Transmission Integrity	32
2.20	Other Security Considerations	32
3	GDPR Notes	34

1 Overview

Laurel Bridge Lighthouse is a centralized management tool that allows users to view the status and information of remote applications, referred to as nodes.

1.1 Which remote applications can be monitored?

- Compass 2.10.0 and newer.
- Navigator 3.0.0 and newer.
- Waypoint 1.12.0 and newer.

2 Installation

2.1 Upgrading from a Previous Version

Prior to upgrading, make sure the license tied to the copy of Lighthouse being upgraded is covered under a valid maintenance contract that isn't expired; licenses that don't have a valid maintenance contract cannot be upgraded.

An older Lighthouse version can be upgraded to a newer Lighthouse version without uninstalling the older version (unless explicitly noted as being necessary for particular cases described in the following sections of this chapter).

When upgrading a copy of Lighthouse that is multiple versions newer than the old version, it is not necessary to install the intermediate versions; the new version will apply all the changes that occurred between the old version and the version currently being installed.

Prior to installing the new version, stop the Lighthouse service.

2.2 Minimum System Specification

Lighthouse runs on dedicated hardware or a virtual machine.

- Intel i7+, 16GB+ RAM, 500GB+ HD 7200+ RPM,
- Windows 10 or newer; Windows Server 2016 or newer.
- SQL Server 2016 x64 or newer.
SQL Express edition may be used in most installations.
The full SQL version must be used for failover cluster configurations.
It is recommended to install the SQL Management Studio as well.

2.3 Prerequisites

Laurel Bridge Lighthouse utilizes several components known as prerequisites that must be installed for the application to work. The following prerequisites must be installed prior to installing Lighthouse:

- Microsoft Visual C++ 2017 Redistributable (x64) - 14.15.26706, (vcredist_x64.exe)
- Microsoft SQL Server
- Microsoft SQL Management Studio

Note, Microsoft Visual C++ 2017 Redistributable is included in the Lighthouse installer and is installed automatically. The installation is dependent on all Windows Updates being installed on the host system.

2.3.1 Installing SQL Server 2016 Express x64

These are instructions for installing SQL Server Express in its most basic configuration for use by Lighthouse. These instructions are valid for Windows 10 or newer and Windows Server 2016 or newer. The installation procedure may differ if a newer version of SQL Server is installed, if the full version of SQL Server is preferred, or if SQL Server authentication mode must be enabled.

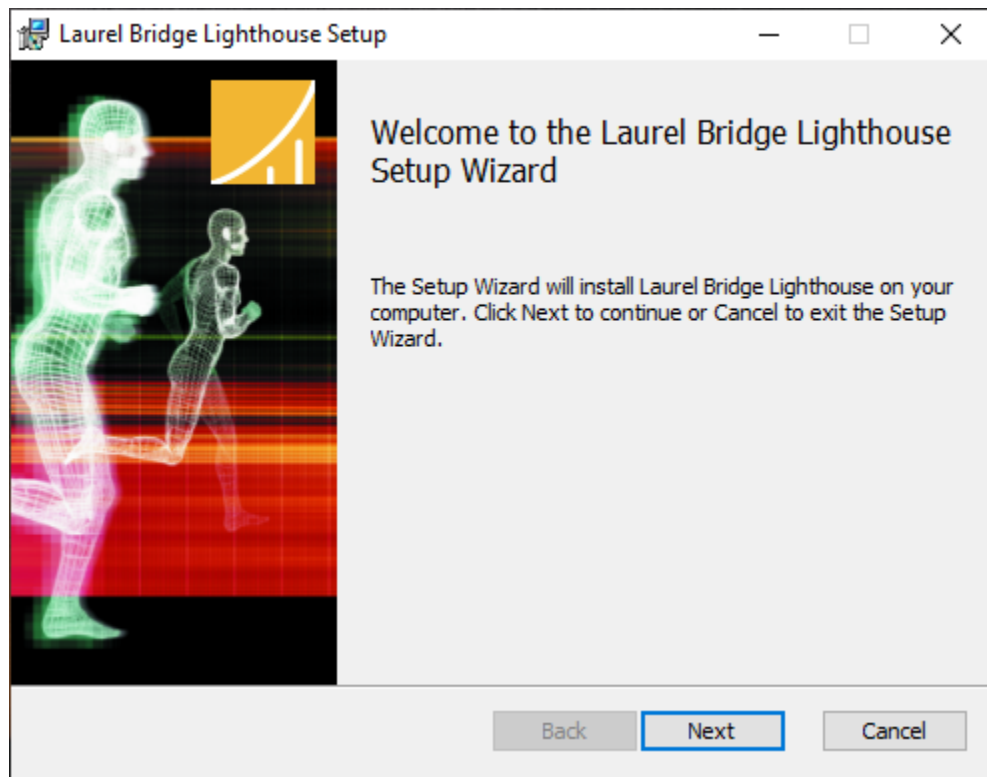
1. Log in to Windows as a user with administrative privileges.
2. Run the [SQL Server 2016 Express x64 with SP2 \(en_sql_server_2016_express_with_service_pack_2_x64_100540591.exe\)](#) installer.
3. On the [Setup](#) screen select [New SQL Server stand-alone installation or add features to an existing installation](#).
4. On the [License Terms](#) screen Accept the license, click the [Next>](#) button.
5. On the [Install Rules](#) screen verify no rules failed, click the [Next>](#) button.
6. On the [Feature Selection](#) screen make sure all the checkboxes are checked for all of the [Instance Features](#). Make sure that the [Management Tools](#) checkboxes are checked, click the [Next>](#) Button.
7. On the [Instance Configuration](#) screen select [Named Instance](#) and enter the instance name, e.g., [SQLEXPRESS2016](#). The [SQL Server Directory](#) is C:\Program Files\Microsoft SQL Server\MSSQL13.<instance id>. Click the [Next>](#) button.
8. On the [Server Configuration](#) screen the defaults should be fine for the [Service Accounts](#) tab and the [Collation](#) tab defaults. Click the [Next>](#) button.
9. On the [Database Engine Configuration](#) screen on the [Account Provisioning](#) tab, select [Windows Authentication Mode](#). 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 two tabs.
 - a. You must also add the 'NT AUTHORITY\SYSTEM' user. Click the [Add...](#) button and type [System](#) into the text box then click the [Check Names](#) button to add to the list and click OK. You should now see 'NT AUTHORITY\SYSTEM (SYSTEM)' in the list of SQL Administrators. Click the [Next>](#) button.
10. Installation should complete in several minutes.

2.4 Installation: Lighthouse Application

After installing the prerequisites, the Lighthouse installer (Lighthouse.msi) can be run. For machines with an older version installed, this installer will upgrade any previous installation while maintaining any current configuration settings.

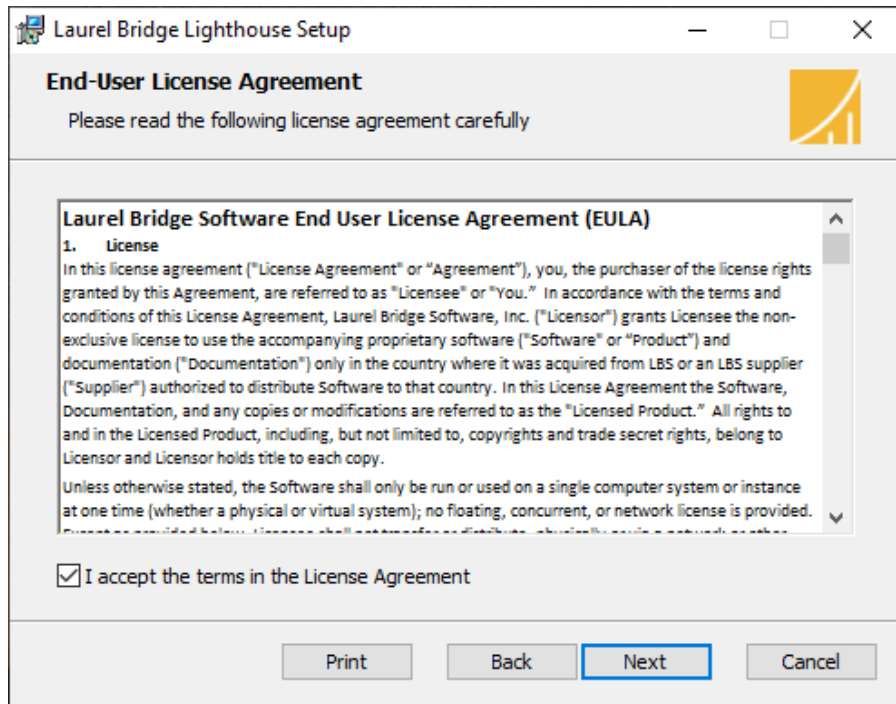
You must have Windows Administrator privileges in order to install Lighthouse correctly.

