Laurel Bridge Waypoint
User Manual

Orchestrating Medical Imaging Workflow

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

Document Version: : 1.12.1
Document Number: LBDC-000112-011201
Last Saved: 1/15/2024 11:11:00 AM

Table of Contents

1 Waypoint Server Basics

1.1 Overview

Waypoint is a repository for Modality Worklist (MWL) orders. MWL Orders generally contain the following data:

- Patient Identifier
  - Patient ID (a.k.a. MRN medical record number)
  - Patient Name
- Patient Demographics
  - Date and Time of Birth
  - Patient Sex
  - Patient Address
  - Patient Account Number
- Scheduled Procedure Step Sequence
  - Scheduled Station AE Title
  - Scheduled Procedure Step Start Date
  - Scheduled Procedure Step Start Time
  - Modality
  - Scheduled Performing Physician
  - Scheduled Procedure Step Description
- Study Instance UID
- Study Date
- Study Time
- Accession Number
- Requested Procedure Description

The purpose of Waypoint is to provide services to allow clients on the network to create, query and update the worklist items. The design and analysis provided by this document, focuses on, but is not restricted to, the following protocols:

- DICOM DIMSE Messages
  - Modality Worklist Information Model - FIND
  - Unified Procedure Step
  - Modality Performed Procedure Step
- HL7 ORM, ORU and ADT messages
- HTTP RESTful services

The traditional DICOM modality workflow management is to create and update worklist items by transmitting HL7 messages from the HIS and RIS to a Modality Worklist Server (MWL Server). The modalities use the DICOM Modality Worklist Information Model – FIND, to query the MWL Server to retrieve scheduled procedures.

The DICOM Modality Performed Procedure Step allows the modality to N-GET and N-SET data from the worklist item. Also, the DICOM standard specifies the Unified Procedure Step to create and acquire worklist data. The Unified Procedure Step is also specified as a Web Service.

This document describes Waypoint in phases as follows:

- Modality Work List Server
    - Windows Service
    - Installer
    - DCF 3.4
    - HL7 Library
    - Web Interface
    - Active Directory, LDAP, and Standalone security credentials, i.e. username and password
    - HTTP RESTful Interface
    - Audit Logging
- Configuration
    - SQL Server
    - DICOM Options
    - HL7 Options
    - DICOM Web Services
- Data Inputs
    - DIMSE Messages
    - HL7 Messages
    - HTTP RESTful Web Messages
- Data Outputs
    - DICOM MWL SCU
    - HTTP RESTFUL
    - WEB Service
    - SQL ODBC

1.2 Use Cases

Use Cases are a UML modeling tool to specify the subject, i.e. Waypoint, the actors that communicate with the subject, and the interactions between the two. This analysis helps identify the boundary interfaces between the actors and the system. Actors are humans, as well as external systems that exchange signals and data with the subject. A use case is the specification

of a set of actions performed by a system, which yields an observable result that is, typically, of value for one or more actors or other stakeholders of the system. For this system, the Actors are:

- Hospital Admissions
- Referring Physician
- Performing Physician
- Modality
- Clinician
- MWL SCU (e.g. Navigator)
- PACS/Image Store
- HIS/RIS
- Service IT
- Software Developers

Waypoint can be used in conjunction with other Laurel Bridge products. These products share many of the same Use Cases listed above. PowerTools is used to test the boundary interfaces defined by the use cases. Compass, Navigator and Exodus can benefit from the services provided by Waypoint.

- Power Tools
  - Query Client
  - Store Server
  - HL7 Sender
  - HL7 Receiver
  - MWL Server Console
- Compass
- Navigator
- Exodus

1.2.1 Hospital Admissions Use Cases

Hospital Admissions has the following Use Cases:

- Query for a Patient Record
- Create New Patient Record

A Patient Record contains the following data:

- Patient's Name
- Patient ID (a.k.a. MRN medical record number)
- Patient's Birth Date
- Patient's Sex

The Patient's Name and Patient ID are qualified together as the Patient Identification. We cannot assume that the Patient ID alone is a primary key. Patient's Birth Date and Patient's Sex are qualified as patient demographics. Waypoint will generate a unique primary key for each patient record that is stored.

1.2.2 Referring Physician Use Cases

Referring Physician has the following Use Cases:

- Submit New Order
- Cancel Existing Order
- Update Existing Order

An Order contains the following data:

- Patient Identifier
  - Patient ID
  - Patient Name
  - Date and Time of Birth
  - Patient Sex
  - Patient Address
  - Patient Account Number
- Scheduled Procedure Steps
  - Scheduled Station AE Title
  - Scheduled Procedure Step Start Date
  - Scheduled Procedure Step Start Time
  - Modality
  - Scheduled Performing Physician
  - Scheduled Procedure Step Description
- Accession Number
- Study Instance UID
- Requested Procedure Description

This use case is the triggering event to create a new patient order. DICOM defines the Unified Procedure Step SOP Class for creating and updating orders. Also, DICOM offers the Modality Performed Procedure Step (MPPS) to update orders. However, the most common message to create a patient order is the HL7 ORM^O01. The first field in the Common Orders segment is Order Control ORC|1. This defines whether to interpret the message as a new order, update, or cancel.

VALUE	Scheduled Status
NW	1 – New Order Created
OK	2 – Scheduled at a modality

IP	3 – In-Progress
CA	4 - Cancel order/service request
CM	5 – Order is completed

1.2.3 Performing Physician/Clinician Use Cases

The Performing Physician has the following Use Cases:

- Query for today's orders
- Assign Orders to Modalities
- Initiate Modality to Create Study/Series/Images

These use cases are focused on querying Waypoint for new orders that are being scheduled to begin processing. This necessitates that each order has a state to distinguish new orders from, in process, complete, cancelled, etc… This ties into Modality Use Cases that will update the state of the worklist item.

1.2.4 Modality Use Cases

The Modality has the following Use Cases:

- Query Worklist to Prefetch today's orders
- Send Modality Performed Procedure Step (MPPS) to MWL SCP
- Update state of worklist item from scheduled, processing, complete, failed, etc…

A Modality Performed Procedure Step has the following data:

- Patient's Name
- Patient ID
- Patient's Birth Date
- Patient's Sex
- Referenced Patient Sequence
    - Referenced SOP Class UID
    - Reference SOP Instance UID
- Scheduled Step Attribute Sequence
    - Study Instance UID
    - Accession Number
    - Scheduled Procedure Step Description
- Performed Procedure Step Start Date
- Performed Procedure Step Start Time

The Modality is the actor that accepts a worklist order and is responsible to notify Waypoint with any changes to the status.

1.2.5 MWL Query Use Cases

As noted earlier, Waypoint does not yield results that are directly observed by the Radiologist. However, viewing stations are often coupled with a prefetch engine, such as Navigator, that may incorporate an MWL query to resolve the list of relevant prior exams. The MWL query searches for worklist items by matching patient demographics and scheduled procedures to retrieve the Study Instance UID from prior exams. Those studies are copied to a viewing station by requesting a C-MOVE from the store server to the viewing station. To accomplish this, Waypoint is coupled with one or many Store Servers. The coupling between Waypoint and Store Server is loose, meaning the Store Server is a separate device, commonly known as a VNA, (Vendor Neutral Archive). Historically, a PACS implemented both the Modality Worklist (MWL) and the Store Query/Retrieve Servers. The Store Server is a Boundary interface to Waypoint. A software tool that includes an MWL query client has the following use cases:

- Query for exams for a date range, e.g. today's exams
- Query for relevant priors for a given patient
- Query for a patient ID to retrieve additional data, such as the Issuer of Patient ID

1.3 Theory of Operation

The primary scope of Waypoint is to provide the Workflow Management category SOP Classes as defined in DICOM PS3.2 2018c – Conformance. Note, the Waypoint DICOM Conformance Statement is available as a separate document. In addition to DICOM, Waypoint offers additional features that are compliant with HL7 and IHE to provide features for external interfaces that are not DICOM based. The Use Cases in the previous section define actors that are DICOM devices, as well as actors that populate and query worklist data using HL7 and HTTP RESTful protocols.

At the heart of Waypoint is a SQL Server database that maintains the persistent data for the worklist items. The system settings, configuration, Application Program Interfaces (APIs), User Interfaces (UI), and security are all tied to populating and querying the SQL database. Clients of Waypoint fall into 3 categories:

1. DICOM SCU
2. HTTP Client (includes DICOM RESTful Services)
3. HL7 Sender

To support these clients, Waypoint has system requirements for DICOM server, HTTP server, and HL7 server that provide the following:

- Starting and stopping the server
- Configuring the server
- Monitoring the server
- Sending notifications from the server

1.3.1 DICOM Service Class Providers

The DICOM Service Class Providers implemented by Waypoint are:

- Verification
- Modality Performed Procedure Step
- Modality Performed Procedure Step Retrieve
- Modality Worklist Information Model – FIND
- Unified Procedure Step – Push
- Unified Procedure Step – Pull

1.3.2 DICOM Service Class Users

Waypoint maintains a database of MWL orders, as well as providing access to federated external Modality Worklist Providers on the hospital network. When Waypoint receives a query message, DICOM Rules provide options to query the local database and/or multi-plex the request to remote MWL Service Class Providers that are configured as Selected DICOM Worklist Provider destinations. See **section 4.3 Creating DICOM Rules** for further information about creating DICOM Rules to control how incoming MWL C-Find requests are processed.

1.3.3 HL7 Receiver

As a basic introduction, the primary data stream for worklist data is HL7 messages transmitted from the Hospital Information System and Radiology Information Systems (HIS/RIS). It is common to use the HL7 ORM^O01 messages to create and update worklist orders. Note, in some cases there is a direct correlation between a field in the HL7 message and the DICOM tag, however, many fields require additional filtering to map the value from the HL7 message to the DICOM item.

The Waypoint HL7 Receiver parses HL7 messages to insert or update worklist items into the SQL database. Each HL7 message has a message type in a message header field, typically field MSH|9. Handling of HL7 messages must be flexible and extensible to support the workflow of the hospital information systems (HIS/RIS). Waypoint configuration defines HL7 Sources, HL7 Rules, and HL7 MWL Mappings to process the incoming HL7 messages. See **section 5 Configuration for HL7** for further information about configuration parameters.

2 Installation

2.1 Upgrading from a Previous Version

Prior to upgrading, make sure the license tied to the copy of Waypoint 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 Waypoint version can be upgraded to a newer Waypoint 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 Waypoint 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, exit the Waypoint client program, and stop the Waypoint service.

After installing and launching the new version, Waypoint's About dialog may be displayed and indicate a product version mismatch (depending on the installed license type). You should activate or install the new license version as described in chapter 3 of this user manual.

2.2 Minimum System Specification

Waypoint runs on dedicated hardware or a virtual machine. Depending on your workflow, your system requirements may differ. For example, a workflow with high-volume exams scheduled and performed and/or long lead times for future exams, e.g. Mammography, may require improvements to the CPU, RAM, disk, network card(s), etc.

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

- Microsoft Visual C++ 2017 Redistributable (x64) - 14.15.26706, (vc_redist.x64.exe)
- Microsoft .NET Framework 4.8
- Microsoft SQL Server
- Microsoft SQL Management Studio

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

Waypoint is dependent on Microsoft .NET Framework 4.8. If .NET Framework 4.8 is not installed on the host system, the first attempt to launch the Waypoint Client will open a web

browser that is automatically connected to Microsoft to download .NET 4.8. This is dependent on the host system having internet access. Otherwise, Microsoft .NET Framework 4.8 must be installed before Waypoint can run.

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 Waypoint. 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.

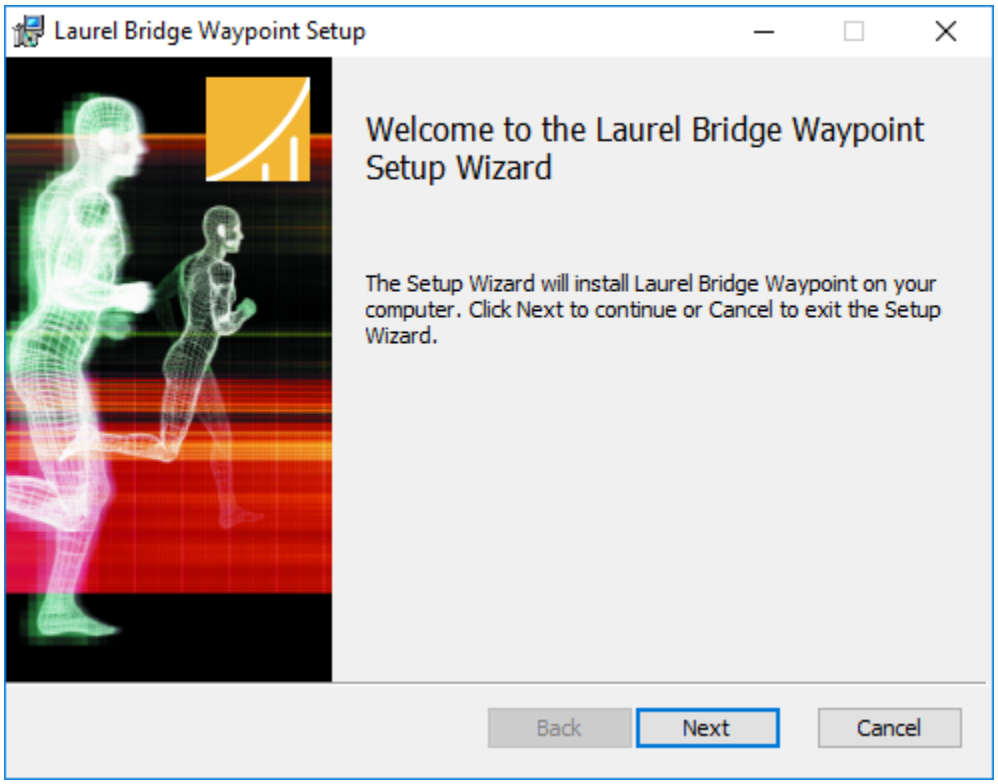
1. Log in to Windows as a user with administrative privileges.
2. Run the **SQL Server 2016 Express x64 with SP2 (en_sql_server_2016_express_with_service_pack_2_x64_100540591.exe)** installer.
3. On the **Setup** screen select **New SQL Server stand-alone installation or add features to an existing installation**.
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: Waypoint Application

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

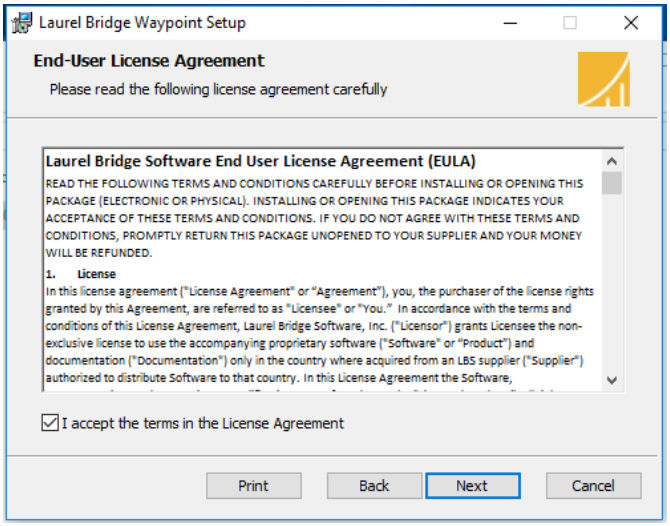
You must have Windows Administrator privileges in order to install Waypoint correctly.

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



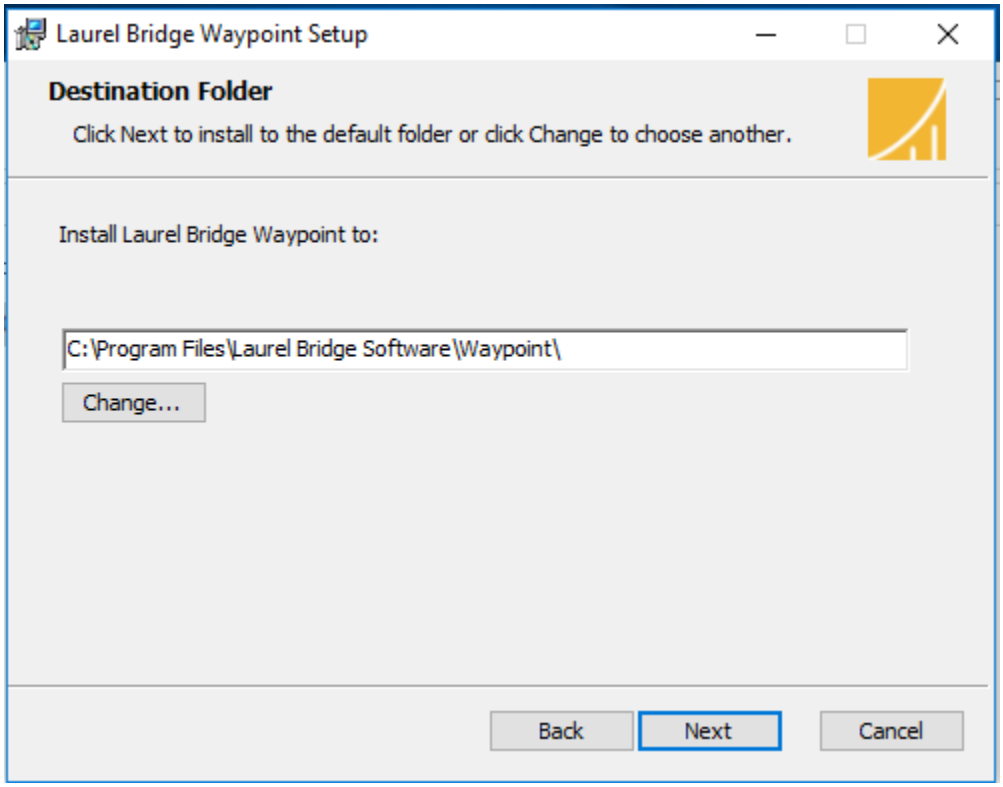
Click the Next button.

The user is then greeted with the License Agreement screen:



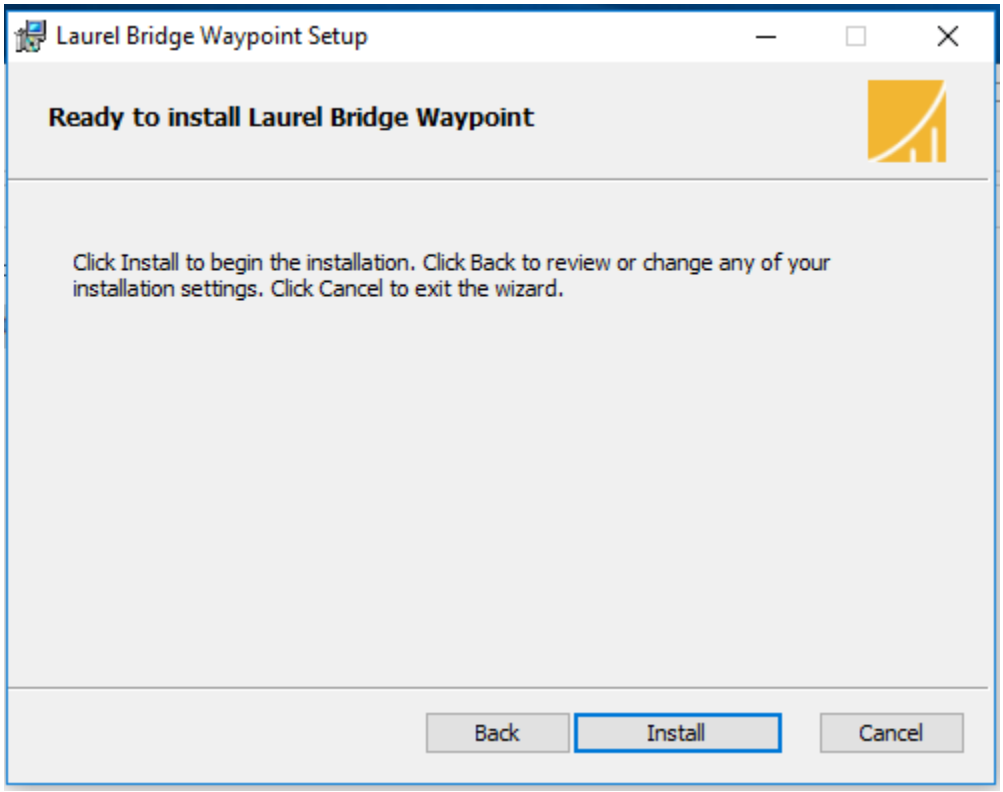
Check ‘I accept the terms in the License Agreement’ and then press the ‘Next >’ button.

The user is then greeted with the Installation Location screen:



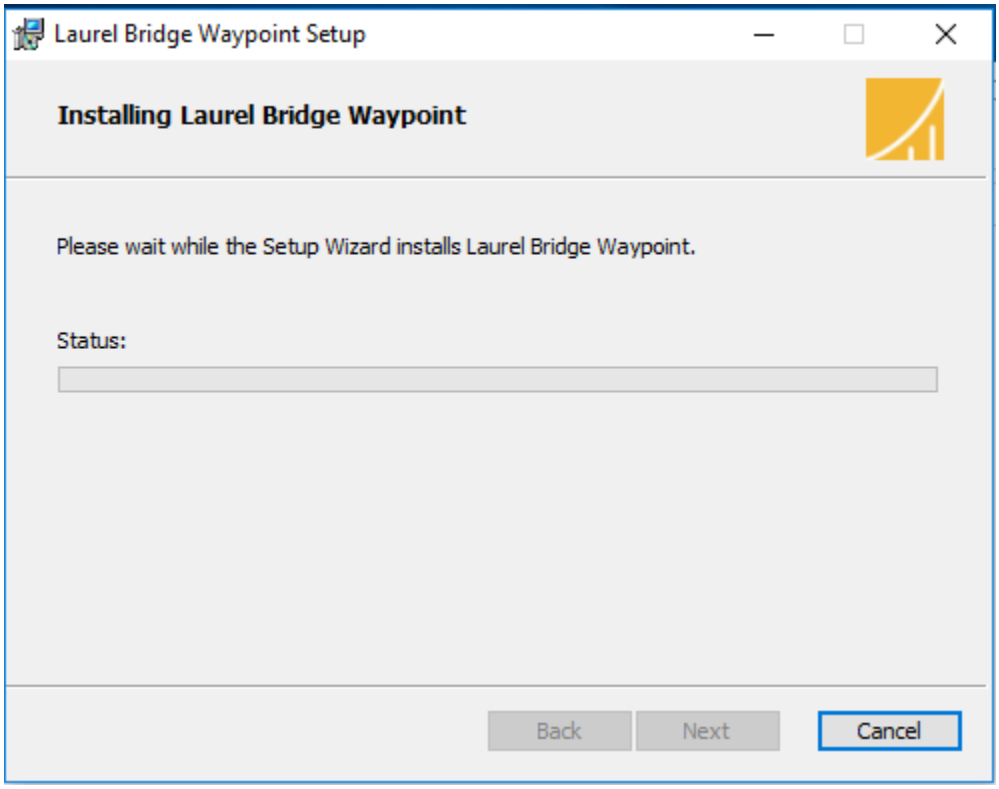
Specify an installation location (the default location is typically the best choice) and then press the ‘Next >’ button.

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

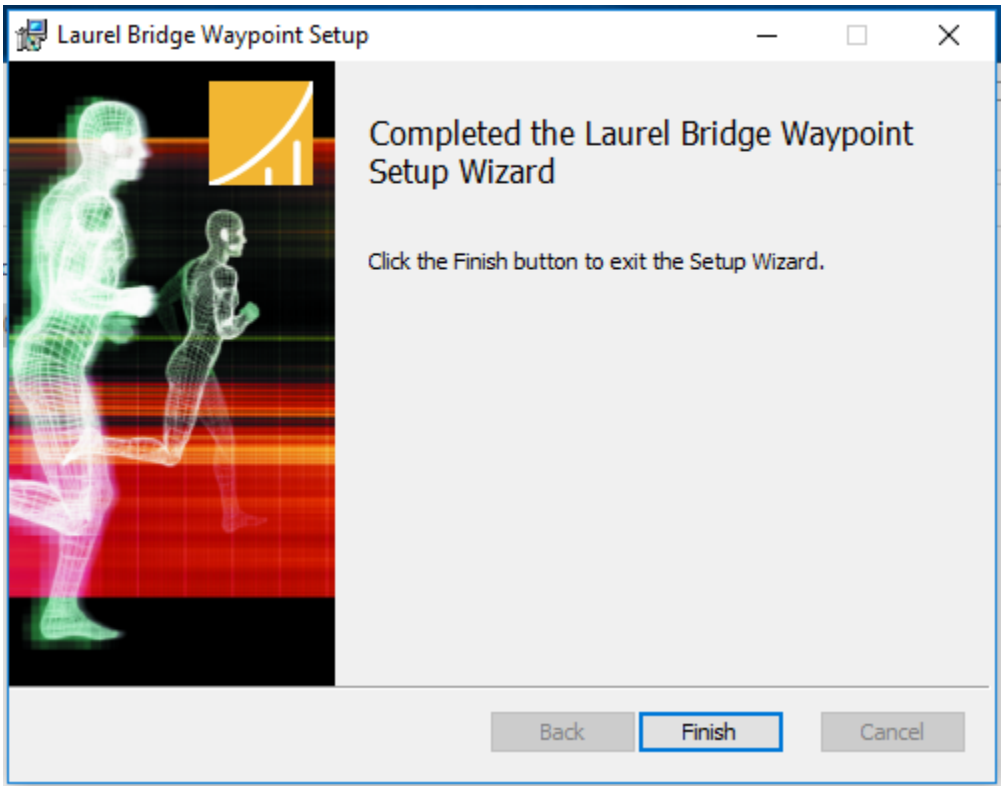


Press the ‘Install’ button.

The user is then greeted with an installation progress screen:



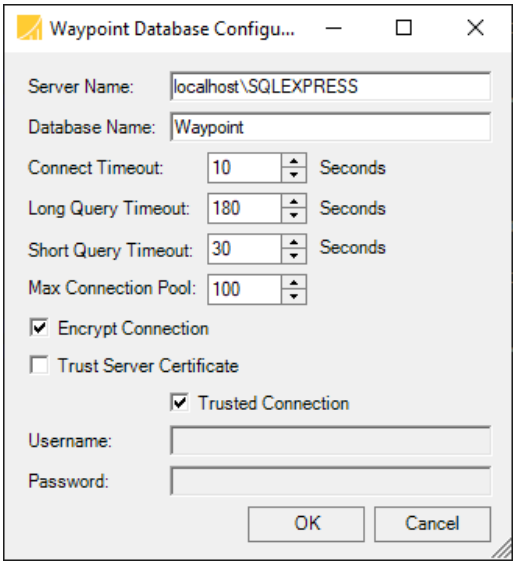
After installation completes, the user is then greeted with the Installation Complete screen:



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

2.5 Configuring Waypoint Database Connectivity

Upon starting Waypoint for the first time, the Waypoint Database Configuration dialog will be displayed, allowing for entry of the database connectivity information. This dialog will also be displayed whenever Waypoint encounters errors while attempting to connect to the database.



In order to connect to a SQL Server instance, enter the SQL Server instance name into the **Server Name** field, using the following format: "`<hostname>\<instance_name>`". Enter the SQL Server database name into the **Database Name** field. The **Connect Timeout**, **Long Query Timeout**, and **Short Query Timeout** fields can be used to change the default timeout values. The **Encrypt Connection** checkbox can be used to enable encryption on the SQL Server connection (only useful if the SQL Server instance is not on the local machine). The **Trust Server Certificate** can be used with an encrypted connection to bypass walking the certificate chain to validate trust. The **Trusted Connection** checkbox can be used to toggle whether

Windows authentication or **Username** / **Password** authentication is used to connect to the SQL Server instance. And finally, when using a non-standard TCP port (i.e., other than 1433) to connect to the SQL Server instance, enter a comma followed by the non-standard port number at the end of the **Server Name** field.

In the event that reconfiguration of the database connectivity information is required, the Waypoint Database Configuration dialog can also be manually started. For example, changing the Server Name from *localhost\SQLExpress* to *localhost\SQLStandard*. In order to do this, the Waypoint service cannot be running. Once the Waypoint service has been stopped, run the following command (which can be run from a command prompt or by creating a shortcut to the following path+parameter and double-clicking the shortcut):

"C:\Program Files\Laurel Bridge Software\Waypoint\WaypointClient.exe /dbconfig"

3 Getting Started

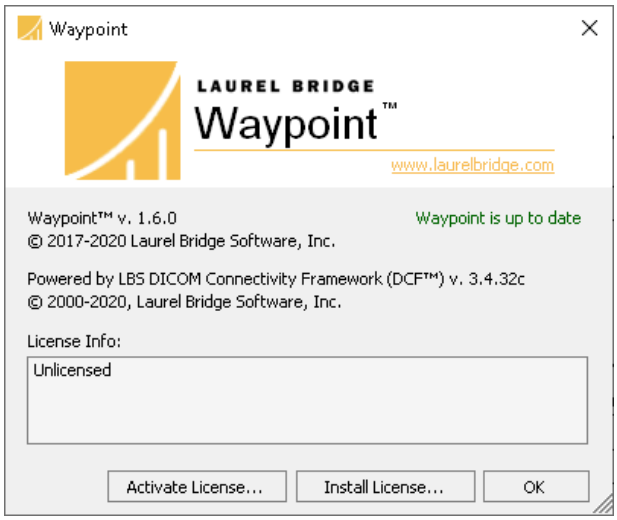
3.1 Overview

The Waypoint application is comprised by the following:

- WaypointService is a Microsoft Windows Service that is the control and data model
- WaypointClient is a Microsoft Windows Forms application that is used to configure the WaypointService
- WaypointRestService is the application entity that provides the Web user interface and support for HTTP RESTful queries

3.2 Installing a License

The first step after launching Waypoint is to install a license. When the **About Laurel Bridge Waypoint** dialog appears, there are two options to install a license. Information on the status of the license, including when it expires, can be found on this dialog available at any time by clicking **Help > About Laurel Bridge Waypoint**.



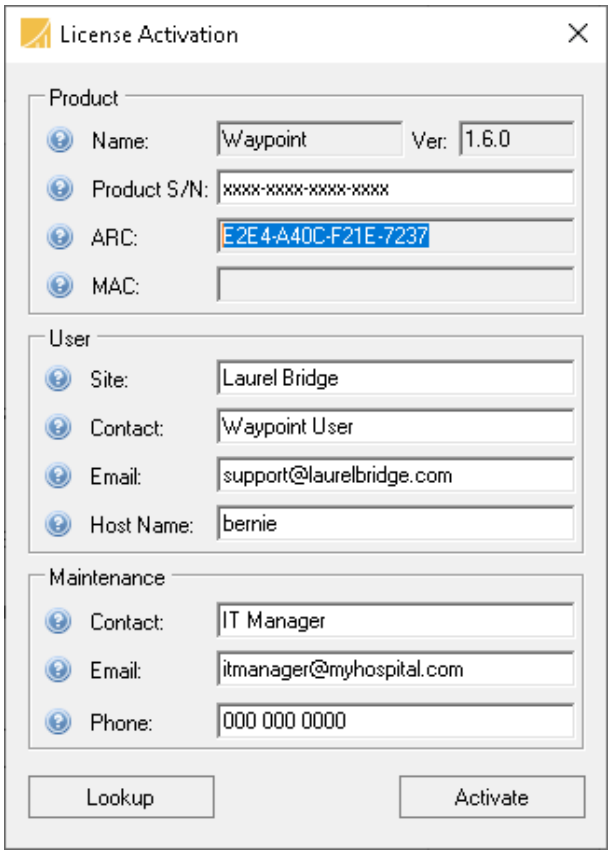
3.2.1 Installing a license file

Clicking the **Install License…** button will open a file searcher dialog allowing you to browse to a fully activated license file. You will use this button to install a license if a fully activated license was provided to you via email (for example, a MAC-based license) or you downloaded from www.laurelbridge.com or you performed a web activation.

