TREK

DATA

USER GUIDE

January 2023

Approved for Public Release; Distribution is Unlimited.

TABLE OF CONTENTS

FIGURES

1   Welcome

The Telescience Resource Kit (TReK) is a suite of software applications and libraries that can be used to monitor and control assets in space or on the ground.

The TReK Data application provides the capability to manage data services such as receiving data, processing data, recording data, forwarding data, and displaying data.

The topics in this user guide require an understanding of the topics covered in the TReK Concepts document. Please be sure you have read the TReK Concepts document before reading this user guide.

1.1   Getting Started

Start with the Introduction which provides an application overview. Next, try the Quick Start Guides for "How Tos" for common functions. For help with details, reference the Details section. See the FAQ and Troubleshooting section for helpful hints and solutions to the common "gotchas".

2   Technical Support

If you are having trouble installing the TReK software or using any of the TReK software, please contact us for technical assistance:

TReK Help Desk E-Mail, Phone & Fax:

E-Mail: trek.help@nasa.gov
Telephone: 256-544-3521 (8:00 a.m. - 4:00 p.m. Central Time)
Fax: 256-544-9353

If you call the TReK Help Desk and you get a recording please leave a message and someone will return your call. E-mail is the preferred contact method for help. The e-mail message is automatically forwarded to the TReK developers and helps cut the response time. The HOSC Help Desk (256-544-5066) can provide assistance as needed and is available 24x7.

3   Introduction

The TReK Data application provides the capability to manage data services such as receiving data, processing data, recording data, forwarding data, and displaying data. It can be configured to receive different types of data from multiple sources simultaneously. The configuration can be saved.

The Data application creates a TReK data store on application initialization. The data store is used by the application to store incoming data so it can be accessed using the

TReK Telemetry Application Programming Interface (API). When using the TReK Telemetry API, you will need the data store name. The Data application uses "DefaultDataStore" as the default data store name. There is an option within the application to change the data store name. The application provides the capability to save the application configuration to a file. When you save the configuration to a file the data store name is saved as part of the configuration. If you start another instance of the Data application, and the "DefaultDataStore" name is already in use, the application will prompt you to enter a new and unique name. If you start the Data application from the command line and pass in a configuration file that contains a data store name that is already in use the application will exit with an error.

4   Overview of the User Interface

4.1   Main Window

The main window consists of three main areas as shown in Figure 1. The top part of the main window contains the list of services. A Service is used to define a set of functions to perform. When you start the Data application the list will be empty. The middle part of the window is the Statistics area. Once you activate one or more services, the Statistics area will display statistics information about each service. It will also provide information about the functions being performed like how many packets were recorded, how many packets were forwarded, etc. The Statistics area can be reconfigured to show several different views. The bottom part of the window is a message area that is used to display important status and information messages about the activities in progress.

You may have noticed that each service row has a color associated with it. The color provides information about the service. For example, when using the default colors, if the packet row is black, this indicates that the packet has not been activated. If the packet row is purple, this indicates that the service is initializing. If the packet row is blue, this indicates the packet has been activated but no data has arrived. If the packet row is green, this indicates that data packets are arriving. The colors are helpful in providing immediate information about the general configuration and status of each service in the list.

Figure 1 shows two services in the Service area. The first service in the list is named **Science Data**. The Science Data service is configured to receive a data stream containing science data. The status is Active and the color is green to indicate that data is arriving. The second service in the list is named Health and Status Data. The status is Inactive and the color is black. This indicates that the service has been configured but not activated. Until the service is active, the Data application is not prepared to handle the incoming data. When a service is activated, it creates all the network sockets and other support needed to support the services requested. As soon as a service goes Active, the application will start applying the configured services to support any data that arrives (processing, recording, etc.).

The Statistics area and the Message Area are dock windows that you can float or dock. To float a dock window, use your left mouse button to click and hold the title area while dragging the window to another area of the screen. To dock, use the title bar to drag the dock window over the main window and drop.
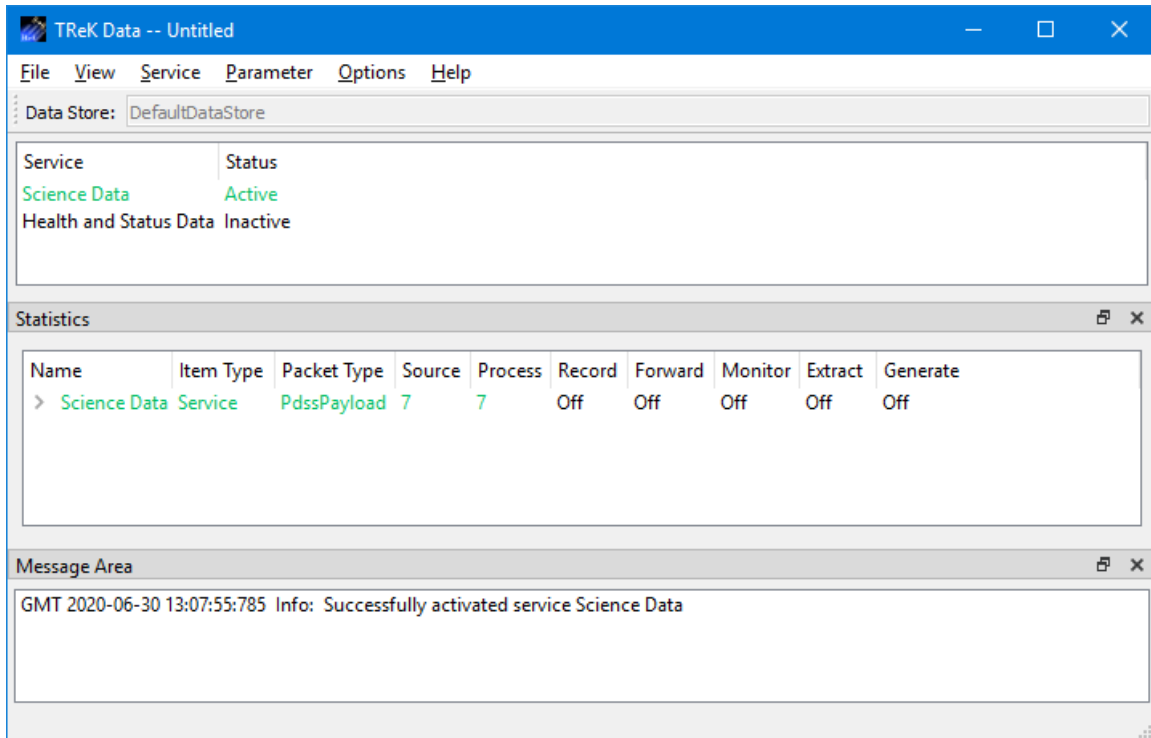
Figure 1 Main Window

Data Store Toolbar
The Data Store toolbar displays the name of the data store currently in use.

Service Area
The Service area provides a list of "Services". A Service defines a set of functions to perform.

Statistics Area
The Statistics area provides real time statistics information for active services.

Message Area
The Message Area displays important information, warning and error messages. The message area can be cleared using the View menu.

4.2   Menus

The application menus are: File, View, Service, Parameter, Options, and Help. Each of these menus is described in more detail below.

<u>File Menu</u>
The File menu provides the capability to create a new configuration, open a configuration, save a configuration, and exit the application.

<u>View Menu</u>
The View menu provides the capability to clear the main window message area and show and hide the main window statistics and message area.

<u>Service Menu</u>
The Service menu provides the capability to perform functions associated with services such as adding a service, activating a service, or deleting a service. The service menu also shows context dependent menu items corresponding to the configuration of the service. The context menu items will only appear when the service is active. For example in Figure 2 there is a service selected that is configured to record data. Therefore, when the service is active and selected there will be additional service menu items to control recording.
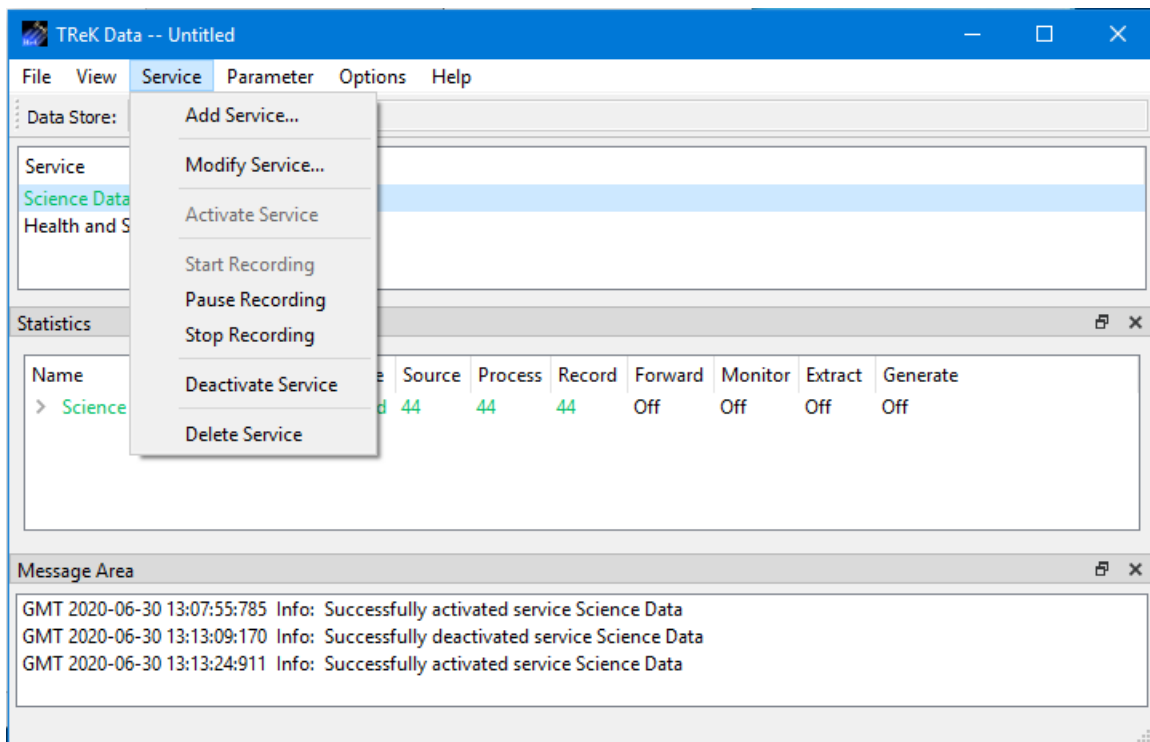
Figure 2 Service Menu Context Specific Menu Items

<u>Parameter Menu</u>

4

The Parameter menu provides access to parameter type capabilities such as displays and parameter monitoring.