After launching the Lighthouse installer by double-clicking Lighthouse.msi, the user is greeted with the Welcome screen:



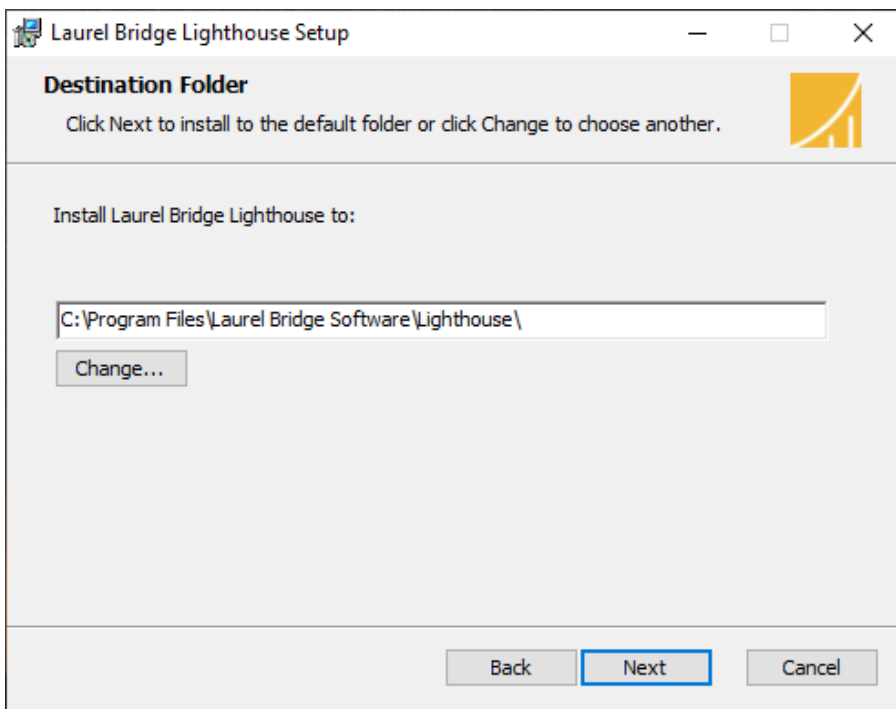
Click the Next button.

The user is then greeted with the License Agreement screen:



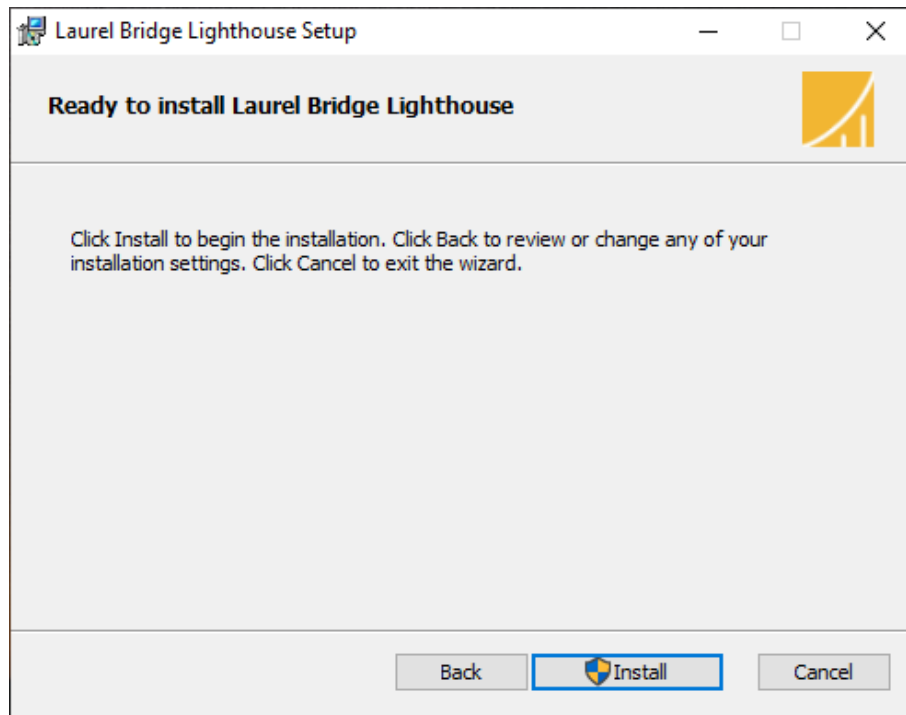
Check 'I accept the terms in the License Agreement' and then press the 'Next >' button.

The user is then greeted with the Installation Location screen:



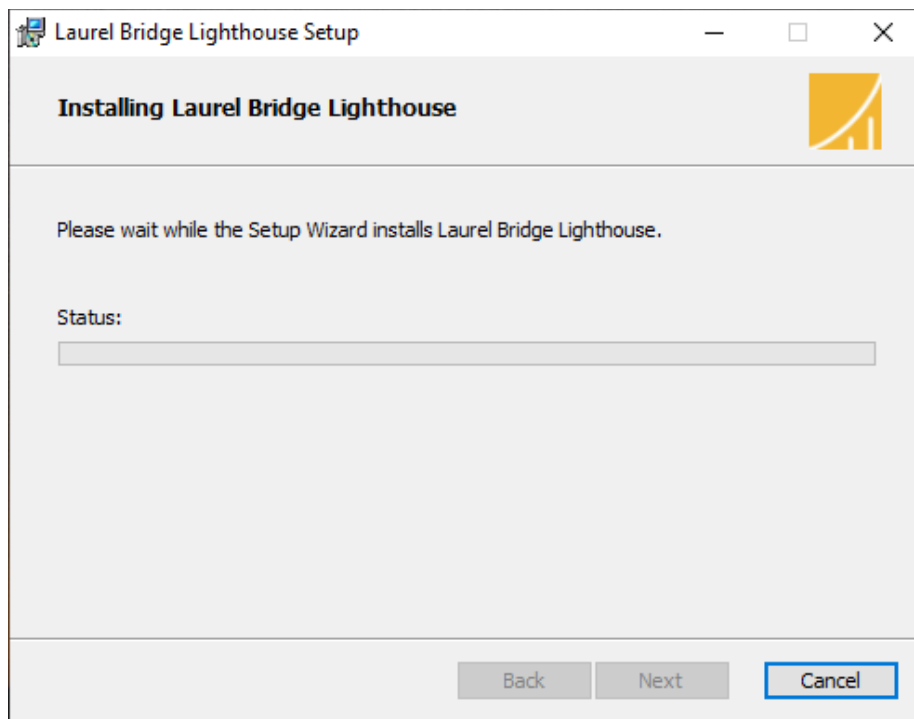
Specify an installation location (the default location is typically the best choice) and then press the 'Next >' button.

The user is then greeted with the ready to install screen:

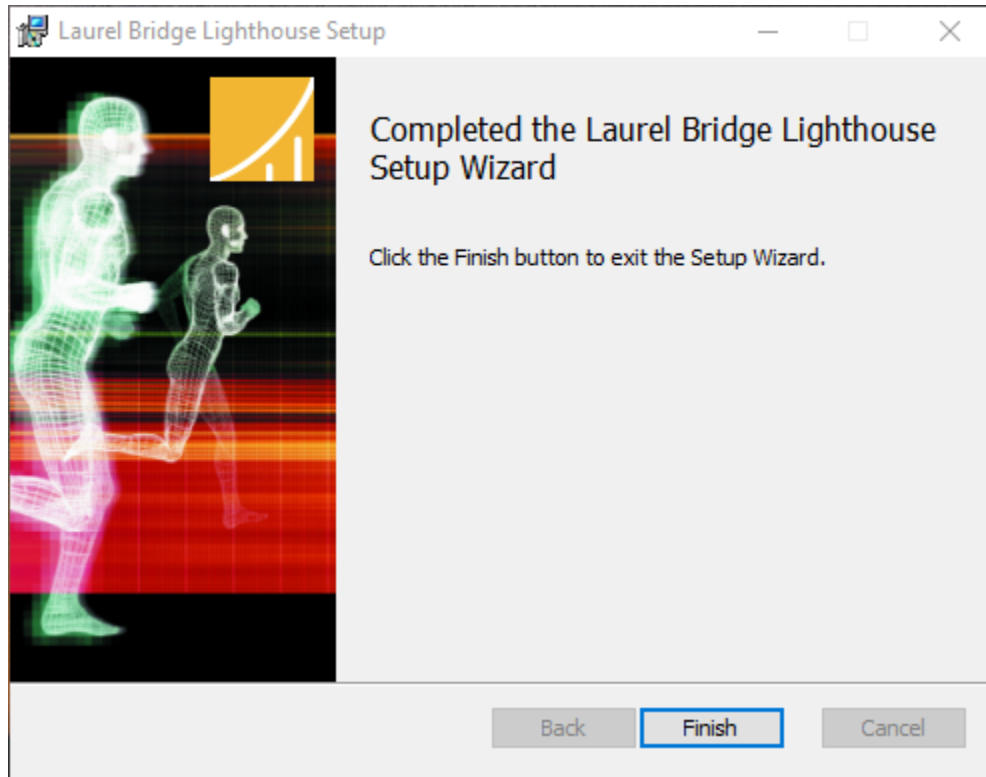


Press the 'Install' button.

The user is then greeted with an installation progress screen:



After installation completes, the user is then greeted with the Installation Complete screen:



Press 'Finish' to complete the installation. The computer should be rebooted after installation.

2.5 Configuring Lighthouse

After installing Lighthouse and rebooting, the Lighthouse Windows Service is running on the default port 10700. Using any web browser, navigate to **<http://localhost:10700>** to view the Lighthouse Web UI. The remainder of this User Manual provides a QuickStart guide for configuring Lighthouse through the Web UI.

3 Workflow Definitions

For Lighthouse to function properly, various workflow configuration items need to be set up correctly. At least one of each of the following types of configuration items must be defined.

3.1 Nodes

Nodes are remote applications that Lighthouse interacts with, retrieving status information and issuing search requests in order to retrieve information.

3.2 Users

A User entry can be created for each user of Lighthouse. There are two predefined users: “Administrator”, and “lighthouse”.