Note: On Windows Server you must copy the license file to the local computer before installation. You cannot install the license from a network share or mapped network drive.

3.2.2 Activating a license over the internet

Clicking the **Activate License…** button will open the **License Activation** form. You will need to provide a **16-digit Product Serial Number** to activate your license. All fields on the form must be filled out. If the Waypoint server does not have internet access you will need the **16-digit Activation Request Code (ARC)** from the **License Activation Form**. You can proceed to `https://www.laurelbridge.com/product_activation.php` and enter your **16-digit Product Serial Number** and the **16-digit Activation Request Code (ARC)**. After completing the steps on the web activation form you can download a fully activated Waypoint license. You can then use the **Install License…** button on the **About Waypoint** dialog to install your activated license.

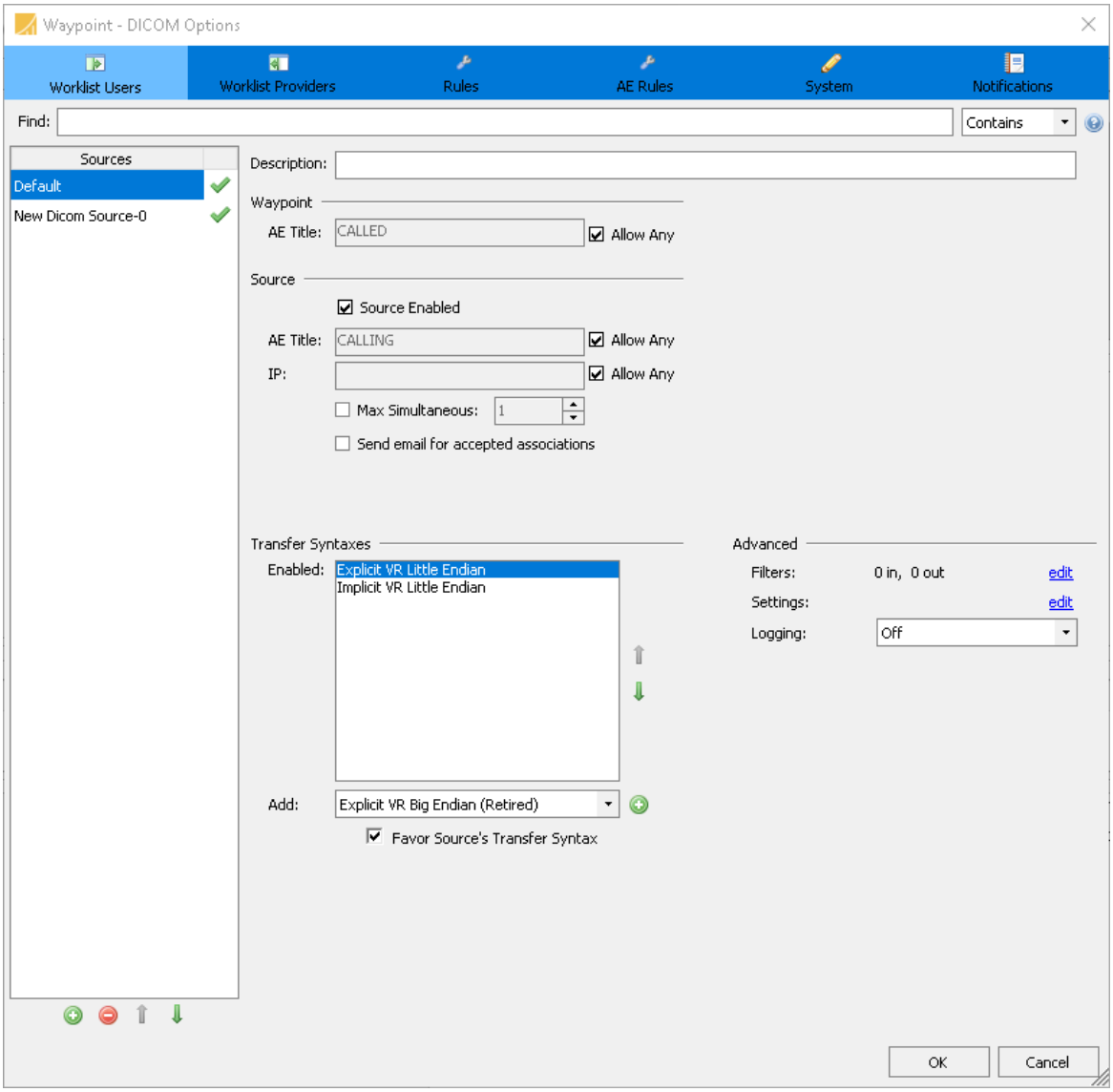


4 Configuration for DICOM

Configuration for DICOM is created and edited by selecting the **Edit > DICOM Options…** from the menu. DICOM configuration categories are:

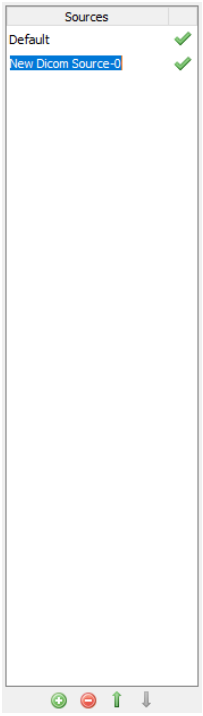
- Worklist Users
- Worklist Providers
- Rules
- AE Rules

Each of the configuration categories contains a predefined item with the name “Default". The configuration form for each of the items has a common format. Using Worklist Users as an example of the format:



The left side of the form displays a menu of the items that have been added in the selected category. The Find tool matches items by name and hides items that do not match the find text. The right side of the form is category specific as described in the following sections.

4.1 Creating a Worklist User

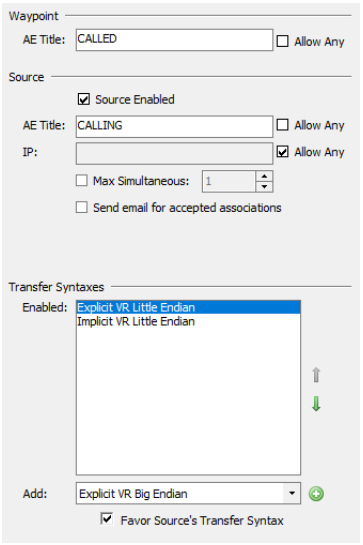


Worklist Users define the Service Class Users (SCU) that are permitted to communicate with Waypoint. Each source has the following list of properties, including the Default source that is required to exist, though it may be disabled:

- Description
- Called AE Title
- Source Enabled
- Calling AE Title
- IP
- Settings (edit DIMSE and PDU properties)

A new Worklist User can be created by selecting **Edit > DICOM Options…** from the menu and then selecting the **Worklist Users** pane. Press the green plus button located under the Sources list. This add a new Worklist User with the default name. See the next section for more information about Worklist Users. The list of Sources may be reordered by selecting a Source and then pressing the up or down arrows next to the green plus and red minus buttons.

4.1.1 Worklist User



A **DICOM Worklist User** is any device that will send DICOM Workflow Management messages to Waypoint via an association. A new Worklist User can be created by selecting **Edit > DICOM Options…** from the menu and then selecting the **Worklist Users** pane. Press the green plus button located under the Sources list. This will create a new **Worklist User** with the name "New Source-?", where "?" is the next available number starting at 0. Source names are customizable and can be modified at any time by clicking on the name. When an SCU requests an association with Waypoint, the Sources list is processed from top to bottom and the first match found is used; therefore, the ordering of the Sources may be important if potentially more than one could match.

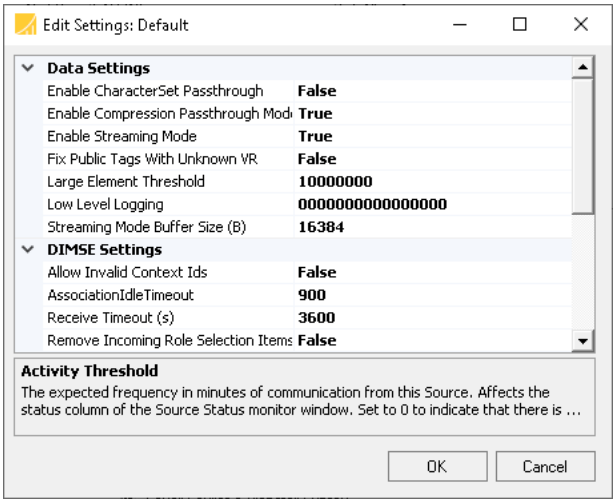
Once a **Worklist User** has been created the next step is to configure its settings.

4.1.2 Worklist User Settings

Under the **Waypoint** heading, the AE Title that Waypoint will accept is listed. The **Allow Any** checkbox can be selected to allow any value for that field.
Under the **Source** heading, settings include configuration options for the remote **AE Title** (AE title of the client), the remote **IP**, the Enabled status of the Source, and an option to limit the number of concurrent associations. The **Allow Any** checkbox following the **AE Title** and **IP** can be selected to allow any value for that field. Select the **Source Enabled** checkbox to enable the specified Source; deselect it to temporarily refuse any connections from the specified Source. To limit the number of concurrent associations allowed by this Source check the **Max Simultaneous** checkbox and specify the desired number.

Under the **Transfer Syntaxes** heading, the list of transfer syntaxes that Waypoint will accept for the specified DICOM Source can be configured. Add the desired **Transfer Syntaxes** to the list of accepted Transfer Syntaxes by selecting the desired Transfer Syntax in the combo box and adding it by pressing the provided button. After building up the list with the desired Transfer Syntaxes, place them in the desired order by selecting each one and moving it up and down in the list by pressing the up and down arrows. The supported Transfer Syntax list is evaluated top-to-bottom when a Source presents its requested presentation context list. If the Favor Source's Transfer Syntax checkbox is checked, then the Transfer Syntax list ordering proposed by the Source will be given priority; otherwise, the list as specified in Waypoint will be given priority.

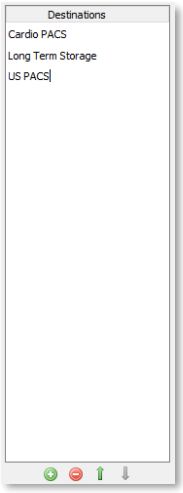
Under the **Advanced** heading, a user can give more in-depth control over how a Worklist User communicates with Waypoint. Data handling options, DIMSE settings, PDU settings, and socket settings are all areas which can be configured in finer detail when editing the **Settings** options. Verbose DICOM logging can be turned on or off on a per Source basis by selecting 'On' or 'Off' in the **Logging** combo box. **Filters** are described in **section 4.7 Filters**.



4.2 Creating a Worklist Provider

Worklist Providers enable Waypoint to communicate with other devices on the network to create and update worklist orders within Waypoint. The worklist provider may be a DICOM compliant Modality Worklist Server, a Web Service, an HTTP RESTful server, or SQL Database. Waypoint will optionally forward MWL C-FIND queries to Worklist Providers that are configured as DICOM Modality Worklist Servers. This option is described in section **4.3.3 Rule Actions**. For non-DICOM devices, Waypoint offers a schedule option to poll the device for worklist orders using the Worklist Provider's configured transport mode, see section **4.2.4 Advanced Settings.**

A new Worklist Provider can be created by selecting **Edit > DICOM Options…** from the menu and then selecting the **Worklist Providers** pane. Press the green plus button located under the Destinations list. This will create a new Destination with the name "New Destination-?" where "?" is the next available number, starting at 0. Destination names are customizable and can be modified at any time by clicking on the name. The list of Destinations may be reordered by selecting a Destination and then pressing the up or down arrows directly below the Destinations list. Unlike Sources, there is no priority associated with Destination ordering; it is merely provided as a convenience.
Once a Destination has been created the next step is to configure its settings.

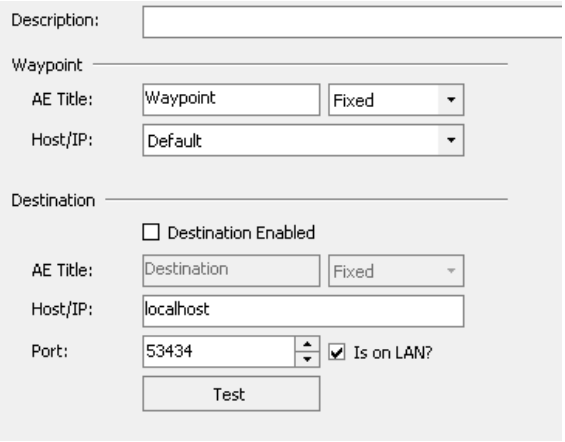


4.2.1 Waypoint Settings

Under the **Waypoint** heading, settings include configuration options for the **AE Title** (Application Entity) and **Host/IP**.

4.2.2 Worklist Provider Settings

Under the **Destination** heading, settings include options for the **AE Title**, the **Host/IP**, the **Port** number, a **Test** button for testing the connection, an **Is on LAN?** checkbox, and the enabled status of the Destination. Selecting the **Destination Enabled** checkbox will allow jobs to be sent to the specified Destination; deselect it to temporarily stop sending jobs to the specified Destination. Checking or unchecking the **Is on LAN?** checkbox will optimize network buffer sizes for that particular network topology.

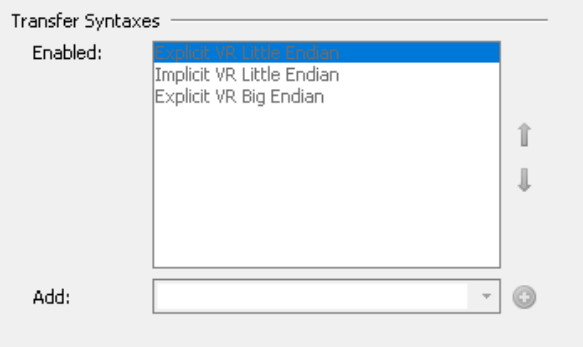


For both the **Waypoint** and **Destination AE Title,** values can be set with a fixed value by selecting **Fixed** in their corresponding combo boxes. Alternately, the AE titles can be set to either **Source Calling** or **Source Called**; this will use the calling or called AE title from the inbound association that created the job for this Destination.

Once values have been specified for the Local AE Title, the Remote AE Title, the Host/IP, and the Port, then the **Test** button can be clicked to issue a DICOM Verification request to the specified Destination. A green check next to the Test button indicates a successful connection; a red X indicates a connection could not be made, or the connection was refused. Hover the mouse pointer over the X to read a tooltip with a message that further describes the failure.

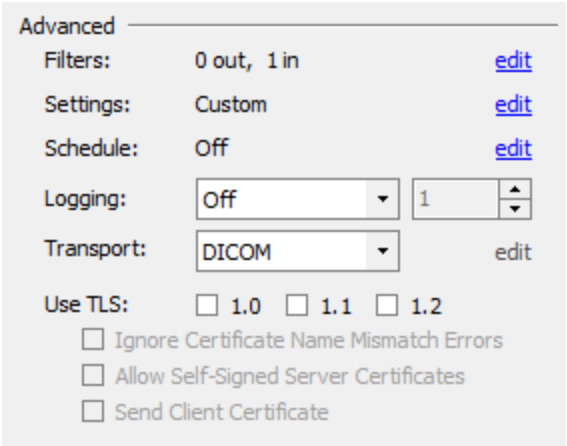
4.2.3 Transfer Syntax Settings

Under the **Transfer Syntaxes** heading, the user can configure the list of allowable transfer syntaxes that Waypoint will negotiate with the specified Destination. Add the desired transfer syntaxes to the list of accepted Transfer Syntaxes by selecting the desired transfer syntax in the combo box and adding it by pressing the provided button. After building up the list with the desired Transfer Syntaxes, place them in the desired order by selecting each one and moving it up and down in the list by pressing the up and down arrows. Note, **Transfer Syntaxes** are specifically for Transport Mode DICOM and are disabled otherwise.

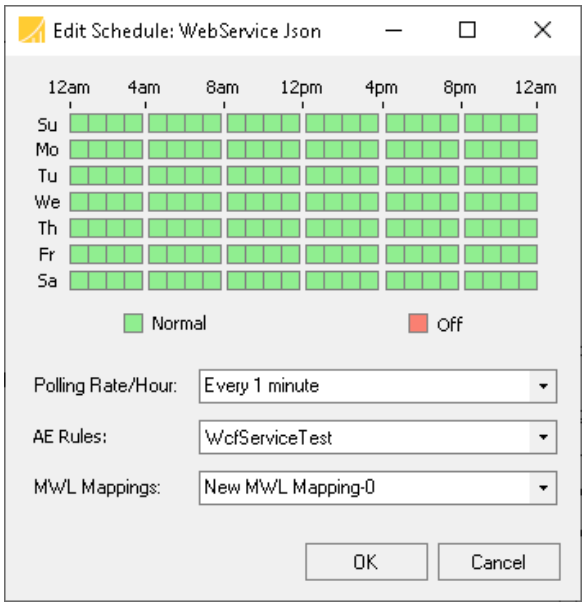


4.2.4 Advanced Settings

Under the **Advanced** heading, a user can give more in-depth control over how Waypoint communicates with a Destination. **Filters** are described in **section 4.7 Filters**. **Settings** options are configured in the same fashion as Worklist Users, see **4.1.2 Worklist User Settings.** The **Use TLS** checkboxes specify whether network communications with the specified DICOM Destination will be encrypted using TLS (as well as which TLS versions will be supported). The **Ignore Certificate Name Mismatch Errors** and **Allow Self-Signed Client Certificates** checkboxes can be used to relax the certificate validation for this Worklist Provider. However, we strongly recommend using these options for testing only, as they greatly reduce security by preventing full TLS authentication from occurring. The **Send Client Certificate** checkbox can be used to control whether or not client certificates (i.e., client authentication) are sent to the Worklist Provider.



4.2.4.1 Schedule



The **Schedule** specifies the time at which a query is sent to the Worklist Provider to poll for worklist orders. A green box for the given day and time means queries may be sent at that time; a red box means that queries may not be sent at that time.
Each hour block represented by a green or red square may be toggled individually; alternatively, right-clicking on the schedule allows the schedule to be set to a commonly used setting. Be aware that choosing one of these predefined settings will replace the currently specified schedule.

Polling Rate/Hour defines how often within each enabled hour to poll the Worklist Provider. The options are:

- Once per Hour
- Every 1 minute
- Every 5 minutes
- Every 10 minutes
- Every 15 minutes
- Every 20 minutes
- Every 30 minutes

AE Rules selects one of the configured AE Rules. This is used to generate the C-Find request that is sent to the Worklist Provider. The AE Rules define which fields the Worklist Provider will match when creating its C-Find responses for the query **see section 4.4 Creating AE Rules** for more information.

MWL Mappings selects one of the configured HL7 MWL Mappings. This is used to map the DICOM Tag values from the C-Find responses to data items in Waypoint's database in order to store the worklist items from the Worklist Provider in Waypoint's database (**see section 5.2 Creating HL7 MWL Mappings** *for more information.)*

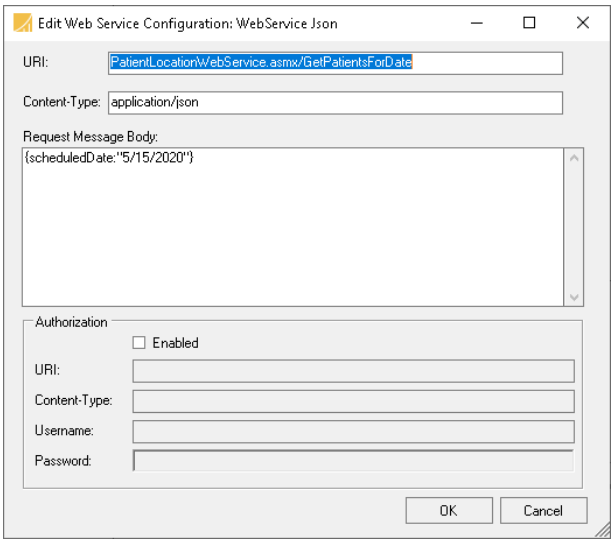
4.2.4.2 Transport Mode

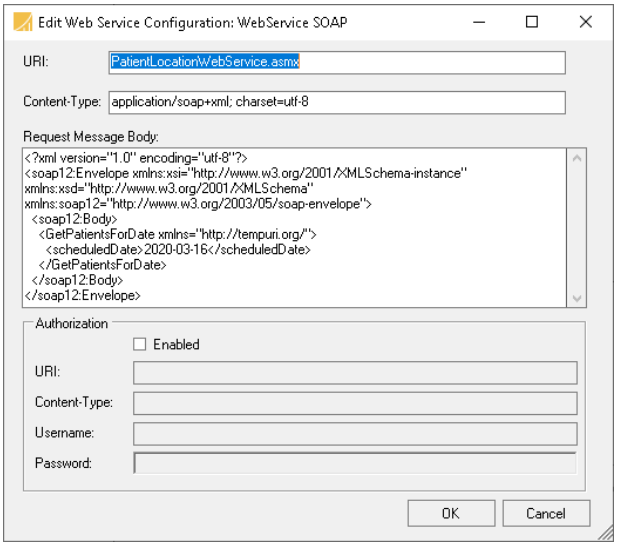
The **Transport** selects one of the available transport modes:

- DICOM
- WEB SERVICE
- HTTP RESTFUL
- SQL ODBC

The **edit** link opens a custom configuration editor for the selected transport mode. Note, the edit link is disabled for DICOM because all required configuration parameters are specified on the Worklist Providers tab.

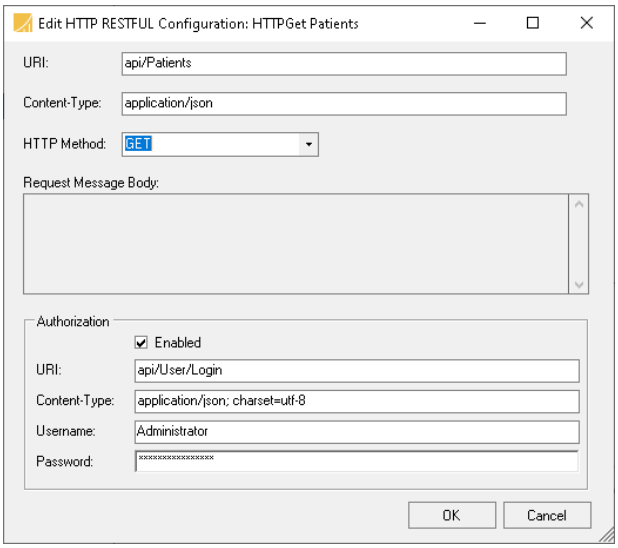
The **WEB SERVICE** transport mode uses the Host/IP and Port from the Destination settings on the Worklist Providers tab. The edit link sets the URI, Content-Type, Request Message Body, and optionally Authorization Credentials for the web service request, as shown for content-types: application/json and application/soap+xml:





Notice, with application/json, the URI contains both the web service and web method names. With SOAP, the web method name is in the Request Message Body and does not appear in the URI. The Authorization selection is described in the next section with HTTP RESTFUL.

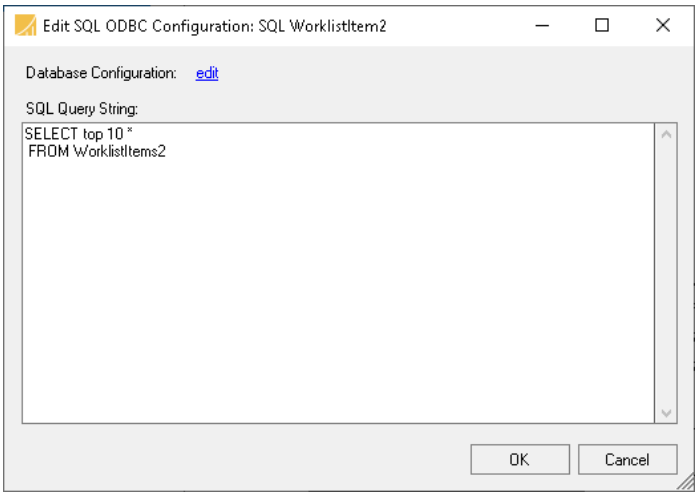
The **HTTP RESTFUL** transport mode uses the Host/IP and Port from the Destination settings on the Worklist Providers tab. The edit link sets the URI, Content-Type, HTTP Method, Request Message Body, and Authorization Credentials for the HTTP request. The HTTP Method selects either POST or GET. The Request Message Body is only used for POST methods and is disabled for GET methods. The Request Message Body sets the parameter values for the web method.

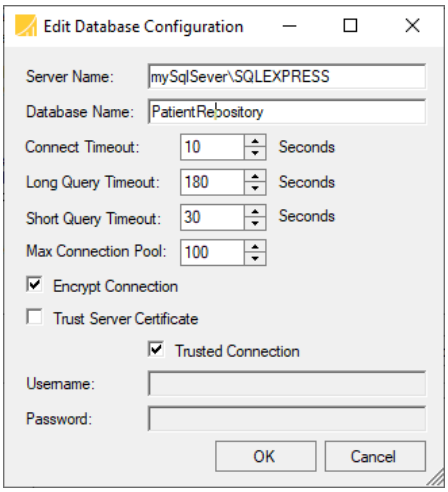


Authorization is an option used with web methods that specify authorization requirements. Authorization configures the web method request that invokes the HTTP POST to login to an HTTP RESTful server. The login method retrieves the access_token from the server that is required to invoke authorized methods on that server. The Worklist Provider first invokes

the login method to the RESTful service. If the authorization was successful, the access_token is extracted from the login response and used to invoke HTTP GET on the method api/Patients. Notice Request Message Body is disabled for HTTP GET. Please see **Appendix F: Communicating with Authorized Web Methods from Waypoint** for additional information.

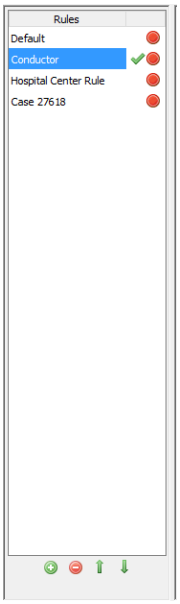
The **SQL ODBC** transport mode does not use the Host/IP or Port from the Destination settings on the Worklist Providers tab. The edit link sets the Database Configuration and the SQL Query String for the SQL Worklist Provider, as shown:





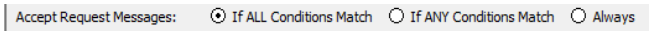
4.3 Creating DICOM Rules

A new Rule can be created by selecting **Edit > DICOM Options…** from the menu and then selecting the **Rules** pane. Press the green plus button located under the Rules list. This will create a new Rule with the name "New Rule -?" where "?" is the next available number, starting at 0. Rule names are customizable and can be modified at any time by clicking on the name. The list of Rules may be reordered by selecting a Rule and then pressing the up or down arrows directly to the right of the Rules list. When Waypoint processes the list of Rules for each received query request, the Rules list is processed from top to bottom and the first match found is used, therefore the ordering of the Rules may be important if potentially more than one could match.



Once a Rule has been created the next step is to configure its Conditions, Selected AE Rules, MWL Mappings, Selected Worklist Providers, and Rule Options.

4.3.1 Rule Conditions

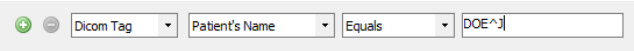


A Rule's Conditions determine whether or not its Actions will be applied to an DICOM request being processed. A Rule may have multiple

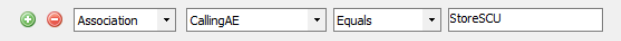
conditions, in which case it may be specified that either all the conditions must apply to the request or that only one condition must apply to the request in order for the Rule to match.

Another option is that the Rule always matches; effectively declaring it to have no Conditions. Selecting one of three radio buttons, **If ALL Conditions Match**, **If ANY Conditions Match**, and **Always**, will implement one of these three scenarios. Note that if it is desired to have a more complex logic to a Rule's conditions (e.g. "(A and B) OR (C and D)"), this can be achieved by using the special **All of** or **Any of** condition which are discussed in more detail below.

The **Dicom Tag** condition allows incoming messages to be selected for this Rule based upon their Dicom Element Tags.

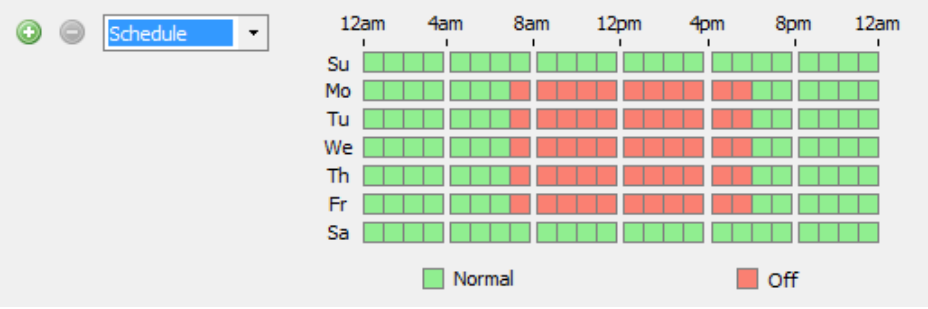


The **Association** condition allows incoming messages to be selected for this Rule based upon their incoming Dicom Association information.



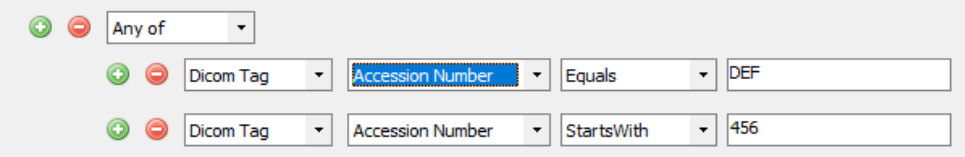
The **Execute** condition allows incoming query requests to be selected for this Rule based upon a custom, user-defined rule condition. Note, following any changes to the custom code file, it is required to edit DICOM options and click OK to load the changed custom code file for execution. See **section 4.3.2 Custom DICOM Rule Condition Example** for an example of a custom rule condition implementation.

The **Schedule** condition allows incoming MWL queries to be selected for this Rule based upon the time of day and day of week that the message was received. Any squares which are green in the schedule represent time/day blocks where the condition is true; any squares which are red represent time/day blocks where the condition is false. Each square can be changed individually by clicking on it. Alternately, the user can right-click to select from a menu of preset schedules for ease of populating the schedule as desired.

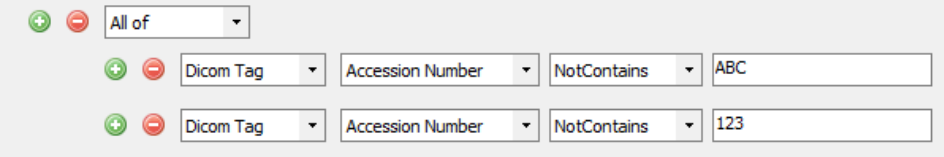


The **Command Tag** condition appears in the menu but is not yet implemented in Waypoint.

The **Any of** condition is a special condition which is true if one or more of its sub-conditions are true. This condition allows the user to formulate more complex logical Rules.



Similarly. the **All of** condition is a special condition which is true if and only if all of its subconditions are true. Again, this condition allows the user to formulate more complex logical Rules.



Configure the condition based upon the desired test. Conditions may be added or removed by pressing the green plus sign or the red minus sign located to the left of each condition.