Options Menu
The Options menu provides the capability to access statistics, reset statistics, configure statistics snapshot recording, and change the data store. It also provides access to the Messages dialog which can be used to display and filter application messages.

Help Menu
The Help menu provides access to on-line help and application version information.

5   Quick Start Guides

This section provides "How Tos" for common functions.

5.1   How to Add a Service

This section describes how to add a service. For additional information and details about the Add Service dialog please reference section 6.1.

1. To add a service, go to the Service menu and select Add Service.
2. Enter a service name unique to this instance of the Data application.
3. To configure the application to receive incoming data, enter the information about how the data will arrive on the Data Source tab. Using this tab you can configure to receive data using a specific communication protocol such as UDP.
4. To define what data the service should accept, enter a description of the data on the Data Description tab. This tab provides a way to control what data will be accepted for processing, recording, or forwarding.
5. To process incoming data, enter the processing information on the Process Tab. You can identify which packets you would like to process along with configuration information such as the number of buffers to use and the length of the buffers.
6. To record incoming data, enter the recording information on the Record Tab. You can specify to record data in a single directory or multiple directories.
7. To forward incoming data, enter the forwarding information on the Forward Tab. You can specify to forward data to one or more destinations selecting the communication protocol to use for each destination.

5.2   How to Activate a Service

This section describes how to activate a service.

1. To activate a service, select the service in the Main Window Service Area. Then go to the Service menu and select Activate Service.

Note: There is also a context sensitive pop-up menu available in the Main Window Service Area. Select the service in the list and then use the right mouse button to access the pop-up menu and select Activate Service.

5.3 How to Deactivate a Service

This section describes how to deactivate a service.

1. To deactivate a service, select the service in the Main Window Service Area. Then go to the Service menu and select Deactivate Service.

Note: There is also a context sensitive pop-up menu available in the Main Window Service Area. Select the service in the list and then use the right mouse button to access the pop-up menu and select Deactivate Service.

5.4 How to View Processed Data

The following steps describe how to view processed data. For additional information and details please reference section 6.3. When a service is configured with processing turned on, the Data application will auto-generate pre-defined displays to view the processed data. The predefined displays can be accessed using the Manage Displays menu item on the Parameter menu. Custom Displays can also be defined. See section 6.3.3 for details.

1. Add a service with Processing set to on.
2. Activate the service.
3. Go to the Parameter menu and select Manage Displays.
4. Select a display in the list and push the Start button. The display is automatically started and will display data if data is being received.

5.5 How to Change the Data Store

The following steps describe how to change the data store. For additional information and details about the Data Store dialog please reference section 6.10. The data store name can only be changed when all data processing services are off. If there are any active services that are processing data, the data store cannot be changed.

1. On the Options menu select Change Data Store.
2. Enter a valid Data Store name. It must be unique and not in use by any other instances of the TReK Data application.
3. Push the OK button to save the data store name and exit the dialog.

If successful, the Data Store toolbar will be updated to reflect the new data store name.

6   Details

This section covers various application details.

6.1   Service

The Service dialog is used to define a set of functions to perform. The Service configuration can only be modified when the Service is inactive.   The Add Service dialog is show in Figure 3. Details are provided below.

Figure 3 Add Service Dialog

Service Name
Each Service must have a unique name.

6.1.1   Service Dialog (Data Source Tab)

The Service Dialog Data Source tab is shown in Figure 4.
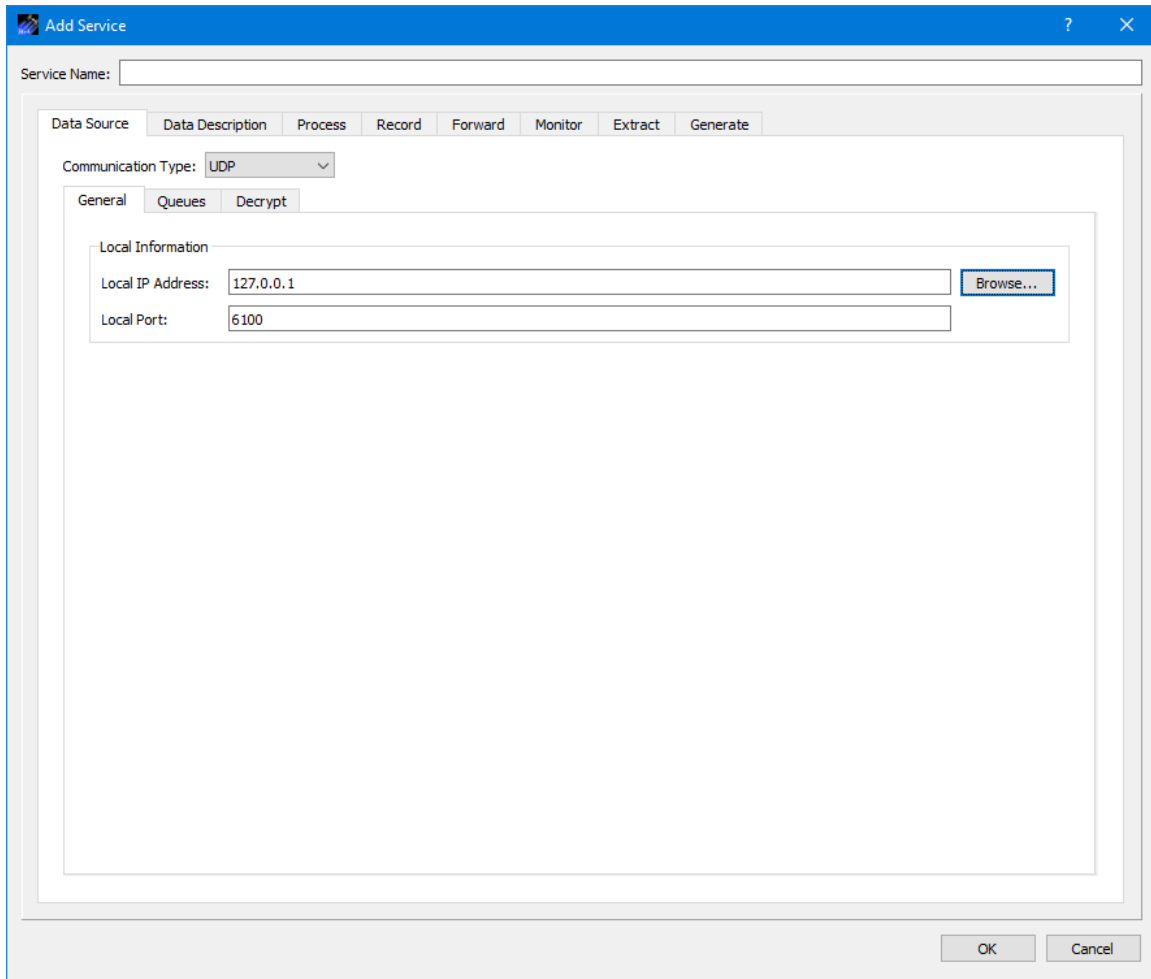
Figure 4 Service Dialog (Data Source General Tab)

6.1.1.1   Data Source General Tab

The Data Source General tab is used to enter information about how the data will be received. The fields that are displayed depend on the Communication Type setting. Communication Types include Bundle Protocol, Multicast, TCP Client, TCP Listener, UDP, and Unix Domain Socket (only available on Linux).

Each communication type configuration is described below.

6.1.1.1.1   Bundle Protocol Configuration

The Bundle Protocol Configuration is shown in Figure 5.

Figure 5 Service Dialog (Bundle Protocol Configuration)

Each field is described below.

Source Service Number
The source service number is ION's configured BP service number. This number is used to receive packets from ION.

Lifespan
The lifespan is the bundle's "time to live" (TTL) in seconds. The bundle is destroyed if its TTL has expired and it has not reached its destination. Minimum value is 1, maximum value is 2,147,483,647 and the default value is 86400.

9

Bundle Protocol Class of Service

The BP class of service defines the transmission priority of outbound bundles from three ION priority queues corresponding to *Bulk Priority*, *Standard Priority*, and *Expedited Priority*. The expedited priority queue must be empty before bundles in the standard or bulk queues are serviced by ION. Therefore, bundles with *Expedited Priority* should only be sent in critical/emergency situations. The default value is *Standard Priority*.

Expedited Priority Ordinal

The expedited priority ordinal is only associated with the *Expedited Priority* class of service. Ordinal values range from 0 (lowest priority) to 254 (highest priority). The default value is 0.