4 Configuration QuickStart

4.1 Access Lighthouse’s Website

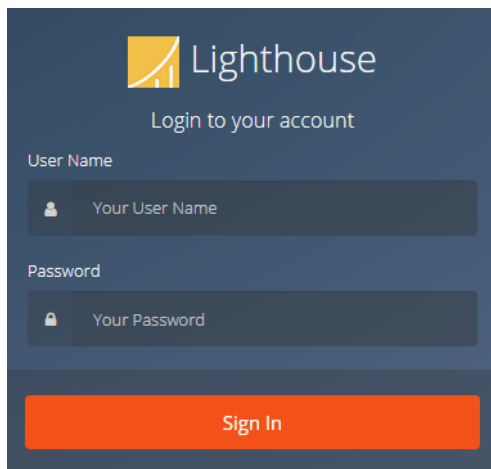
In a web browser, navigate to **http://localhost:10700**

4.2 Log In

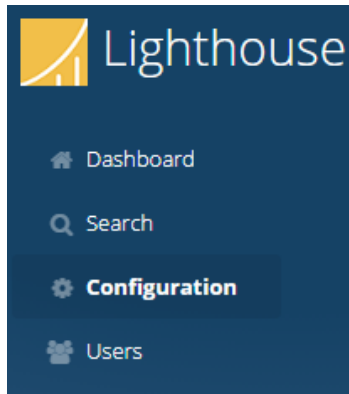
Press the “arrow” icon:



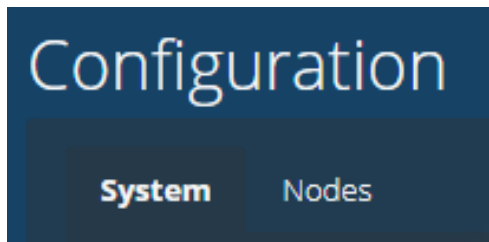
Type in the username “Administrator” (without the quotes) and password “LaurelBridge1234” (without the quotes):

A screenshot of the Lighthouse login interface. It features a dark blue background. At the top left is the Lighthouse logo (a yellow square with a white diagonal line) and the word "Lighthouse" in white. Below the logo is the text "Login to your account". There are two input fields: "User Name" with a placeholder "Your User Name" and a person icon, and "Password" with a placeholder "Your Password" and a lock icon. At the bottom is a large orange button labeled "Sign In".

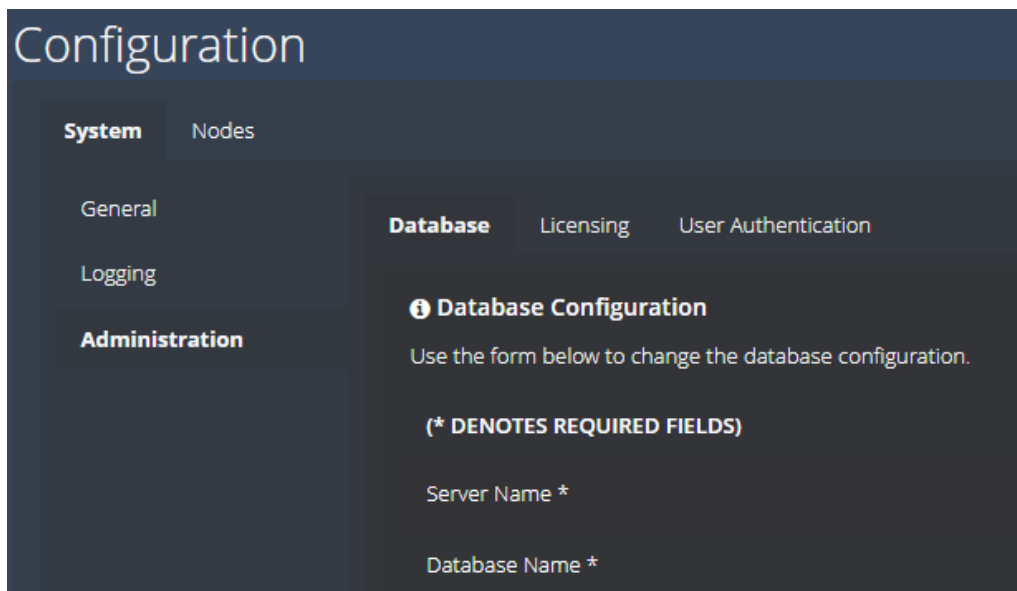
4.3 Click “Configuration”



4.4 Click “System”

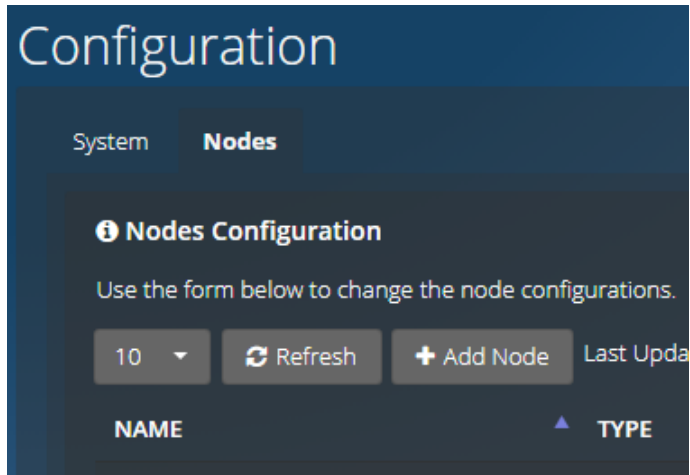


4.4.1 Click “Database” under the “System->Administration” tab



Configure the database settings for your particular scenario.

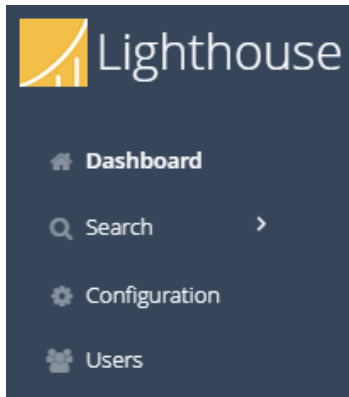
4.5 Click “Nodes”



Add a Node. Assign it a unique name (or acquire the name from the node itself) and specify values for the required fields and, if desired, the optional fields:

- **IP Address:** The IP address of the computer where Compass or Navigator is installed.
- **Port:** Compass, Navigator and Lighthouse communicate status and command information via a protocol called gRPC. Lighthouse must be configured to know the gRPC port that Compass or Navigator is using for gRPC communication. Compass and Navigator contain a Lighthouse Configuration dialog on the System tab; the default value is 54500.
- **URL:** The URL of the Compass or Navigator web interface. Lighthouse displays several URLs for navigating directly to the Compass or Navigator web interface. This value should be a combination of the hostname where Compass or Navigator is running, and the port number specified on the Compass or Navigator System dialog. For example, if Compass is installed on IP address **1.2.3.4**, and the HTTP checkbox is checked and a port number of **10400** has been specified for HTTP, then the url would be **http://1.2.3.4:10400**.
- **Tags:** Zero or more tags may be assigned to a node. This tag name can then be used as a search parameter on the **Dashboard** screen. The same tag can be applied to multiple nodes. For example, the tag **East** can be assigned. On the **Dashboard** screen, the search string **tag:East** would display all nodes labeled with the tag **East**. Multiple tags can also be specified by using AND/OR logic. For example, **tag:East AND Tag:West**

4.6 Click “Dashboard”



Click the “Dashboard” icon on the side of the screen. Note: information on the Dashboard is updated every 30 seconds. It is possible that changes made to the configuration (node addition/deletion/rename, etc.) will not be updated until the next refresh.

5 Web Client: Lighthouse Web Interface Details

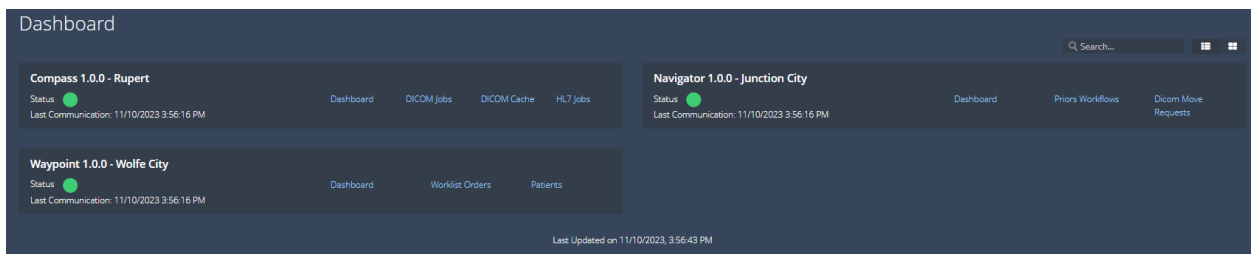
5.1 Dashboard

The Dashboard has two views for displaying the status of defined nodes: **List View**, and **Details View**. The view selection can be made by toggling the two buttons to the right of the Search bar. The Search bar can be used to filter the list of displayed nodes by searching the node names.



5.1.1 Dashboard List View

List View gives a concise list of information for each node:



5.1.2 Dashboard Details View

Details View provides more detailed information on each node.