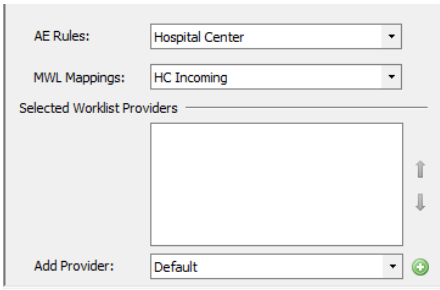
4.3.2 Custom DICOM Rule Condition Example

Custom rule conditions are used to help determine whether a particular DICOM query matches a particular rule. The following example shows a custom rule condition:

```
using System;
using System.Collections.Generic;
using LaurelBridge.DCF;
using LaurelBridge.DCF.Dicom;
using LaurelBridge.DCF.Dicom.Dimse;
using LaurelBridge.DCF.IO;
using LaurelBridge.Waypoint.Core;
using LaurelBridge.Waypoint.Core.Conditions;
using LaurelBridge.Waypoint.Core.Plugins;

namespace LaurelBridge.Waypoint.Custom
{
   public class DicomExecuteConditionExample : IExecuteCondition
   {
      public bool Matches(IAssociationParameters assocParams,
         DicomDataSet dicomDataSet)
      {
         string name = dicomDataSet.GetElementStringValue(Tags.PatientName);
         name = name.Trim();
         if (name.Length % 2 == 0)
            return true;
         else
            return false;
      }
   }
}
```


4.3.3 Rule Actions



If the logic for the Rule conditions is satisfied, then the request currently being processed will have the selected properties for the rule applied to the request.

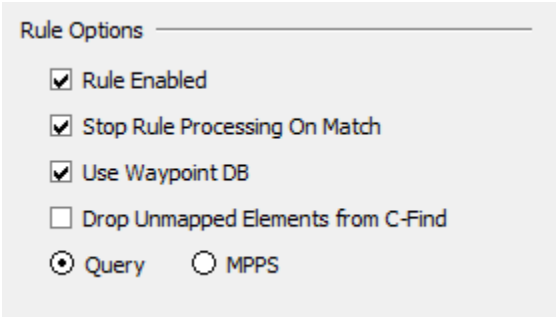
AE Rules cause Waypoint to add, remove, or modify elements in the C-Find request message before processing the message, **see section 4.4 Creating AE Rules** *for more information*. Note, AE Rules are only applied to Query rules. AE Rules selection is disabled for MPPS Rules.

MWL Mappings define how Waypoint decodes the responses to the request by the mapping between the database value and the DICOM tag to use. The mapping may also contain a Pattern Replacement to modify the value that is set in the response message, **see section 5.2 Creating HL7 MWL Mappings.** Note, be sure to select an HL7 MWL Mapping that was created using Worklist Defaults for Query Rules and one that was created using Procedure Step Defaults for MPPS Rules.

Selected Worklist Providers is an option to allow you to add a list of Worklist Providers to the Rule Action. When Selected Worklist Providers are specified, the request message is forwarded to those Worklist Providers. The handling of the responses from the selected worklist providers is controlled by the currently selected Rule Options, specifically whether or not *Use Waypoint DB* is checked, **see section 4.3.4 Rule Options** *for more information*. To add a Selected Worklist Providers to the **Selected Worklist Providers** list, select the desired Worklist Provider in the **Add Provider** combo box and press the green plus sign. To remove a Destination from the list, right-click on the desired Worklist Provider and choose **Remove Selected** in the context menu.

4.3.4 Rule Options

Uncheck the **Rule Enabled** checkbox to disable the selected Rule. If unchecked, the Rule will be passed over during Rule processing. The remaining Rule Options are dependent on the rule type being Query or MPPS. Check the **Stop Rule Processing On Match** checkbox if no further Rules in the Rules list should be processed if this Rule matches (Rules are processed sequentially from the top of the list to the bottom of the list). If unchecked, Rule processing will proceed to the next Rule even if this Rule matches. For MPPS, **Stop Rule Processing On Match** is always checked and enabled. **Use Waypoint DB** is used in conjunction with Selected Worklist Providers. If it is checked, Waypoint updates its database with the responses from the selected worklist providers. Once all responses are received, a consolidated list of the unique responses are sent to the calling SCU. If Use Waypoint DB is not checked, all responses from the selected worklist



providers are sent back to the calling SCU and Waypoint does not update its database from the response data. For MPPS, **Use Waypoint DB** is always checked and enabled. **Drop Unmapped Elements from C-Find** controls how the selected MWL Mapping is applied to the C-Find response data. When checked, which is the default, any DICOM element in the C-FIND request whose DICOM tag is not found in the MWL Mapping is dropped from the C-Find response. When Drop Unmapped Elements from C-Find is unchecked, a response value is provided for all elements from the C-Find request. For MPPS, **Drop Unmapped Elements from C-Find** is always unchecked and disabled. In the case where the C-Find request contains an empty sequence element, all child elements for the sequence are returned in the response. For example, Waypoint receives a C-Find request that contains Requested Procedure Code Sequence (0032,1064) with an empty dataset and Drop Unmapped Elements from C-Find is disabled. The C-Find response will contain:

- Code Value (0032,1064.0008,0100)
- Coding Scheme Designator (0032,1064.0008,0102)
- Coding Scheme Version (0032,1064.0008,0103)
- Code Meaning (0032,1064.0008,0104)

4.4 Creating AE Rules

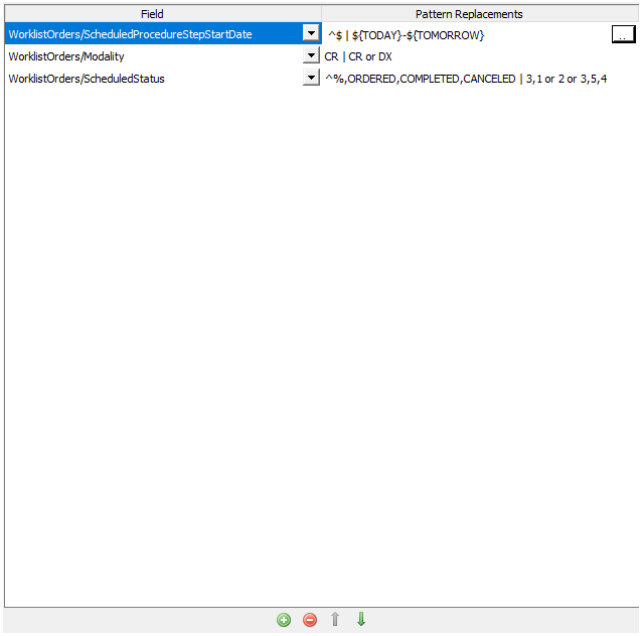
AE Rules define a list of substitution patterns that are applied to the C-Find requests received by Waypoint. Each AE rule has the following list of properties:

- Field
- Pattern Replacements

A new **AE Rule** can be created by selecting **Edit > DICOM Options…** from the menu and then selecting the **AE Rules** pane. Press the green plus button located under the AE Rules list. This adds a new AE Rule with the default name “New AE Rule-?”, where “?” is the next available number starting at 0. See the next section for more information about AE Rules. The list of AE Rules may be reordered by selecting an AE Rule and then pressing the up or down arrows next to the green plus and red minus buttons.

4.4.1 AE Rule

AE Rules allow you to modify C-Find requests at the point that they are first received by Waypoint. This allows you to control which fields to match and what data to return in the responses to the modality. The Field property is selected from any item in Waypoint's database schema. The Pattern Replacements defines substitutions that may be performed on the incoming data request. For example, the AE Rule shown to the right defines Pattern Replacements on:



- ScheduledProcedureStepStartDate
- Modality
- ScheduledStatus

The Pattern Replacement for WorklistOrders/ScheduledProcedureStepStartDate is:

Match	Replacement
^$	${TODAY}-${TOMORROW}

The Match is the regular expression ^$ which matches the empty string. The Replacement is the date range today thru tomorrow, specified as macros. This means if the C-Find request from the modality has an empty value for Schedule Procedure Step Start Date, Waypoint will automatically match the date range today thru tomorrow. If Scheduled Procedure Step Start Date has a non-empty value in the C-Find request, the data value from the DICOM message will be used.

As a second example, the Pattern Replacement for Modality is:

Match	Replacement
CR	CR or DX

This means if the C-Find request contains CR as the matching value for Modality, Waypoint will automatically match CR or DX worklist orders. If the C-Find request has any other value, Waypoint will use the value contained in the DICOM message.

4.4.1.1 Using Macros as the AE Rule Replacement Value

Waypoint offers a list of macros that can be used as the replacement value for an AE Rule. As shown above with the ScheduledProcedureStepStartDate, the most common usage of this feature is to specify the date range as:

```
${TODAY}-${TOMORROW}
```

This constrains the query date range to only retrieve orders scheduled today or tomorrow. The ScheduledProcedureStepStartDate can also limit the query to a time range in hours. The macro

${NOW} constrains the query to the current hour. To specify a time range, hours can be added or subtracted from the current time as follows:

```
${NOW-12}-${NOW+12}
```

This constrains the query range to retrieve orders scheduled for the previous 12 hours through the next 12 hours based on the current time. The macro is conditionally applied by evaluating the regular expression that is specified in the Match criteria, for example:

```
^$
```

The replacement value is only used if the element value in the C-FIND request is empty. Alternatively, if the Match is set to:

```
^.*$
```

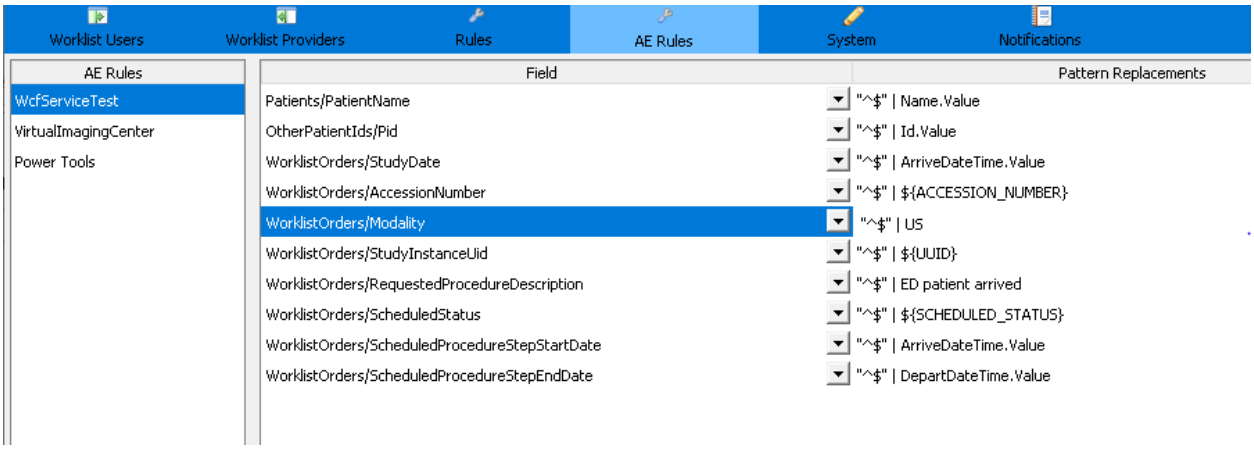
The element value in the C-FIND request is ignored and the Replacement is always used. The following tables defines the entire list of macros.

Macro Name	Note
${CALLING_AE}	**Calling AE title used for the association, VR AE**
${CALLED_AE}	**Called AE title used for the association, VR AE**
${CONNECTION_ID}	**Connection ID used for the association**
${IP_ADDRESS}	**IP Address used for the association**
${SOURCE_NAME}	**Source Name used for the association**
${TIMESTAMP}	**Date and time now, encoded as DICOM date and time, VR DT**
${YESTERDAY}	**Yesterday's date encoded as a DICOM date, VR DA**
${TODAY}	**Today's date encoded as a DICOM date, VR DA**
${TODAY-*n*}	**Date corresponding to today's date *minus n days.***
${TODAY+*n*}	**Date corresponding to today's date *plus n days.***
${NOW}	**The date and hour now as a DICOM date/time, VR DT**
${NOW-*n*}	**The date and hour corresponding to now *minus n hours.***
${NOW+*n*}	**The date and hour corresponding to now *plus n hours.***
${TOMORROW}	**Tomorrow's date encoded as a DICOM date, VR DA**

${UUID}	**Generate a derived UID with the format "2.25.xxx". Used for Study Instance UID, Referenced SOP Instance UID, and Referenced Patient SOP Instance UID, VR UI**
${NEWUID}	**Generate a derived UID with the format "1.2.840.114089.xxx". Used for Study Instance UID, Referenced SOP Instance UID, and Referenced Patient SOP Instance UID, VR UI**
${ACCESSION_NUMBER}	**Generate an Accession Number with the format "ANyyJJJhhmmssfff", where yy is year, JJJ is Julian day of year, and hhmmssfff is hour, minute, second, and msec when accession number was generated.**
${SCHEDULED_STATUS}	**Create the new order with the Scheduled Status set to "1" meaning a new order. If the order is updated with a Scheduled Procedure Step End Date the status is automatically changed to "4" meaning canceled, on the condition that the order has not started or completed yet.**

4.4.1.2 Pattern Replacements for Polling Web Services or SQL Worklist Providers

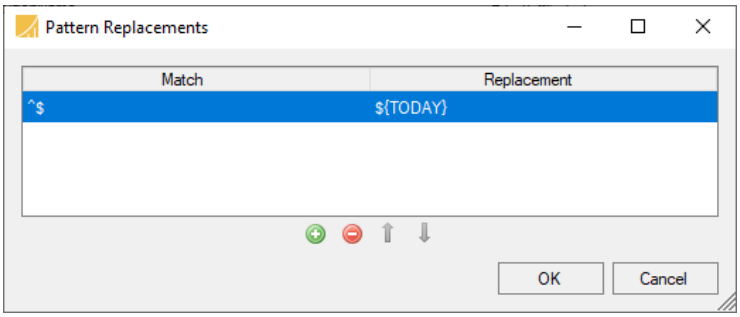
For non-DICOM Worklist Provider which are: WEBSERVICE, HTTP RESTFUL, and SQL ODBC, the Pattern Replacements in the AE Rules are used to extract field values from the response data to store in Waypoint's database. The naming convention to identify the SQL field or WEB SERVICE property is *PropertyName*.**VALUE.** The *PropertyName* is the Json property name or SQL field name in the response message from the Worklist Provider. The keyword **VALUE** triggers Waypoint to extract the value for this property as the value for the given field in the worklist order. The following example uses the value for the Name property for the PatientName, Id property for the Pid, ArriveDateTime for the ScheduledProcedureStepStart Date, and DepartDateTime for the ScheduledProcedureStepEndDate. Notice the ${ACCESSION_NUMBER} and ${SCHEDULED_STATUS} macros are used for AccessionNumber and ScheduledStatus respectively.

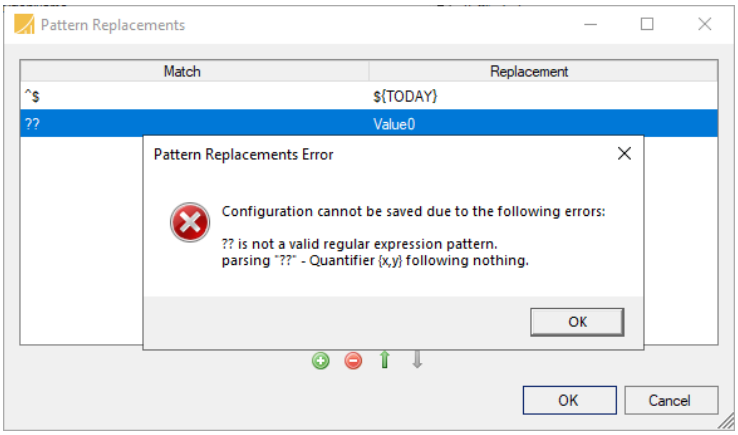


The above AE Rules are used for the configuration of a non-DICOM Worklist Provider as shown in section **4.2.4.1 Schedule**.

4.5 Pattern Replacements

Both AE Rules and HL7 MWL Mappings provide a very powerful feature called Pattern Replacements. To add a new pattern replacement, press the green plus button located below the Match Replacement grid. This will create a new Pattern Replacement with Match "Regex0" and the Replacement "Value0". Replace "Regex0" with the regular expression to match against the AE Rule Field to which it is being applied. For example the regular expression "^$" matches if the Field has an empty value and "^.*" matches if the Field as any value including empty. If the regular expression matches, the Field value is replaced with the Replacement value. Click OK to save the pattern replacements. On save, the regular expressions are validated and if the validation fails an error dialog is displayed. The regular expressions must all be valid to save the pattern replacement.





4.5.1.1 Pattern Replacements for ScheduledStatus

If the WorklistOrders/ScheduledStatus value is using a pattern replacement to convert a value to an integer code (see section 5.2.1), a corresponding pattern replacement should be used when searching for orders via an MWL C-Find query. For example, if a query is received that is

attempted to find results where the ScheduledStatus is “Scheduled”, then a pattern mapping that replaces “Scheduled” with “2” should be defined. If a query is received that has no value for ScheduledStatus and the desired behavior is to match all orders that are “New” or “Scheduled” (as defined in section 5.2.1), then a pattern mapping that has a Match value of “^$” and a Replacement value of “1 or 2” should be defined.

4.6 Import, Export and More on the Context Menu

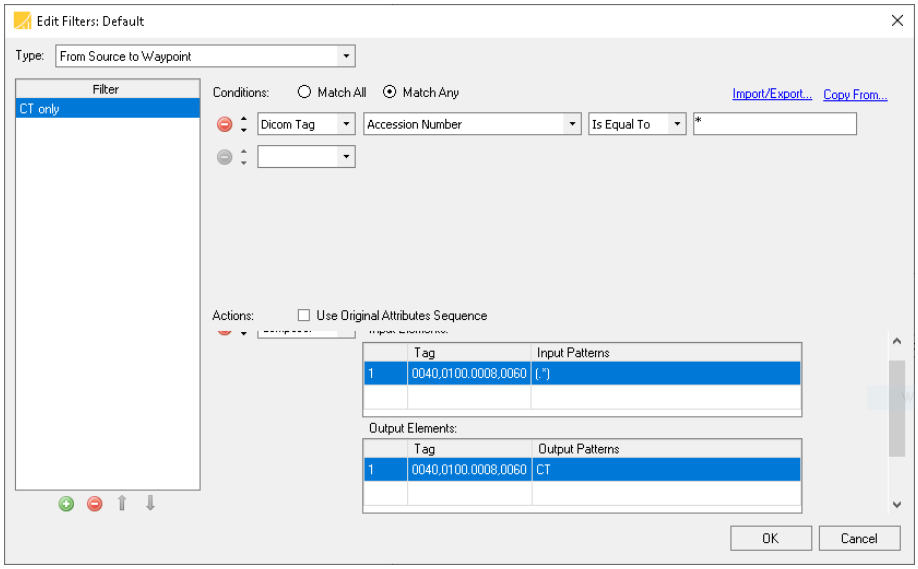
Each of the previous configuration sections provide an option to export the configuration to an XML file and import the configuration to the same or another Waypoint server. This greatly speeds up the process when configuring multiple instances of Waypoint and ensures all instances of Waypoint are using the same configuration.

Worklist Users, Worklist Providers, Rules, and AE Rules all show a grid on the left side of the configuration pane to add and remove new entries. Right-clicking on the grid displays a context menu with the following menu items:

- **Add**, adds a new entry in the same manner as the green-plus button.
- **Remove**, removes an existing entry in the same manner as the red-minus button.
- **Rename**, changes the name of an existing entry.
- **Copy**: creates a copy of the selected entry with a “*” appended to the name. Use Rename to change the name of the new entry.
- **Enabled**, enables the selected entry in the same manner as the Enable checkbox on the configuration pane.
- **Stop Matching**: toggles the *Stop Rule Processing On Match* in the same manner as the checkbox on the configuration pane. Note, this menu item only applies to Rules and HL7 Rules.
- **Import**: displays a file chooser message box to select an XML configuration file to import into Waypoint. Import compares the contents of the file against the current configuration. All new entries are imported. Entries that have the same UID as existing configuration items display a dialog box giving the option to: Replace, Skip, or Cancel the import of any duplicates.
- **Export Selection**: displays a file chooser message box to enter a filename to store the configuration for the currently selected item.
- **Export All:** displays a file chooser message box to enter a filename to store the configuration for all the items in the list.

4.7 Filters

Filters allow a message’s response data to be changed as Waypoint receives it from a Worklist User or as Waypoint sends it out to a Worklist Provider. **Actions** are only applied if the **Conditions** are met.

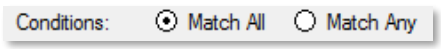


A new Filter can be created by selecting **Edit > DICOM Options…** from the menu, selecting a Worklist User or Worklist Provider, and then selecting the **Filters edit** link. The Type selector at the top allows choice between the Filter direction (to or from Waypoint) and defaults to the usual choice ("Source to Waypoint" for Worklist Users and "Waypoint to Destination" for Worklist Providers). To add a new filter, press the green plus button located under the Filters list. This will create a new Filter with the name "New Filter ?" where "?" is the next available number, starting at 0. Filter names are customizable and can be modified at any time by clicking on the name. The list of Filters may be reordered by selecting a Filter and then pressing the up or down arrows. Filters are applied in order, top to bottom, so ordering is important.

Another way to create a new Filter is to copy from another Source or Destination. Pressing the "Copy From…" link in the upper-right section of the Filter Editor allows you to copy individual Filters defined in the other Sources and Destinations. There is also an option to copy all the Filters from a specific Source or Destination by selecting the menu item named "All" listed below the defined Filters. If a Filter already exists with the same name when copying a Filter, the new Filter will have an asterisk (*) appended to its name.

Once a Filter has been created the next step is to configure its Conditions and Actions.

4.7.1 Conditions



A Filter's Conditions determine whether or not its Actions will be applied to the DIMSE message being processed. A Filter may have multiple conditions, therefore an option is provided that all Conditions must match, or any Conditions can match in order for the Filter to be applied.

For each Condition select the **Dicom Tag** condition type (additional types may be added in the future). Configure the rest of the Condition based upon the desired test. Conditions may be removed by pressing the red minus sign located to the left of each condition and sorted via the up and down arrow buttons.

4.7.2 Actions

If the Conditions testing was satisfied, then any defined Actions will be applied to the DIMSE message.

4.7.3 Composer Action Examples

The Composer action uses .NET regular expressions to parse an element's value and combine the parts into new elements.

1) **Swap two tags** – This example shows how to swap the values from two tags. The first Input Pattern captures the Patient's Name and the second Input Pattern captures the Patient ID into capturing groups:

Tag	Input Pattern
0010,0010	(.*)
0010,0020	(.*)

Then the Output Patterns swap the capturing groups as the value for the other tag:

Tag	Output Pattern
0010,0010	${2.1}
0010,0020	${1.1}

This results in the first pattern ${1.1} from the first input tag ${1.1} being put into the second output tag (0010,0020), and the first pattern ${2.1} from the second input tag ${2.1} being put into the first output tag (0010,0010). (In this case, the first pattern is also the entire value.) So, if you started with "`John Doe`" and "`1.2.3.4.5`" in Name and ID respectively, your result would be a Patient ID of "`John Doe`" and a Patient's Name of "`1.2.3.4.5`".

2) **Split one tag into two tags** – This example shows how to split the value from one tag into separate values for two tags. The Input Pattern takes the Accession Number (0008,0050) and captures the first 10 characters as the first capturing group and captures the remaining characters as the second capturing group:

Tag	Input Pattern
0008,0050	(^.{10})(.*)

Then the Output Patterns assign each of the capturing groups to a tag:

Tag	Output Pattern
0008,0050	${1.1}
0040,1001	${1.2}

This means that the first capturing group – the first 10 characters – will go into the Accession Number; everything else from the Accession Number will go into the Requested Procedure ID. If the initial Accession Number was

"ABCDEF1234567890", then you would have "ABCDEF1234" as the Accession Number and "567890" as the Requested Procedure ID. (Note that the output tag does not necessarily have to be parsed as an input.)

3) **Combine two tags** – This example shows how to combine the values from two tags as the value for a tag. The first Input Pattern splits the Accession Number into two capturing groups in the same manner as the previous example. The second Input Pattern splits the Requested Procedure ID capturing the first 6 characters then capturing the next 4 characters:

Tag	Input Pattern
0008,0050	(^.{10})(.*)
0040,1001	(^.{6})(.{4})

Then the Output Patterns concatenate the captured data along with plain text as the value for the tags:

Tag	Output Pattern
0008,0050	${1.1}---${2.2}---${2.1}
0040,1001	${2.1}${1.2}

If the initial Accession Number was "ABCDEF1234567890" and the initial Requested Procedure ID was "1.2.3.4.5.6.7.8.9.0", then the resulting Accession Number would be "ABCDEF1234---4.5.---1.2.3."; the resulting Requested Procedure ID would be "1.2.3.567890".

Note that the patterns can be used multiple times, as well as, combined with plain text.

4) **Insert a tag that does not exist** – This example shows how to insert a new tag that was not present in the query request from the worklist user. The condition for this example is *Specific Character Set – Does Not Exist*. The Input Pattern specifies that tag 0008,0005 does not have a value:

Tag	Input Pattern
0008,0005	

Then the Output Pattern provides the value to insert for the Specific Character Set:

Tag	Output Pattern
0008,0005	ISO_IR 100

4.7.3.1 Working with DICOM sequences

A sequence may be entered as a tag by appending it to a numeric tag (the traditional group-element pair) with a period ("."). You may also indicate an item in the sequence with "#" and the sequence

item ID, followed by the tag indicating the sequence. There may be multiple sequences and sequence IDs as part of one "tag". Examples are shown below:

- Simple tag - `0010,0010`
- Tag within sequence - `0040,0100.0008,0060`
- Tag within specific sequence item - `0040,0100.#0.0008,0060`
- Tag within nested sequence with sequence items - `0040,0100.#1.0040,0008.#0.0008,0120`

If no item number is specified, the first item (#0) is assumed. Specify the last element in a sequence by "#L" (upper-case is important!) if the number of sequence items is unknown. Specify the next item in the sequence via "#N" (again, case is important) to append to the sequence.
For example: `0040,0100.#L.0040,0008.#N.0008,0120`
Please notice that:

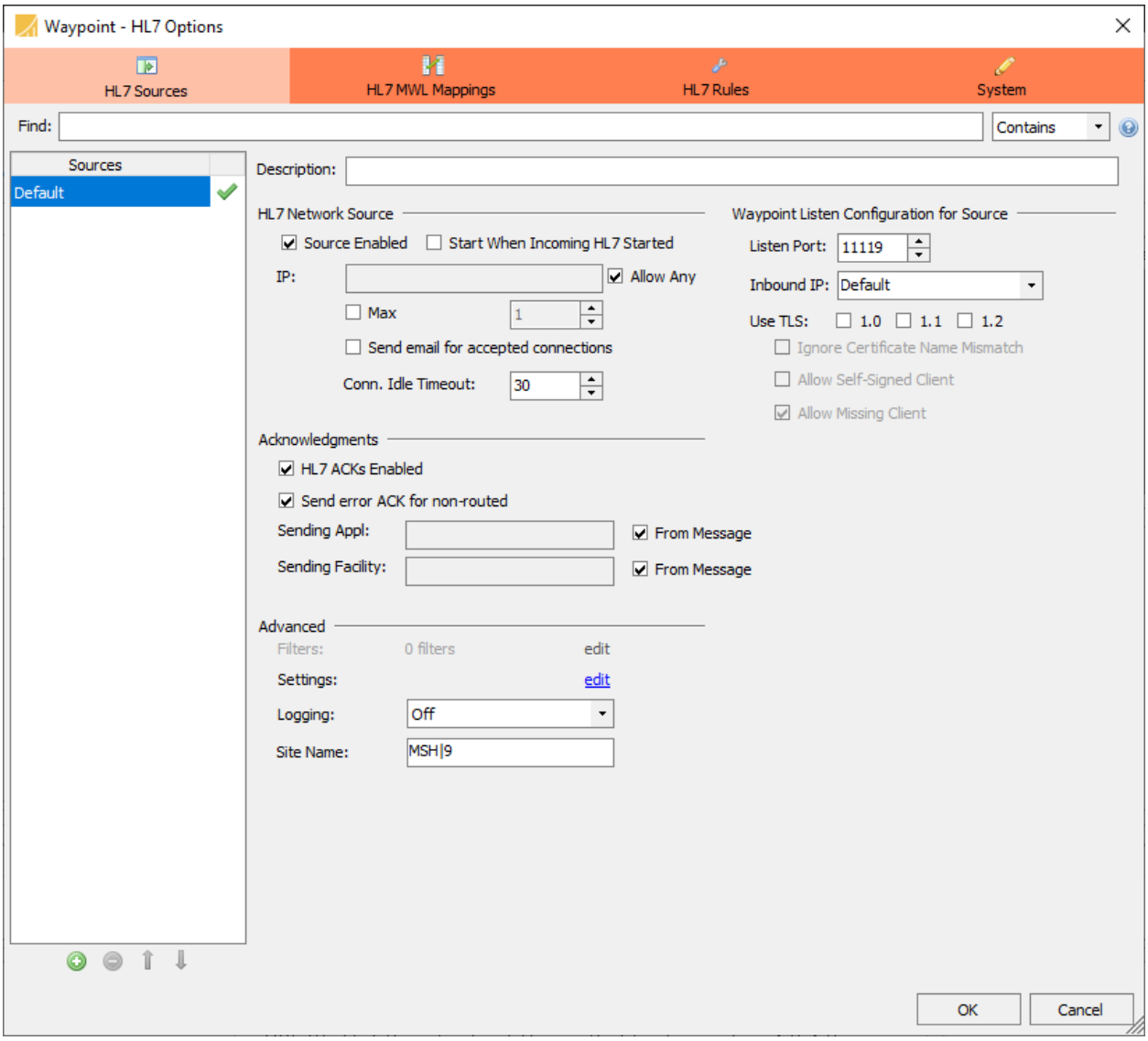
- The sequence IDs (e.g., #1) and the tag-value pairs for the sequences are all separated by periods (".").
- The tags for the sequences are simple group-element pairs themselves.

5 Configuration for HL7

Configuration for HL7 is created and edited by selecting the **Edit > HL7 Options…** from the menu. HL7 configuration categories are:

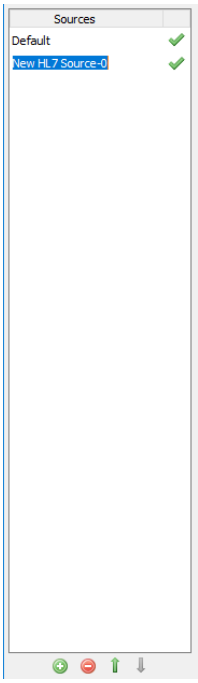
- HL7 Sources
- HL7 MWL Mappings
- HL7 Rules

Each of the configuration categories contains a predefined item with the name "Default". The configuration form for each of the items has a common format. Using HL7 Sources as an example of the format:



The left side of the form displays a menu of the items that have been added in the selected category. The Find tool matches items by name and hides items that do not match the find text. The right side of the form is category specific as described in the following sections. Creating new items in each category are described in the following sections.

5.1 Creating HL7 Sources



A new Source can be created by selecting **Edit > HL7 Options…** from the menu and then selecting the **HL7 Sources** pane. Press the green plus button located under the Sources list. This create a new HL7 Source. The list of Sources may be reordered by selecting a Source and then pressing the up or down arrows next to the green plus and red minus buttons.