Transmission Mode

The transmission mode defines the reliability of bundle delivery to a destination. The three transmission mode parameter values are *Best Effort*, *Assured*, and *Assured with Custody Transfer*. *Best Effort* relies upon the underlying convergence-layer protocol (e.g., Transmission Control Protocol or TCP) to retransmit missing bundles. *Assured* is a step up in reliability and includes BP support in detecting a lost TCP connection and re-forwarding of bundles assumed aborted by the convergence-layer protocol failure. *Assured with Custody Transfer* requires the reception, by the sending node, of a custody acceptance or refusal signal (packaged in a bundle) from the receiving node. The default value is *Assured*.

Criticality

A critical bundle is one that has to reach its destination as soon as is physically possible. For this reason, bundles flagged as critical may not include custody transfer and require an ION configuration with contact graph routing. In some cases, a critical bundle may be sent over multiple routes to ensure delivery to its final destination. Critical bundles are placed in the expedited priority queue and should only be used in emergency situations. The two criticality parameters are *Not Critical* and *Critical*. The default value is *Not Critical*.

6.1.1.1.2   Multicast Configuration

The Multicast Configuration is shown in Figure 6.

Figure 6 Service Dialog (Multicast Configuration)

Each field is described below.

Local IP Address
This is the local IP address used for the UDP socket used for the multicast communication.

Local Port
This is the local port used for the UDP socket used for the multicast communication.

Multicast Information
Use the + and – buttons to add and delete multicast address groups to the Multicast Address Group List.

6.1.1.1.3   TCP Client Configuration

The TCP Client Configuration is shown in Figure 7.

Figure 7 Service Dialog (TCP Client Configuration)

Each field is described below.

12

Local IP Address
This is the local IP address used for the TCP Client socket.

Local Port
This is the local port used for the TCP Client socket.

Host Name
This is the host name of the remote computer.

IP Address
This is the IP address of the remote computer.

Port
This is the port of the remote computer.

6.1.1.1.4   TCP Listener Configuration
The TCP Listener Configuration is shown in Figure 8.
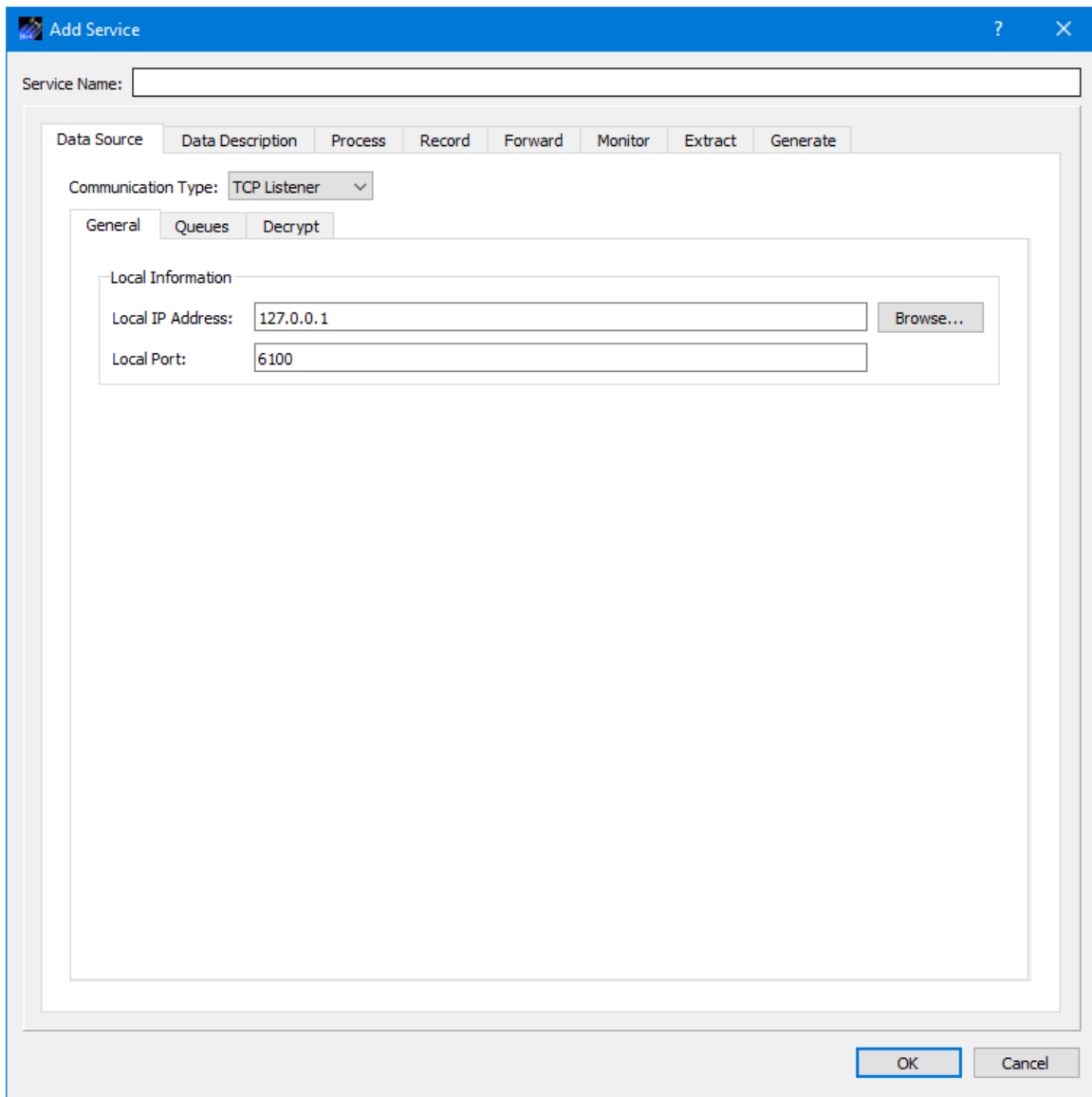
Figure 8 Service Dialog (TCP Listener Configuration)

Each field is described below.

Local IP Address
This is the local IP address used for the TCP Listener socket.

Local Port
This is the local port used for the TCP Listener socket.

6.1.1.1.5   UDP Configuration

The UDP Configuration is shown in Figure 9.

Figure 9 Service Dialog (UDP Configuration)

Each field is described below.
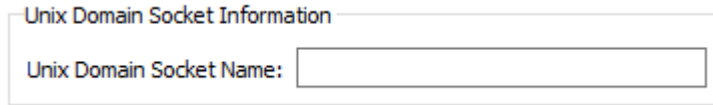
Local IP Address
This is the local IP address used for the UDP socket.

Local Port
This is the local port used for the UDP socket.

6.1.1.1.6   Unix Domain Socket Configuration

The UNIX Domain Socket Configuration is shown in Figure 10.

Unix Domain Socket Information

Unix Domain Socket Name: [   ]

Figure 10 Service Dialog (UNIX Domain Socket Configuration)

Each field is described below.

UNIX Domain Socket Name
This is the name to use when creating the UNIX Domain socket. The name will be NUL (\0) prefixed when the socket is created to use an abstract namespace.

6.1.1.2   Data Source Queues Tab
Each configuration includes the capability to configure properties associated with the memory queue used to hold incoming data. The Queues Tab is shown in Figure 11. Settings on the Queues tab are available for each communication type and provide the capability to size the queue and the buffer size of the queue. A queue size of zero implies no buffer for incoming data.
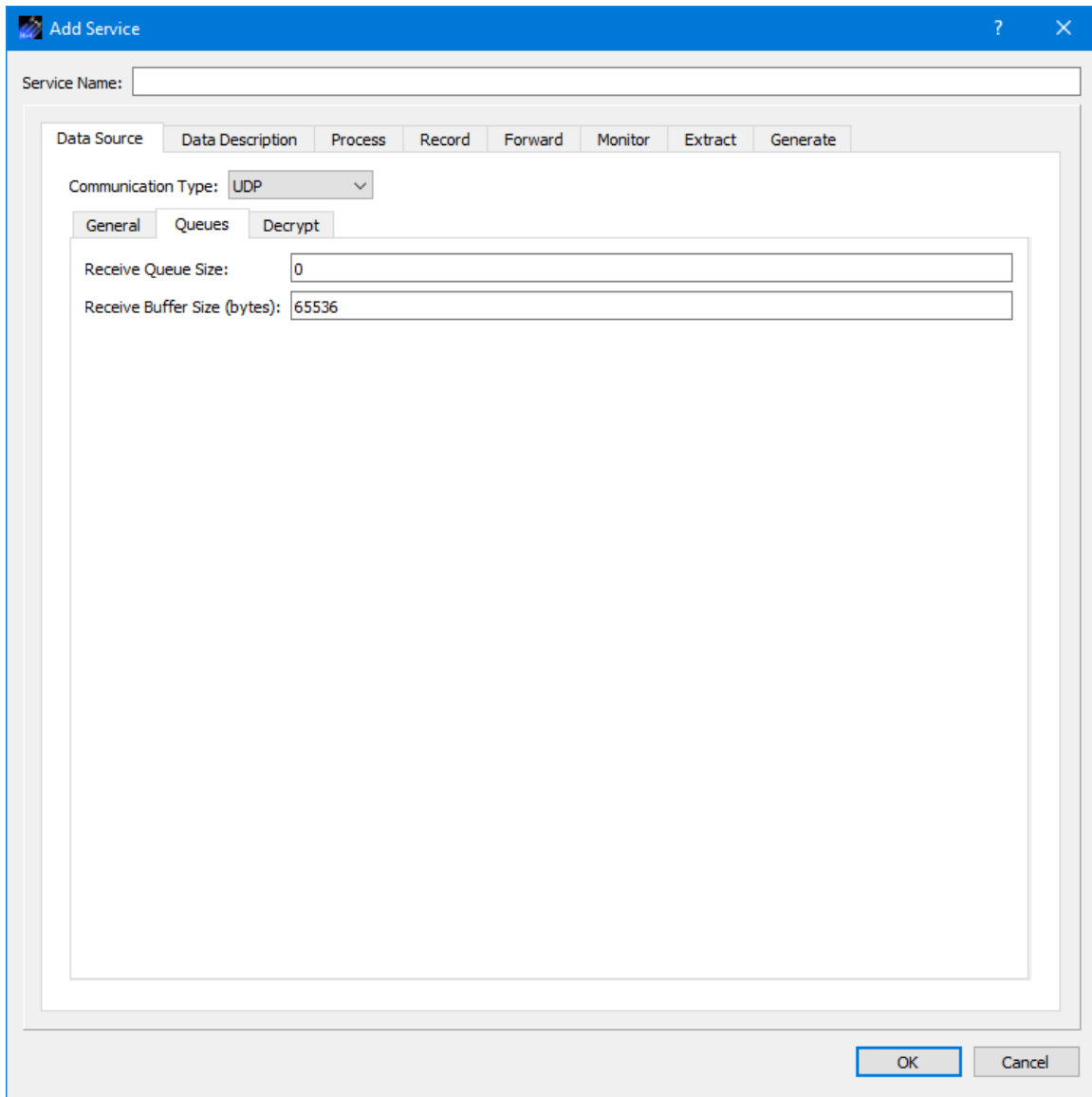
Figure 11 Service Dialog (Data Source Queues Tab)