5.1.2.1 Dashboard Details View - Compass

For Compass, the “play” and “pause” buttons can be pressed to start and stop the Incoming and Outgoing status of DICOM and HL7 input and output. The lower section of the Compass Detail View Dashboard displays two histograms: the number of DICOM Jobs in each state and the number of HL7 Jobs in each state:



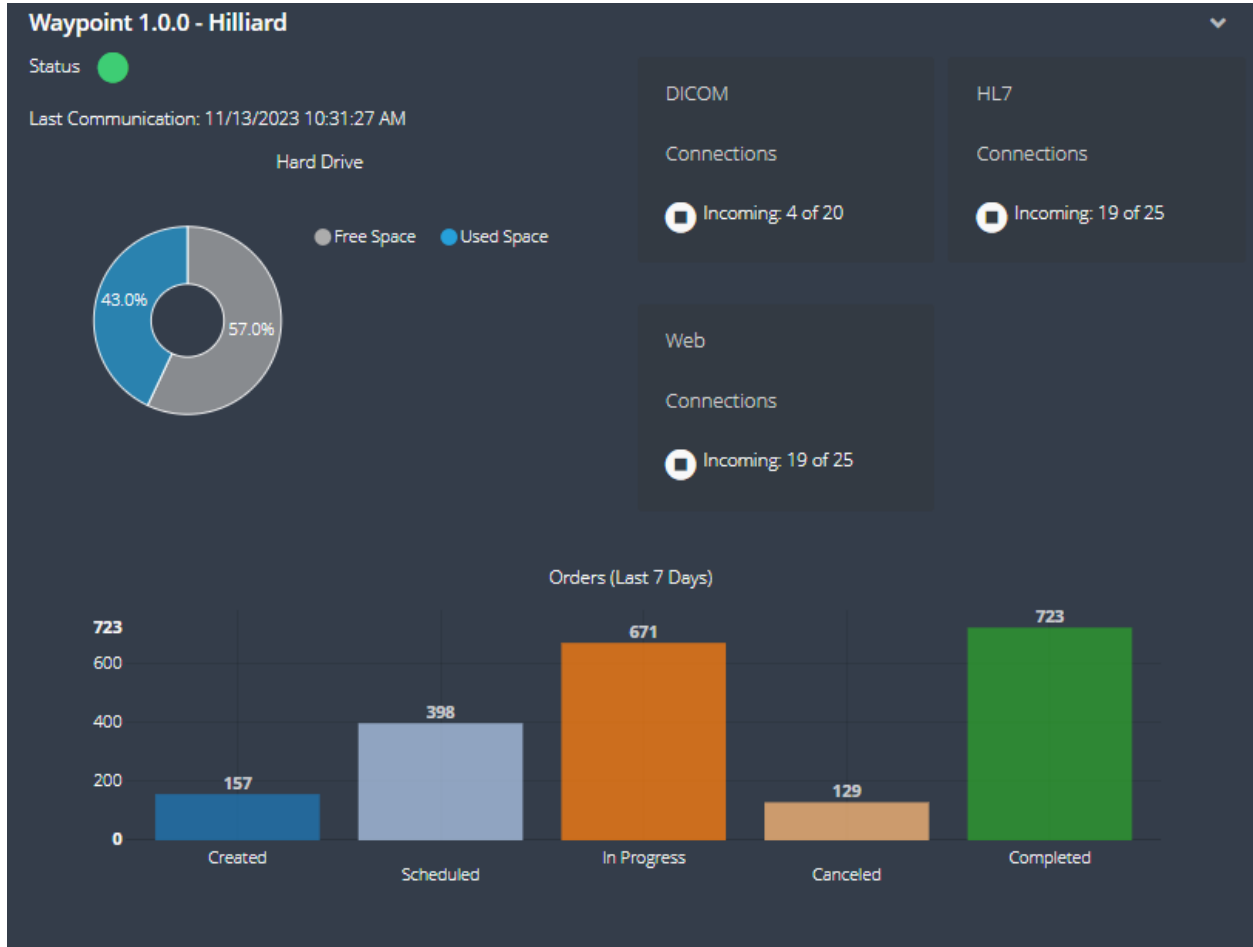
5.1.2.2 Dashboard Details View – Navigator

For Navigator, the “play and “pause” button can be pressed to start and stop the processing of workflows, move requests, and trigger events. The lower section of the Navigator Detail View Dashboard displays two histograms: the number of Priors Workflows in each state and the number of Dicom Move Requests in each state:



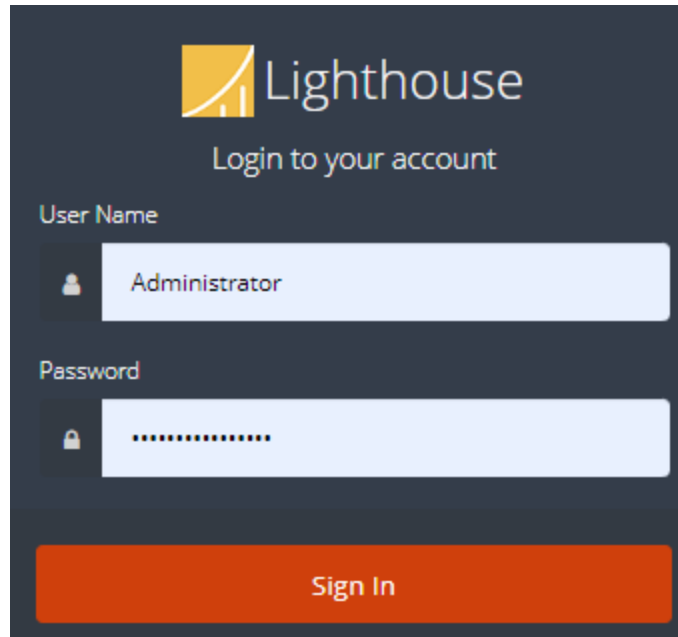
5.1.2.3 Dashboard Details View - Waypoint

For Waypoint, the “play and “pause” button can be pressed to start and stop the Incoming status of DICOM, HL7, and Web input. The lower section of the Waypoint Detail View Dashboard displays one histogram: the number of Worklist Orders in each state:



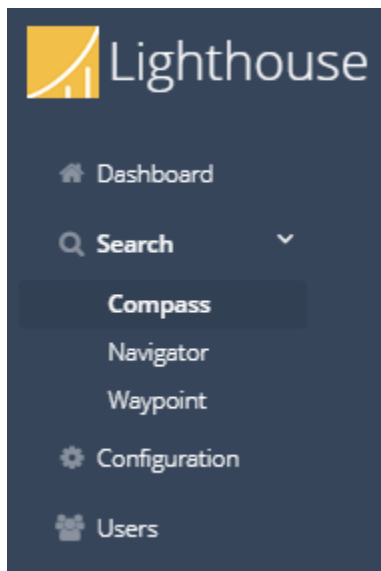
5.2 Login

The [Search](#), [Configuration](#), and [Users](#) pages all require the user to log in. Lighthouse allows administrative accounts to create, edit, and delete application specific usernames, passwords, and roles. Individual users may also manage their own passwords. Alternatively, Active Directory may be configured and used for user authentication and authorization. Either Lighthouse-specific accounts may be used, or Active Directory accounts may be used; they cannot be used simultaneously. See the [System](#) tab on the [Options](#) dialog to configure this functionality.

The image shows the Lighthouse login interface. At the top, there is a yellow Lighthouse logo consisting of a stylized 'L' and the word 'Lighthouse'. Below the logo, the text 'Login to your account' is displayed. The login form has two input fields: 'User Name' with a person icon and 'Password' with a lock icon. The 'User Name' field contains the text 'Administrator', and the 'Password' field contains a series of dots. Below these fields is a large orange button labeled 'Sign In'.

5.3 Search

Lighthouse provides a search screen for Compass, Navigator, and Waypoint as a centralized and convenient way to View, Add, Edit, and Remove items from each of those applications. The **Search** menu is directly below the **Dashboard** menu on the Web UI:



All search screens include a filter to select the data that is displayed. Note, for all filters at least one **Node** must be selected to enable searching.

5.3.1 Compass

The **Compass** search tabs are:

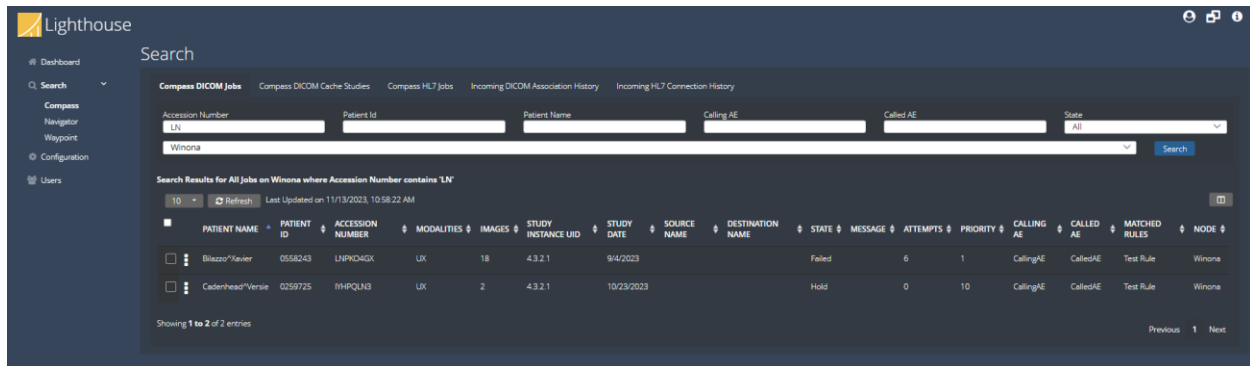
- Compass DICOM Jobs

- Compass DICOM Cache Studies
- Compass HL7 Jobs
- Incoming DICOM Association History
- Incoming HL7 Connection History