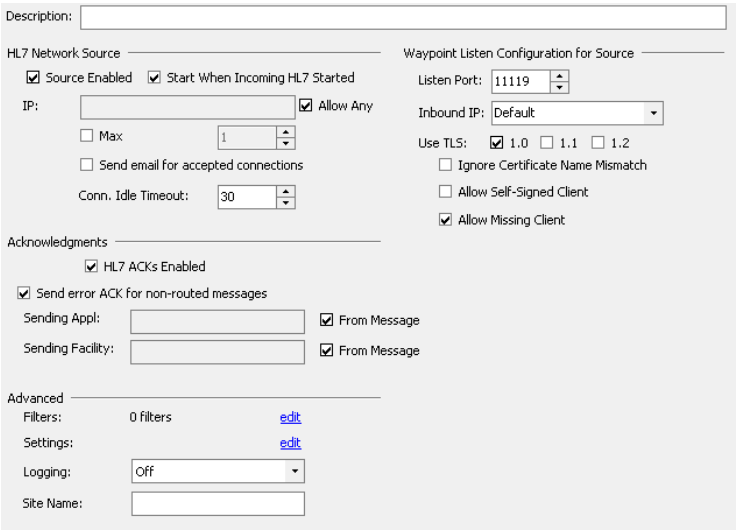
5.1.1 HL7 Source

An **HL7 Source** is any network device that will connect to Waypoint and send HL7 messages. Selecting **HL7 Source** will create a new Source with the name "New HL7 Source-?", where "?" is the next available number starting at 0. Source names are customizable and can be modified at any time by clicking on the name. When a network sender connects with Waypoint, the Sources list is processed from top to bottom and the first match found is used (excluding HL7 Web Sources); therefore, the ordering of the Sources may be important if potentially more than one could match.

Once an **HL7 Source** has been created the next step is to configure its settings.

5.1.2 HL7 Settings

Under the **HL7 Source** heading, settings include configuration options for the remote **IP**, the Enabled status of the Source, the autostart option, an option to limit the number of concurrent connections, and the type of responses that are sent back to the Source for non-routed messages. The **Allow Any** checkbox following the **IP** can be selected to allow any value for that field.



To limit the number of concurrent connections allowed by this Source check the **Max Simultaneous** checkbox and specify the desired number.

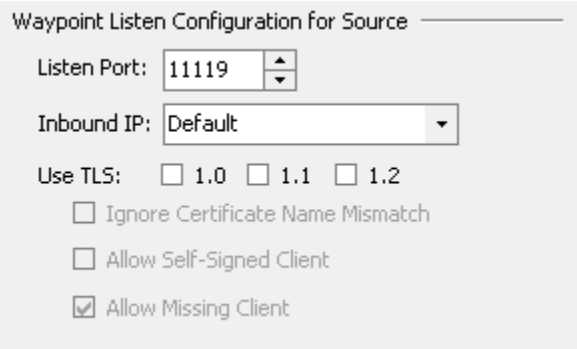
The enabled status for HL7 Sources works differently than for DICOM Destinations. For HL7 routing, it is desirable to be able to individually start and stop network traffic from a particular node. It may also be desirable to have a node configuration that exists but can never be started (e.g. during a maintenance cycle, or as an example configuration). As such, the following definitions apply:

Enabled – this means that the node is allowed to be started.
Disabled – this means that the node is not allowed to be started.
Started – this means that Waypoint has opened a listening socket on the specified IP/port for the source and either has an open network connection from that source or is waiting for such a connection.
Stopped – this means that Waypoint is not listening for connections from that source; any such connection attempt from the source will fail.

Given these definitions, the settings are easily understood. Selecting the **Source Enabled** checkbox enables the source (allowing it to be started) but does not actually start the source; deselect it to prevent the specified Source from starting. Select **Start When Incoming HL7 Started** to start this particular HL7 Source when the HL7 Incoming button on the main screen is started.

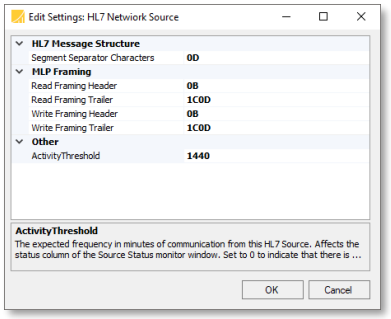
The type of response from Waypoint that will be sent to the Source can also be configured. HL7 acknowledgments can be enabled in the **HL7 ACKs Enabled** field. The acknowledgment code for messages that fail processing can also be configured. Messages fail processing if they don't match any of the defined Rules. Waypoint's default behavior is to report an error back to the Source for unprocessed messages; this is indicated by selecting the checkbox **Send error ACK for non-routed messages**. By deselecting this checkbox, Waypoint will always report back to the Source that it received the message successfully. The Sending Application and Sending Facility for the ACK messages can also be controlled. The default behavior is to use the Sending/Receiving application/facility from a received message in the reply. The user can override this behavior by unchecking **From Message** and supplying a desired value.

Under the **Waypoint Listen Configuration for Source** heading, a user specifies which network port Waypoint will use to listen for traffic from this source. In this way, HL7 Network Sources differ from DICOM Sources; each HL7 Network Source has its own unique listening port. The **Inbound IP** combo box is used to determine which system IP address Waypoint will use for listening purposes for this Source.



The **Use TLS** checkboxes specify whether network communications with the specified HL7 Source will be encrypted using TLS (as well as which TLS versions will be supported). The **Ignore Certificate Name Mismatch Errors** and **Allow Self-Signed Client Certificates** checkboxes can be used to relax the Waypoint certificate validation for this HL7 Source. However, we strongly recommend using these options for testing only, as they greatly reduce security by preventing full TLS authentication from occurring. The **Allow Missing Client Certificates** checkbox can be used to control whether or not client certificates (i.e., client authentication) are required (note that server authentication is always mandatory).

Using TLS also requires that the TLS certificate information is configured correctly in the **System** pane – **see section 7.2.5 Waypoint TLS Certificate Configuration** for more information. **See also Appendix C:, Section 1.3 Configuring Secure HL7 Communication** for more details about using Waypoint TLS support.



Under the **Advanced** heading, a user can give more in-depth control over how a Source communicates with Waypoint. The **Filters** link is currently unavailable – it will be supported in future Waypoint releases. Data handling options and link-level framing characters are areas which can be configured in finer detail when editing the **Settings** options. Verbose logging can be turned on or off on a per Source basis by selecting 'On' or 'Off' in the **Logging** combo box. When sending an outbound job, the IP address Waypoint will use can be specified by the **Source** via the **Outbound IP** combo box, if and only if the Destination that the job is targeted for has its **Host/IP** combo box set to Default. The **Site Name** field is a free-form text field which is used to help the user group/view Sources and Destinations on the main user interface screen. The user may type any text in this field he desires.

5.2 Creating HL7 MWL Mappings

A new MWL Mapping can be created by selecting **Edit > HL7 Options…** from the menu and then selecting the **HL7 MWL Mappings** pane. The MWL Mapping presents Waypoint's database schema as Groups, i.e. database tables, and Mapping Groups, i.e. columns within the selected Group. For each Mapping Group, **HL7 MWL Mappings** allow you to specify:

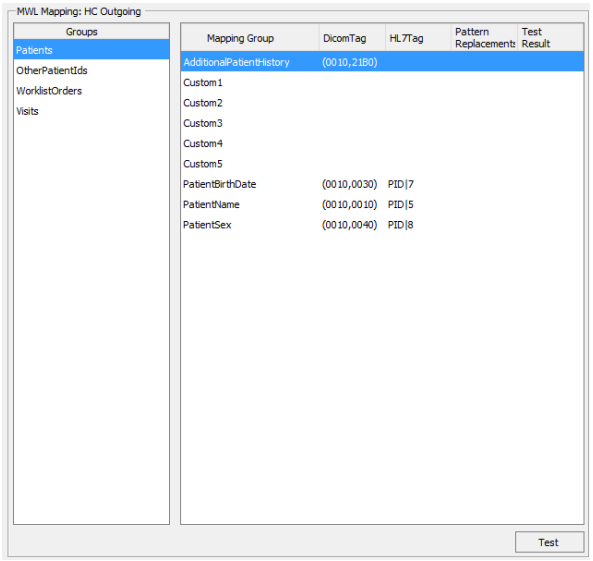
- Dicom Tag
- HL7 Tag
- Pattern Replacements

To aid with configuring an HL7 MWL Mapping, see **section 5.2.4 Testing HL7 MWL Mappings** for a description of the testing tool that is provided.

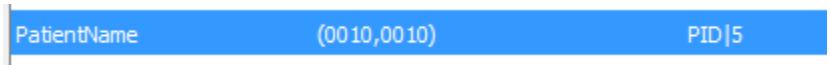
HL7 MWL Mappings define rules for how to parse HL7 incoming messages for storage in Waypoint's database, when they are applied to HL7 Rules. MWL Mappings are also used to define rules to parse the data stored in Waypoint's database for outgoing DICOM response messages when they are applied to DICOM Rules. Press the green plus button located under the MWL Mappings list. A context menu for adding a new HL7 MWL Mappings is displayed that contains two entries: *Worklist Defaults* and *Procedure Step Defaults*. Selecting *Worklist Defaults* creates the traditional HL7 MWL Mapping as seen in previous versions of Waypoint with DICOM Tags and HL7 Tags that are the common values for the

DICOM Modality Worklist Service. Selecting *Procedure Step Defaults* creates an HL7 MWL Mapping with DICOM tags that are the common values for DICOM Modality Performed Procedure Step. Note, HL7 tags are not defined for Modality Performed Procedure Steps. The new MWL Mapping will be created with the name "New MWL Mapping-?" or "New MPPS Mapping-?"", where "?" is the next available number starting at 0. Mapping names are customizable and can be modified at any time by clicking on the name. The Mappings can be re-ordered using the up and down arrows at the bottom of the list. The ordering of the Mappings are strictly for display purposes and do not affect how HL7 or DICOM Rules apply the MWL Mapping. Once an **HL7 MWL Mapping** has been created the next step is to configure its settings.

Under the **MWL Mapping: <name>** heading, settings include configuration options for the Dicom Tag, HL7 Tag, and Pattern Replacements for the currently selected Mapping Group. The new HL7 MWL Mapping is initialized with default values that are shown in the Waypoint DICOM Conformance Statement. The Dicom Tag uses the `(group,element)` format as defined in the DICOM Standard. A sequence element has the format: (SQgroup,SQelement.group,element) The HL7 tag has the SEGMENT|FIELD format as defined by the HL7 version 2 standard. **See section 5.3 Creating HL7 Rules** for more information about HL7 message formats.



For example, Patients/PatientName has the DICOM Tag `(0010,0010)` with the HL7 Tag `PID|5`:



As an example of a sequence element, the Schedule Procedure Step Modality is the Modality element in the Scheduled Procedure Step Sequence, therefore the DICOM Tag is `(0040,0100.0008,0060)` and for this example, the HL7 Tag is `OBR|21.1`:

Waypoint stores the following items as datetime values in the database:

- PatientBirthDate
- ScheduledProcedureStepStartDate
- ScheduledProcedureStepEndDate
- StudyDate

Each of these values must be presented in a valid date/time format to be stored in the database. The field in the HL7 message can be either in the DICOM format (yyyymmdd) or in the common format (mm/dd/yyyy).

5.2.1 Pattern Replacements

Pattern Replacements provide a powerful tool to filter the data from the HL7 message before it is stored in the database. The Match can be a literal constant or a Regular Expression and the Replacement is substituted for the value when a match occurs. The most common Regular expressions used for Pattern Replacements are:

- ^$ - matches an empty value
- ^.*$ - matches any value

For example, ScheduledProcedureStepStartDate may have the Pattern Replacement:

Match: ^$
Replacement: ${YESTERDAY}-${TOMORROW}

The affect is, if the ScheduledProcedureStepStartDate has a value, then use the value to search for worklist orders. If ScheduledProcedureStepStartDate does not have a value, substitute the date range for yesterday thru tomorrow.
As another example, Modality may have the Pattern Replacement:

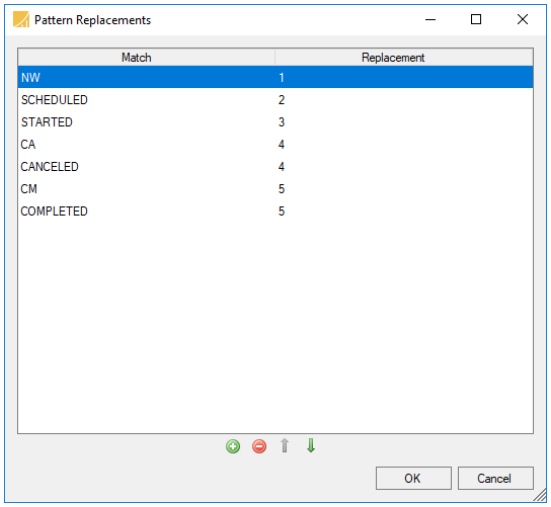
Match: ^.*$
Replacement: DR or XA

The affect is, ignore the value for Modality and only match “DR” or “XA”.

As a final example, the Radiology Information System (RIS) creates orders with a new order status, NW, then sends updates to change the scheduled status to started then completed or canceled. The order status field in an HL7 ORM message is ORC|5, however, some systems use the order control field ORC|1. If the status is originally a numerical value or it is mapped to a numerical value, Waypoint will enforce a policy as a form of flow control whereby values cannot be set to a lesser value. For example, a 5 (Completed) cannot be updated to a status of 2 (Scheduled). Only scheduled status values stored as integers adhere to this policy. Non-integer scheduled status values are not restricted in their transition to another scheduled status value.

Example scheduled status values:

Value	Status
1	New
2	Scheduled
3	Started
4	Canceled
5	Completed



The Pattern Replacements feature allows you to create substitution patterns to replace the value from the HL7 message with the numerical value from the table above to store in the worklist order. This Pattern Replacements shows the value to match from ORC|5 with the replacement value to store for the worklist item. Note, the match values shown here may not be the same as the status values used in your organization.

Each Match has a corresponding Replacement value that is used when the match is successful. This first example was a simple replacement map from one value to another, e.g., NW is replaced with 1. As described above, the match performs full regular expression parsing including the ability to capture data from the input string and insert those values into the replacement string. As an example of this feature, the following HL7 message has the modality as the first word in the HL7 field ORC|24:

```
OBR|1|A100Z^MESA_ORDPLC|B100Z^MESA_ORDFIL|P1^Proce dure 1^ERL_MESA^X1_A1^SP Action Item
X1_A1^DSS_MESA|||||||||xxx||Radiology^^^^R|7101^ES
TRADA^JAIME^P^^DR||XR999999|RP123456|SPS123456||||MR on chest and
abdomen|||1^once^^^^S|||WALK||||||||||A|||RP_X1^RP Action Item RP_X1^DSS_MESA
```

Field OBR|24 contains the value “MR on chest and abdomen”. The regular expression “^([^\s]+)” captures the first word in this field as the modality. The replacement “{1}” designates the first captured value and is stored as the Modality of this order. Note, multiple captured values are accessed using the format index as the replacement value, e.g. {1}, {2}, {3}, ... A full description of regular expressions is beyond the scope of this user manual. Please refer to other documentation for more information on regular expressions.

Mapping Group	DicomTag	HL7Tag	Pattern Replacements	Test Result
AccessionNumber	(0008,0050)	ZDS|1.1.2 ?? ...		100
Custom1				
Custom2				
Custom3				
Custom4				
Custom5				
FillerOrderNumber	(0040,2017)			
InstitutionName	(0008,0080)	OBR|20.4		
Modality	(0040,0100.0008,0060)	OBR|24	"^([^\s]+)" | {1}	MR

5.2.2 HL7 MWL Mappings for DICOM Rule Actions

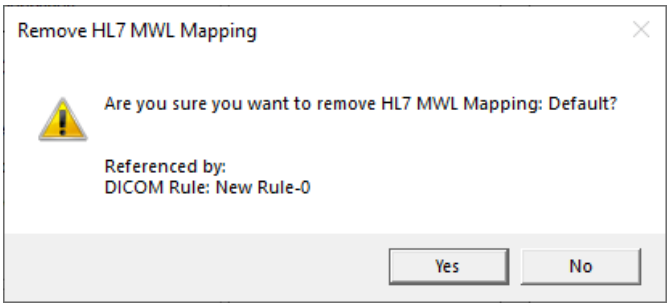
As mentioned in **section 4.3.3 Rule Actions** a selected HL7 MWL Mapping is used to define how to generate the C-Find response message for a query request. The HL7 MWL Mapping specifies the:

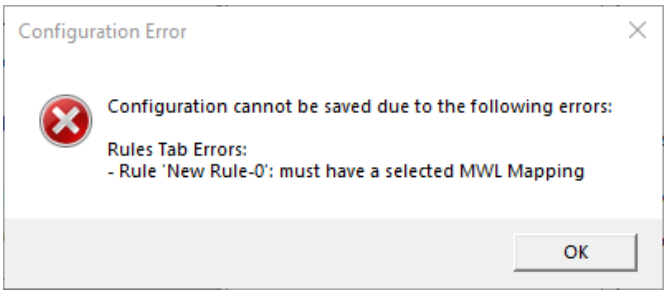
- Group and Mapping Group that defines the database table and column to select
- DicomTag to use in the response message
- Pattern Replacements option to filter the data before the value is inserted into the response message.

The Pattern Replacements feature is used to provide default values for DICOM elements that were not populated by an HL7 message and therefore do not have a value in the database. For example, the Requested Procedure Code Sequence/Coding Scheme Designator (0032,1064.0008,0102) has the default value “LOCAL, as shown:

5.2.3 Removing HL7 MWL Mappings

The context menu for HL7 MWL Mappings includes a menu item to Remove the selected HL7 MWL Mapping, see **section 4.6 Import, Export and More on the Context Menu**. As a safeguard, if the selected HL7 MWL Mapping is referenced by a HL7 Rule, DICOM Rule or DICOM Worklist Provider, a warning dialog box is displayed to acknowledge with either Yes or No to proceed with removing the selected HLMWL Mapping.





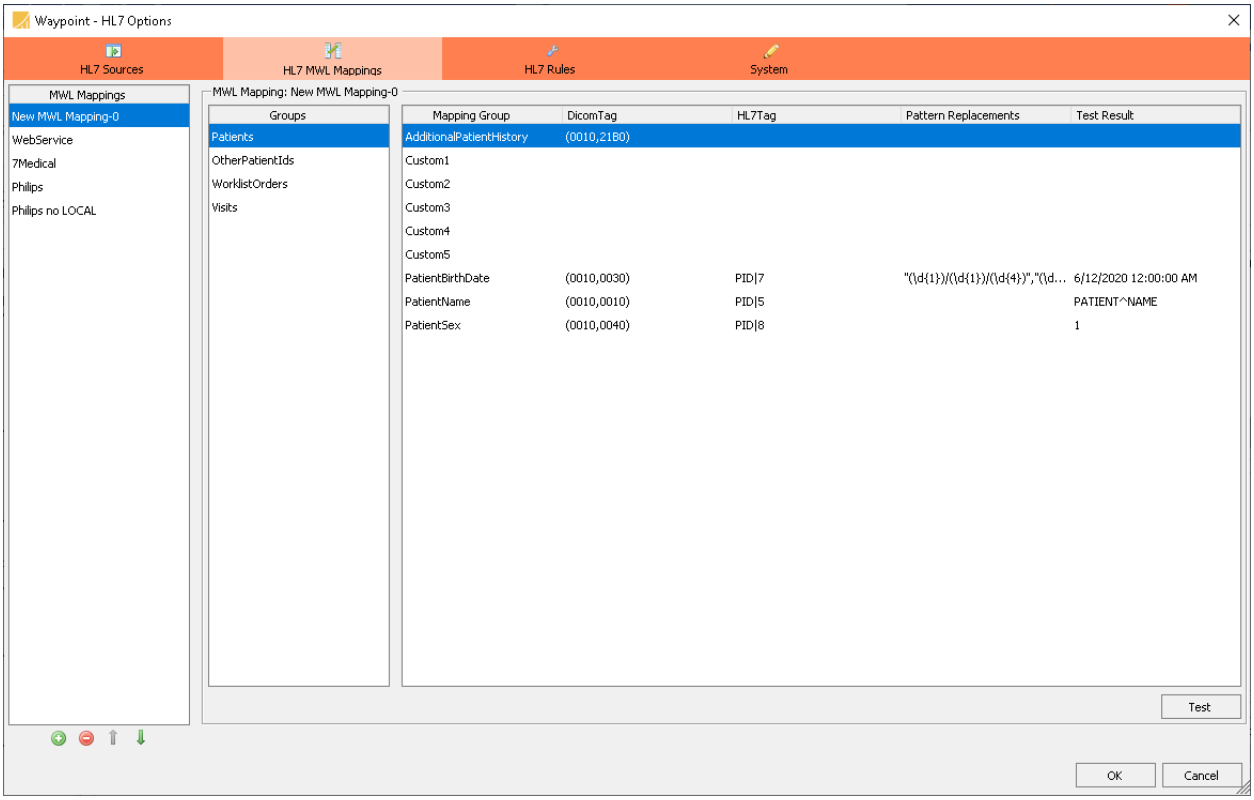
If Yes is selected, a new HL7 MWL Mapping must be selected for the Rule or Worklist Provider that was referencing the deleted HL7 MWL Mapping.

5.2.4 Testing HL7 MWL Mappings

HL7 MWL Mappings provides a convenient user interface to test mapping results against an actual HL7 message. To initiate the test, click the Test button in the lower right corner of the HL7 MWL Mapping pane.
The next step is to copy an HL7 message into the system clipboard by highlighting the text of 06 1message from an editor, such as Notepad, and typing control-C to copy the text to the clipboard. When you click the Test button, a new MWL Mappings window will open to allow you to examine the contents of the HL7 message. Click the Paste button at the bottom and the window: As you click in the Message Template, the lower panels show the HL7 tags that apply to the field you clicked on in the message template. In this example, clicking on “PID1~PID2~PID3” in the PID segment shows:

- PID|3 field name is Patient Identifier List
- PID|3 is “IPID1&PID1^IPID2&PID2^IPID3&PID3”
- PID|3.1 is “IPID1&PID1^IPID2&PID2^IPID3&PID3”
- PID|3.1.1 is “IPID1&PID1”
- PID|3.1.1.2 is “PID1”

Click the OK button to see how the MWL Mapping was applied to this HL7 message in the Test Result column:



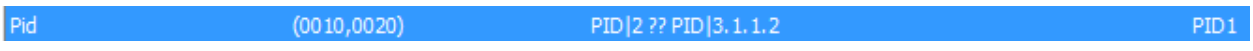
Note, the expected results for Patient demographics were obtained:

- PatientBirthDate from PID|7 was 6/12/2020 and is displayed in the full date/time format that is stored in Waypoint's database for this value.
- PatientName from PID|5 was "PATIENT^NAME"
- PatientSex from PID|8 was 1, (note Male is 0 and Female is 1 in Waypoint)

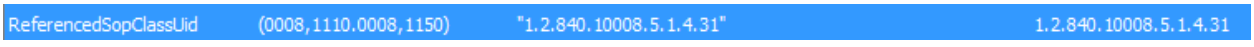
The HL7 MWL Mappings for WorklistOrders shows a variety of features available with HL7 Tags and Pattern Replacements. In addition to extracting fields directly from the HL7 message you can also:

- Select an alternate field when the message has an empty value for the first selection
- Ignore the HL7 message and provide a string constant
- Concatenate string constants with one or multiple HL7 fields
- Apply a Pattern Replacement to any of the above values to generate the final value

The Patient ID prefers PID|2 if it has a value, then uses PID|3.1.1.2 when PID|2 is empty:



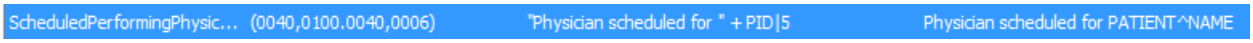
Here is an example of using the string constant `1.2.840.10008.5.1.4.31` for the ReferencedSopClassUid:



Here is an example of using the ${UUID} macro to generate the ReferencedSopInstanceUid:

Here is an example of using the ${NEWUID} macro to generate the ReferencedPatientSopInstanceUid:

Here is an example of concatenating a string constant to the patient name from PID|5:

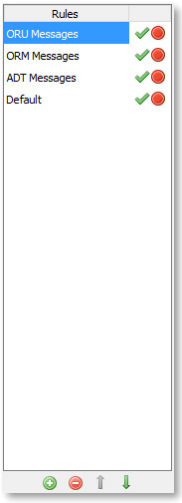


When the Logging Verbosity is set to Verbose, a detailed message is written to Waypoint Client logs showing the results of the HL7 MWL Mapping test. This helps diagnose unexpected test results indicating the HL7 tag or pattern replacement is incorrect. For example:

```
[Debug 2020-06-17T11:15:51.195 LaurelBridge.Waypoint.Core.Logging
20200617T094227222P16924N1]
Worklist-HL7:
  PatientName="PATFIRSTNAME^PATLASTNAME":24
  PatientBirthDate="19450800":8
"19450800" from HL7 tag PID|7 is an invalid value for PatientBirthDate
Reason: 19450800 is not a valid DA or DT
```

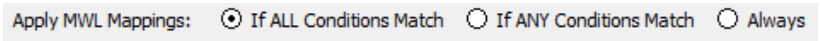
This log message shows the PatientBirthDate is invalid because the date is 00.

5.3 Creating HL7 Rules



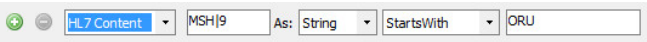
A new Rule can be created by selecting **Edit > HL7 Options…** from the menu and then selecting the **Rules** pane. Press the green plus button located under the Rules list. This will create a new Rule with the name "New Rule -?" where "?" is the next available number, starting at 0. Rule names are customizable and can be modified at any time by clicking on the name. The list of Rules may be reordered by selecting a Rule and then pressing the up or down arrows directly to the right of the Rules list. When Waypoint processes the list of Rules for each received HL7 message, the Rules list is processed from top to bottom and the first match found is used, therefore the ordering of the Rules may be important if potentially more than one could match.
Once a Rule has been created the next step is to configure its Conditions, MWL Mapping and Rule Options.

5.3.1 HL7 Rule Conditions



A Rule's Conditions determine whether or not its Actions will be applied to a message being processed. A Rule may have multiple conditions, in which case it may be specified that either all the conditions must apply to the message or that only one condition must apply to the message in order for the Rule to match.

Another option is that the Rule always matches; effectively declaring it to have no Conditions. Selecting one of three radio buttons, **If ALL Conditions Match**, **If ANY Conditions Match**, and **Always**, will implement one of these three scenarios.
The **HL7 Content** condition allows incoming worklist items to be selected for this Rule based upon their contents.



When using this condition, the user specifies which piece of the HL7 message is being considered. The specified piece is described with a "query string" which takes one of the following forms:

```
XYZ|f
XYZ|f.r
XYZ|f.r.c
XYZ|f.r.c.s
```

Where the pieces are:

`XYZ` the three-letter code which indicates which segment in the HL7 message is being examined. Examples might include `MSH`, `PID`, `ORC`, `OBR`, etc.
`f` a number, starting at 1, to indicate which *field* in the specified segment is being examined.
`r` a number, starting at 1, to indicate which *repetition* in the specified field is being examined.
`c` a number, starting at 1, to indicate which *component* in the specified repetition is being examined.
`s` a number, starting at 1, to indicate which *subcomponent* in the specified field is being examined.

Example query strings:
`MSH|9` – the 9th field of the MSH segment
`PID|5.1` – the 1st repetition of the 5th field of the PID segment
`PID|5.1.2` – the 2nd component of the 1st repetition of the 5th field of the PID segment
`PID|5.1.2.3` – the 3rd subcomponent of the 2nd component of the 1st repetition of the 5th field of the PID segment

A typical encoding of an HL7 2.x message separates its contents into segments, one per line, starting with a 3-letter segment code. Usually, the pipe character (|) is used to separate fields within that segment. Each field can then be divided into repetitions, usually via the tilde character (~). Repetitions may be divided into components, typically via the caret character (^). Finally, components may be divided into subcomponents, usually with the ampersand character (&). One important note: in common HL7 parlance, components may be described via the segment, field number, and component number. For example: one might speak of "PID 5-2" to mean "Patient Name, First Name". However, Waypoint needs to be able to allow users the ability to address particular repetitions of fields, even if the field has only one repetition in a particular message. As such, to address a particular component, the query string must specify the repetition number as well. So, in Waypoint, to address the 2nd component of a single-repetition Patient Name, the query string would be "`PID|5.1.2`", even if only one repetition exists.
Consider the following example segment:

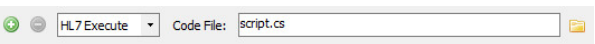

```
PID|1||597871^^^^EPI||ZZTEST^JOHN-
PUBLIC^Q||19611116|F|TEST^PATIENT^~ZZTEST^JOHNPUBLIC^F^|NH|1 SITENAME
```

The following table shows some examples of using query strings in the **HL7 Content** condition to access different parts of the message:

Query String	Value	Comment
PID|3	597871^^^^EPI	The entirety of field 3 in the PID segment
PID|3.1	597871^^^^EPI	The entirety of the first repetition of field 3. Note that for this segment, this is the same value as PID|3, as there is only one repetition in this field (no ~ character).
PID|3.2	Error	This would be the second repetition of field 3, but since there is only one repetition present, this would be an error.
PID|3.1.1	597871	First component of first repetition of field 3
PID|3.1.5	EPI	Fifth component of first repetition of field 3
PID|4	<empty>	Field 4 is empty
PID|5	ZZTEST^JOHN-PUBLIC^Q	The entirety of field 5 in the PID segment
PID|5.1	ZZTEST^JOHN-PUBLIC^Q	The entirety of the first repetition of field 5. Note that for th segment, this is the same value as PID|5, as there is only on repetition in this field (no ~ character).
PID|5.1.1	ZZTEST	First component of first repetition of field 5
PID|5.1.2	JOHN-PUBLIC	Second component of first repetition of field 5
PID|5.1.3	Q	Third component of first repetition of field 5
PID|7	19611116	The entirety of field 7 in the PID segment
PID|8	F	The entirety of field 8 in the PID segment
PID|9	TEST^PATIENT^~ZZTEST^JOHNPUBLIC^F^	The entirety of field 9 in the PID segment
PID|9.1	TEST^PATIENT^	The entirety of the first repetition of field 9.
PID|9.2	ZZTEST^JOHNPUBLIC^F^	The entirety of the second repetition of field 9.
PID|9.2.2	JOHNPUBLIC	Second component of second repetition of field 9.

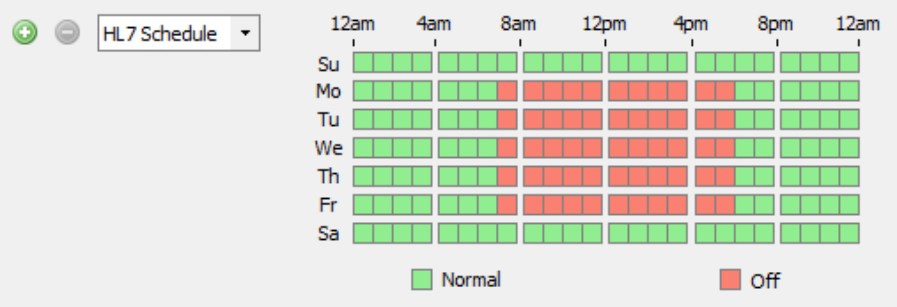
The **HL7 Connection** condition allows incoming messages to be selected for this Rule based upon their incoming HL7 Connection information.

The **HL7 Execute** condition allows incoming messages to be selected for this Rule based upon a custom, user-defined rule condition. Note, following any changes to the custom code file, it is required to edit HL7 options and click OK to load the changed custom code file for execution. See **section 5.3.3 Custom HL7 Rule Condition Example** for an example of a custom rule condition implementation.



The **HL7 Schedule** condition allows incoming messages to be selected for this Rule based upon the time of day and day of week that the message was received. Any squares which are green in

the schedule represent time/day blocks where the condition is true; any squares which are red represent time/day blocks where the condition is false. Each square can be changed individually by clicking on it. Alternately, the user can right-click to select from a menu of preset schedules for ease of populating the schedule as desired.