6.1.1.3   Data Source Decrypt Tab

The Decrypt Tab is shown in Figure 12. If the incoming data is encrypted, information provided on the Decrypt tab can be used to decrypt the data. To decrypt incoming data, the TReK software needs the Peer Public Key for the encrypted data. If all incoming encrypted data being received by the decryption service was encrypted using the same source Public and Private key pair, set the Sender IP Address or Sender Node Number to N/A (the default setting) and identify the absolute path to the one and only Peer Public Key (i.e., the Public key that was used to encrypt all the data). If the incoming encrypted data is being sent from sources with different IP addresses or node numbers, and the encryption sources are using different Public and Private key pairs, the decryption service may decrypt the various encrypted data streams by associating the correct Peer Public Key with the IP address or node number of the source that is sending the encrypted data.

To decrypt incoming data, the Decrypt Incoming Data checkbox should be checked and the Peer Public Key Pathname Information should be populated. The Add button is used to add an entry. The Delete button is used to Delete an entry. The Peer Public Key button is used to browse the local disk for a peer public key file. One or more rows must be selected to use the Delete and Set Peer Public Key buttons.
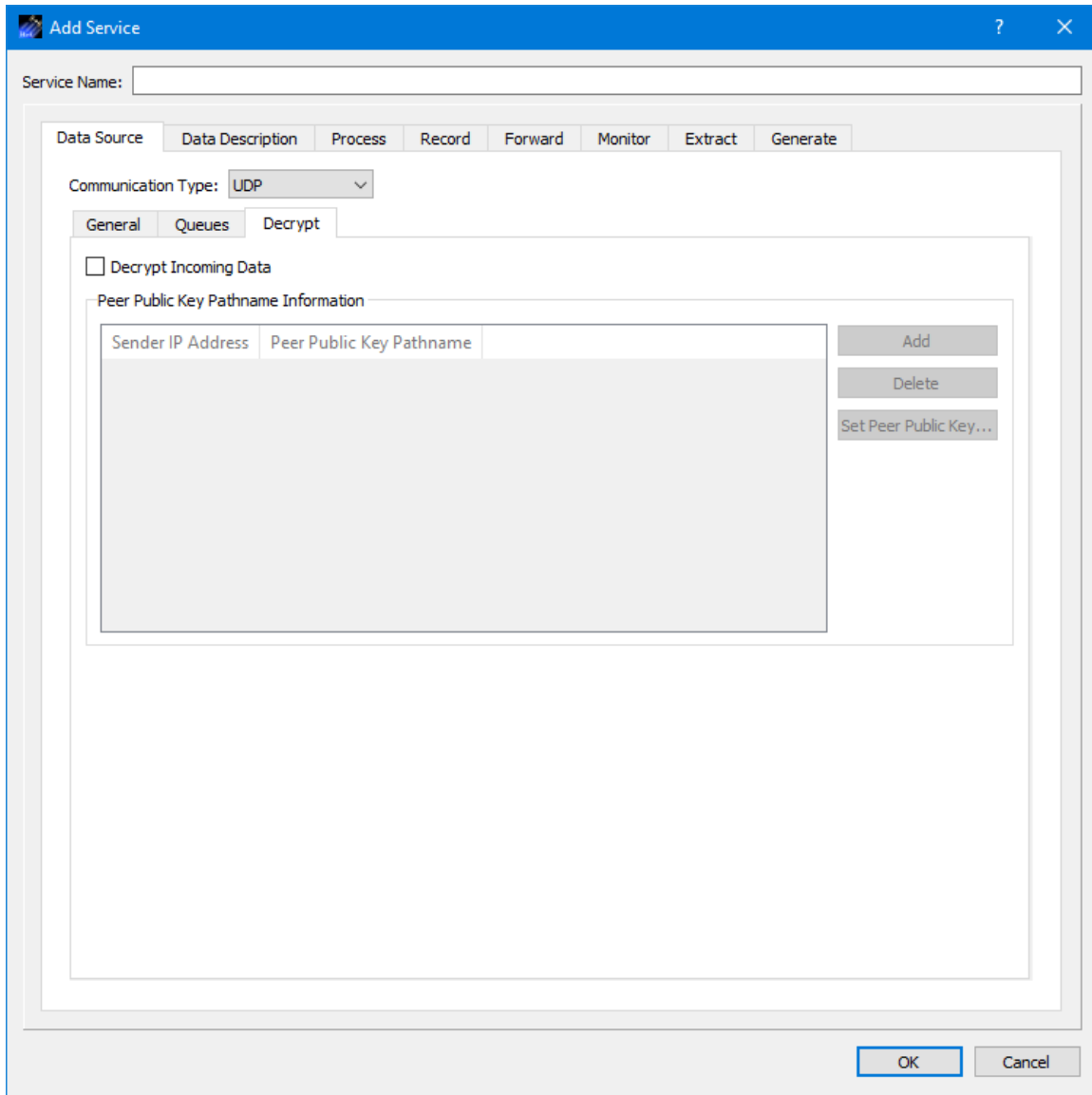
Figure 12 Service Dialog (Data Source Decrypt Tab)

6.1.2   Service Dialog (Data Description Tab)

The Data Description tab is shown in Figure 13. The Data Description tab provides a way to filter incoming data that will be processed, recorded, or forwarded.
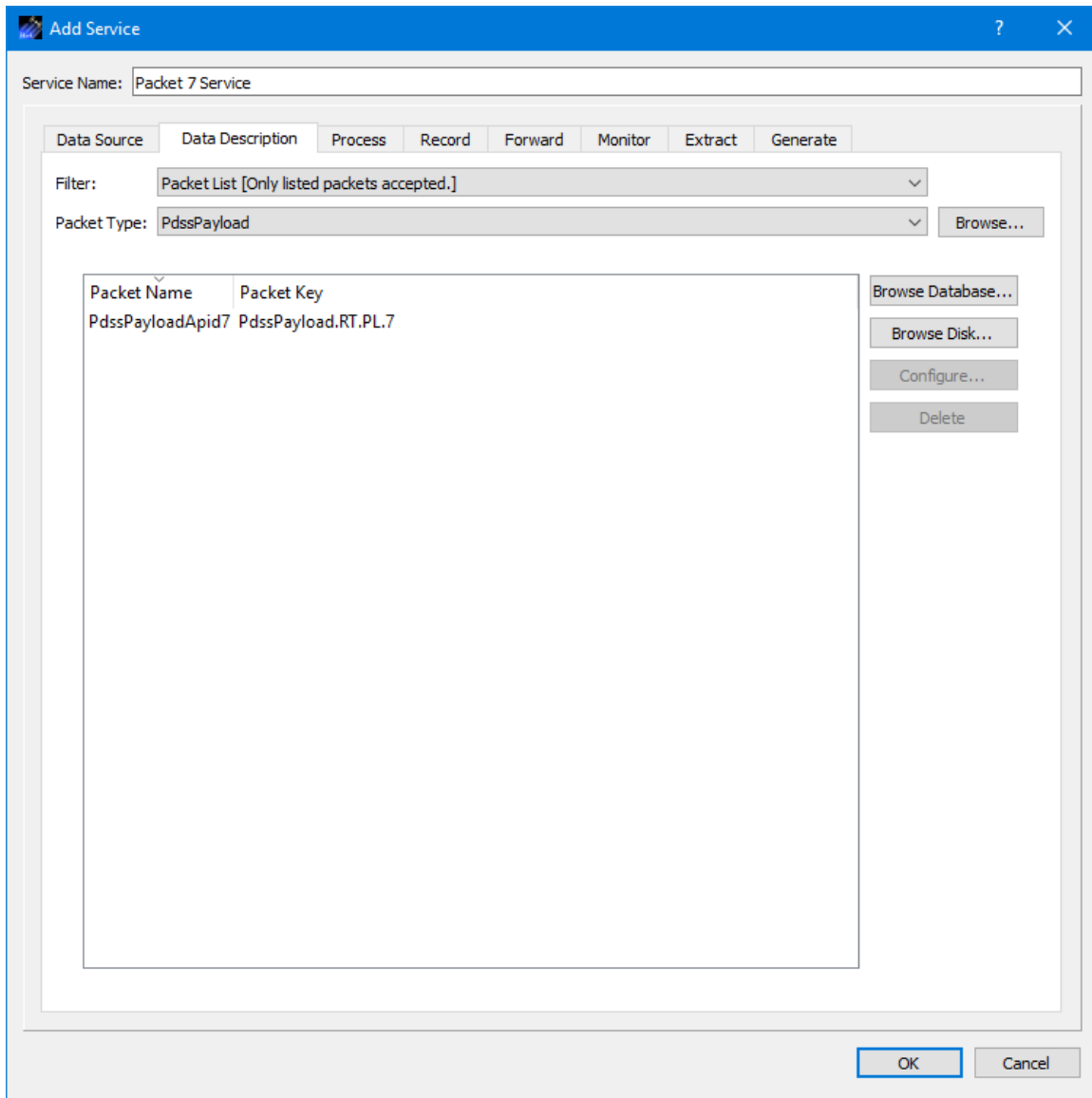
Figure 13 Service Dialog (Data Description Tab)