5.3.1.1 Compass DICOM Jobs

The **Compass DICOM Jobs** page displays the DICOM jobs that match the search filter. The columns are Patient Name, Patient ID, Accession Number, Modalities, Images, Study Instance UID, Study Date, Source Name, Destination Name, State, Message, Attempts, Priority, Calling AE, Called AE, Matched Rules, and Node. The **More Options** context menu to the right of the selection checkbox contains:

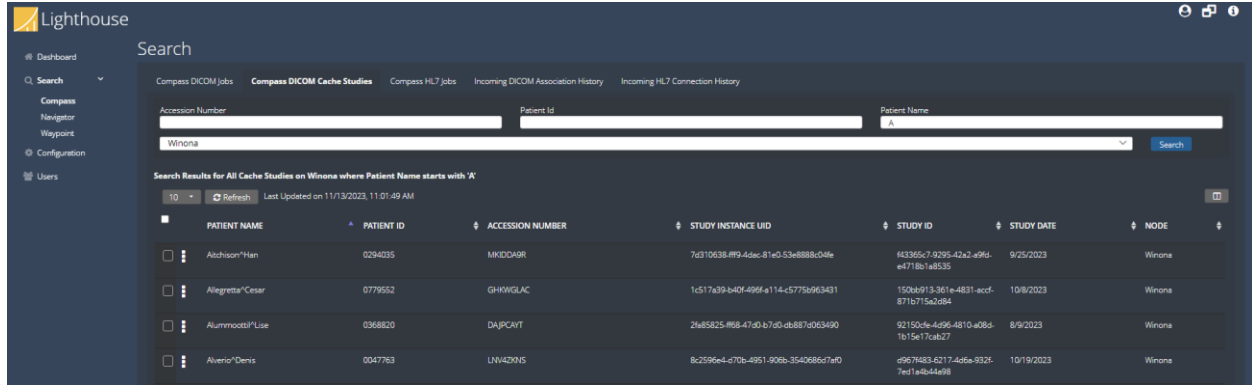
- Copy Selected Row(s) to Clipboard
- Export Selected Row(s) to CSV
- Abort Incoming Associations
- Cancel



5.3.1.2 Compass DICOM Cache Studies

The **Compass DICOM Cache Studies** page displays the DICOM studies currently stored in Compass' cache that match the search filter. The columns are Patient Name, Patient ID, Accession Number, Study Instance UID, Study ID, Study Date, and Node. The **More Options** context menu to the right of the selection checkbox contains:

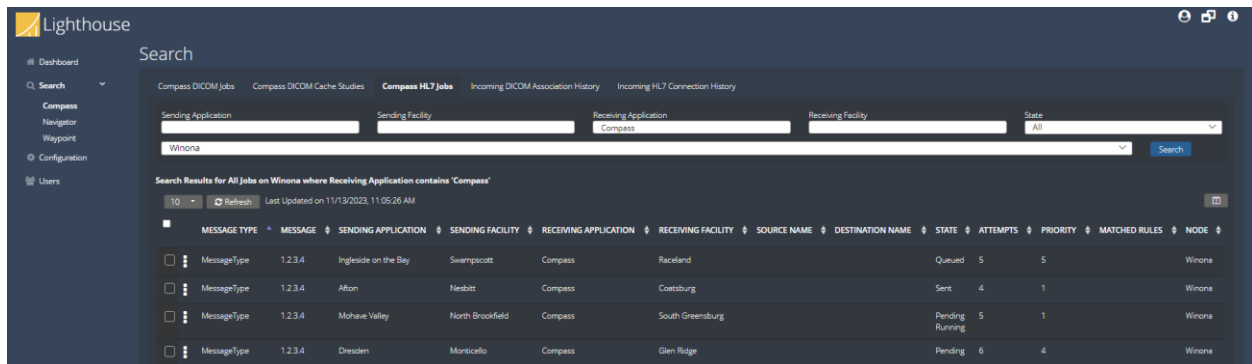
- Send To > list of Compass Destinations
- Move to Penalty Box
- Download Images
- Copy Selected Row(s) to Clipboard
- Export Selected Row(s) to CSV
- Remove



5.3.1.3 Compass HL7 Jobs

The **Compass HL7 Jobs** page displays the HL7 jobs that match the search filter. The columns are Message Type, Message, Sending Application, Sending Facility, Receiving Application, Receiving Facility, Source Name, Destination Name, State, Attempts, Priority, Matched Rules, and Node. The **More Options** context menu to the right of the selection checkbox contains:

- Details
- Hold
- Send to > *HL7 Destination*
- Copy and Send to > *HL7 Destination*
- Set Priority > *Priority Level*
- Copy Selected Row(s) to Clipboard
- Export Selected Row(s) to CSV
- View Job Report
- Remove



5.3.1.4 Incoming DICOM Association History

The **Compass Incoming DICOM Association History** page displays the DICOM associations that match the search filter. The columns are Source Name, Calling AE, Called AE, Host, Session Name, Start Time, End Time, Result, and Node. The **More Options** context menu to the right of the selection checkbox contains:

- Copy

SOURCE NAME	CALLING AE	CALLED AE	HOST	SESSION NAME	START TIME	END TIME	RESULT	NODE
Amloa	Crygla	Compass	192.168.14.154	SessionName	11/11/2023 9:28:57 PM	11/13/2023 10:28:57 AM	Bad Ip Address	Winona
Albany	Waverly Hall	Compass	192.168.14.154	SessionName	11/10/2023 2:28:57 AM	11/13/2023 10:28:57 AM	Bad Calling Title	Winona
Andoch	Mitchell Heights	Compass	192.168.14.154	SessionName	11/12/2023 8:28:57 AM	11/13/2023 10:28:57 AM	Bad Called Title	Winona
Aurora	Hindsboro	Compass	192.168.14.154	SessionName	11/10/2023 6:28:57 AM	11/13/2023 10:28:57 AM	Max Concurrent Associations For Source Exceeded	Winona

5.3.1.5 Incoming HL7 Connection History

The **Compass Incoming HL7 Connection History** page displays the HL7 connections that match the search filter. The columns are Source Name, Host, Connection Type, Start Time, End Time, Result, and Node. The **More Options** context menu to the right of the selection checkbox contains:

- Copy

SOURCE NAME	HOST	CONNECTION TYPE	START TIME	END TIME	RESULT	NODE
Albany	192.168.14.154	IP	11/9/2023 2:28:57 PM	11/13/2023 10:28:57 AM	Max Concurrent Associations For Source Exceeded	Winona
Albany	192.168.14.154	IP	11/10/2023 4:28:57 PM	11/13/2023 10:28:57 AM	Source Is Disabled	Winona
Bainbridge	192.168.14.154	IP	11/11/2023 10:28:57 PM	11/13/2023 10:28:57 AM	Source Is Disabled	Winona
Baldwin City	192.168.14.154	IP	11/12/2023 6:28:57 AM	11/13/2023 10:28:57 AM	Source Is Disabled	Winona
Bayamón zona urbana	192.168.14.154	IP	11/12/2023 7:28:57 PM	11/13/2023 10:28:57 AM	Unknown	Winona

5.3.2 Navigator

The **Navigator** search tabs are:

- Navigator Priors Workflows
- Navigator Move Requests
- Navigator Trigger Event Cache
- Navigator Trigger Event History
- Navigator API Events

5.3.2.1 Navigator Priors Workflows

The **Navigator Priors Workflows** page displays the priors workflow requests messages in a table format. The columns are Patient Name, Patient ID, Accession Number, Patient Birthdate, Patient Sex, SPSS Start Date, Created timestamp, Last Modified timestamp, Scheduled Station AE Title,

Modality, Workflow Name, Rule, Priority, Status, Status Info, Attempts, Trigger Type, and Node. The **More Options** context menu to the right of the selection checkbox contains:

- View Move Requests
- View Trigger Event Payload
- View Priors Info
- View Logs
- View History
- Copy Selected Row(s) to Clipboard
- Export Selected Row(s) to CSV
- Requeue
- Remove

PATIENT NAME	PATIENT ID	ACCESSION NUMBER	PATIENT BIRTH DATE	PATIENT SEX	SPS START DATE	CREATED	LAST MODIFIED	SCHEDULED STATION AE TITLE	MODALITY	WORKFLOW NAME	RULE	PRIORITY	STATUS	STATUS INFO	ATTEMPTS	TRIGGER TYPE	NODE
Strett*Rayford	MADOLINY	RKTYOB	8/27/2023	BLFSQMA4	9/9/2023	11/9/2023 10:28:57 AM	11/13/2023 10:28:57 AM	Lorem Ipsum	UK		Matched Rule	4	Failed	Lorem Ipsum	2	MWL	Manulle
Brackemyne*Bart	GBTLPG	SGFYH4H	8/17/2023	CE4YD2QA	9/9/2023	11/9/2023 10:28:57 AM	11/13/2023 10:28:57 AM	Lorem Ipsum	UK		Matched Rule	4	Init	Lorem Ipsum	8	MWL	Manulle
Patz*Omer	APV5VPA	D5GQJEN	9/19/2023	LUCPHRE	9/26/2023	11/2/2023 10:28:57 AM	11/13/2023 10:28:57 AM	Lorem Ipsum	UK		Matched Rule	4	Init	Lorem Ipsum	20	MWL	Manulle
Korome*Jessie	6CSDQEN6	UWF639S8	10/29/2023	AQBLNDIM	10/17/2023	11/2/2023 10:28:57 AM	11/13/2023 10:28:57 AM	Lorem Ipsum	UK		Matched Rule	4	Init	Lorem Ipsum	2	MWL	Manulle
Batman*Vernie	AB8H+EL1	ZOWFC31	9/30/2023	UC6SLFA	8/21/2023	10/30/2023 10:28:57 AM	11/13/2023 10:28:57 AM	Lorem Ipsum	UK		Matched Rule	4	Interrupted	Lorem Ipsum	13	MWL	Manulle