Configure the condition based upon the desired test. Conditions may be added or removed by pressing the green plus sign or the red minus sign located to the left of each condition.

5.3.2 Custom HL7 Rule Condition Example

The rule can be created to execute custom condition code to determine whether a particular HL7 message matches a particular HL7 rule. When the condition for an HL7 Rule uses the HL7 Execute condition, Waypoint loads and compiles the specified source file. The custom source file provides the implementation for the Match condition and returns true for an accepted match or false for a rejected match. The HL7 Connection Parameters and the HL7 message are passed to the Match function to evaluate the condition. Note, the last parameter is a custom config data dictionary that is not yet implemented by Waypoint.

The following examples show custom rule conditions:

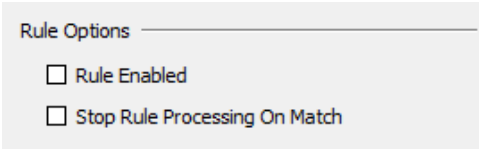
```
using System;
using System.Collections.Generic;
using System.IO;
using LaurelBridge.DCF;
using LaurelBridge.DCF.Dicom;
using LaurelBridge.DCF.Dicom.Dimse;
using LaurelBridge.DCF.Dicom.Elements;
using LaurelBridge.DCF.Dicom.IODs;
using LaurelBridge.DCF.Dicom.ProcedureStep;
using LaurelBridge.DCF.IO;
using LaurelBridge.HL7;
using LaurelBridge.Waypoint.ClientCore;
using LaurelBridge.Waypoint.Core;
using LaurelBridge.Waypoint.Core.Conditions;
using LaurelBridge.Waypoint.Core.Plugins;
using LaurelBridge.Waypoint.Core.Repositories;

namespace Example
{
   public class CustomHL7ExecuteCondition : IHL7ExecuteCondition
   {
      public bool Matches(
```



```
        IHL7ConnectionParameters connParameters,
        HL7Message hl7msg,
        Dictionary<string, string> parentRuleCustomConfigData)
    {
        return true;
    }
  }
}
```

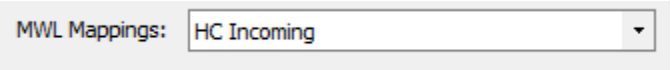
5.3.3 Rule Options



Uncheck the **Rule Enabled** checkbox to disable the selected Rule. If unchecked, the Rule will be passed over during Rule processing.
Check the **Stop Rule Processing On Match** checkbox if no further Rules in the Rules list should be processed if this Rule matches (Rules are processed sequentially from the top of the list to the bottom of the list). If unchecked, Rule processing will proceed to the next Rule even if this Rule matches.

5.3.4 Rule Actions

If all of the Conditions for the Rule pass, then the message currently being processed will have the currently selected MWL Mapping applied. The drop-down list contains the names of all available HL7 MWL Mappings.



5.4 Import, Export and More on the Context Menu

HL7 Sources, HL7 MWL Mappings, and HL7 Rules provide the same context menu described previously for DICOM Configuration. See **section 4.6 Import, Export and More on the Context Menu** for a description of the Context Menu.

6 DICOM Web Services

Waypoint supports the DICOM Web Service UPS-RS Search for UPS. Additional Web Services may be supported in future Waypoint releases.

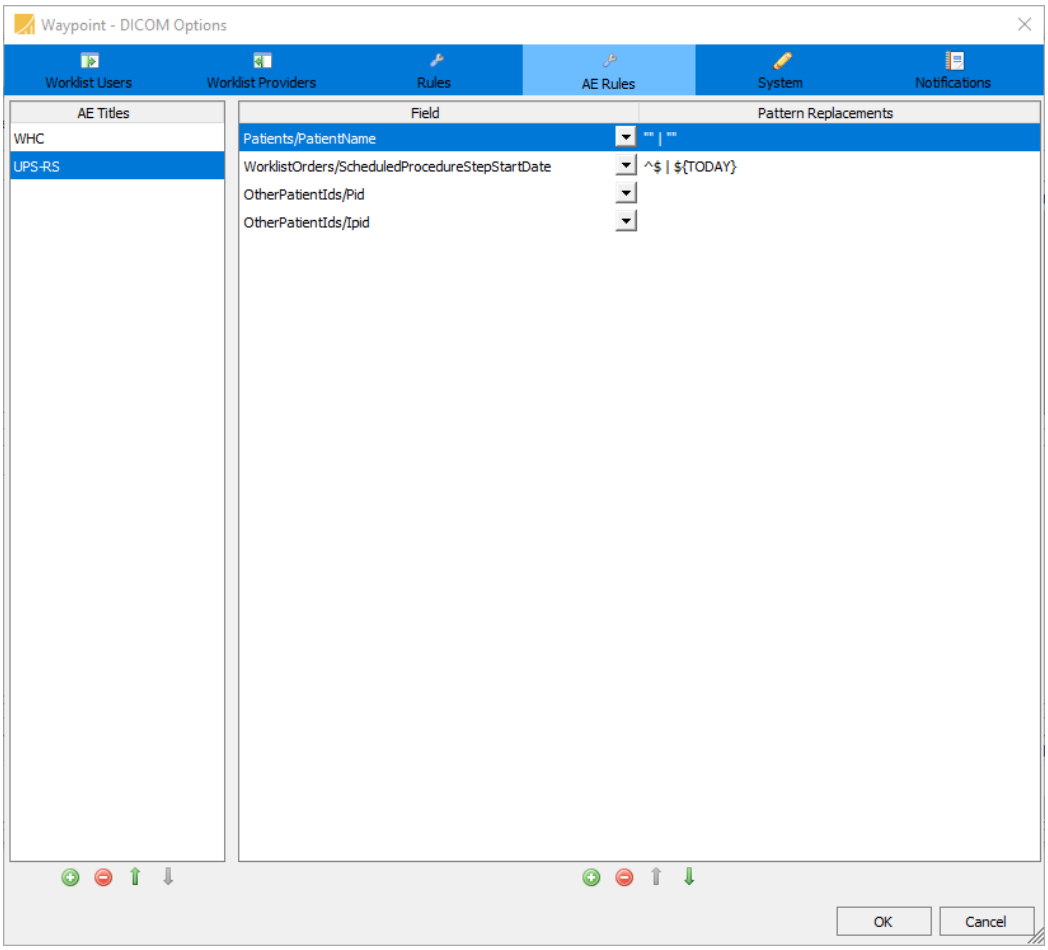
6.1 UPS-RS SearchForUPS

SearchForUPS is a UPS RESTful query that is very much like a MWL C-Find request, except through HTTP UPS-RS interface. The query string specifies the matching and returning fields from the query. The following sample URL shows a SearchForUPS query that matches Scheduled Procedure Step Start Date for 20181126 and all Accession Numbers that match the pattern “160159*”.

```
http://localhost:12347/api/workitems?00400100.00400002=20181126&00080050=160159*
```

The AE Rules in Waypoint configuration allow you to append DICOM tags to the query to automatically match or retrieve additional DICOM tags data without having to build them into the query string.
The AE Rules shown below perform the following:

- Return all Patient Names if the query string does not contain a matching Patient Name
- If the query string does not have a specific Scheduled Procedure Start Date, automatically match orders with today’s date



The SearchForUPS query shown above returns the following responses encoded in JSON. Note, each response contains:

- Accession Number (00080050), from query string
- Patient Name (00100010), from AE Rule
- Patient's ID (00100020), from AE Rule
- Issuer of PID (00100021), from AE Rule
- Scheduled Procedure Step Start Date (00400100.00400002), from query string


```
"[{\"00080050\":{\"vr\":\"SH\",\"Value\":[\"1601593\"]}},{\"00100010\":{\"vr\
":\"PN\",\"Value\":[\"TEBBETTS^JOELLE\"]}},{\"00100020\":{\"vr\":\"LO\",\"Val
ue\":[\"884353\"]}},{\"00100021\":{\"vr\":\"LO\",\"Value\":[\"Laurel
Bridge\"]}},{\"00400100\":{\"vr\":\"SQ\",\"Value\":[[{\"00400002\":{\"vr\":\"
DA\",\"Value\":[\"20181126\"]}}]]}}]","[{\"00080050\":{\"vr\":\"SH\",\"Value\
":[\"1601594\"]}},{\"00100010\":{\"vr\":\"PN\",\"Value\":[\"LONGIE^ZOE\"]}},{
\"00100020\":{\"vr\":\"LO\",\"Value\":[\"756037\"]}},{\"00100021\":{\"vr\":\"
LO\",\"Value\":[\"Laurel
Bridge\"]}},{\"00400100\":{\"vr\":\"SQ\",\"Value\":[[{\"00400002\":{\"vr\":\"
DA\",\"Value\":[\"20181126\"]}}]]}}]","[{\"00080050\":{\"vr\":\"SH\",\"Value\
":[\"1601598\"]}},{\"00100010\":{\"vr\":\"PN\",\"Value\":[\"BROOKSKENNEDY^MAR
NIE\"]}},{\"00100020\":{\"vr\":\"LO\",\"Value\":[\"671626\"]}},{\"00100021\":
{\"vr\":\"LO\",\"Value\":[\"Laurel
Bridge\"]}},{\"00400100\":{\"vr\":\"SQ\",\"Value\":[[{\"00400002\":{\"vr\":\"
DA\",\"Value\":[\"20181126\"]}}]]}}]","[{\"00080050\":{\"vr\":\"SH\",\"Value\
```



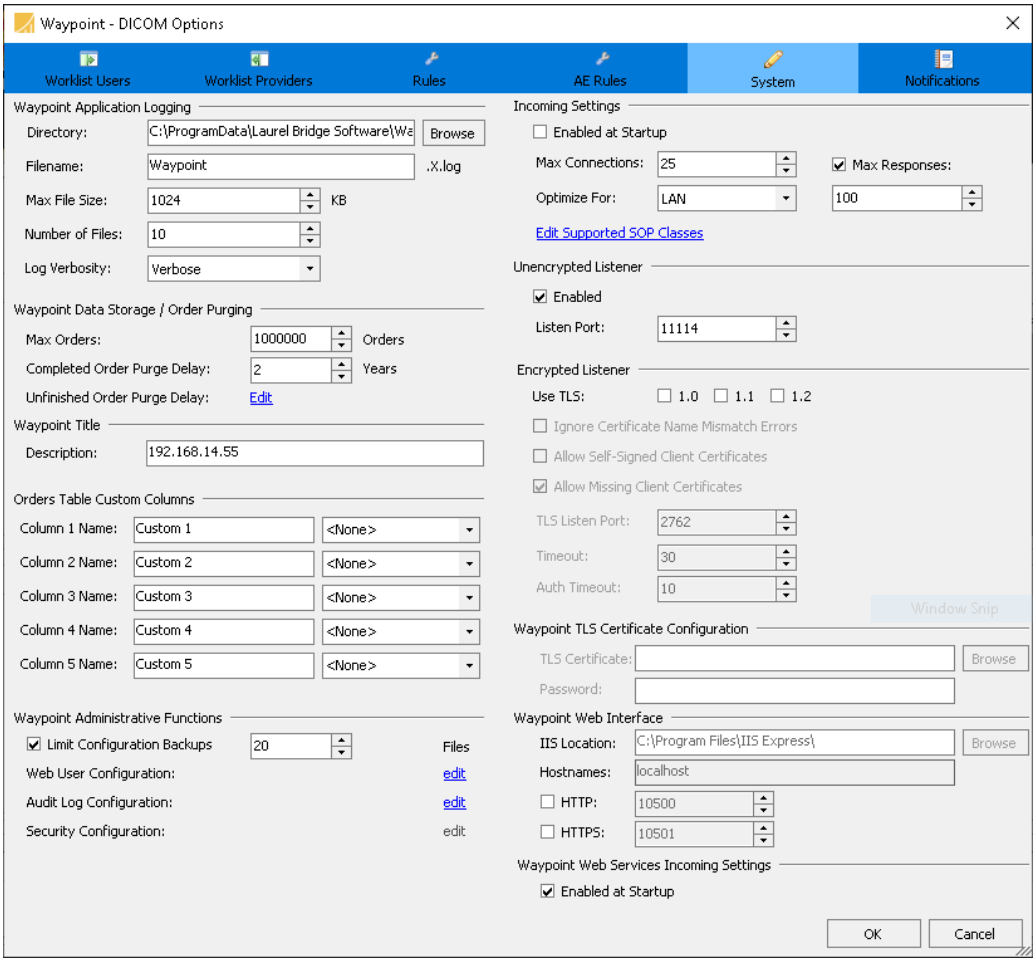
```
":[\"1601595\"]}},{\"00100010\":{\"vr\":\"PN\",\"Value\":[\"FELDKER^CASSIDY\"
]}},{\"00100020\":{\"vr\":\"LO\",\"Value\":[\"339938\"]}},{\"00100021\":{\"vr
\":\"LO\",\"Value\":[\"Laurel
Bridge\"]}},{\"00400100\":{\"vr\":\"SQ\",\"Value\":[[{\"00400002\":{\"vr\":\"
DA\",\"Value\":[\"20181126\"]}}]]}}]","[{\"00080050\":{\"vr\":\"SH\",\"Value\
":[\"1601597\"]}},{\"00100010\":{\"vr\":\"PN\",\"Value\":[\"KUBE^VICTOR\"]}},
{\"00100020\":{\"vr\":\"LO\",\"Value\":[\"724845\"]}},{\"00100021\":{\"vr\":\
"LO\",\"Value\":[\"Laurel
Bridge\"]}},{\"00400100\":{\"vr\":\"SQ\",\"Value\":[[{\"00400002\":{\"vr\":\"
DA\",\"Value\":[\"20181126\"]}}]]}}]","[{\"00080050\":{\"vr\":\"SH\",\"Value\
":[\"1601599\"]}},{\"00100010\":{\"vr\":\"PN\",\"Value\":[\"DANOS^ROGELIO\"]}
},{\"00100020\":{\"vr\":\"LO\",\"Value\":[\"791444\"]}},{\"00100021\":{\"vr\"
:\"LO\",\"Value\":[\"Laurel
Bridge\"]}},{\"00400100\":{\"vr\":\"SQ\",\"Value\":[[{\"00400002\":{\"vr\":\"
DA\",\"Value\":[\"20181126\"]}}]]}}]","[{\"00080050\":{\"vr\":\"SH\",\"Value\
":[\"1601591\"]}},{\"00100010\":{\"vr\":\"PN\",\"Value\":[\"SALVETTI^GUY\"]}}
,{\"00100020\":{\"vr\":\"LO\",\"Value\":[\"412308\"]}},{\"00100021\":{\"vr\":
\"LO\",\"Value\":[\"Laurel
Bridge\"]}},{\"00400100\":{\"vr\":\"SQ\",\"Value\":[[{\"00400002\":{\"vr\":\"
DA\",\"Value\":[\"20181126\"]}}]]}}]","[{\"00080050\":{\"vr\":\"SH\",\"Value\
":[\"1601592\"]}},{\"00100010\":{\"vr\":\"PN\",\"Value\":[\"ENGELKING^KALYN\"
]}},{\"00100020\":{\"vr\":\"LO\",\"Value\":[\"863022\"]}},{\"00100021\":{\"vr
\":\"LO\",\"Value\":[\"Laurel
Bridge\"]}},{\"00400100\":{\"vr\":\"SQ\",\"Value\":[[{\"00400002\":{\"vr\":\"
DA\",\"Value\":[\"20181126\"]}}]]}}]","[{\"00080050\":{\"vr\":\"SH\",\"Value\
":[\"1601590\"]}},{\"00100010\":{\"vr\":\"PN\",\"Value\":[\"POTH^ANGIE\"]}},{
\"00100020\":{\"vr\":\"LO\",\"Value\":[\"681408\"]}},{\"00100021\":{\"vr\":\"
LO\",\"Value\":[\"Laurel
Bridge\"]}},{\"00400100\":{\"vr\":\"SQ\",\"Value\":[[{\"00400002\":{\"vr\":\"
DA\",\"Value\":[\"20181126\"]}}]]}}]","[{\"00080050\":{\"vr\":\"SH\",\"Value\
":[\"1601596\"]}},{\"00100010\":{\"vr\":\"PN\",\"Value\":[\"SHANBERG^VAN\"]}}
,{\"00100020\":{\"vr\":\"LO\",\"Value\":[\"428960\"]}},{\"00100021\":{\"vr\":
\"LO\",\"Value\":[\"Laurel
Bridge\"]}},{\"00400100\":{\"vr\":\"SQ\",\"Value\":[[{\"00400002\":{\"vr\":\"
DA\",\"Value\":[\"20181126\"]}}]]}}]"
```


7 System Settings

System settings can be configured by selecting either the **Edit > DICOM Options…** or **Edit > HL7 Options** from the menu and then selecting the **System** pane. Some options are universal across both the DICOM and HL7 facets of Waypoint; these options can be changed via either menu option. Options which apply to both DICOM and HL7 typically have a header which says "Waypoint" (e.g. "Waypoint Application Logging").

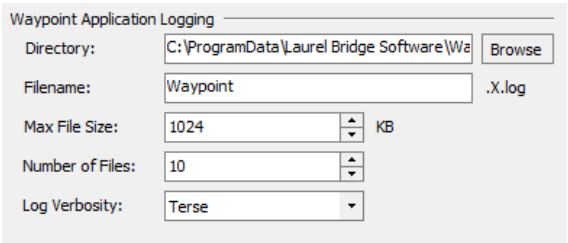
7.1 DICOM System Settings

DICOM System Settings are organized in sections with a section heading. Each of the System Settings sections are described in the following paragraphs.



7.1.1 Waypoint Application Logging

Waypoint provides the ability to log a varying level of information to the application log files. The location, name, and size of the log files are configurable. The application log files are also implemented as rolling log files, meaning that when a log file reaches the specified maximum file

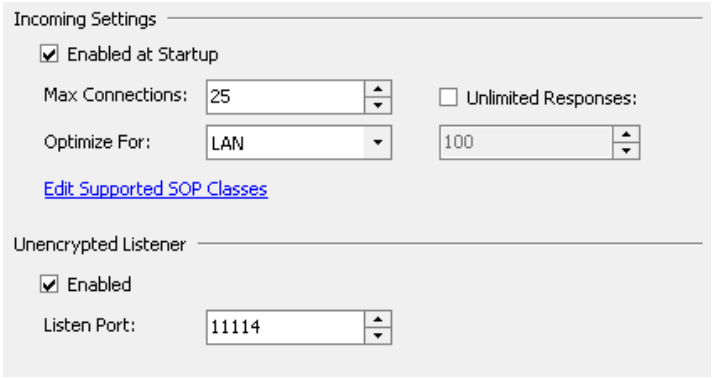


size, a new application log file with a new name will be created and become the new application log. The rolling log file name has an incrementing number in the filename which increments each time the log file rolls over to the new file. It is also possible to configure how many of these rolling log files should be kept, as well as the verbosity of the log data. This is helpful for a variety of reasons, such as being able to see in detail what is being communicated between Waypoint and other devices.

The log files for the Waypoint Service use the root log file name as configured on the **Edit > DICOM Options > System** pane. The log files for the Waypoint Client use the root log file name with a "-client" suffix. The log files for the Waypoint Web Server use the root log file name with a "-web" suffix. The current log file for each Waypoint component can be viewed from the Waypoint Client by selecting **View > Current Application Logs** and selecting the desired log file.

7.1.2 DICOM Incoming

Waypoint will begin listening for incoming associations at launch if the **Enabled at Startup** checkbox is selected.

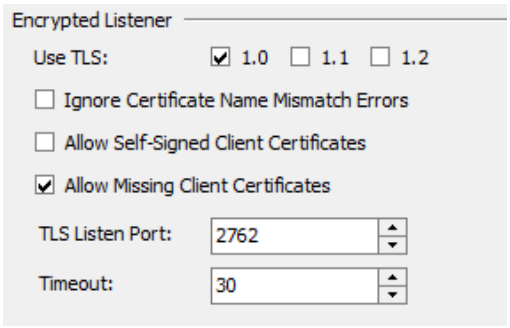


The port Waypoint uses to listen for DICOM association requests can be configured by specifying the port number in the **Listen Port** chooser.

The maximum number of concurrent associations from Sources that Waypoint will process can be specified by using the **Max Connections** chooser. This is the absolute maximum number of incoming concurrent connections; if a Source has its individual maximum connections specified higher than this number then this number takes precedence.

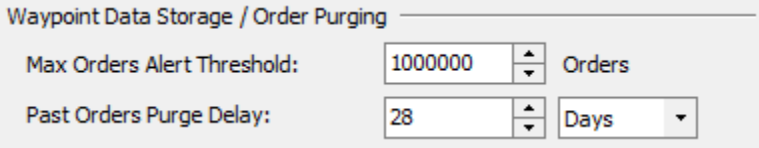
The **Optimize For** chooser will direct Waypoint to optimize its network buffers for your particular network topology. If many of your Sources connect to Waypoint via the Internet, it is recommended that you choose WAN for this setting. Otherwise, the default setting of LAN is appropriate.

The **Use TLS** checkboxes specify whether network communications with the specified DICOM TLS listen port will be encrypted using TLS (as well as which TLS versions will be supported). The **TLS Listen Port** is used to specify the port on which Waypoint will receive TLS-encrypted DICOM associations. The **Ignore Certificate Name Mismatch Errors** and **Allow Self-Signed Server Certificates** checkboxes can be used to relax the Waypoint certificate validation for these connections. However, we strongly recommend using



these options for testing only, as they greatly reduce security by preventing full TLS authentication from occurring. The **Allow Missing Client Certificates** checkbox can be used to control whether client certificates (i.e., client authentication) are required (note that server authentication is always mandatory). The default is to allow missing client certificates (no client authentication), which is similar to how web browsers work. The **Timeout** is the maximum number of seconds to allow reading or writing messages to complete before an error is generated.

7.1.3 Waypoint Data Storage / Order Purging

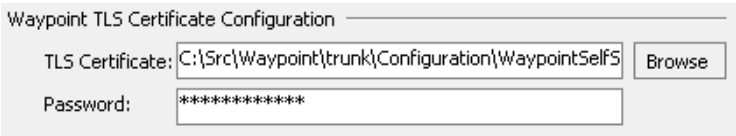


The **Max Orders Alert Threshold** allows an alert threshold for the number of orders stored in the database to be configured. This threshold should be set to a value slightly higher than (e.g., 120% of) the expected steady-state number of orders, which can be calculated by multiplying the average daily order volume by the number of days orders will be held. Note that the number of days that orders will be held includes both the length of time into the future that orders are scheduled, plus the configured number of days in the past that orders are held (see the **Past Order Purge Delay** below). If the number of orders in the database exceeds this alert threshold, an alert will be posted in the Waypoint Client. This alert is for informational purposes only and may be an indication of potential purging problems. Further investigation may be warranted.

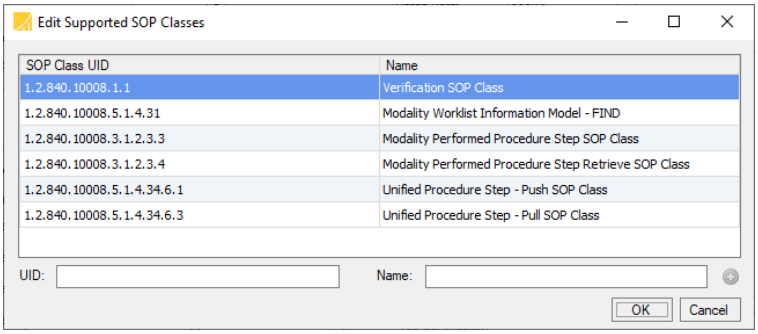
Order data storage is limited using the **Past Order Purge Delay** chooser. Orders that are at least as far in the past as the configured delay will be automatically deleted. The available units for the delay are **Days**, **Weeks**, **Months**, and **Years**. Note, these limits never prevent a new order from being stored in Waypoint. Order purging occurs once per hour. The number of orders stored in Waypoint directly affects how long it takes to insert new orders, update existing orders, and perform queries.

7.1.4 Waypoint TLS Certificate Configuration

Using TLS also requires that the TLS certificate information is configured. The **TLS Certificate** should be set to the location of the certificate that Waypoint should present for identification to clients. It is suggested that the certificate be a standard PKCS#12 certificate and it must contain an exportable private key. Finally, the **Password** must be set to the password for the private key in the certificate. Using a certificate format that does not password protect the private key allows this setting to be ignored (not recommended for security reasons).



See also Appendix D, Section 1.2 Configuring Secure DICOM Communication for more details about using Waypoint TLS support.



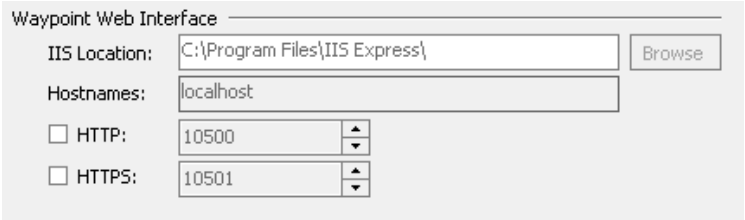
The Supported SOP classes accepted by Waypoint are configurable via the **Supported SOP Classes** table. To add support for a new SOP class, enter its UID in the **UID** text field, its name in the **Name** text field, and press the green plus button. Note, if the UID was found in the data dictionary, the **Name** field is automatically populated. To remove support for a particular SOP class simply select the desired SOP class, right-click for the context menu, and choose the **Remove Selected** menu item. It is also possible to press the Delete key to remove the selected SOP class(es). To select a contiguous group of SOP classes for removal, select a SOP class by left-clicking it with the mouse and then select another SOP class while holding down the Shift key. To select a non-contiguous group of SOP classes for removal, select each individual SOP class while holding down the Ctrl key. Alternately, typing Ctrl+A will select all of the SOP classes in the table.

7.1.5 Waypoint Title

The Waypoint Title is displayed in the title bar of the Waypoint Client. The title is also displayed on the web browser tab when a connection is made to Waypoint's Web User Interface. The default value for Waypoint Title is the IP Address of the system hosting Waypoint.

7.1.6 Waypoint Web Interface

Waypoint provides a web interface accessible via HTTP and/or HTTPS. You can customize the port numbers on which the interface will be hosted as well as the hostnames by which it is reachable. For example, if the computer that Waypoint is installed on is named `mwlbroker` and the HTTP web interface is configured for port 10500, then you would add `mwlbroker` to the **Hostnames** list. It would then be reachable with the URL `http://mwlbroker:10500`. If you wanted to specify the fully qualified name of the computer and your domain is `mycompany.com`, you would add `mwlbroker.mycompany.com` to the **Hostnames** list, and the URL would be `http://mwlbroker.mycompany.com:10500`. Note that the default port for HTTP (to avoid specifying a port number on the client side) is 80.



The same is true for secure HTTPS connections to the Web service, except that the port number would be the specified port number in the "HTTPS:" setting, and the URL would begin with "`https:`". Note that, in order to use HTTPS, you must specify the **TLS Certificate** and **Password**

in the spaces provided (see **Appendix D – Communicating Securely with Waypoint** for more information). **Do not put the protocol portion of the address (i.e., "`http://`" or "`https://`"), in the Hostnames list**. Note that the default port for HTTPS (to avoid specifying a port number on the client side) is 443.

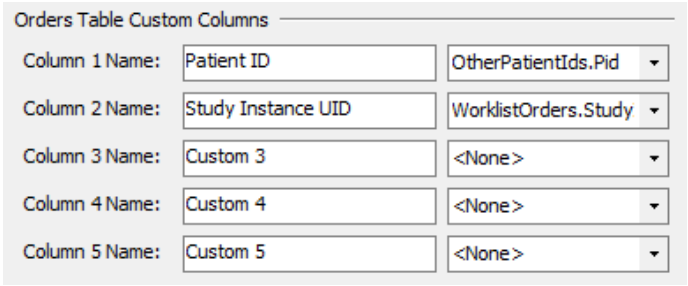
In order for the web server binding to exactly match the TLS certificate, the fully qualified hostname must be entered into the **Hostnames** list exactly as given in the certificate. To see the hostname(s) given in the certificate, Control-click (hold Control while clicking on) the **TLS Certificate** label to bring up the X.509 certificate viewer, select the Details tab, then locate and click on one of the following fields:

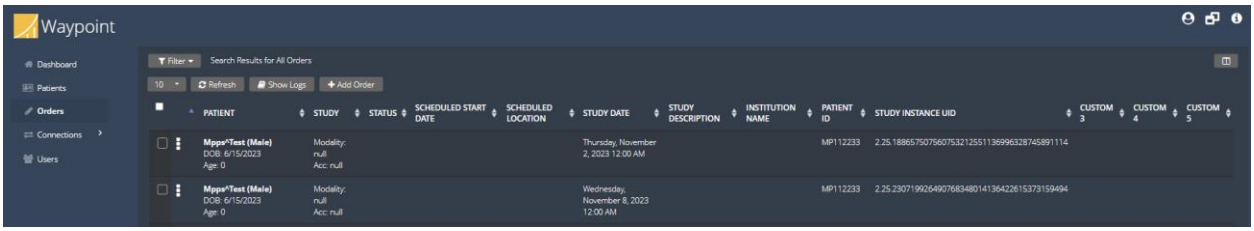
- Click on "Subject Alternative Name" – The value(s) following each of the "DNS Name=" prefixes are the subject alternative names, which are the matching hostnames.
- If the above extension cannot be found, click on "Subject" – The value following the "CN=" prefix is the subject distinguished name, which is the matching hostname.

Note that it is possible for the certificate hostname to be wildcarded (in which case the certificate is what is known as a wildcard certificate). A wildcard certificate will match any hostname in the same subdomain as the wildcard value ("*") given in the hostname. In this case, the actual fully qualified hostname must be entered into the **Hostnames** list (i.e., not the wildcarded hostname).

7.1.7 Orders Table Custom Columns

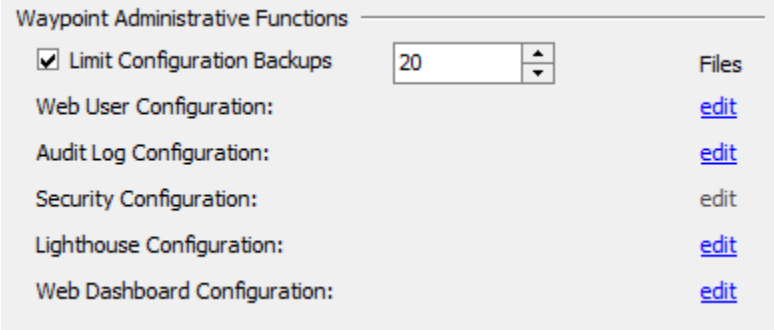
The Orders table on the Waypoint Web Interface is shown in section 11.4 Orders. In addition to the predefined columns, there are 5 Custom Columns that can be configured to show other values from the data stored for the order. This examples assigns OtherPatientIds.Ipid to Custom Column1 with the header "Issuer of Patient ID." Waypoint web user interface displays the custom column as follows:





7.1.8 Waypoint Administrative Functions

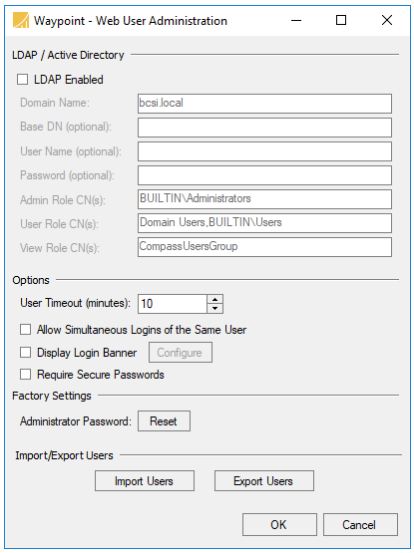
The following sections describe the configuration settings that are organized under **Waypoint Administrative Functions**.