Filter
The Filter menu contains three choices. Each is described below.

Packet List [Only listed packets accepted]
Packet List provides a way to identify specific packets that should be accepted. Packet information is added to the list by browsing the database or by selecting a metadata definition file stored on the local file system disk.   When a packet is added to the list the Packet Name and Packet Key are displayed. The Packet Key contains the values for each unique identifier defined by the packet type. Some packet types contain packet identifiers that are user selectable. When adding a packet to the list you will be prompted to select a value for any user selectable identifiers if a default value is not provided in the

packet definition. The Configure button can be used to change the value of a user selectable identifier after a packet has been added to the list.   The Delete button can be used to delete a packet from the list. The 'Packet List' option is required if processing is turned on.

Pattern Match Using Packet Type [Only packets that match pattern accepted. Processing Not Available.]
Pattern Match Using Packet Type provides a way to filter incoming packets using the identification fields unique to the packet type. Figure 14 shows the identifiers that can be used to filter incoming PDSS Payload packets.   The Data Mode (EHSP=DataMode) value has been set to '*' (wildcard) to indicate that any data mode value should be accepted (Real-Time, Dump1, Dump2, etc.). The EHS Secondary Protocol Header Type (EHSP=SecHdrType) is a fixed identifier so the value cannot be changed. The APID (CP=APID) is set to '7' to indicate that the APID value must be 7 or the packet should be filtered out. Therefore any PDSS Payload packets with APID 7 will be accepted using this Filter.
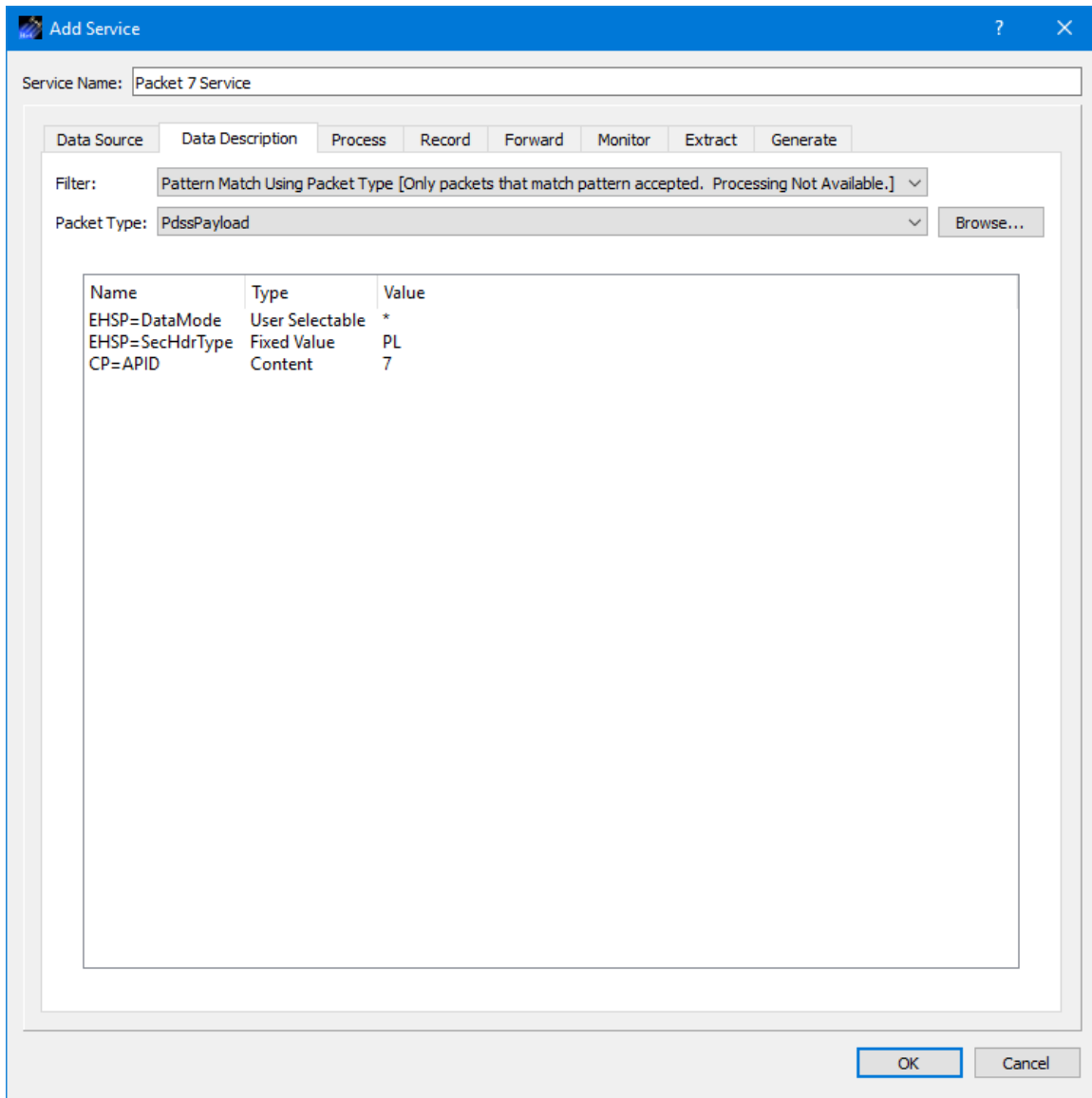
Figure 14 Pattern Match Using Packet Type

None [All arriving data accepted. Processing Not Available]
None indicates no filtering should be used. If the Filter is set to 'None' all data received will be accepted. When 'None' is selected, processing is not available.

Packet Type
The Packet Type menu is used to provide information about the incoming data. Some services like processing require a Packet Type. Other services like recording and forwarding do not require a Packet Type. However, you may decide to select a Packet Type since it can be used to filter incoming data. For example, suppose you had two streams of data arriving on the same network socket. One data stream of packets all had CCSDS headers. The other data stream of packets had no header. Suppose you only wanted to record the packets that had a CCSDS header. In this case you could set the

Packet Type to CCSDS and the Data application would assume the incoming packets are CCSDS packets and would only record the packets if the bits corresponding to APID were a match. [Note: If a non-CCSDS packet arrives the Data application will assume it is a CCSDS packet and attempt to handle it as such.] For more information about Packet Types, please reference the TReK Concepts document.

Encrypted Data
When the Filter Type is set to None, the Packet Type options are None and Encrypted. If you will be receiving encrypted data, and you do not want to decrypt the data, set the Filter Type to None and the Packet Type to Encrypted. The incoming encrypted data can be recorded or forwarded. If you will be receiving encrypted data and choose to decrypt the data, select the type of Filtering you would like to apply and the packet type that describes the decrypted data. The Packet Type should not be set to Encrypted since the data will be decrypted.