5.3.2.2 Navigator Move Requests

The **Navigator Move Requests** page displays the move request messages in a table format. The columns are Study Instance UID, Series Instance UID, Accession Number, Patient ID, Source, Destination, Modality, Study Description, Priority, Status, Status Info, Sub-Ops, Created timestamp, Rule, and Node. The **More Options** context menu to the right of the selection checkbox contains:

- View Parent Workflow
- View Logs
- Copy Selected Row(s) to Clipboard
- Export Selected Row(s) to CSV

STUDY INSTANCE UID	SERIES INSTANCE UID	ACCESSION NUMBER	PATIENT ID	SOURCE	DESTINATION	MODALITY	STUDY DESCRIPTION	PRIORITY	STATUS	STATUS INFO	SUB-OPS	CREATED	RULE	NODE
1.2.3.4	4.3.2.1	HWRARKTR	Patid344	Source 1	Dest 2	UX	Lorem Ipsum	4	Interrupted	Lorem Ipsum	85%	11/9/2023 10:28:57 AM		Mainville
1.2.3.4	4.3.2.1	BUZIGCLS	Patid344	Source 1	Dest 2	UX	Lorem Ipsum	4	Init	Lorem Ipsum	85%	11/9/2023 10:28:57 AM		Mainville
1.2.3.4	4.3.2.1	7BPWGBPB	Patid344	Source 1	Dest 2	UX	Lorem Ipsum	4	Completed	Lorem Ipsum	85%	10/21/2023 10:28:57 AM		Mainville
1.2.3.4	4.3.2.1	DKLRKDL	Patid344	Source 1	Dest 2	UX	Lorem Ipsum	4	Queued	Lorem Ipsum	85%	10/23/2023 10:28:57 AM		Mainville
1.2.3.4	4.3.2.1	XJZGZHC	Patid344	Source 1	Dest 2	UX	Lorem Ipsum	4	Delete Requested	Lorem Ipsum	85%	10/20/2023 10:28:57 AM		Mainville

5.3.2.3 Navigator Trigger Event Cache

The **Navigator Trigger Event Cache** page displays the trigger events currently stored in Navigator's trigger event cache. The columns are Key, Created timestamp, Expiration timestamp, Trigger Name, Trigger Type, and Node. The **More Options** context menu to the right of the selection checkbox contains:

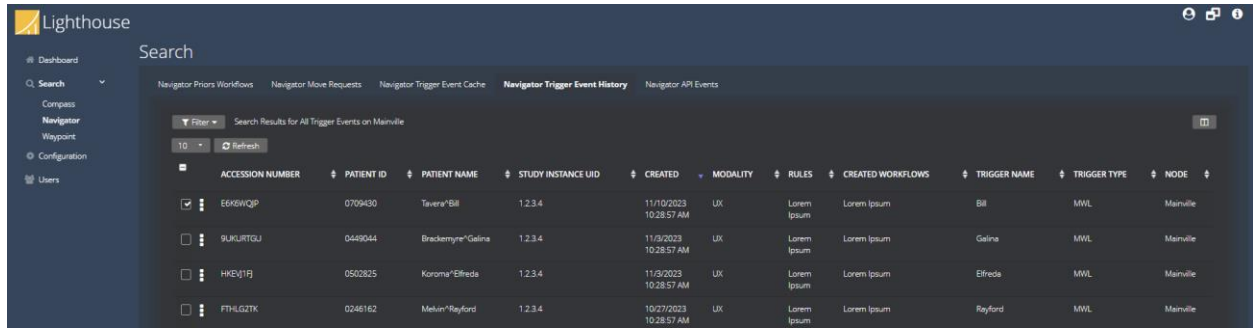
- View Details
- Remove

KEY	CREATED	EXPIRATION	TRIGGER NAME	TRIGGER TYPE	NODE
Ks3Rp4HOHEM30wLeq	11/11/2023 10:28:57 AM	11/10/2023 10:28:57 AM	e3e1Moe81eh8E	CSV	Mainville
ieB1ab2GAaj311m7z	11/11/2023 10:28:57 AM	11/10/2023 10:28:57 AM	YDS259tq4tL7p	RESTful	Mainville
W4MRqOp6WHnHq5	11/11/2023 10:28:57 AM	11/10/2023 10:28:57 AM	cLqgJqHRTYQqN	HL7	Mainville
OM3q9aRwTPMWSFWM	11/11/2023 10:28:57 AM	11/10/2023 10:28:57 AM	wT1BUs6EtUcA	MWL	Mainville
vNncCK3Q4gvG47k9y	11/11/2023 10:28:57 AM	11/10/2023 10:28:57 AM	g1g4e6Vng7drtg	RESTful	Mainville

5.3.2.4 Navigator Trigger Event History

The **Navigator Trigger Event History** page displays the trigger event history that matches the search filter. The columns are Accession Number, Patient ID, Patient Name, Study Instance UID, Created timestamp, Modality, Rules, Created Workflows, Trigger Name, Trigger Type, and Node. The **More Options** context menu to the right of the selection checkbox contains:

- View Payload
- View Logs
- Copy Selected Row(s) to Clipboard
- Export Selected Row(s) to CSV

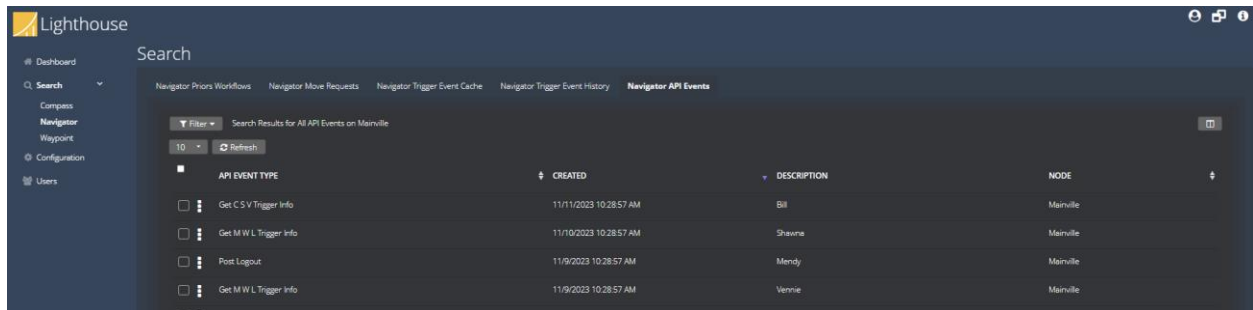


	Accession Number	Patient ID	Patient Name	Study Instance UID	Created	Modality	Rules	Created Workflows	Trigger Name	Trigger Type	Node
<input checked="" type="checkbox"/>	E6K6WQP	0709430	Taverna Bill	1.2.3.4	11/10/2023 10:28:57 AM	UX	Lorem Ipsum	Lorem Ipsum	Bill	MWL	Mainville
<input type="checkbox"/>	9UKJRTGJ	0448044	Brackemyne Gailna	1.2.3.4	11/9/2023 10:28:57 AM	UX	Lorem Ipsum	Lorem Ipsum	Gailna	MWL	Mainville
<input type="checkbox"/>	HKEV1PJ	0503825	Korona Elfreda	1.2.3.4	11/9/2023 10:28:57 AM	UX	Lorem Ipsum	Lorem Ipsum	Elfreda	MWL	Mainville
<input type="checkbox"/>	FTHLGZTK	0246162	Mekin Rayford	1.2.3.4	10/27/2023 10:28:57 AM	UX	Lorem Ipsum	Lorem Ipsum	Rayford	MWL	Mainville

5.3.2.5 Navigator API Events

The **Navigator API Events** page displays the API events that matches the search filter. The columns are API Event Type, Created timestamp, Description, and Node. The **More Options** context menu to the right of the selection checkbox contains:

- Copy Selected Row(s) to Clipboard
- Export Selected Row(s) to CSV



	API Event Type	Created	Description	Node
<input type="checkbox"/>	Get C S V Trigger Info	11/11/2023 10:28:57 AM	Bill	Mainville
<input type="checkbox"/>	Get M W L Trigger Info	11/10/2023 10:28:57 AM	Shawna	Mainville
<input type="checkbox"/>	Post Logout	11/9/2023 10:28:57 AM	Mendy	Mainville
<input type="checkbox"/>	Get M W L Trigger Info	11/9/2023 10:28:57 AM	Vernie	Mainville