7.1.8.1 Configuration Backups

When the Waypoint configuration is modified, Waypoint creates an automatic backup of the previous configuration (see **Appendix E** for more information). This backup feature can be limited to a particular number of backup files by checking the **Limit Configuration Backups** checkbox and providing the maximum number of backup files to keep.

7.1.8.2 Web User Administration



For Web User Administration, select the **Web User Configuration edit** link. The **Waypoint – Web User Administration** dialog will be displayed as shown to the right. Waypoint supports **LDAP / Active Directory** for user account login to the Waypoint Web Interface. If enabled, the LDAP **Domain Name** can be specified. There are three optional fields: **Base DN**, **User Name** and **Password**. **Base DN** specifies the root from which all queries will be performed, i.e. “dc=example, dc=com”. **User Name** and **Password** are the credentials used to connect to the server. The three account types (as described below) will be mapped to the **User/Admin/View Role CN** (i.e., the LDAP Common Name, which, for Active Directory, corresponds to the Group Name) as configured. The CNs are comma-separated to allow for specifying multiple values that map to a single role.

If LDAP is not enabled, there are three types of built-in user accounts for the web interface: “Admin” accounts, “User” accounts and “ViewOnly” accounts. “Admin” and “User” accounts are allowed to affect existing jobs. Only “Admin” accounts can create and remove users.

The default “Admin” username for the web interface is “Administrator” and the password is “LaurelBridge1234”. It is highly recommended that you change the default password to a secure value (12+ characters, including uppercase and lowercase characters plus numeric digits) after successfully logging in. Since the “Admin” role allows modification of any user account, it is recommended that you only give access to your users as either “User” or “ViewOnly” accounts.

The default “ViewOnly” username for the web interface is “waypoint”, and the password is “Password1234”. It is highly recommended that you change the default password after

successfully logging in. You should create “ViewOnly” users for anyone that is allowed to view Waypoint jobs and any associated patient health information but not modify them.

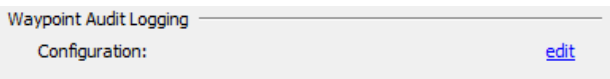
There are no default “User” accounts. It is recommended that you create “User” level accounts for anyone authorized to affect changes on Waypoint worklist items and view patient protected health information.
The **User Timeout** specifies the duration before a user logged in to the Web Interface will be logged out automatically. The **Allow Simultaneous Logins of the Same User** checkbox controls whether to enforce that users can only be logged on from a single browser (multiple tabs within the same browser count as a single logon). The **Require Secure Passwords** checkbox (enabled if LDAP is disabled) changes the minimum password length from the default 8 characters to 12 characters. It also adds the requirement that passwords contain at least one numeric digit (in addition to the default of both uppercase and lowercase letters). The **Administrator Password – Reset** button (enabled if LDAP is disabled) resets the password for the built-in “Administrator” Admin user back to the default value given earlier. This password should be immediately changed to a non-default, secure value (12+ characters, including uppercase and lowercase characters plus numeric digits) after successfully logging in.

If not using LDAP and the sharing of local web users is desired, the **Import/Export Users** buttons can be used to transport user information between Waypoint instances. The **Export Users** button (enabled if LDAP is disabled) exports the list of built-in users (and their properties) to an XML file which can then be imported at a later time or on a different Waypoint system. The **Import Users** button (enabled if LDAP is disabled) imports these XML user lists. These buttons can also be used to backup and restore the local web users.

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 highly 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 **User Timeout** functionality discussed earlier 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.

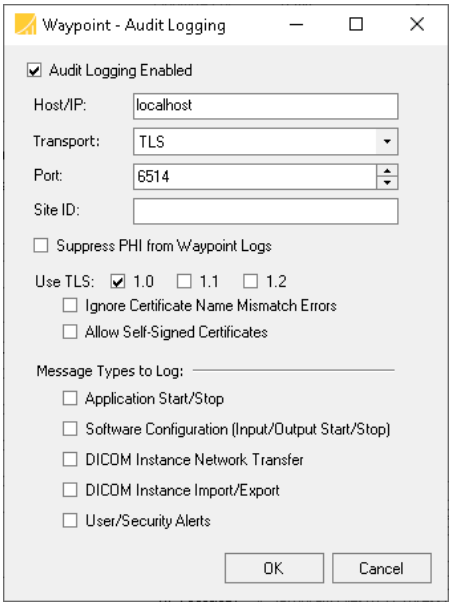
7.1.8.3 Waypoint Audit Logging

To configure Waypoint audit logging capabilities, select the **Waypoint Audit Logging Configuration edit** link. The **Waypoint – Audit Logging** dialog will be displayed as shown to the right. This dialog allows the Waypoint audit logging capabilities (an implementation of DICOM PS 3.15 Appendix A.5 “Audit Trail Using Syslog” functionality) to be enabled or



disabled. Waypoint audit log messages are sent to a remote (secured) syslog server.

If audit logging is enabled, the syslog server **Host/IP** address, **Transport** protocol, and **Port** can be configured. (Note that if the **Host/IP** address is left blank, audit logging will still be enabled locally.) The **Site ID** field allows configuration of the audit enterprise site ID, which is used to uniquely identify this Waypoint instance within the enterprise.

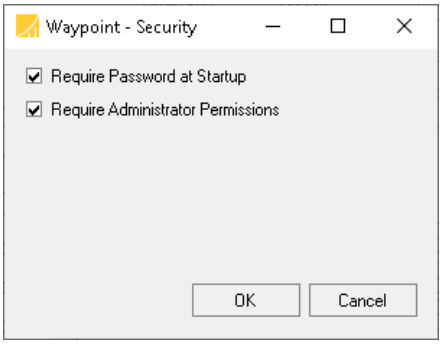


If the **UDP** transport option is selected, the port defaults to the well-known port 514. If the **TCP** transport option is selected, the port defaults to the well-known port 601. If **TLS** transport is selected, the port defaults to the well-known port 6514. In addition, the supported version(s) of TLS can be configured, as well as whether or not to ignore certificate name mismatch errors and whether or not to allow self-signed certificates. Per RFC 5424, use of the **TLS** transport option is strongly recommended unless the underlying network is secure.

Finally, the types of messages to be audit logged can be configured. Enabling **Application Start/Stop** messages will log a message each time the Waypoint application (both the Waypoint service and the client application) is started or stopped. Enabling **Software Configuration** messages will log a message each time an input (DICOM or HL7) is started or stopped. Enabling **User/Security Alerts** will log a message whenever a user logs in/out, whenever a user is added/removed/modified.

7.1.8.4 Waypoint Security

To configure Waypoint security capabilities, select the **Security Configuration edit** link. The **Waypoint – Security** dialog will be displayed as shown to the right. This dialog allows the Waypoint security capabilities to be enabled or disabled. If **Require Password at Startup** is enabled, the Waypoint Client will require entry of the valid password for the currently-logged-in Windows user before starting up. This prevents unauthorized users from being able to access the Waypoint Client if the console on the host Windows system is left unlocked. This setting is recommended if the Windows console is not kept locked whenever not in use.

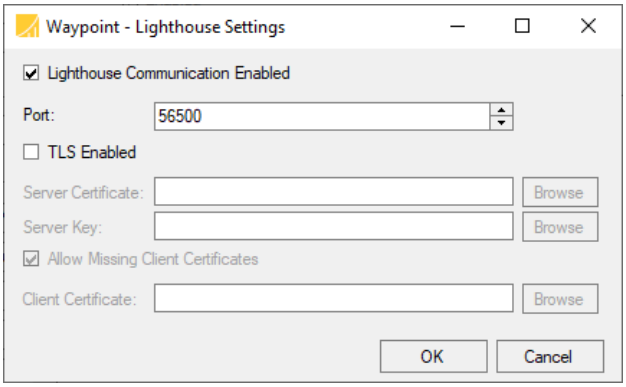


If **Require Administrator Permissions** is enabled, the Waypoint Client will require administrator permissions before starting up (i.e., it must be started by right-clicking the executable or shortcut

and selecting “Run as administrator”). Note that this has the additional, beneficial side effect of locking down the Compass data directory (as entered on the **System** pane, section **Compass Data Storage**, as the **Path** – the default value is “C:\ProgramData\Laurel Bridge Software\Waypoint”), so that only users with administrator privileges can view or modify Waypoint configuration and log files. This setting is recommended if any users of the host Windows system are not authorized to view PHI.

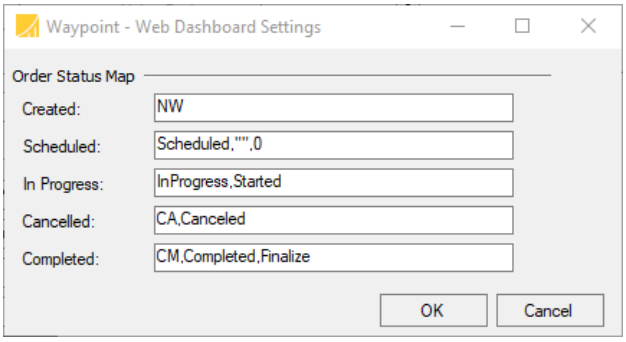
7.1.8.5 Lighthouse Configuration

To configure Waypoint communication with Lighthouse, select the Lighthouse Configuration edit link. The Waypoint – Lighthouse Settings dialog will be displayed as shown to the right. This dialog allows the Waypoint Lighthouse Communication to be enabled or disabled. If Lighthouse communication is enabled, the Port can be configured. The default port is 56500. If TLS transport is selected, the Server Certificate and Server Key become enabled. Click on the corresponding Browse button to open the file chooser dialog to select the Server Certificate and Server Key files. Finally, an optional Client Certificate can be selected when Allow Missing Client Certificates is disabled.



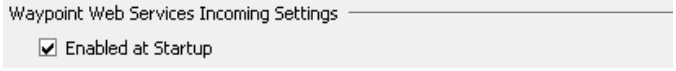
7.1.8.6 Web Dashboard Configuration

To configure Waypoint Web Dashboard Settings, select the Web Dashboard Configuration Configuration edit link. The Waypoint – Web Dashboard Settings dialog will be displayed as shown to the right. This dialog configures the mapping between the orders status columns on the Web UI dashboard with the scheduled status values stored in the database for each worklist order. Enter the comma separated scheduled stataus values that map to each of the order statuses: Created, Scheduled, In Progress, Cancelled, and Completed. For more information on the Web UI Dashboard see **section 11.1 Dashboard**.



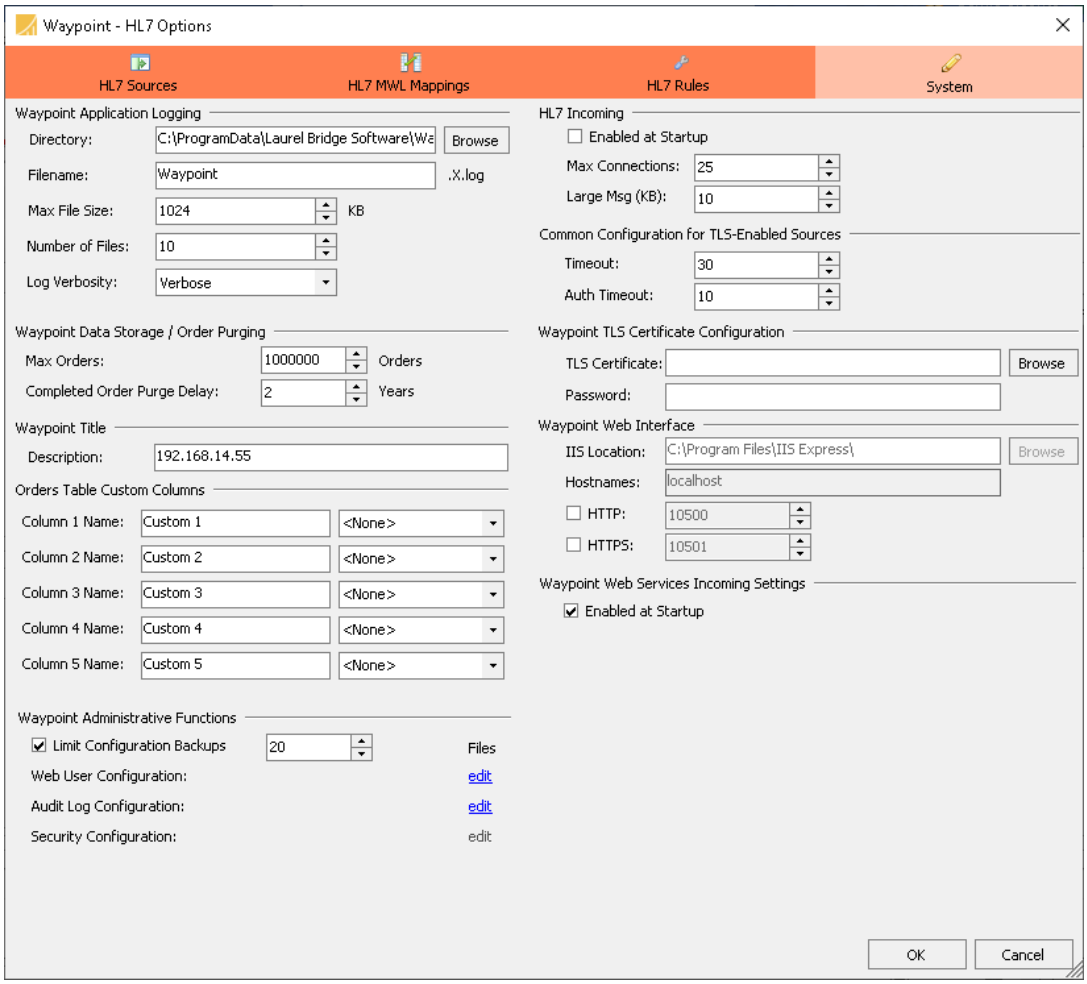
7.1.9 Waypoint Web Services Incoming Settings

Waypoint will begin listening for incoming Web Services connections at launch if the **Enabled at Startup** checkbox is selected. See **section 6 DICOM Web Services** for more information on the DICOM Web Services implemented by Waypoint.



7.2 HL7 System Settings

As mentioned in section 7, Waypoint System settings can be configured from either the DICOM Options or HL7 Options screens. All sections denoted with the header "Waypoint" are common system settings. See above section under DICOM System Settings for configuring the Waypoint common settings.



7.2.1 Waypoint Application Logging

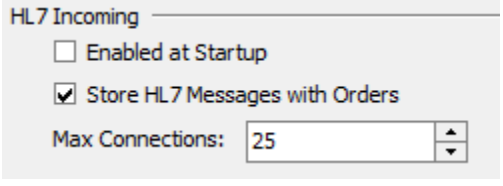
See above section under DICOM System Settings.

7.2.2 Waypoint Data Storage / Order Purging

See above section under DICOM System Settings.

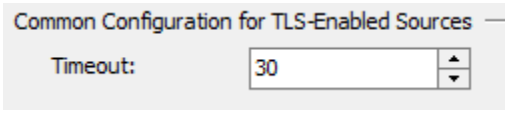
7.2.3 HL7 Incoming

Waypoint will begin listening for incoming HL7 connections at launch if the **Enabled at Startup** checkbox is selected. Only sources which are configured to **Start When Incoming HL7 Started** will be able to receive connections as a result of this setting.



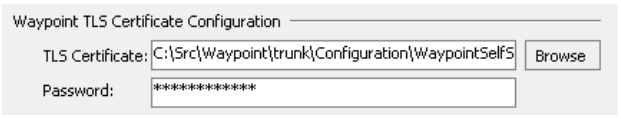
Any sources which are not so configured must be manually started to receive connections. The **Store HL7 Messages with Orders** checkbox determines whether the raw HL7 messages will be stored along with the worklist orders. The maximum number of concurrent connections from Sources that Waypoint will process can be specified by using the **Max Connections** chooser. This is the absolute maximum number of incoming concurrent connections; if a Source has its individual maximum connections specified higher than this number, then this number takes precedence.

7.2.4 Common Configuration for TLS-Enabled Sources



The **Timeout** specifies the maximum number of seconds to allow reading or writing messages to complete with a TLS-Enabled HL7 Source.

7.2.5 Waypoint TLS Certificate Configuration



As mentioned in **section 5.1.2 HL7 Settings**, the **Waypoint Listen Configuration for Source** area will configure the TLS settings for any HL7 Source which is configured as **Use TLS**, allowing incoming encrypted connections to Waypoint. To properly configure incoming TLS connections, the **TLS Certificate** and/or **Password** must be set. The **TLS Certificate** should be set to the location of the certificate that Waypoint should present for identification to clients. It is suggested that the certificate be a standard PKCS#12 certificate and it must contain an exportable private key. Finally, the **Password** must be set to the password for the private key in the certificate. Using a certificate format that does not password protect the private key allows this setting to be ignored.

7.2.6 Waypoint Title

See above section under DICOM System Settings.

7.2.7 Waypoint Web Interface

See above section under DICOM System Settings.

7.2.8 Orders Table Custom Columns

See above section under DICOM System Settings.

7.2.9 Waypoint Administrative Functions

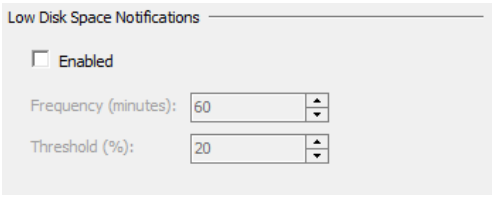
See above section under DICOM System Settings.

7.2.10 Waypoint Web Services Incoming Settings

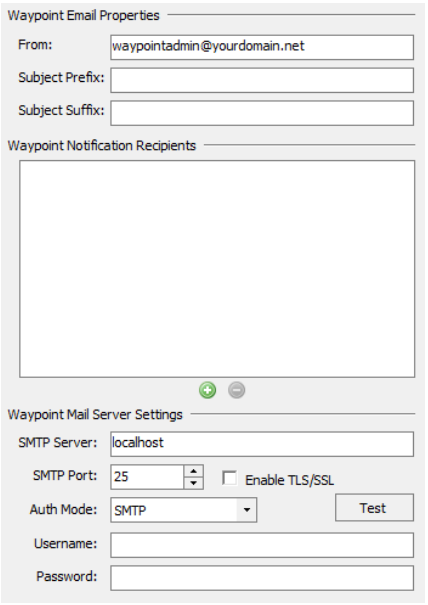
See above section under DICOM System Settings.

8 Notifications

Notifications can be configured by selecting **Edit > DICOM Options…** from the menu and then selecting the **Notifications** pane. All Notification options are universal across both the DICOM and HL7 facets of Waypoint.



To add a new recipient, press the green add button located beneath the list of **Notification Recipients**. Specify the recipient's email address and press the Enter key. The sender of the email can be specified as well. Emails may also optionally contain a provided **Subject Prefix** and/or **Subject Suffix**.

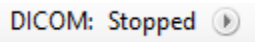


It is necessary to include valid **Mail Server Settings** in order to send emails to the listed recipients. At a minimum, an **SMTP Server Host** and **SMTP Port** are required, and optionally SSL can be enabled by selecting the **Enable TLS/SSL** checkbox. A **Username** and **Password** are also required if the mail server requires authentication.

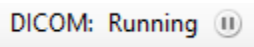
9 Enabling Input

9.1 DICOM Input

To allow Waypoint to accept incoming DICOM association requests, press the **Play** button icon on the **DICOM** toolbar.

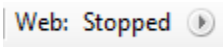


To disable Waypoint from accepting any new incoming association requests, press the **Pause** button icon on the **DICOM** toolbar. Pressing the **Pause** button icon on the **Input** toolbar does not affect any currently open associations.

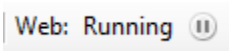


9.2 Web Input

To allow Waypoint to accept incoming DICOM Web Service connections, press the **Play** button icon on the **Web** toolbar.



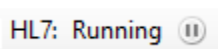
To disable Waypoint from accepting any new incoming Web connections, press the **Pause** button icon on the **Web** toolbar. Pressing the **Pause** button icon on the **Web** toolbar does not affect any currently open connections. Any new connections attempts while **Web** is stopped will fail with HTTP Error 401 Unauthorized.



9.3 HL7 Input

To allow Waypoint to accept incoming connections, press the **Play** button icon on the **HL7 Input** toolbar. This serves to start any HL7 Sources which are configured to **Start When HL7 Incoming Started**. Only sources which are started can receive incoming connections. If this **Play** button is pushed and there are sources which are not configured to **Start When HL7 Incoming Started**, these sources will still be stopped; they must be manually started to receive connections.

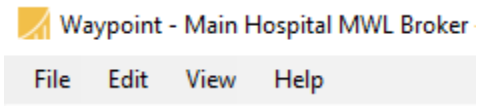
To disable Waypoint from accepting any new incoming connections, press the **Pause** button icon on the **HL7** toolbar. Pressing the **Pause** button icon on the **HL7 Input** toolbar will stop any HL7 Network Sources which are started, closing their open connections.



10 Thick Client: Waypoint User Interface Details

10.1 Menu Bar

A menu bar is available at the top of the main window:

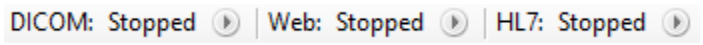


- **File > Import Configuration:** Imports an existing configuration file. Both **Input** and **Output** must be stopped to enable this menu item.
- **File > Export Configuration:** Exports the current configuration to a chosen location.
- **File > Exit:** Exits the program (after completing any incoming and outgoing associations).
- **Edit > DICOM Options:** Opens the main options dialog for DICOM settings and some application-wide settings
- **Edit > HL7 Options:** Opens the main options dialog for HL7 settings and some application-wide settings
- **View > Current Application Log:** Opens the application log file.
- **View > Application Log Directory:** Opens Windows Explorer to view the Waypoint log file directory.
- **Help > User Manual:** Opens the Waypoint user manual.
- **Help > DICOM Conformance Statement:** Opens the DICOM Conformance Claim.
- **Help > Send Feedback:** Provides a mechanism to send feedback to Laurel Bridge or to request support.
- **Help > About Laurel Bridge Waypoint:** Displays an "About" dialog containing program and license information.

10.2 Tool Bar

The tool bar contains the components to enable and disable DICOM and HL7 as described in **section 9 Enabling Input**.

When Stopped, the **Play** button is active:



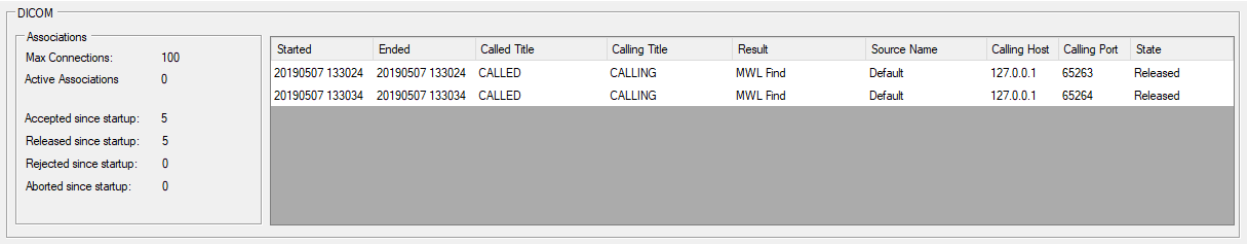
When Running, the **Pause** button is active:

10.3 DICOM Connections History

The DICOM Connections History table provides a summary view of the 100 most recent DICOM Associations with Waypoint. The table columns are:

- **Started**: date and time when the association was opened
- **Ended**: date and time when the association was closed
- **Called Title**: of the association
- **Calling Title**: of the association
- **Result**: accepting SOP Class, e.g. "MWL Find" or reason for rejection
- **Source Name**: Worklist User Source that matched the association

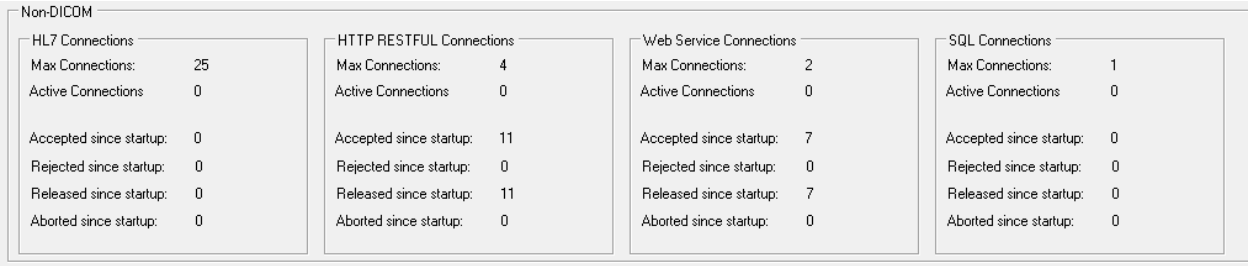
- **Calling Host**: hostname of SCU
- **Calling Port**: IP port of SCU
- **State**: current state of association: Accepted, Released, or Rejected



10.4 Non-DICOM Connections

The Non-DICOM section shows the connection summary status for incoming HL7 connections and the connection summary status for each of the outgoing connections from the Worklist Provider transport modes:

- HTTP RESTFUL
- WEB SERVICE
- SQL



10.4.1 HL7 Connections

HL7 Connections shows a summary status of the connections made to Waypoint since the Waypoint Service was last started. The items displayed are:

- **Max Connections**: as configured on **HL7 Options>System** pane
- **Active Connections**: count of connections currently active
- **Accepted since startup**: count of HL7 messages received by Waypoint
- **Rejected since startup**: count of rejected acknowledgement codes sent as responses to HL7 messages
- **Released since startup**: count of accepted acknowledgement codes sent as responses to HL7 messages
- **Aborted since startup**: count of number of internal errors that occurred while processing HL7 messages

10.4.2 HTTP RESTFUL, WEB SERVICE, and SQL Connections

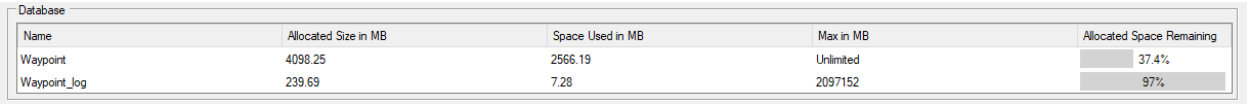
HTTP RESTFUL, WEB SERVICE, and SQL Connections shows a summary status of the connections made by Worklist Providers with the given transport mode since the Waypoint Service was last started. The items displayed are:

- **Max Connections**: the number of Worklist Providers with the given transport mode
- **Active Connections**: count of connections currently active
- **Accepted since startup**: count of connections successfully made to its server
- **Rejected since startup**: count of connections that failed, e.g. Destination is unreachable, Authorization Failed.
- **Released since startup**: count of HTTP methods that completed with OK status or SQL commands that completed successfully.
- **Aborted since startup**: count of HTTP methods that did not complete with OK status or SQL commands that failed.

10.5 Database Status

The Database status table shows the Database Files properties and current disk space usage of the Waypoint database and LOG files. The data displayed is:

- **Waypoint**: Logical Name of the database
- **Waypoint_log**: Logical Name of the database LOG file
- **Allocated Size in MB**: Initial Size of database file
- **Space Used in MB**: current usage of disk space
- **Max in MB**: Autogrowth /Maxsize of database file
- **Allocated Space Remaining**: chart of percentage of allocated space remaining

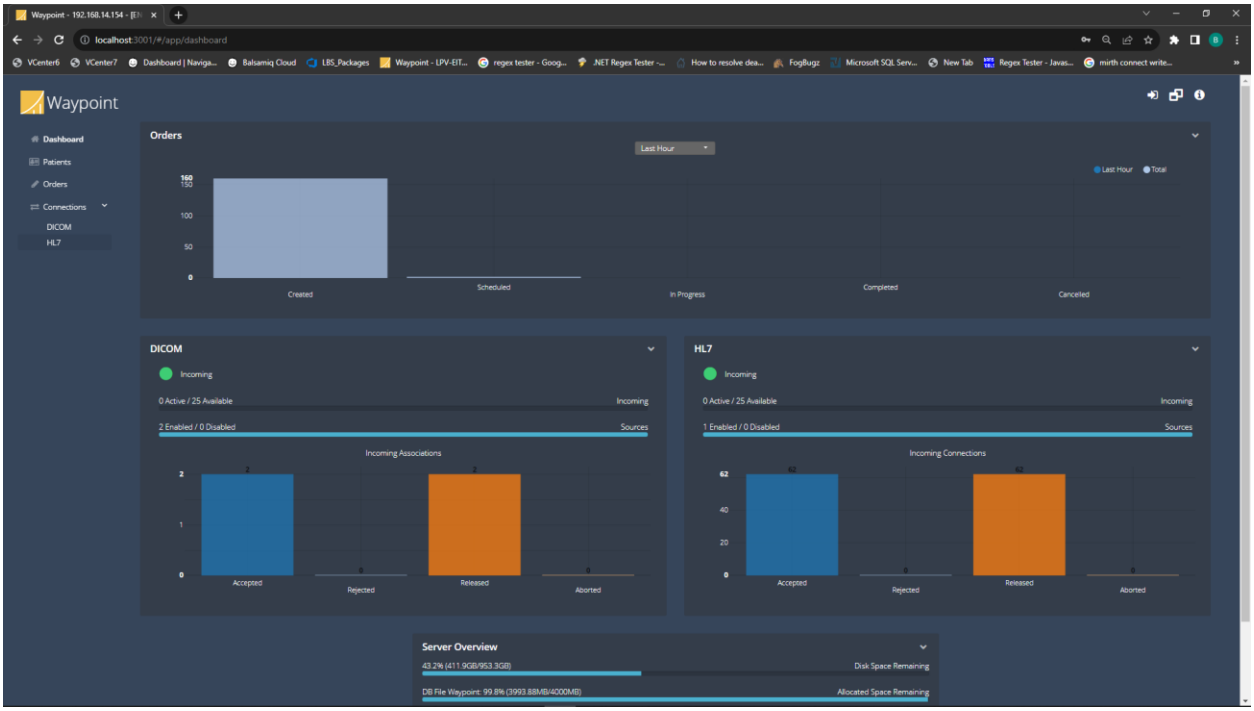

Database

Name	Allocated Size in MB	Space Used in MB	Max in MB	Allocated Space Remaining
Waypoint	4098.25	2566.19	Unlimited	37.4%
Waypoint_log	239.69	7.28	2097152	97%

11 Web Client: Waypoint Web Interface Details

11.1 Dashboard

The Web User Interface is accessed through any common web browser from a personal computer, tablet, or smart phone. The default port is 10500 and it can be changed from the **DICOM Options > System** tab on the Waypoint Client user interface. The home screen for the web user interface is a dashboard as shown:



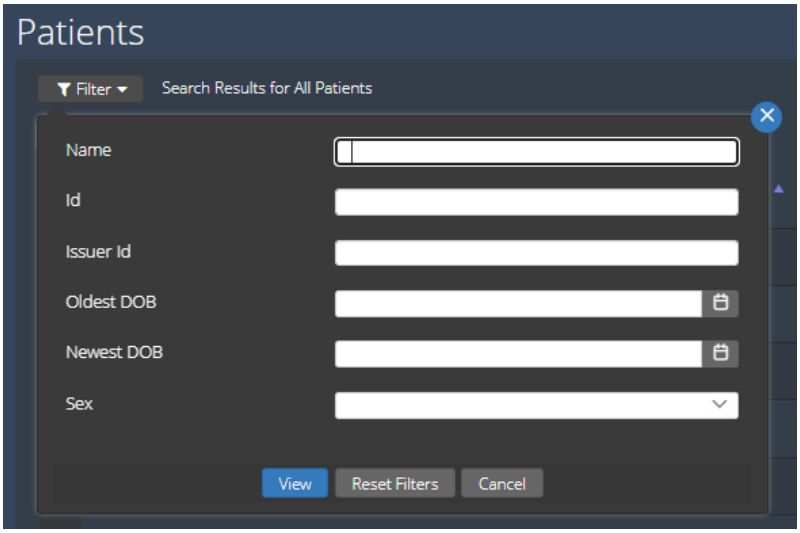
The Orders graph shows cumulative status of the orders that have been received by Waypoint. The orders are most commonly received as HL7 ORM messages, however, orders can also be created and updated using DICOM MPPS. The remaining menu items: Patients, Orders, Connections and Users require a login to access. The default login user is “Administrator” with password “LaurelBridge1234”. This can be changed from the Users screen. There is also support for accessing the site’s Active Directory for user login authentication.