6.1.3   Service Dialog (Process Tab)

The Service Dialog Process tab is shown in Figure 15. The Process tab is used to configure the service to process incoming data and identify the packets that should be processed.
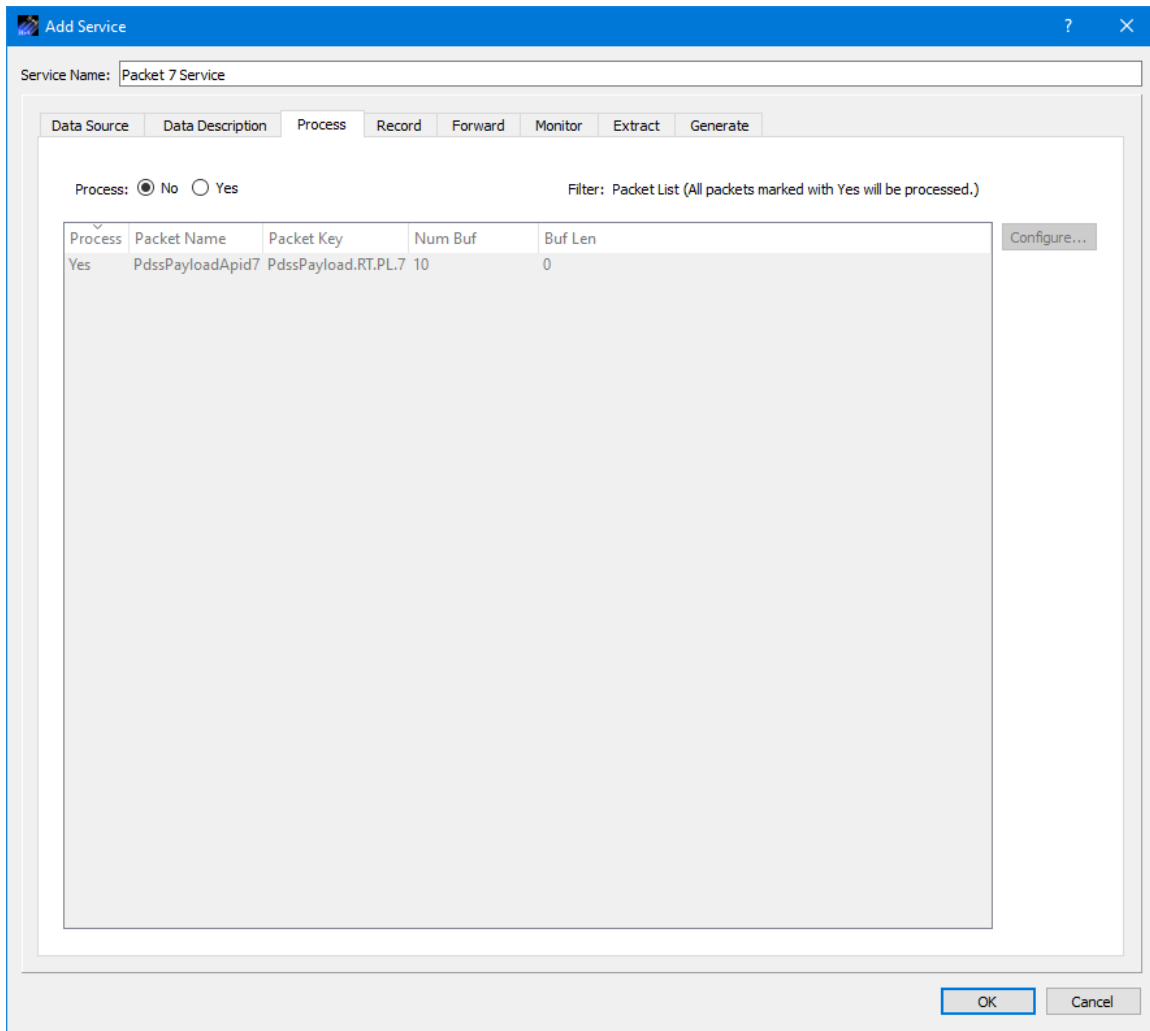
Figure 15 Service Dialog (Processing Tab)

Each field is described below.

Process Radio Buttons
The No and Yes radio buttons disable or enable Processing.

Packet List
If processing is turned on, the packet list is used to identify the list of incoming packets that should be processed.   The packets displayed in the Packet List are the ones that were entered on the Data Description tab. You may configure the service to receive multiple packets and use this list to limit the packets that are processed. The Process column Yes or No value indicates whether the packet should be processed. The Configure button is used to configure one or more properties associated with processing the packet. Multiple packets can be selected and modified at the same time. The 'Num Buf' column identifies the number of buffers to use for arriving packets and the 'Buf Len' column identifies the length of the buffers. These properties can be configured using the Configure dialog accessed by the Configure button.

Configure

The Configure button is used to modify processing properties associated with the packets selected. This includes whether the packet should be processed, the Number of Buffers, and the Buffer Length.   A value of 0 for the Buffer Length indicates the length should be calculated using information in the packet definition.
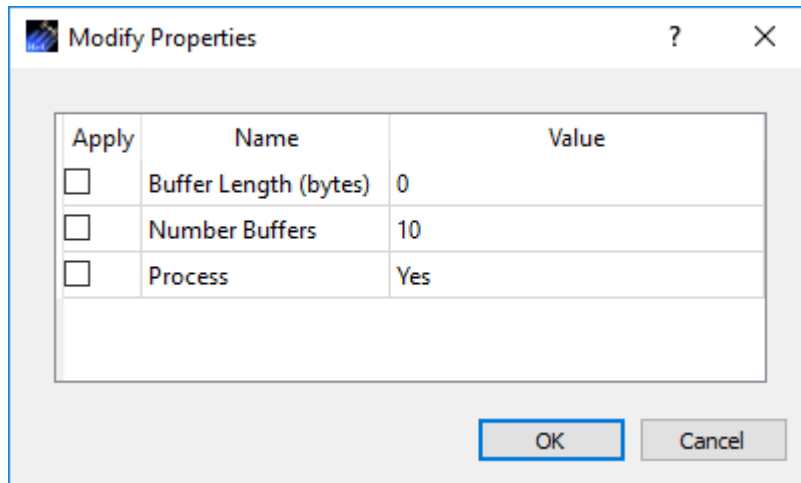
Figure 16 Service Dialog Processing Tab Modify Properties Dialog

6.1.4   Service Dialog (Record Tab)

The Service Dialog Record tab is shown in Figure 17. The Record tab is used to configure the service to record incoming data and other properties associated with recording.
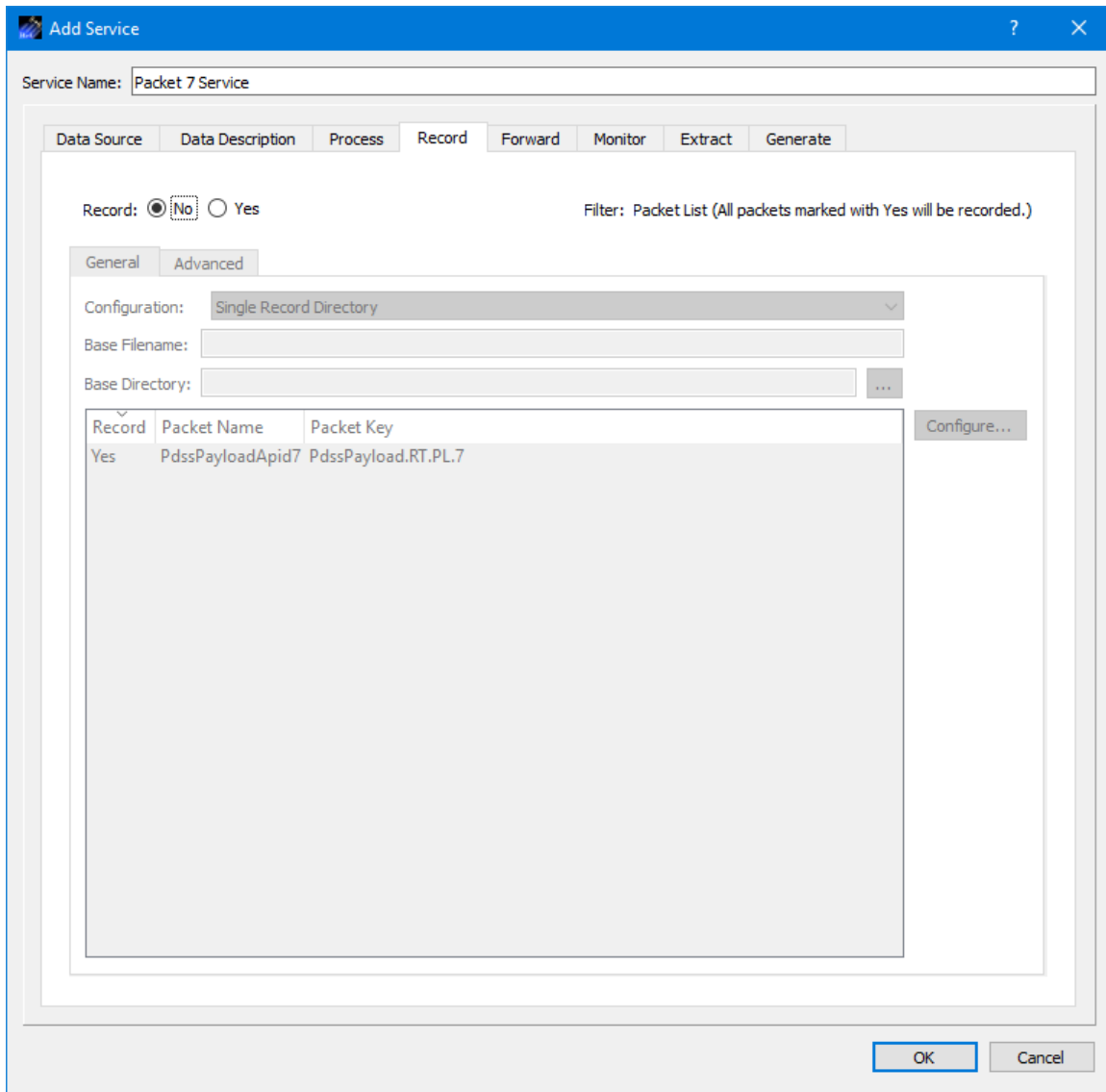
Figure 17 Service Dialog (Record Tab)