5.3.3 Waypoint

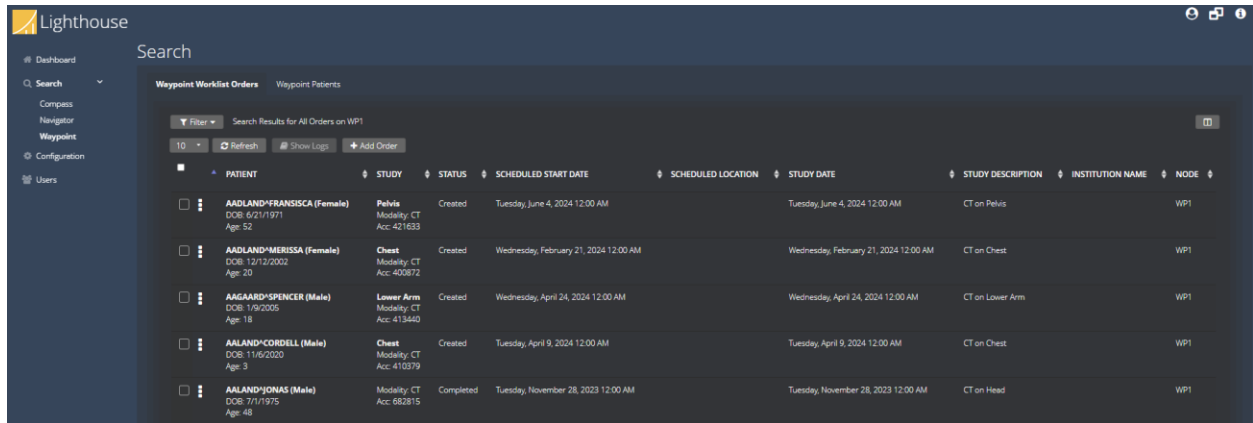
The Waypoint search tabs are:

- Waypoint Worklist Orders
- Waypoint Patients

5.3.3.1 Waypoint Worklist Orders

The **Waypoint Worklist Orders** page displays the worklist orders stored in Waypoint that match the search filter. The columns are Patient, Study, Status, Scheduled Start Date, Scheduled Location, Study Date, Study Description, Institution Name, and Node. The **More Options** context menu to the right of the selection checkbox contains:

- View Messages
- Remove



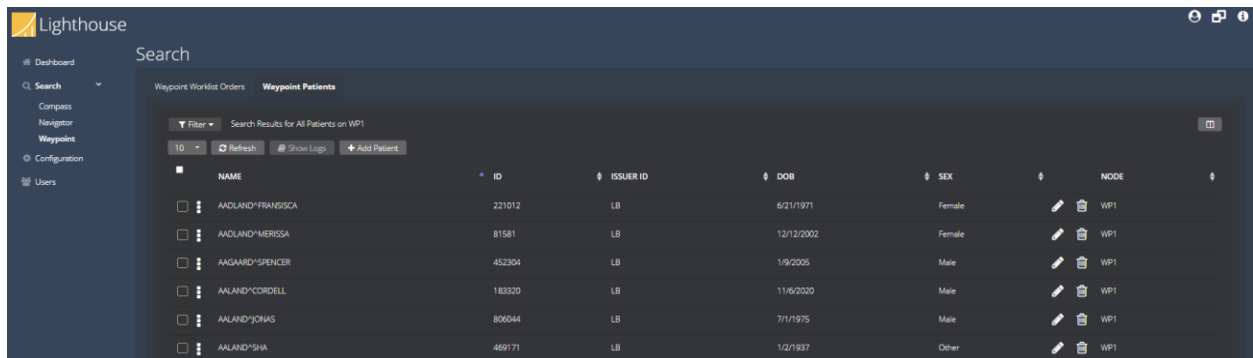
The screenshot shows the 'Waypoint Patients' table in the Lighthouse application. The table has a search bar at the top and a filter dropdown set to 'Filter'. The table columns are: PATIENT, STUDY, STATUS, SCHEDULED START DATE, SCHEDULED LOCATION, STUDY DATE, STUDY DESCRIPTION, INSTITUTION NAME, and NODE. The data rows are as follows:

PATIENT	STUDY	STATUS	SCHEDULED START DATE	SCHEDULED LOCATION	STUDY DATE	STUDY DESCRIPTION	INSTITUTION NAME	NODE
AADLAND*FRANSISCA (Female) DOB: 6/21/1971 Age: 52	Pelvis Modality: CT Acc: 421633	Created	Tuesday, June 4, 2024 12:00 AM		Tuesday, June 4, 2024 12:00 AM	CT on Pelvis		WP1
AADLAND*MERISSA (Female) DOB: 12/12/2002 Age: 20	Chest Modality: CT Acc: 400872	Created	Wednesday, February 21, 2024 12:00 AM		Wednesday, February 21, 2024 12:00 AM	CT on Chest		WP1
AAGAARD*SPENCER (Male) DOB: 1/9/2005 Age: 18	Lower Arm Modality: CT Acc: 413440	Created	Wednesday, April 24, 2024 12:00 AM		Wednesday, April 24, 2024 12:00 AM	CT on Lower Arm		WP1
AALAND*CORDELL (Male) DOB: 11/6/2020 Age: 3	Chest Modality: CT Acc: 410379	Created	Tuesday, April 9, 2024 12:00 AM		Tuesday, April 9, 2024 12:00 AM	CT on Chest		WP1
AALAND*JONAS (Male) DOB: 7/1/1975 Age: 48	Modality: CT Acc: 682815	Completed	Tuesday, November 28, 2023 12:00 AM		Tuesday, November 28, 2023 12:00 AM	CT on Head		WP1

5.3.3.2 Waypoint Patients

The **Waypoint Patients** page displays the patients stored in Waypoint that match the search filter. The columns are Name, ID, Issuer ID, DOB, Sex, and Node. The **More Options** context menu to the right of the selection checkbox contains:

- Edit
- Remove



The screenshot shows the 'Waypoint Patients' table in the Lighthouse application. The table has a search bar at the top and a filter dropdown set to 'Filter'. The table columns are: NAME, ID, ISSUER ID, DOB, SEX, and NODE. The data rows are as follows:

NAME	ID	ISSUER ID	DOB	SEX	NODE
AADLAND*FRANSISCA	221012	LB	6/21/1971	Female	WP1
AADLAND*MERISSA	81581	LB	12/12/2002	Female	WP1
AAGAARD*SPENCER	452304	LB	1/9/2005	Male	WP1
AALAND*CORDELL	183320	LB	11/6/2020	Male	WP1
AALAND*JONAS	806044	LB	7/1/1975	Male	WP1
AALAND*SHA	469171	LB	1/2/1937	Other	WP1

5.4 Configuration

The Configuration tabs are:

- System
- Nodes

5.4.1 System Configuration

System-wide settings for Navigator can be configured via the **Configuration > System** tab. The **System** tab contains three sub-menus:

- General
- Logging: Application and Audit Log
- Administration

5.4.1.1 General

The **General** section specifies the host names and ports that are used to communicate with Lighthouse.

The screenshot shows the 'Configuration' window with the 'General' tab selected. The left sidebar has 'System' and 'Nodes' tabs, with 'General' highlighted under 'System'. The main area is titled 'General Configuration' and contains a form with the following fields: 'Title' (empty), 'Description' (192.168.14.154), 'TLS Certificate Configuration' (empty), 'TLS Certificate File Path' (empty), 'Password' (empty), 'Application Web Interface' (empty), 'Hostnames' (localhost, bicomme2021), 'HTTP' (10700, enabled), 'HTTPS' (10701, disabled), and 'Disable HTTP/2' (disabled). A 'Save' button is at the bottom right.

5.4.1.2 Logging

The **Logging** configuration tabs are:

- Application Logging
- Audit Log

5.4.1.2.1 Application Logging

The **Application Logging** section specifies the file paths and verbosity level used for logs messages for the Lighthouse application.

The screenshot shows the 'Configuration' window with the 'Application Logging' tab selected. The left sidebar has 'System' and 'Nodes' tabs, with 'Application Logging' highlighted under 'System'. The main area is titled 'Application Logging Configuration' and contains a form with the following fields: 'Directory' (C:\ProgramData\Laurel Bridge Software\Lighthouse\Logs), 'Filename Prefix (Xlog)' (LighthouseService), 'Max File Size in KB' (1024), 'Number of Files' (10), and 'Log Verbosity' (Terse). A 'Save' button is at the bottom right.

5.4.1.2.2 Audit Log

The **Audit Log** section specifies whether to enable audit logging and the parameters to connect with the Windows Audit Event logger.

The screenshot shows the 'Configuration' page with the 'System' tab selected. The 'Audit Log' sub-tab is active. The page title is 'Configuration'. On the right, there is a 'Snapshot Configuration' button. The left sidebar has 'System' and 'Nodes' tabs, with 'System' containing 'General', 'Logging', and 'Administration'. The 'Audit Log Configuration' section includes a description: 'Use the form below to change the audit log configuration.' Below this, a note states '(* DENOTES REQUIRED FIELDS)'. The configuration fields are: 'Enabled' (checkbox, checked), 'Host/IP' (text input), 'Transport *' (dropdown menu showing 'UDP'), 'Port' (text input showing '514'), 'Site ID' (text input), 'Suppress PHI From Application Logs' (checkbox, checked), 'Enable TLS 1.0' (checkbox, checked), 'Enable TLS 1.1' (checkbox, checked), 'Enable TLS 1.2' (checkbox, checked), 'Ignore Certificate Name Mismatch Errors' (checkbox, checked), 'Allow Self-Signed Certificates' (checkbox, checked), and 'Message Types to Log' (checkboxes for 'Application Start/Stop', 'Software Configuration (Input/Output Start/Stop)', and 'User/Security Alerts', all checked). A 'Save' button is at the bottom right.

5.4.1.3 Administration

The **Administration** tabs are:

- Database
- Licensing
- User Authentication

5.4.1.3.1 Database

The **Database** section specifies the parameters to connect with the SQL Server database.