11.2 Login

The DICOM Jobs, HL7 Jobs, and Details pages all require the user to log in. Waypoint 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 Waypoint -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.

11.3 Patients

The Patients screen shows a grid of the Patients stored in Waypoint. There is a filtering system to allow you to fully control viewing only a specified list of patients. The **Filter** menu contains the following menu items:

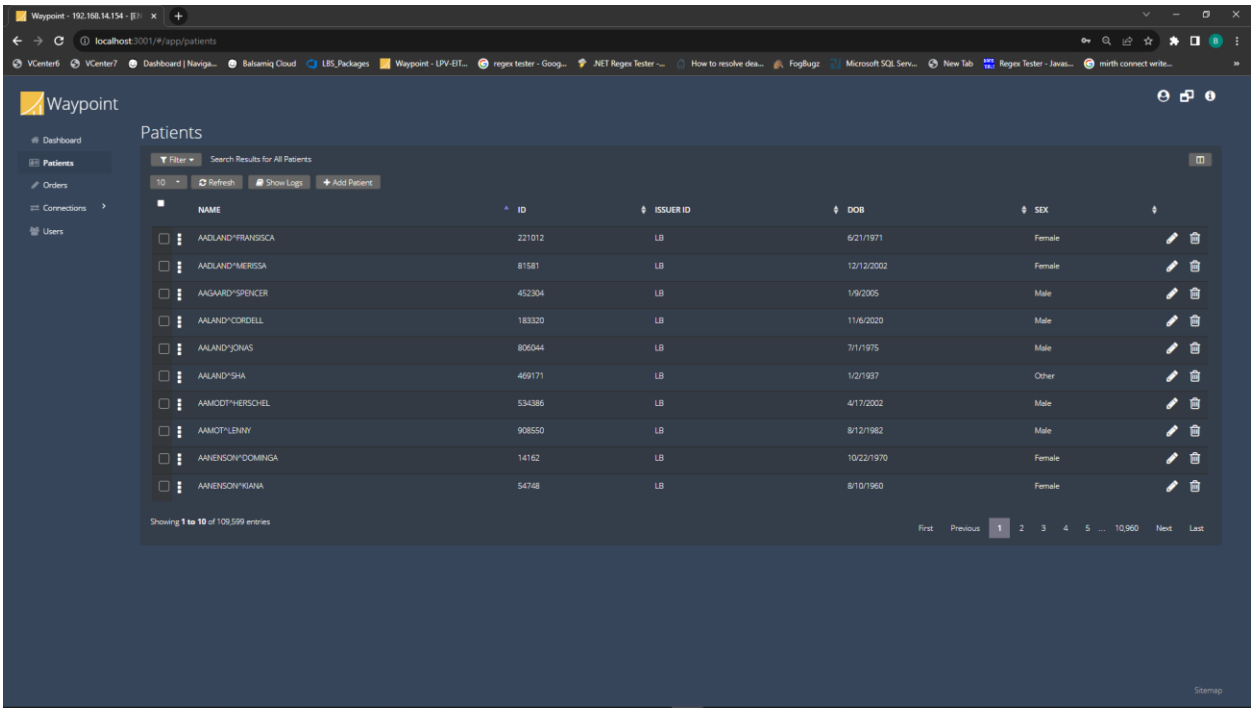


Name, Id, and Issuer Id are **String Filters**. *Oldest DOB and Newest DOB* are **Date Filters** which includes a calendar tool to select the matching date. *Sex* is an **Enumerated List Filter** that provides a drop-down list of matching values to check. **String Filters** support expressions to control how the match is performed on the value. The keywords for the **String Filter** expressions are:

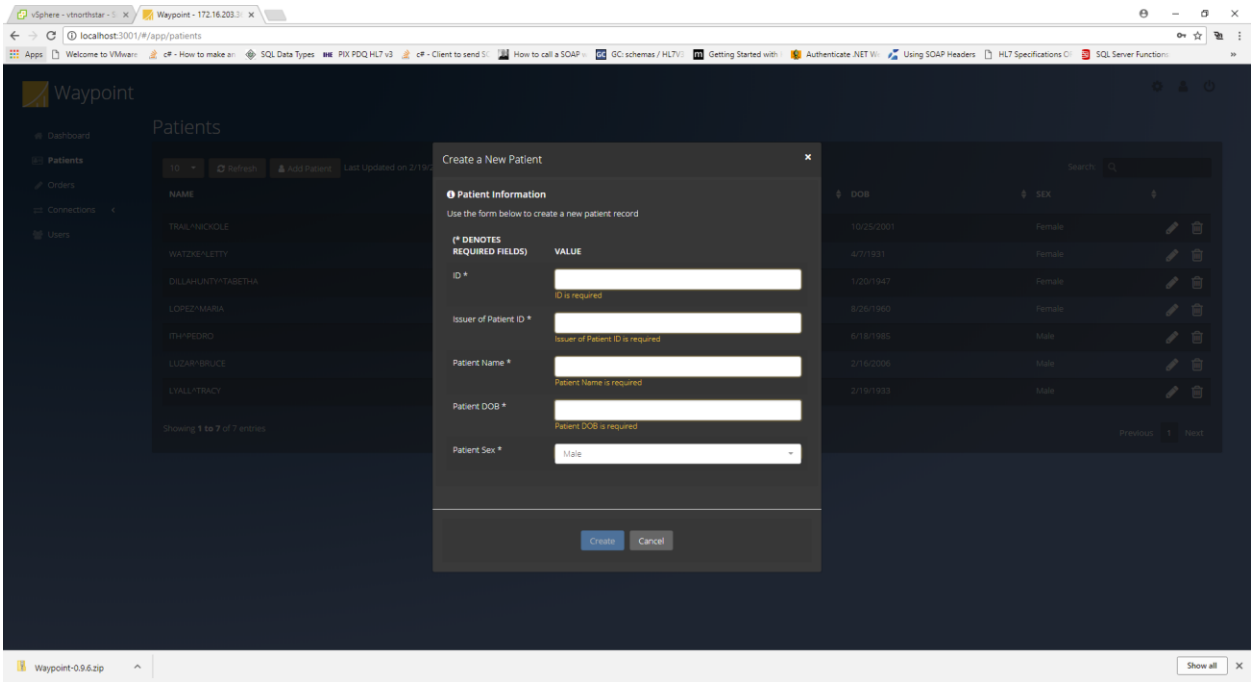
- equals:
- starts:
- ends:

The keyword is immediately followed by the string to match, for example **equals:1234**, matches the value “1234” only, **starts:1234**, matches any value that starts with “1234”, and **ends:1234**, matches any value that ends with "1234”. If no keyword is used, the **contains** expression is matched, for example “1234” matches any value that contains the sequence of characters “1234” preceded or followed by any other values, including no other value. The wildcard character **%** can be used anywhere in the matching value with **starts**, **ends** or **contains**. The wildcard character is not used with **equals**.

The Patients screen is shown below:

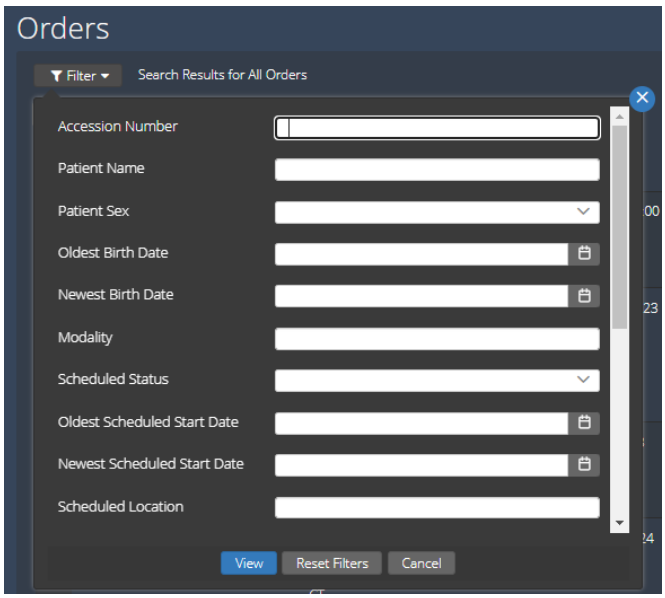


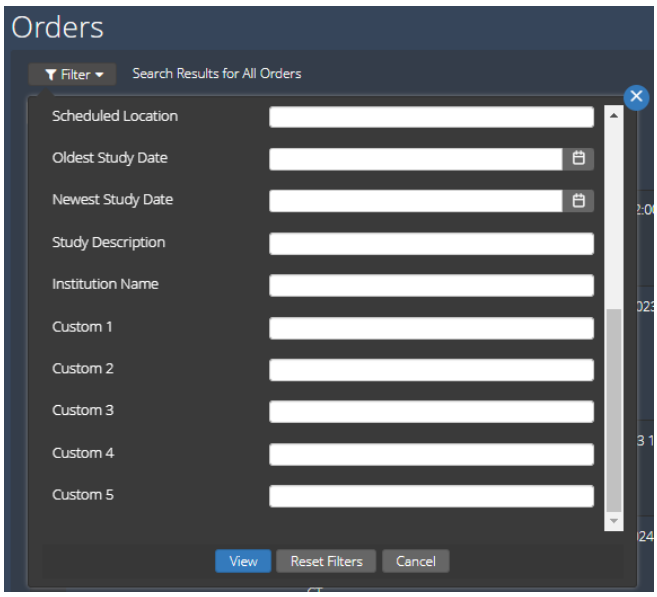
Notice the Add Patient button that allows you to create new patients, as shown:



11.4 Orders

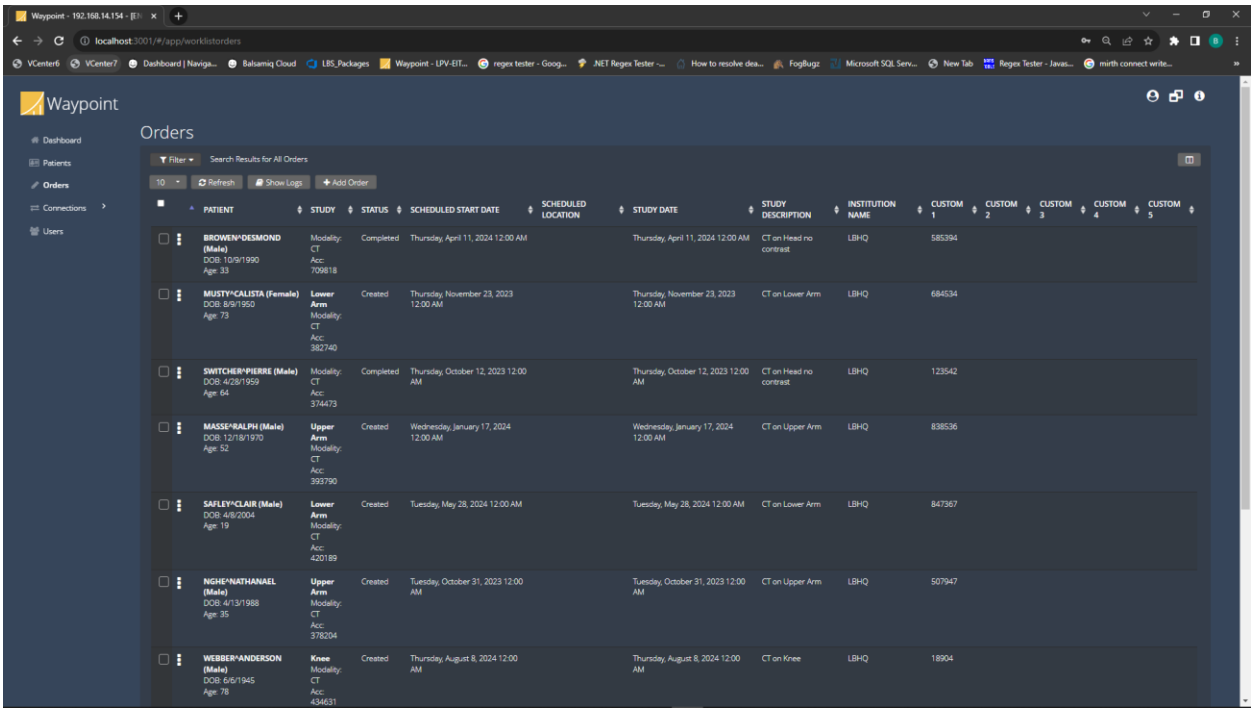
The Orders screen shows a grid of the orders stored in Waypoint. There is a filtering system to allow you to fully control viewing only a specified set of orders. The **Filter** menu contains the following menu items:



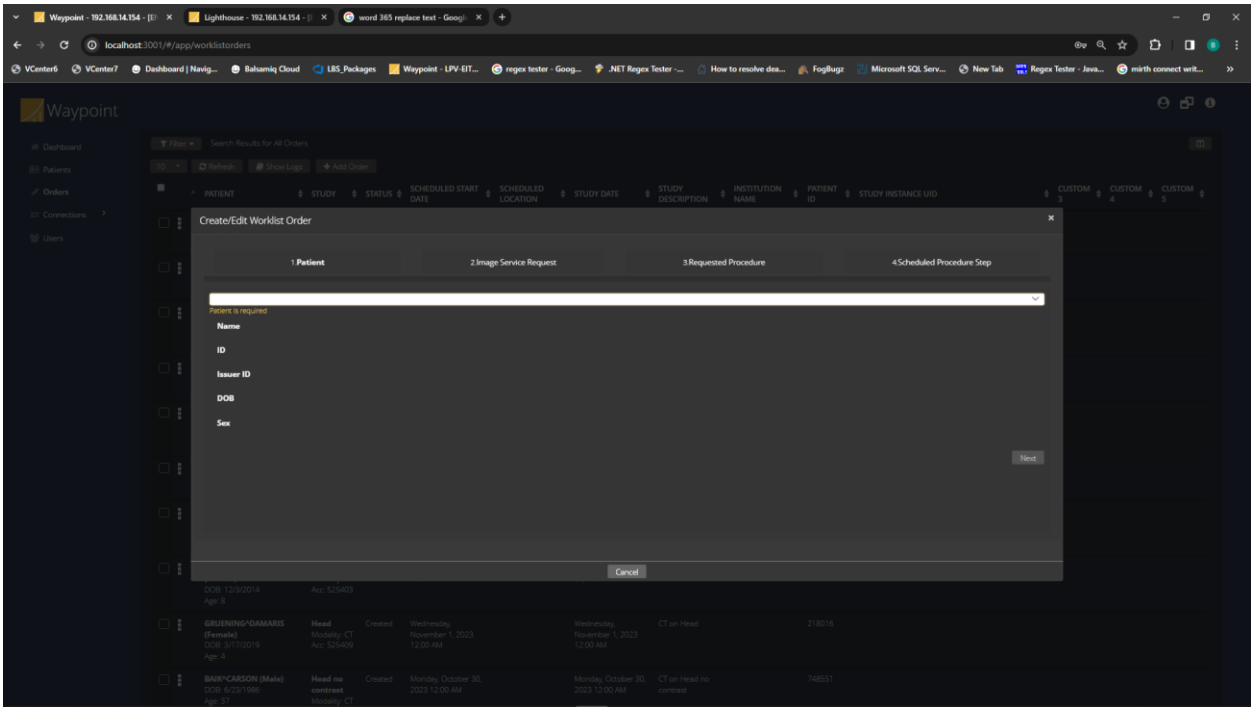


Accession Number, *Patient Name*, *Modality*, *Scheduled Location*, *Study Description*, *Institution Name*, *Custom 1*, *Custom 2*, *Custom 3*, *Custom 4*, *and Custom 5* are **String Filters**. *Oldest Birth Date*, *Newest Birth Date*, *Oldest Scheduled Start Date*, *Newest Scheduled Start Date*, *Oldest Study Date*, *and Newest Study Date* are **Date Filters**. *Patient Sex and Scheduled Status* are **Enumerated List Filters**. See **section 11.3 Patients** for information about the features of each filter type. See **section 7.1.7 Orders Table Custom Columns** for information about configuring custom columns on the Orders table.

Each Order provides a **More Options** menu after the selection checkbox to *View Messages* and *Remove* the selected order. The Orders screen is shown below:



Notice on the Orders screen is a button to Add Order. This allows you to search for, edit existing orders, or create new orders, as shown:

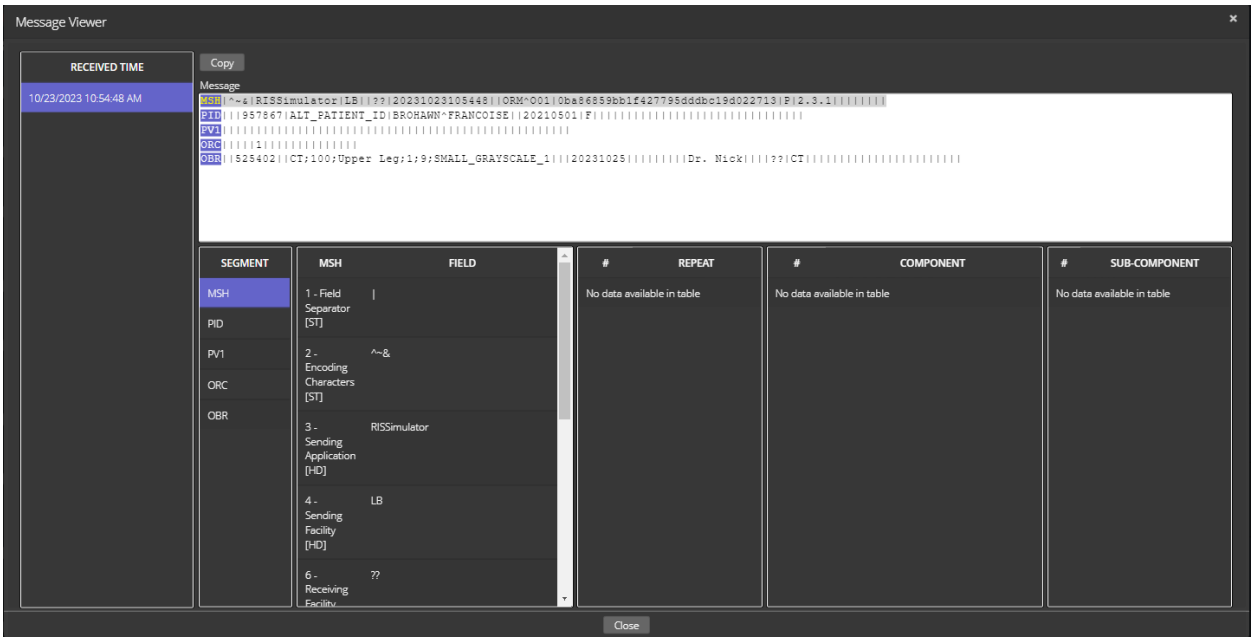


11.4.1 Orders Message Viewer

To view order messages, click on the **More Options** icon next to the Patient on the Orders screen and select *View Messages* from the context menu to open the *Message Viewer*. The Message Viewer displays the Received Time for the messages that created or updated the selected order. The Message Viewer recognizes three message formats as shown in the following section.

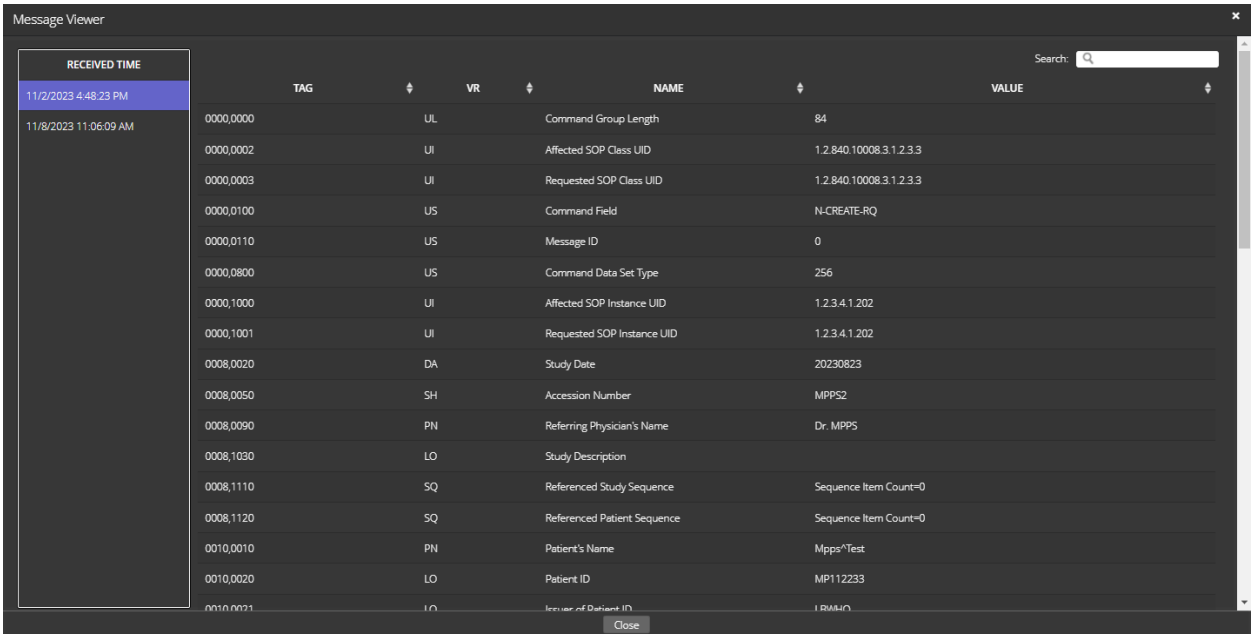
11.4.1.1 HL7 Message Viewer

The HL7 Message Viewer displays the original message in the top panel. The lower panels display the Segment, Field, Repeat, Component, and Sub-Component of the value the was clicked in the message.



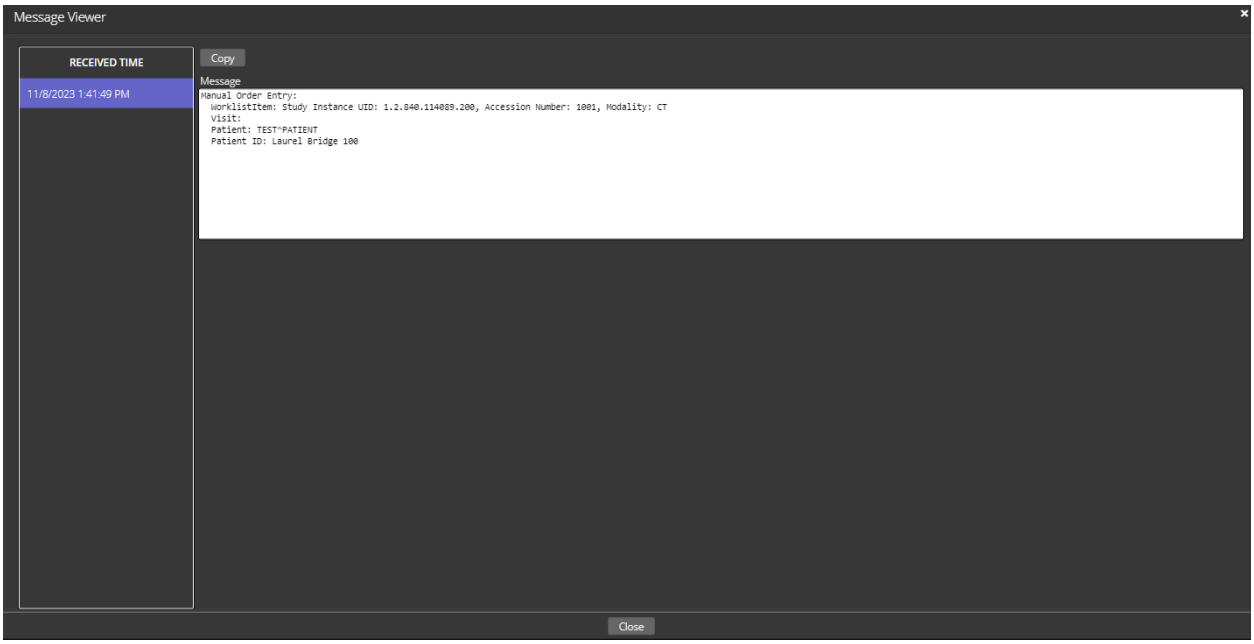
11.4.1.2 MPPS Message Viewer

The MPPS Message Viewer displays the MPPS request message in a table format where each row is a DICOM Element. The columns are: TAG, VR, NAME and VALUE.



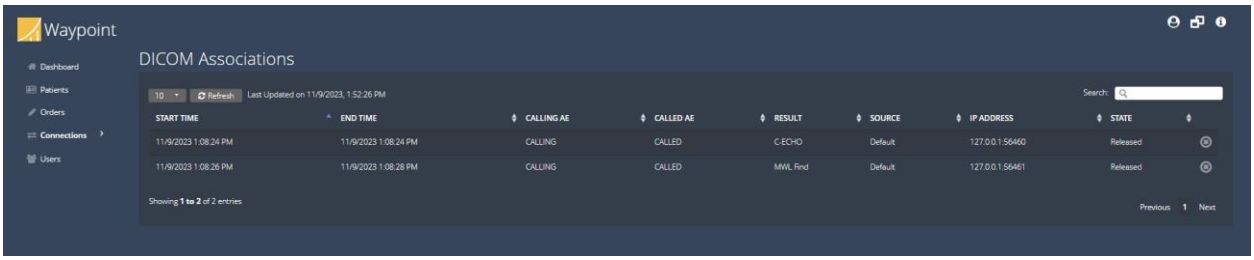
11.4.1.3 Plain Text Message Viewer

Orders that were added using the Orders Web UI are displayed as a plain text message as shown below.

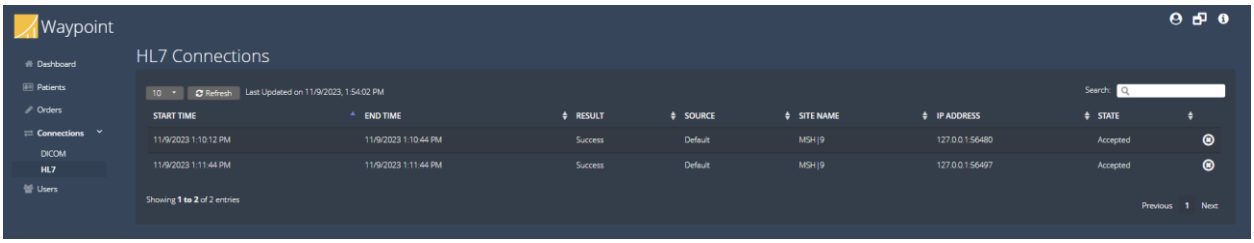


11.5 Connections

11.5.1 DICOM Associations

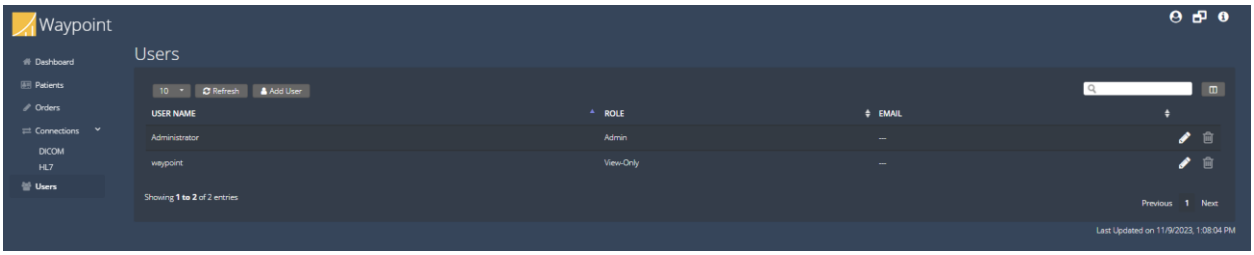


11.5.2 HL7 Connections



11.6 Waypoint Web Users

Viewing, editing, and deleting user accounts is accomplished via the Users link in the navigation bar:



12 Network Connection Security

There are numerous mechanisms available within Waypoint to help ensure that user data is secure and protected.

12.1 Network Connections

In order to support communicating with devices that either do not support or are not configured to use encrypted connections, Waypoint is able to establish unencrypted connections to Sources and Destinations. However, Waypoint can support TLS 1.0, 1.1, and 1.2 encrypted connections on a per-Source and per-Destination basis. It is recommended that TLS encrypted connections be used wherever possible. The option to choose an encrypted connection is available on each Source's and Destination's configuration screen in the **Options** dialog. Also, the certificate configuration can be found on the **System** tab in the **Options** dialog. See Appendix D, Sections 1.2 and 1.3 for details.

12.2 Database Connections

In order to support communicating with SQL Server that has not been configured to support encrypted connections, Waypoint is able to establish unencrypted connections to SQL Server. However, it is recommended that encrypted connections to SQL Server be used, if possible. The option to choose an encrypted connection to SQL Server is available via the **Encrypt Connection** checkbox on the **Waypoint Database Configuration** dialog.

Appendix A: Waypoint Privacy and Security Statement

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

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

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

1 Management of Private Data

The Laurel Bridge Waypoint application acts as a worklist server for DICOM messages and as a receiver for HL7 version 2.x messages, both of which may contain protected health information (PHI). Waypoint can route these messages from one or more sources to one or more destinations. Consequently, Waypoint can ingest, store, display, and transmit PHI. However, since the PHI only resides in Waypoint temporarily, Waypoint 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 Waypoint 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 Waypoint 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
- Patient financial information

1.2 Persistence of Private Data

Waypoint 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. Data can be imported from or exported to other medical

systems via network-mounted hot folders or removable media, but these features must be explicitly configured by the Waypoint customer, and their use remains under the full control of the customer. Available security features to protect PHI when at rest are described below and, in more detail, elsewhere in this Waypoint User Manual.

Note: Due to the sensitive nature of the PHI that Waypoint handles, the only non-destructive and completely safe way to decommission a (non-virtual) computer system on which a production Waypoint 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 via DICOM, HL7, or other messages. The ability to configure and control the behavior of this functionality is under the full control of the Waypoint 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 Waypoint User Manual.

Because Waypoint 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 Waypoint application is comprised of three parts:

1. **Waypoint Service**, which runs as a Windows Service
2. **Waypoint Client**, a Windows Forms-based (UI) application which is used to configure and monitor the Waypoint Service
3. **Waypoint Web**, an optional web interface that allows configured web users to monitor and manage jobs

Note that the Waypoint Client does not need to be running for the Waypoint Service to run, accept, process, and send messages.
The following sections briefly describe available security features of the Waypoint application. For more details, see the Waypoint User Manual.