6.1.4.1 Record Tab (General Tab)

The Record Tab General Tab is shown in Figure 18. It is used to enter general recording information. The Filter selection will determine which packets are recorded. The packets displayed in the Packet List are the ones that were entered on the Data Description tab. You may configure the service to receive multiple packets and use this list to limit the packets that are recorded. The Record column Yes or No value indicates whether the packet should be recorded. The Configure button is used to configure the Yes or No property. Multiple packets can be selected and modified at the same time.
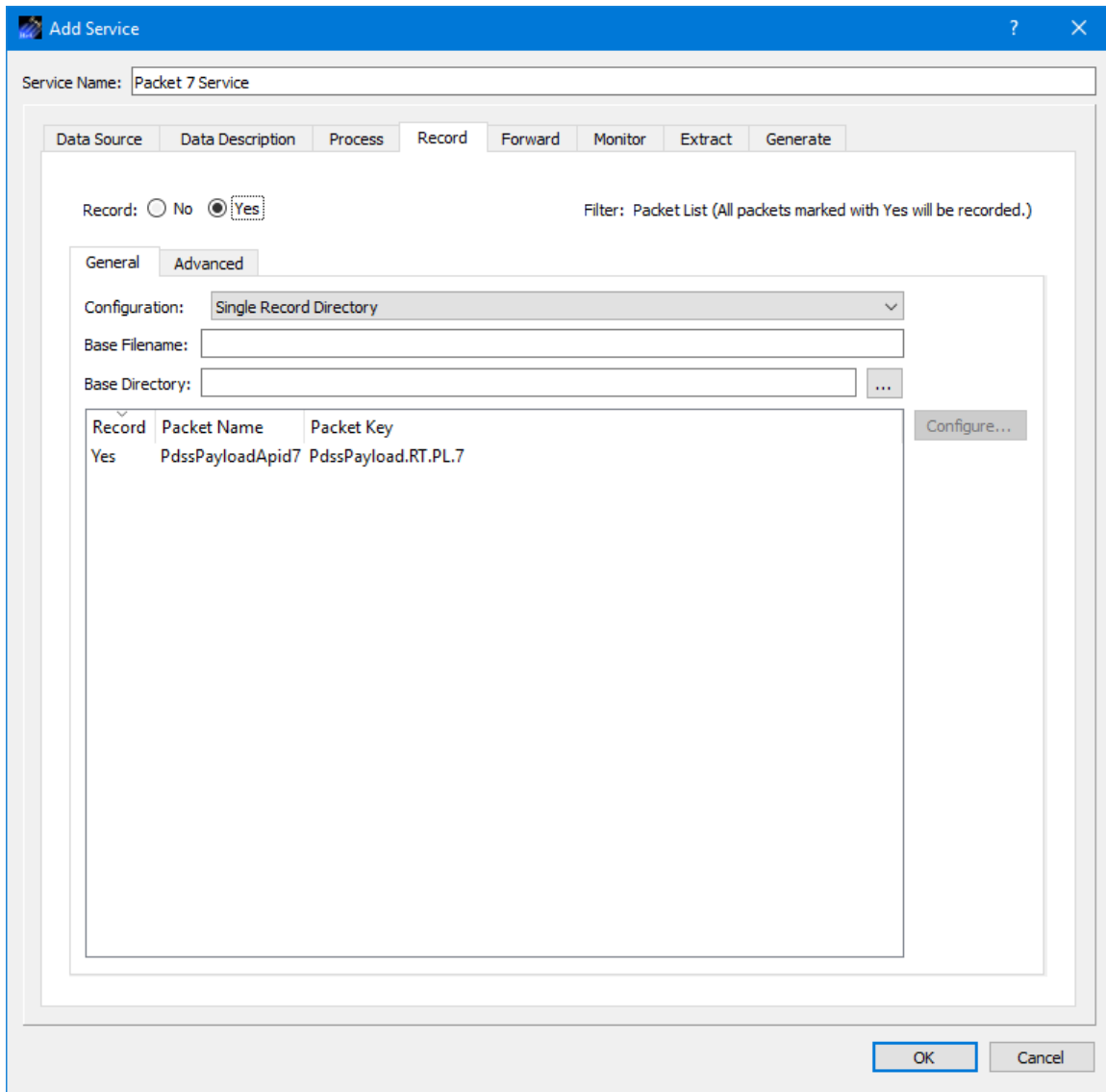
Figure 18 Service Dialog Record Tab (General Tab)

Each field is described below.

Record
The No and Yes radio buttons disable or enable data recording. The Filter setting determines which packets are recorded. If the Filter is set to Packet List, the Record column determines which packets will be recorded.

Configuration
The recording configuration identifies the configuration to use when recording the incoming data. The Configuration option menu contains three choices. Each is described below.

Single Record Directory

The Single Record Directory option will record all the data into a single directory. The configuration for this option is shown in Figure 18. This configuration requires an entry for Base Filename and Base Directory.

Base Filename

Single Record Directory requires a Base Filename.   When a packet is recorded, the raw packet data is stored in one or more files in a local directory. A base filename (provided by you) is used for part of the filename and the rest of the filename is generated by the TReK software. The complete filename indicates the time the file was created or the embedded time of the first packet in the file if an embedded time field was identified in the packet definition. You may also choose to create a complete filename the includes both the open and close time of the file or the embedded time of the first and last packet in the file if an embedded time field was identified in the packet definition. When you want to play the data back, you will be asked to provide this Base Filename.

Base Directory

Single Record Directory requires a Base Directory.   The Directory information is used to identify which directory should be used for the recorded data files. When you want to play the data back, you will be asked to provide this Directory information so the TReK Playback application can find the files. This field requires a complete directory path. An example of this is C:\Users\<username>\trek_workspace\recorded_data\. If you don't like to type or you need help defining the complete path, you can push the … (dot dot dot) button located to the right of the Directory field. This will bring up a Browse dialog you can use to select the local directory where you want to store the recorded data files.

Multiple Record Directories Auto-Generated Based on Incoming Data

The Multiple Record Directories Auto-Generated Based on Incoming Data option will record data into multiple sub-directories based on the packet key. Figure 19 shows the configuration of this option. A Base Directory is required.
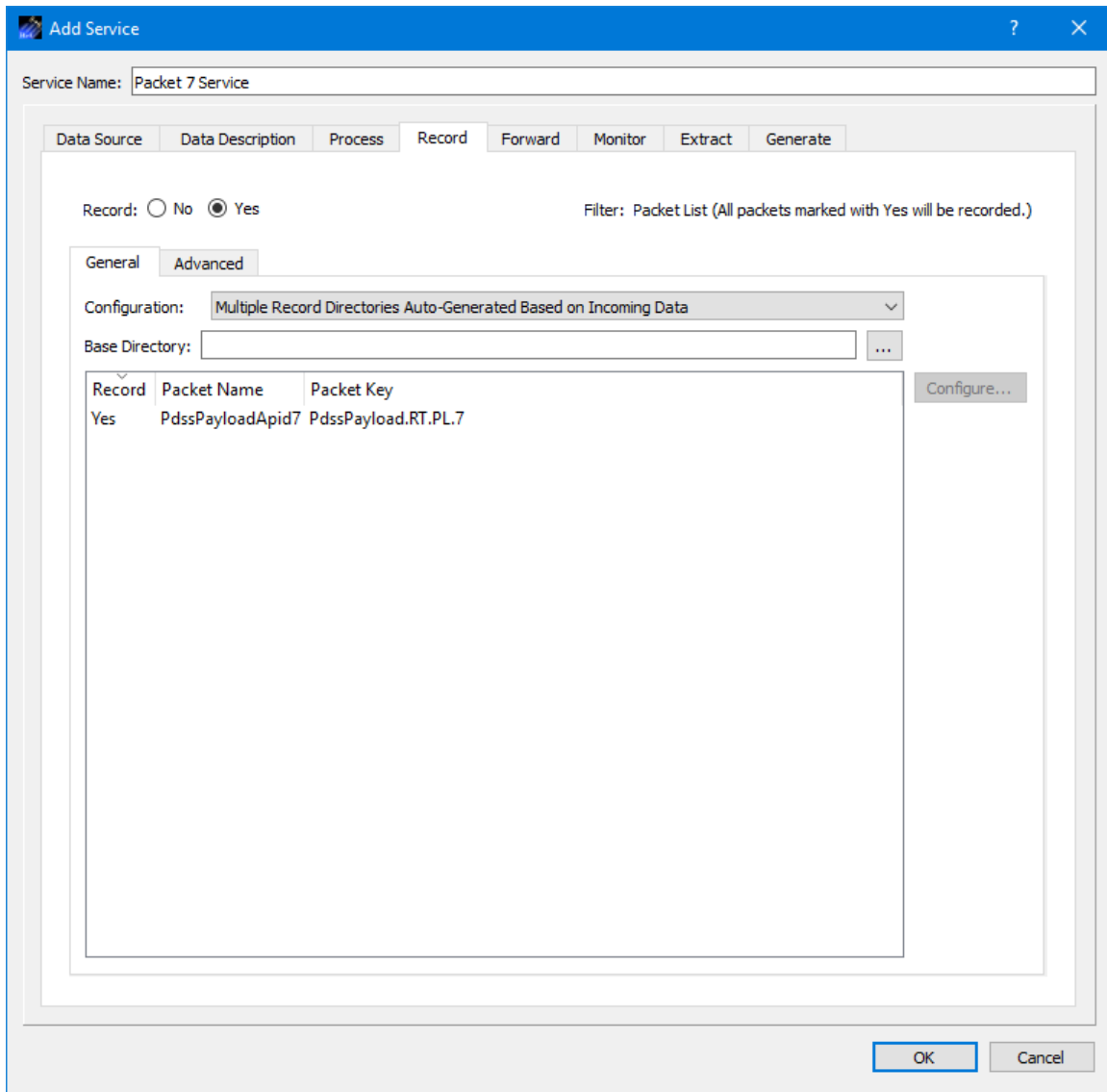
Figure 19 Multiple Record Directories Auto-Generated on Incoming Data

Base Directory

The Base Directory is used to identify the top level directory for the recorded data files that will be stored in subdirectories according to packet type. Figure 20 shows an example of Auto-Generated subfolders.