The screenshot shows the 'Configuration' page with the 'System' tab selected. The 'Database' sub-tab is active. The page title is 'Configuration'. On the right, there is a 'Snapshot Configuration' button. The left sidebar has 'System' and 'Nodes' tabs, with 'System' containing 'General', 'Logging', and 'Administration'. The 'Database Configuration' section includes a description: 'Use the form below to change the database configuration.' Below this, a note states '(* DENOTES REQUIRED FIELDS)'. The configuration fields are: 'Server Name *' (text input showing '.\SQLEXPRESS'), 'Database Name *' (text input showing 'Lighthouse'), 'Connection Timeout in Seconds *' (text input showing '15'), 'Long Query Timeout in Seconds *' (text input showing '180'), 'Short Query Timeout in Seconds *' (text input showing '30'), 'Max Connection Pool *' (text input showing '100'), 'Encrypt Connection' (checkbox, checked), 'Trust Server Certificate' (checkbox, checked), 'Trusted Connection' (checkbox, checked), 'Username' (text input), and 'Password' (text input). A 'Save' button is at the bottom right.

5.4.1.3.2 Licensing

The **Licensing** section specifies the parameters to install or activate the Lighthouse license.

The screenshot shows the 'Configuration' page with the 'System' tab selected and the 'Licensing' sub-tab active. The left sidebar shows 'Administration' as the selected category. The main content area is titled 'Licensing' and includes a description: 'Use the form below to change your licensing information.' Below this is a note: '(* DENOTES REQUIRED FIELDS)'. The form contains several fields: 'Product' (empty), 'Name' (filled with 'Lighthouse'), 'Version' (filled with '3.0.0'), 'Product Serial Number *' (filled with 'AAAA-BBBB-CCCC-DDDD'), 'ARC' (filled with 'C05E-A637-24EA-7237'), 'MAC' (empty), 'User' (empty), 'Site *' (filled with 'LBS WHQ'), 'Contact *' (filled with 'Contact Name'), 'Email *' (filled with 'Contact@mailserver.com'), 'Host Name *' (filled with 'myhostname'), and 'Maintenance' (empty). A 'Snapshot Configuration' button is visible in the top right corner.

5.4.1.3.3 User Authentication

The **User Authentication** section specifies the parameters to pass to LDAP/Active Directory for authenticating login accounts that are not locally administered by Lighthouse.

The screenshot shows the 'Configuration' page with the 'System' tab selected and the 'User Authentication' sub-tab active. The left sidebar shows 'Administration' as the selected category. The main content area is titled 'User Authentication Configuration' and includes a description: 'Use the form below to change the user authentication configuration.' Below this is a note: '(* DENOTES REQUIRED FIELDS)'. The form contains several fields: 'Authentication Type *' (a dropdown menu set to 'Local'), 'LDAP / Active Directory' (empty), 'Domain Name' (empty), 'Base DN' (empty), 'Username' (empty), 'Password' (empty), 'Admin Role CN(s)' (empty), 'User Role CN(s)' (empty), 'View Role CN(s)' (empty), 'Test' (a button labeled 'Test'), 'Options' (empty), 'User Timeout in Minutes *' (filled with '10'), 'Allow Simultaneous Logins of the Same User' (checkbox), 'Display Login Banner' (checkbox with a 'Configure' button), and 'Require Secure Passwords' (checkbox). A 'Snapshot Configuration' button is visible in the top right corner.

5.5 Users

The **Users** section displays the user logins that are locally administered by Lighthouse. Users can be added, edited, or removed from the **Users** configuration screen.

Appendix A: Lighthouse Privacy and Security Statement

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

An overview of the Lighthouse application privacy and security features is given in the sections below, roughly following the format given in the HIMSS/NEMA Standard HN 1-2013, “Manufacturer Disclosure Statement for Medical Device Security”, or MDS2 for short. For more details about this form or to download it, see <http://www.himss.org/resource/library/MDS2> (NEMA Document ID: 100382).

The headers in the following sections map directly to the headers in the MDS2 document. The Lighthouse MDS2 document for a particular release is available upon request from LBS.

1 Management of Private Data

Laurel Bridge Lighthouse is a centralized management tool that allows users to view the status and information of remote applications, referred to as nodes. Lighthouse retrieves data that may contain protected health information (PHI) for display purposes only. The data is not maintained or stored by Lighthouse, and thus is not maintaining part of the designated record set (as defined by HIPAA). Also, the Lighthouse 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 Lighthouse is able to retrieve 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
- Patient financial information

1.2 Persistence of Private Data

Lighthouse maintains PHI only temporarily in memory (while running) and does not store this data 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 Lighthouse User Manual.

Note: Due to the sensitive nature of the PHI that Lighthouse handles, the only non-destructive and completely safe way to decommission a (non-virtual) computer system on which a production Lighthouse 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) may be sufficient.

1.3 Transmission of Private Data

PHI can be transmitted or received over the network when requesting Lighthouse to view DICOM, HL7, or other messages. The ability to configure and control the behavior of this functionality is under the full control of the Lighthouse 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 Lighthouse User Manual. Because Lighthouse 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 Lighthouse application is comprised of two parts:

1. **Lighthouse Service**, which runs as a Windows Service
2. **Lighthouse Web**, a web interface that allows configured web users to monitor and manage nodes.

The following sections briefly describe available security features of the Lighthouse application.

2.1 Automatic Logoff

The Lighthouse Web interface can be configured to automatically log off Lighthouse users in a configurable number of minutes. The default timeout is 10 minutes, and the timeout can be configured to any value from 1 minute to 65536 minutes. Note that enabling the web auto-refresh functionality on the status screen disables the web user auto-logoff.

2.2 Audit Controls

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

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

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

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

- **Application Activity**
 - Application Start
 - Application Stop
- **Security Alert**
 - Security Configuration
 - Software Configuration
 - User Security Attributes Changed
- **User Authentication**
 - Login
 - Logout

2.3 User Authorization

The Lighthouse Web users can either be locally administered (by the Lighthouse Web module), or they can be administered using LDAP / Active Directory. This is done by the Lighthouse

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

2.5 Security Updates

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

2.6 De-Identification of PHI

Lighthouse does not support the ability to configure de-identification of PHI. Lighthouse displays DICOM or HL7 messages as they are provided by the node.

2.7 Backup and Restore

The Lighthouse customer has full responsibility to both install and maintain the SQL Server database which provides the data storage for Lighthouse user logins only. 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 Lighthouse customer has full control over the installation and configuration of both the host system and the Lighthouse 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 Lighthouse is to display data that was generated by DICOM and HL7 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 Windows Authentication to ensure that unauthorized Windows users cannot access the host Windows system on which Lighthouse is installed.

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

Lighthouse 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 the SQL Server database repository.

2.10 Malware Protection

Since the Lighthouse customer has full control over the installation and configuration of both the host Windows system and the Lighthouse application itself, it is up to the customer to install and maintain malware protection technology. Lighthouse 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 network router performance, it is generally recommended that antivirus checking be turned off for the SQL data directories used by Lighthouse.

2.11 Node Authentication

Node authentication (the ability to confirm the identity of both the sender and receiver of DICOM and HL7 data) can be implemented using TLS protocol on the network connection. Lighthouse supports TLS as a client to the node. Secure Connections can be enabled on the Lighthouse node configuration. The node that has Lighthouse communication enabled, e.g., Compass, Navigator, or Lighthouse, can enable TLS on the Lighthouse Settings. Nodes that are not Laurel Bridge applications can also enable TLS on their Lighthouse communication settings. More details about how to do this and further security details can be found elsewhere in this Lighthouse User Manual.

2.12 Person Authentication

As mentioned earlier, user authentication for the host Windows system can be controlled locally, using a domain with technology such as LDAP / Active Directory. 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 only two default accounts, “administrator” and a view-only user “Lighthouse”). 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 the default behavior is to only allow a user to log on from a single computer at a time. Local users’ passwords cannot currently be configured to expire.

2.12.2 LDAP Enabled Web User Administration

When web users are administered with LDAP Enabled, the rules regarding users and passwords are up to the LDAP/AD 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 Lighthouse customer owns and has full control over the host Windows system on which Lighthouse is installed, it is up to the customer to maintain the physical security of the host system.

2.14 Device Life Cycle Roadmap

The Lighthouse application currently supports the following Windows operating systems:

- Windows 10 or newer
- Windows Server 2016 or newer

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

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

- SQL Server (can be 2016 x64 or newer)
- SQL Server Management Studio
- .NET 6.0

See section 2.2 Minimum System Specification and section 2.3 Prerequisites.

2.15 System and Application Hardening

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

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

- Use of Authenticode digital signatures (currently SHA256) for all LBS executables and DLLs
- Support for TLS encryption for data in transit
- 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 Lighthouse 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
- Enabling of Windows password-protected, inactivity-activated screen lockout
- 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 Lighthouse application are described in detail in this Lighthouse User Manual.

2.17 Data Storage Confidentiality

Lighthouse does not encrypt data while at rest on the hard drive(s). PHI is stored both in the SQL Server database, as well as in the cached data files. 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. Lighthouse 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

Lighthouse can be configured to encrypt data in transit (using TLS), which will protect the data against interception by unauthorized parties. And as mentioned above, Lighthouse 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., via man-in-the-middle attacks). Lighthouse will only transmit data to destinations that have been explicitly configured within the application by the customer.

2.20 Other Security Considerations

Lighthouse can be serviced remotely by LBS only with the express permission of the Lighthouse customer, as access to the host system onto which Lighthouse is installed is completely controlled by the customer. Lighthouse does not contain any service backdoors, nor does it contain any secret service accounts. All LBS access to an installed Lighthouse 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 Lighthouse application. Note that these can all be changed by the Lighthouse customer, if so desired.

- HTTP port = **10700** (**10701** 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 Lighthouse 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 Lighthouse 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.
- 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.