2.1 Automatic Logoff

The Waypoint Client (the UI used to configure the Waypoint application) does not automatically time out or log a Windows user off, so LBS recommends that the Windows password-protected, inactivity-activated screen lockout functionality be enabled for all users with Waypoint privileges on the host Windows system, to help avoid unintended administrative access by unauthorized users.
The Waypoint Web interface can be configured to automatically log off Waypoint 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

Waypoint 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 Waypoint:

- **Application Activity**
  - Application Start
  - Application Stop

- **Security Alert**
  - Security Configuration
  - Software Configuration
  - User Security Attributes Changed
- **User Authentication**
  - Login
  - Logout

2.3 User Authorization

Windows Authentication (whether locally administered or domain-based) is used to control access to the Waypoint Client (and thus the ability to configure the Waypoint Service). It is up to the customer to lock down administrative control of Waypoint (e.g., by using a custom Windows user-level group), if desired.
The Waypoint Web users can either be locally administered (by the Waypoint Web module), or they can be administered using LDAP / Active Directory. This is done by the Waypoint 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 Waypoint customer has full control over and responsibility for the security of Waypoint, both through the ability to lock down the Windows system on which Waypoint is installed, as well as through the ability to configure the security features built into the Waypoint application. Extensive information about how to do this is found in this Waypoint User Manual.

2.5 Security Updates

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

2.6 De-Identification of PHI

Waypoint does not support the ability to configure de-identification of PHI, due to the consequences this would have on the usability of the DICOM and HL7 messages.

2.7 Backup and Restore

The Waypoint customer has full responsibility to both install and maintain the SQL Server database which provides the backing store for the Waypoint data. 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 Waypoint customer has full control over the installation and configuration of both the host system and the Waypoint 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 Waypoint is to modify and route 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 Waypoint is installed.
- Use Waypoint Web authentication (either locally administered or based on Windows Authentication) to ensure that unauthorized web users cannot access the Waypoint 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.

Waypoint 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 Waypoint customer has full control over the installation and configuration of both the host Windows system and the Waypoint application itself, it is up to the customer to install and maintain malware protection technology. Waypoint 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 Waypoint.

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 protocols on all network connections. Waypoint supports TLS versions 1.0, 1.1, and 1.2 as both client and server. TLS must be enabled separately on both DICOM and HL7 inputs and outputs, as well as on the Waypoint Web interface. More details about how to do this and further security details can be found elsewhere in this Waypoint 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 “waypoint”). 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 Waypoint customer owns and has full control over the host Windows system on which Waypoint is installed, it is up to the customer to maintain the physical security of the host system.

2.14 Device Life Cycle Roadmap

The Waypoint 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 Waypoint application has the following software dependencies:

- SQL Server (can be 2016 x64 or newer)
- SQL Server Management Studio
- .NET Framework 4.8 (or later)

See section 2.2 Minimum System Specification and section 2.3 Prerequisites.

2.15 System and Application Hardening

Since the Waypoint customer provides, configures, owns, and has full control over the host system on which Waypoint is installed, it is up to the customer to perform system hardening, as well as to configure the Waypoint application for the desired level of application hardening. More details about hardening of the host Windows system and the Waypoint application can be found elsewhere in this Waypoint User Manual.
Some specific application hardening techniques that are supported by and/or implemented in Waypoint include:

- Use of Authenticode digital signatures (currently SHA256) for all LBS executables and DLLs
- Support for TLS encryption for data in transit
- Provision of instructions for how to lock down the TLS protocols and ciphers, which affects both the Waypoint Web interface, as well as any DICOM or HL7 connections which are configured to use TLS encryption (see User Manual, Appendix C: Communicating Securely with Waypoint)
- Support for sign on (Windows Authentication / Active Directory)

The implementation of the following lockdown techniques on the host Windows system is the responsibility of the Waypoint 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 Waypoint application are described in detail in this Waypoint User Manual.

2.17 Data Storage Confidentiality

Waypoint 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. Waypoint 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

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

2.20 Other Security Considerations

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

- DICOM input port = **11114** (**2762** if using TLS)
- HL7 input port = **11119** (same if using TLS)
- HTTP port = **10500** (**10501** 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 Waypoint 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 Waypoint 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.

Appendix B: Waypoint FAQs

1 How can I map my HL7 ORM messages to patient and worklist items stored in Waypoint's database?

Edit the HL7 Options and select the HL7 MWL Mappings tab. To store HL7 Messages sent to Waypoint in the database:

- Create an MWL Mappings for incoming HL7 ORM messages, e.g. "ORM Incoming". Note, different departments or modalities may have unique formats to the HL7 messages they send to Waypont, therefore, you may need multiple mapping rules:
    - ORM Radiology Incoming
    - ORM Oncology Incoming
    - ORM Mammo Incoming
- As Mentioned in section 5.2, Test MWL Mapping, copy a sample HL7 message into the system clipboard then paste the message into the Message Template on the MWL Mappings Test screen. When you click the OK button, the Test Result column is populated with the results of applying the MWL Mapping the HL7 test message. Continue modifying the HL7Tags, and Pattern Replacements until the Test Results match your requirements for the Mapping Group, which are the fields stored in Waypoint's database.

2 How can I map the data stored in Waypoint's database to elements in the MWL query response messages?

Edit the HL7 Options and select the HL7 MWL Mappings tab. To specify the mapping of worklist items in Waypoint's database for MWL C-Find Response messages:

- Create an MWL Mappings for outgoing DICOM C-Find response messages, e.g. "MWL Outgoing". Note, different departments or modalities may have unique formats for the MWL C-Find response messages they receive from Waypoint, therefore, you may need multiple mapping rules:
    - MWL Radiology Outgoing
    - MWL Oncology Outgoing
    - MWL Mammo Outgoing
- As Mentioned in section 5.2, each Mapping Group in the MWL Mapping has a Dicom Tag that defines the DICOM element in the C-Find response message that is used to match or retrieve the value from Waypoint's database. The default values from taken from the DICOM 3.0 Standard and therefore are generally the expected DICOM tag for the field. However, you are free to change the DICOM tag to the whatever the receiving MWL SCU is expecting. Also, each Group has 5 Custom fields, that can be used for any DICOM Tag that is required by the SCU.

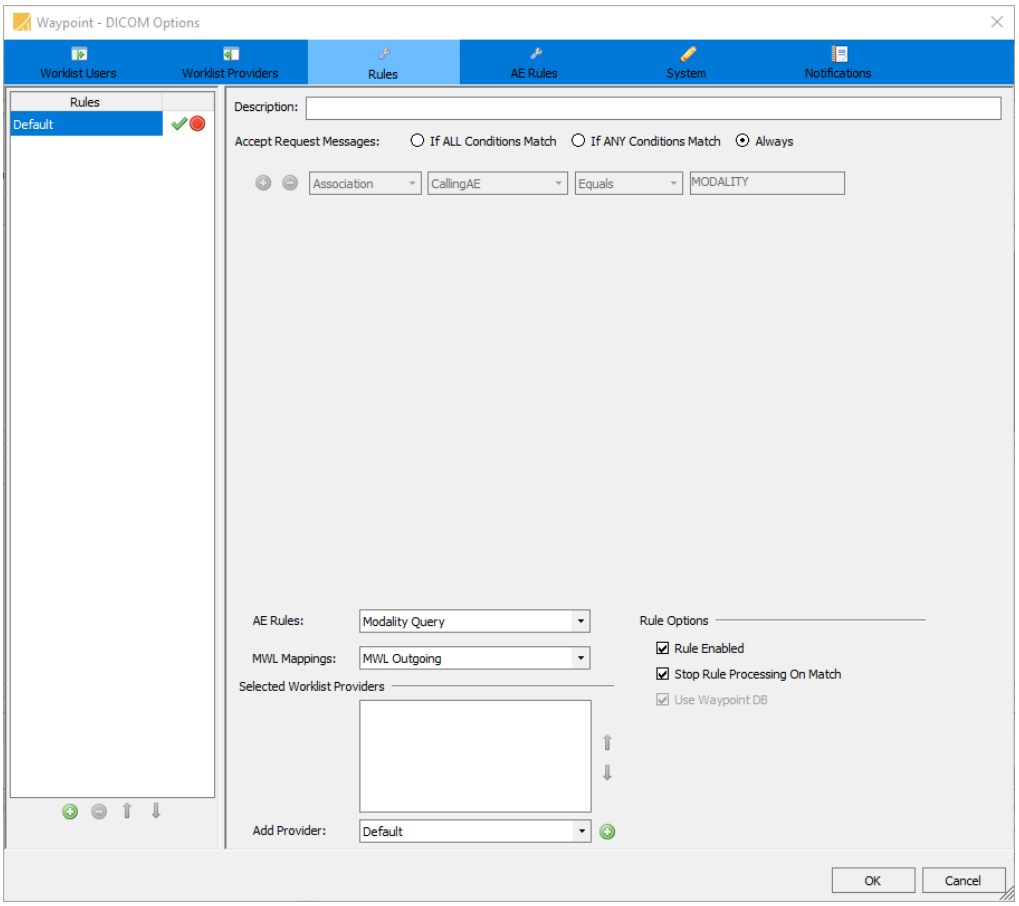
3 How and where are the HL7 MWL Mappings used by Waypoint?

Both the HL7 Rules and DICOM Rules define a condition that selects an HL7 MWL Mapping. As mentioned above, HL7 Rules select an Incoming HL7 MWL Mapping, whereas DICOM Rules select an Outgoing HL7 MWL Mapping.

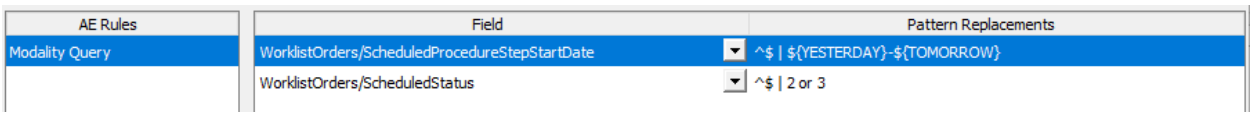
4 How do I configure Waypoint so the modalities only receive worklist orders that are scheduled for yesterday through tomorrow and are for patient's that have arrived for their exam?

The purpose of the AE Rules are to append new DICOM elements or modify existing DICOM elements in the C-Find request with alternate data values when a Waypoint DICOM Rule is triggered. For example, this feature is used to modify the Scheduled Procedure Step Start Date to match yesterday through tomorrow's date range. Also, modify the Scheduled Procedure Status to only match worklist items in the STARTED state. Note, this example implies that the RIS updates worklist items to the STARTED state when the patient arrives for the exam by sending an HL7 message to Waypoint with scheduled status set to STARTED.

The following screen shot shows a DICOM Rule that selects "Modality Query" for its AE Rule and "MWL Outgoing" for its HL7 MWL Mapping:



The selected AE Rule, "Modality Query" has the following setting:



The Scheduled Procedure Step Start Date has the Pattern Replacement that matches the regular expression ^$ and replaces it with "${YESTERDAY}-${TOMORROW}". The regular expression only matches if the value in the C-Find request for Scheduled Procedure Step Start Date is empty. If a specific date or date range is being requested, Waypoint will honor the date range from the original C-Find request. Similarly, if the Scheduled Procedure Step Status in the C-Find request is empty, Waypoint will automatically match worklist items that have a Scheduled Status value of 2 or 3. This excludes new orders with value 1, canceled orders with value 4, and completed orders with value 5.

Appendix C: Communicating Securely with Waypoint

1 Secure DICOM and HL7 Communication with Waypoint

The Waypoint application may be configured to communicate securely with another device by enabling the appropriate TLS (Transport Layer Security) options. Typically, this feature is used to enable secure DICOM communications between the RIS and Modalities to Waypoint .

1.1 Overview

Waypoint supports the Basic TLS Secure Transport Connection Profile (See DICOM PS3.15 2015c Security and System Management Profiles, Appendix B.1) for authentication and encryption of communication between it and other DICOM clients and servers. Waypoint supports TLS version 1.0 as required by this profile.

1.2 Configuring Secure DICOM Communication

For secure DICOM communication to another DICOM MWL provider, one should select the **Use TLS** option under the **Advanced** section of the DICOM **Worklist Providers** pane (by selecting one or more TLS versions to support). See Section 4.2.5 Advanced Settings for more details. For secure DICOM communication from another DICOM application, one should select the **Encrypted Listener** option under the DICOM **System** pane (by selecting one or more TLS versions to support). See Section 6.1.2 DICOM Incoming for more details.

When TLS is enabled on a **Worklist Provider** (i.e., Waypoint is the client), Waypoint will use the TLS secure communication mechanism to request the server's certificate when it makes a connection to the server. It will then authenticate the server and encrypt all communications with the server. Waypoint can optionally be configured to send the client's certificate when making a connection, which allows the server to authenticate the client as well.

When TLS is enabled on the **DICOM System** pane (i.e., Waypoint is the server), Waypoint will use the TLS secure communication mechanism to request the client's certificate when it makes a connection to the client. If a certificate is sent, it will authenticate the client. Regardless of whether a certificate is sent, it will encrypt all communications with the client. Waypoint can optionally be configured to require the client's certificate when making a connection. In this case, if the client does not send its certificate, the connection will be refused. The default is to allow missing client certificates (no client authentication), which is similar to how web browsers work.

On both the client and server sides, Waypoint may optionally be configured to accept self-signed certificates or to ignore certificate name mismatch errors. These options are primarily intended for testing purposes, and for optimal security, we recommend that these be left unchecked. 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 (see Appendix E for instructions), manually (and securely) copied to the remote computer, and installed into the certificate store on that computer as a trusted root certificate.

To properly configure incoming DICOM TLS connections, on the DICOM **System** pane, the **TLS Listen Port**, **TLS Certificate** path and certificate **Password** must be set. The **TLS Listen Port** default is port 2762, as recommended by the standard; it is the port on which Waypoint will receive TLS encrypted communications (e.g., DICOM associations). The **TLS Certificate** path should be set to the file system location of the certificate that Waypoint should present for identification to clients. It is suggested that the certificate be a standard PKCS#12 certificate and it must contain an exportable private key. The **Password** must be set to the password for the private key in the certificate. Note: Using a certificate format that does not password-protect the private key allows the password setting to be ignored, but we highly recommend keeping private keys password-protected. This appendix does not describe the procedures that are required to obtain TLS certificates.

This configured certificate information will be provided to any DICOM TLS client that connects to Waypoint on the TLS listen port. This configured certificate information can also be provided to any server that Waypoint connects to, if configured to do so. All communication over this connection is then encrypted using the exchanged certificate(s). Note that this TLS-level authentication is in addition to the DICOM-level authentication that Waypoint provides based on DICOM AE titles and IP addresses (which are used to determine whether or not to allow a DICOM client to open a DICOM association to Waypoint).

See DICOM PS3.15 2015c Security and System Management Profiles, Appendix B.1, for a further description of the Basic TLS Secure Transport Connection Profile. This document may be found at: http://medical.nema.org/standard.html.

1.3 Configuring Secure HL7 Communication

For secure HL7 communication from another HL7 application, one should select the **Use TLS** option under the **Waypoint Listen Configuration for Source** section of the **HL7 Sources** pane (by selecting one or more TLS versions to support). See Section 5.1.1.1 Settings for more details. When TLS is enabled on an **HL7 Source** (i.e., Waypoint is the server), Waypoint will use the TLS secure communication mechanism to request the client's certificate when it makes a connection to the client. If a certificate is sent, it will authenticate the client. Regardless of whether a certificate is sent, it will encrypt all communications with the client. Waypoint can optionally be configured to require the client's certificate when making a connection. In this case, if the client does not send its certificate, the connection will be refused. The default is to allow missing client certificates (no client authentication), which is similar to how web browsers work.

Waypoint may optionally be configured to accept self-signed certificates or to ignore certificate name mismatch errors. These options are primarily intended for testing purposes, and for optimal security, we recommend that these be left unchecked. 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 (see Appendix E for instructions), manually (and securely) copied to the remote computer, and installed into the certificate store on that computer as a trusted root certificate.

To properly configure incoming HL7 TLS connections, the **Listen Port** must be set on the **HL7 Sources pane**, and the **TLS Certificate** path and certificate **Password** must be set on the HL7 **System** pane. The **TLS Certificate** path should be set to the file system location of the certificate that Waypoint should present for identification to clients. It is suggested that the certificate be a standard PKCS#12 certificate, and it must contain an exportable private key. The **Password** must be set to the password for the private key in the certificate. Note: Using a certificate format that does not password-protect the private key allows the password setting to be ignored, but we highly recommend keeping private keys password-protected. This appendix does not describe the procedures that are required to obtain TLS certificates.

This configured certificate information will be provided to any HL7 TLS client that connects to Waypoint on a TLS listen port. All communication over this connection is then encrypted using the exchanged certificate(s).

2 Secure Communication with Waypoint Web

There are several configuration changes that can be made to the Windows computer on which Waypoint is installed to enhance the security of the Waypoint web interface. These changes assume that HTTPS (TLS) is used exclusively to access the Waypoint web interface (which we strongly recommend), and they primarily involve changes to the supported TLS protocols and ciphers. Some of these changes only apply to certain supported Windows versions, while others apply to all the supported Windows versions. These changes include the following:

- Disabling support for the SSL 3.0 protocol (if supported)
- Disabling support for the TLS 1.0 protocol (if older browsers must be supported)
- Enabling support for the TLS 1.1 and 1.2 protocols (if not already supported)
- Disabling support for the RC4 cipher suite
- Disabling support for the Triple DES (3DES) cipher suite

The changes discussed below can either be made manually using `regedit`.

2.1 Disabling SSL 3.0 Support

SSL 3.0 is an older encryption protocol that is no longer considered cryptographically secure (due to its POODLE attack vulnerability). While the protocol is no longer supported by modern browsers, it is still supported by some older versions of Windows, including Windows 7 and Windows Server 2008 R2, so its use can still be negotiated by certain older browsers when connecting to these systems. We recommend that its use be disabled if running either of the above operating systems.

To disable SSL 3.0 manually, start Windows `regedit` and do the following:

- Navigate to: `HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols`
- Add the subkey "`SSL 3.0`".
- Under subkey "`SSL 3.0`", add the subkeys "`Client`" and "`Server`".
- Under subkey "`Client`", add the DWORD entry "`DisabledByDefault`" and set it to one.
- Under subkey "`Server`", add the DWORD entry "`Enabled`" and set it to zero.

Once the above changes have been made, restart Windows to complete the process. The change can be confirmed using `Nmap` to enumerate the supported protocols and ciphers on the HTTPS port, as described above.

2.2 Disabling TLS 1.0 Support

TLS 1.0 is an older encryption protocol that is considered cryptographically weak (due to its potential BEAST attack vulnerability when using obsolete browsers). We recommend that its use be disabled, unless all clients connecting to Waypoint will be using modern (evergreen) browsers such as Chrome, Firefox, and Edge.

To disable TLS 1.0 manually, start Windows `regedit` and do the following:

- Navigate to: `HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols`
- Add the subkey `"TLS 1.0"`.
- Under subkey `"TLS 1.0"`, add the subkeys `"Client"` and `"Server"`.
- Under subkey `"Client"`, add the DWORD entry `"DisabledByDefault"` and set it to one.
- Under subkey `"Server"`, add the DWORD entry `"Enabled"` and set it to zero.

Once the above changes have been made, restart Windows to complete the process. The change can be confirmed using `Nmap` to enumerate the supported protocols and ciphers on the HTTPS port, as described above.

2.3 Enabling TLS 1.1 and 1.2 Support

TLS 1.1 and 1.2 are newer encryption protocols that are considered cryptographically secure. We strongly recommend that these protocols be used whenever possible. However, some older versions of Windows, including Windows 7 and Windows Server 2008 R2, do not support TLS 1.1 and 1.2 by default. If the Windows updates for the above operating systems are up-to-date (specifically, if KB3140245 is installed), the protocols themselves are available, but they must be manually enabled.

To enable TLS 1.1 and 1.2 manually, start Windows `regedit` and do the following:

- Navigate to: `HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols`
- Add the subkey `"TLS 1.1"` and `"TLS 1.2"`.
- Under subkey `"TLS 1.1"`, add the subkeys `"Client"` and `"Server"`.
- Under subkey `"TLS 1.2"`, add the subkeys `"Client"` and `"Server"`.
- Under subkey `"Client"` for both protocols, add the DWORD entry `"DisabledByDefault"` and set it to one.
- Under subkey `"Server"` for both protocols, add the DWORD entry `"Enabled"` and set it to zero.

Once the above changes have been made, restart Windows to complete the process. The changes can be confirmed using `Nmap` to enumerate the supported protocols and ciphers on the HTTPS port, as described above.

2.4 Disabling Support for the RC4 Cipher Suite

RC4 is a family of encryption ciphers that is no longer considered cryptographically secure (due to its NOMORE attack vulnerability – see RFC 7465 for details). Unfortunately, this cipher suite is supported by all three versions of TLS (1.0, 1.1, and 1.2), so its use can still be negotiated by certain modern browsers. We recommend that its use be disabled if possible (i.e., as long as all supported clients support other, more secure, ciphers).

To disable RC4 manually, start Windows `regedit` and do the following:

- Navigate to:
  `HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers`
- Add the subkey `"RC4 128/128"`.
- Add the subkey `"RC4 40/128"`.
- Add the subkey `"RC4 56/128"`.
- Under subkey `"RC4 128/128"`, add the DWORD entry `"Enabled"` and set it to zero.
- Under subkey `"RC4 40/128"`, add the DWORD entry `"Enabled"` and set it to zero.
- Under subkey `"RC4 56/128"`, add the DWORD entry `"Enabled"` and set it to zero.

Once the above changes have been made, restart Windows to complete the process. The change can be confirmed using `Nmap` to enumerate the supported protocols and ciphers on the HTTPS port, as described above.

2.5 Disabling Support for the Triple DES (3DES) Cipher Suite

Triple DES is a family of encryption ciphers that is no longer considered cryptographically secure (due to its SWEET32 attack vulnerability). Unfortunately, this cipher suite is supported by all three versions of TLS (1.0, 1.1, and 1.2), so its use can still be negotiated by certain modern browsers. We recommend that its use be disabled if possible (i.e., as long as all supported clients support other, more secure, ciphers).

To disable Triple DES manually, start Windows `regedit` and do the following:

- Navigate to:
  `HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers`
- Add the subkey `"Triple DES 168"`.
- Under subkey `"Triple DES 168"`, add the DWORD entry `"Enabled"` and set it to zero.

Once the above changes have been made, restart Windows to complete the process. The change can be confirmed using `Nmap` to enumerate the supported protocols and ciphers on the HTTPS port, as described above.

3 A Note About FIPS 140-2 Compliance

Laurel Bridge Software neither provides nor configures the computer on which Waypoint runs and thus has no way to know a priori which cryptographic modules will be available in a particular installation. Since FIPS 140-2 compliance is based on the evaluation and certification of particular implementations of cryptographic modules (and not the algorithms themselves), Laurel Bridge Software cannot make any assertions regarding the FIPS 140-2 compliance of a specific Waypoint installation. Microsoft does provide a means by which a Windows system can be locked down so that only FIPS 140-2 compliant modules are used, but their current guidance no longer recommends running in this FIPS 140-2 compliant mode, unless doing so is explicitly required by government regulations. For more details on why this is so, see the article at `https://blogs.technet.microsoft.com/secguide/2014/04/07/why-were-not-recommending-fips-mode-anymore`.

Appendix D: Waypoint Configuration Backup Files

Waypoint' configuration is persisted in a file named `waypoint-config.xml`, and is typically located at:
"`C:\ProgramData\Laurel Bridge Software\Waypoint\waypoint-config.xml`".

Any time you save a new configuration by clicking "OK" on either the DICOM Options dialog or the HL7 Options dialog, a backup of your previous configuration is copied and saved to "`waypoint-config-autobackup-yyyy-MM-dd-HHmmss.xml`" in a subfolder called "`backup`", where:

- `yyyy` is the year
- `MM` is the month
- `dd` is the day
- `HH` is the hour (in 24-hour format)
- `mm` is the minutes
- `ss` is the seconds

Waypoint will allow the user to configure whether or not the number of configuration backup files it keeps is limited (see the **System Settings** section for more information). If the user has chosen to limit the number of configuration backup files, then whenever a backup is created, Waypoint will only keep the configured number (keeping the most recent files). If the number of configuration backup files is not being limited and more than 20 backup files exist, a message box will be displayed reminding the user of how many backup files exist; with this setting, it is up to the user to remove any unwanted backup files.

Appendix E: Create and Export a Self-Signed TLS Certificate

1 Using IIS Manager

The following are instructions on how to create and export a self-signed certificate using Windows and Windows Server using the IIS Manager. See **Appendix C**.

Once enabled, run the Internet Information Services (IIS) Manager program. Then perform the following actions:

4. Double-click "Server Certificates"
5. Under "Actions" (on the right side of the dialog), click "Create Self-Signed Certificate..."
6. A dialog will pop up; type in a friendly name (anything will do). The certificate store combo box should be "Personal". Click "OK".
7. Your certificate should now be in the list. Select the newly created certificate, and then click "Export..." under the "Actions" area (on the right side of the dialog).
8. Type in a filename and specify a password. Click "OK".
9. Verify that the file was created.
10. Import this certificate into Waypoint specifying the newly created file and corresponding password.

2 Using PowerShell

To create a self-signed TLS certificate using PowerShell, first start a PowerShell instance as Administrator. Then enter a command similar to one of the following (note that Tab-completion can be used to enter command, including parameter names):

```
PS> New-SelfSignedCertificate -CertStoreLocation Cert:\LocalMachine\My
    -DnsName "www.mydomain.com"  # a normal TLS certificate

PS> New-SelfSignedCertificate -CertStoreLocation Cert:\LocalMachine\My
    -DnsName "*.mydomain.com"    # a wildcard TLS certificate

PS> New-SelfSignedCertificate -CertStoreLocation Cert:\LocalMachine\My
    -DnsName "www.mydomain.com","ftp.mydomain.com"  # a SAN TLS certificate
```

This will create the self-signed certificate and install it into the local machine repository. To export this certificate, run "certlm.msc", expand "Personal", click "Certificates", then right-click the newly-created certificate. Select "All Tasks", then "Export...". A wizard will pop up. Click Next to continue, choose to export the private key, then click Next, check the "Export all extended properties" under the .PFX section then click Next, enter a password (twice) then click Next, enter a filename for the .PFX file then click Next, and click Finish to generate the .PFX file containing the exported certificate (including the private key).

Appendix F: Communicating with Authorized Web Methods from Waypoint

An HTTP method that is decorated with the Authorize attribute requires that the HTTP client provide an access token in the Authorization header of the HTTP request. The access token is formatted as JWT, Json Web Token. In the absence of the Authorization header or invalid access token the method will fail with status code Unauthorized (401). An example of the Authorize attribute is:

```
[Authorize]
[Route("")]
[HttpGet]
public async Task<IActionResult> Get() {…}
```

Waypoint offers the ability to access authorized HTTP methods provided that the HTTP server implements a login method that Waypoint invokes to retrieve an access token. Once the token is retrieved, Waypoint adds the access token to the Authorization header when accessing HTTP methods that require authorization.

1 The Login Method

The Login method allows the HTTP Service to support simple authentication for its authorized methods. The Login method is an HttpPost method that receives the login request containing a Json object with the UserName and Password properties.
The message body for the login request is:

```
{“UserName”:"USERNAME", “Password”:"PASSWORD"}
```

If the given USERNAME and PASSWORD are accepted, the next step is to generate and store a unique JWT access token for the login request. The response from the Login method is a Json encoded object created from the class:
`LaurelBridge.AppFramework.Web.Model.LoginResponseModel`.

The final step is to construct and set the properties on the LoginResonseModel then return it to the HTTP client. A simple Login example follows:

```
[WebMethod]
[WebInvoke(Method = "POST", UriTemplate = "Login",
 ResponseFormat = WebMessageFormat.Json,
 RequestFormat = WebMessageFormat.Json)]
public LoginResponseModel Login(string jsonLogin)
{
   LoginModel login = new JavaScriptSerializer().Deserialize<LoginModel>(jsonLogin);

   DateTimeOffset now = DateTimeOffset.Now;
   JwtPayload payload = GenerateJSONWebToken(login.UserName, login.Password);

   LoginResponseModel responseModel = new LoginResponseModel
   {
      Token = new Token
```



```
        {
           access_token = payload["jti"].ToString(),
           expires_in = ((int) (DateTimeOffset.FromUnixTimeSeconds(
               (long) payload["exp"]) - now).TotalMinutes)
        },
        Succeeded = true,
        User = new User()
        {
           Name = login.UserName,
        },
        ErrorMessage = string.Empty
     };

     return responseModel;
  }
```

1.1 LoginResponseModel

The *LoginResponseModel* is a class contained in the *LaurelBridge.AppFramework.Web* assembly. The *Token* property contains the access token that is sent from the Authorized HTTP Server to Waypoint. The declaration for the *LoginResponseModel* is:

```
public class LoginResponseModel
  {
    /// <summary>Gets or sets the token.</summary>
    /// <value>The token.</value>
    [DataMember(Name = "token")]
    public Token Token { get; set; }
    /// <summary>Gets or sets the user.</summary>
    /// <value>The user.</value>
    [DataMember(Name = "user")]
    public User User { get; set; }
    /// <summary>
    /// Gets or sets a value indicating whether this
    /// <see cref="T:LaurelBridge.AppFramework.Web.Model.LoginResponseModel" />
    /// is succeeded.
    /// </summary>
    /// <value>
    ///   <c>true</c> if succeeded; otherwise, <c>false</c>.
    /// </value>
    [DataMember(Name = "succeeded")]
    public bool Succeeded { get; set; }
    /// <summary>Gets or sets the error message.</summary>
    /// <value>The error message.</value>
    [DataMember(Name = "errorMessage")]
    public string ErrorMessage { get; set; }
  }
```

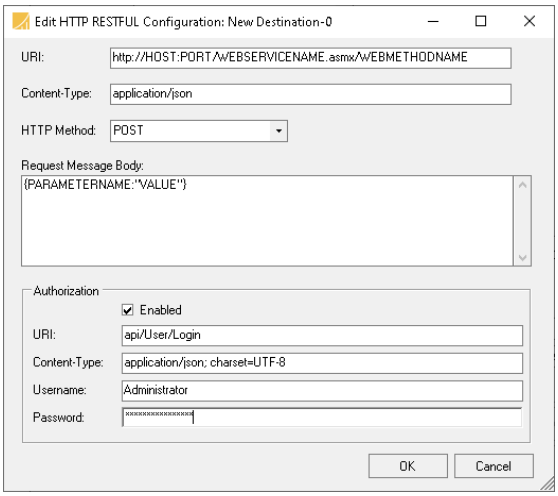
The *Token* property contains the access token for the login request:

```
public class Token
{
/// <summary>Gets or sets the access token.</summary>
/// <value>The access token.</value>
[DataMember(Name = "access_token")]
public string access_token { get; set; }
/// <summary>Gets or sets the expires in.</summary>
/// <value>The expires in.</value>
[DataMember(Name = "expires_in")]
public int expires_in { get; set; }
}
```


1.2 Configuring Waypoint

The Waypoint User Manual **section 4.2.4.2 Transport Mode** contains the description for configuring Waypoint to communicate with an HTTP RESTful service that has Authorization Enabled. In summary:

- Create a Worklist Provider with Transport Mode: HTTP RESTFUL



- On the Edit HTTP RESTFUL Configuration form, the upper section is the Authorized method being invoked. The lower section provides the configuration to:
  - Enable Authorization
  - Specify the URI of the Login method
  - Specify the Content Type for the message body of the Login method
  - Provide the Username
  - Provide the Password

1.3 Authorized HTTP RESTFUL Method Sequence of Actions

When the HTTP RESTFUL Worklist Provider is scheduled to trigger, the following actions are performed:

- Request an HTTP Post request to the Authorization URI with a Json encoded message body containing the Username and Password
- Extract the access token from the Login response message
- Send the HTTP Request for the authorized method with the Authorization header containing the access token received from the Login method.

1.4 References

The following link is a reference for how to generate the JWT access token described above.
https://www.c-sharpcorner.com/article/jwt-json-web-token-authentication-in-asp-net-core/