28

Figure 20 Auto-Generated Folders for Recorded Data Files

User Specified Record Directories and Base Filenames

The User Specified Record Directories and Base Filenames option provide a way to enter a user specified directory and base filename for each individual packet in the list. The Filter option must be set to 'Packet List' to use this option. Figure 21 shows the configuration for this option. The Configure dialog is used to enter a Base Filename and Base Directory for each packet in the list.
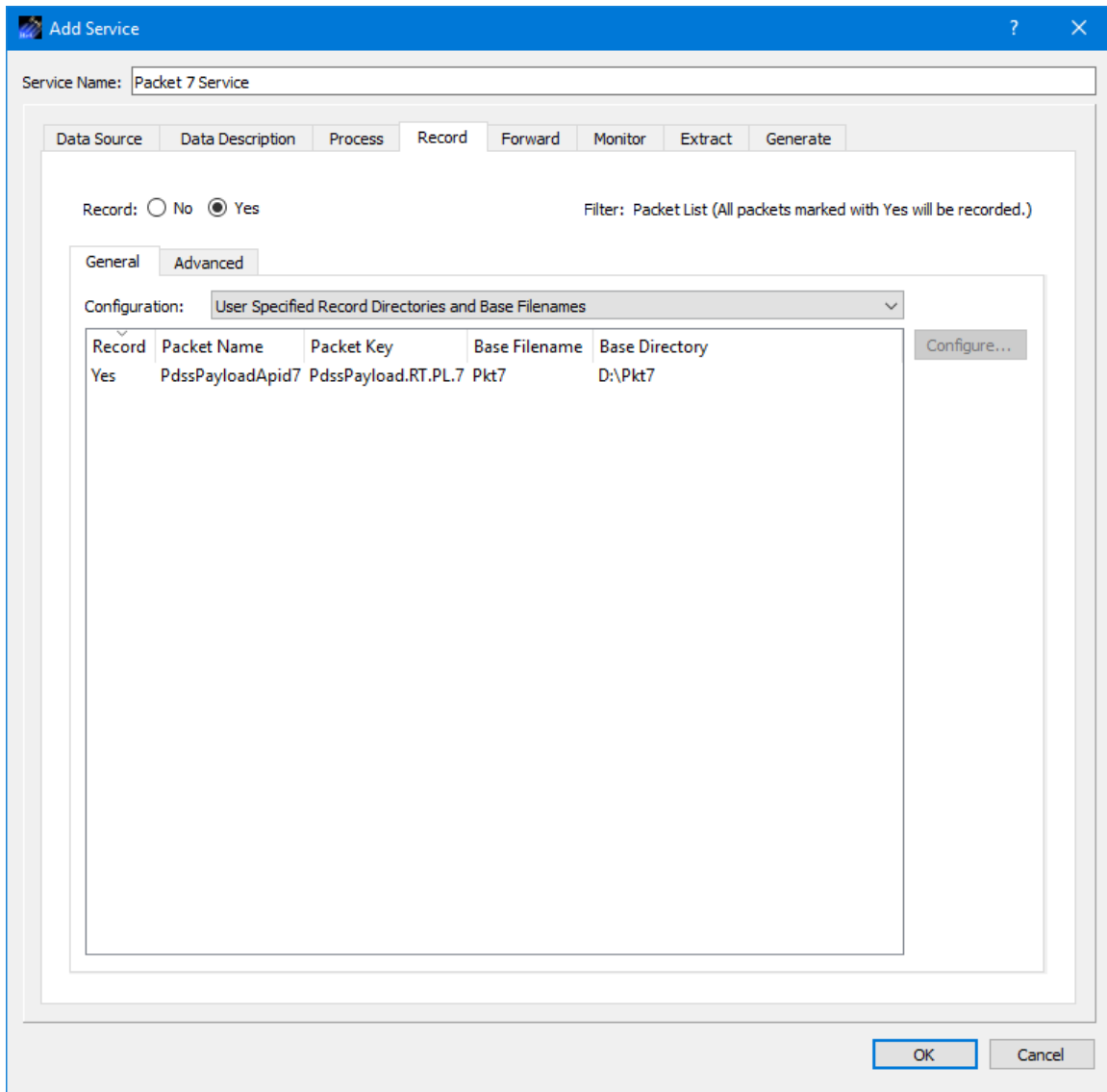
Figure 21 User Specified Record Directories and Base Filenames

6.1.4.2   Record Tab (Advanced Tab)
The Record Tab Advanced Tab is shown in Figure 22. It is used to enter advanced recording information.
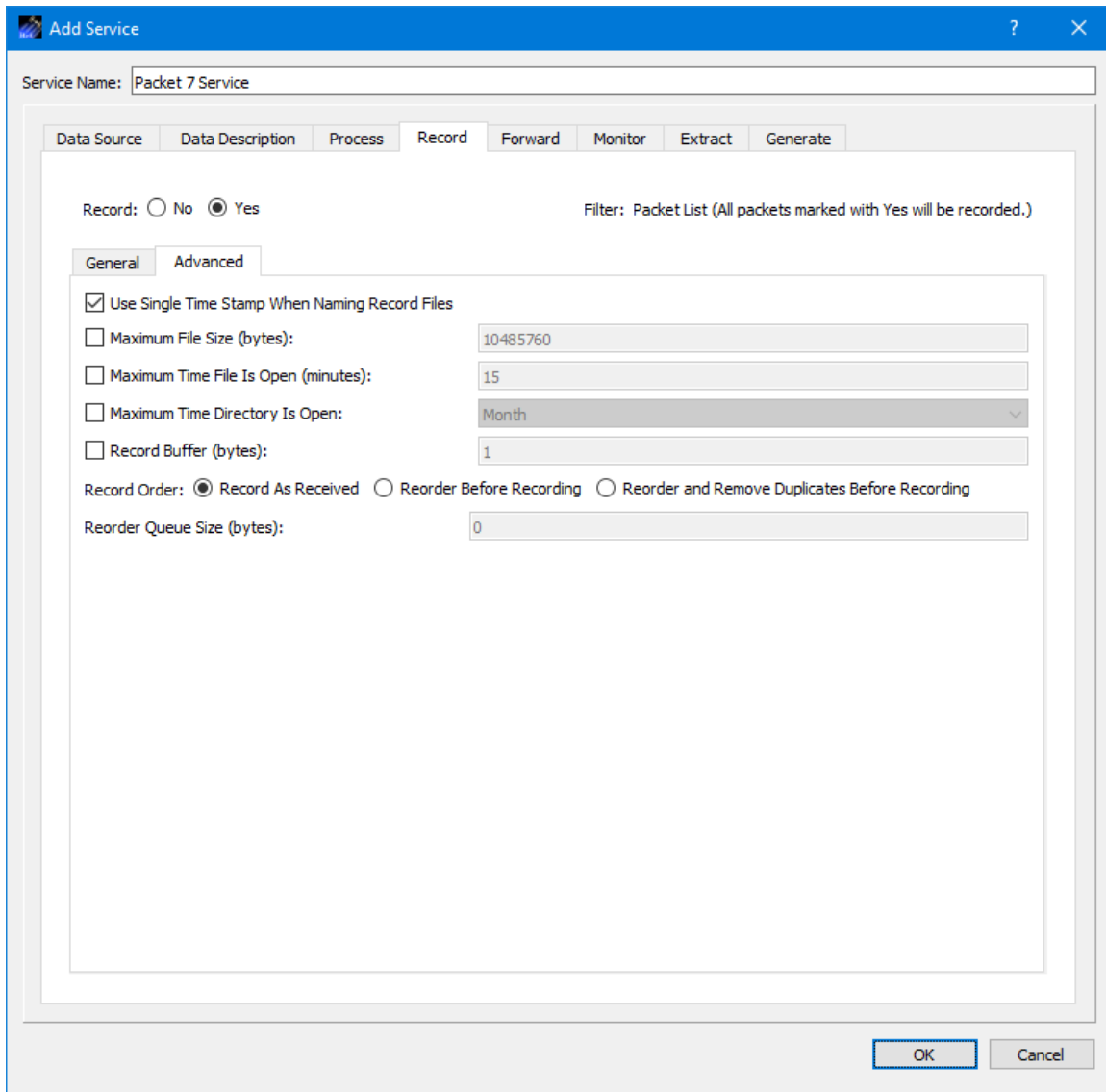
Figure 22 Service Dialog Record Tab (Advanced Tab)

Each field is described below.

Use Single Time Stamp When Naming Record Files
If this is checked, the recorded data files will use a single time stamp when adding timestamp information to the filename. If this is not checked, the recorded data files will contain start time and a stop time when timestamp information is added to the filename.

Maximum File Size
The Maximum File Size information is used to determine when to close a recorded data file. A new record file is opened immediately after the current record file is closed.

Maximum Time File Is Open

The Maximum Time File Is Open Checkbox is used to indicate whether the file should be closed based on a maximum time. The Maximum Time File Is Open property is used in addition to the Maximum File Size property. If the maximum file size is reached before the maximum time, the file will be closed based on maximum file size. However, if the maximum time is reached before the maximum size is reached, the file will be closed based on the maximum time. The file open timer starts when the record file is created. A new record file is opened immediately after the current record file is closed. A record file will not be closed based on maximum time if no packets have been recorded in the file.

Maximum Time Directory Is Open

The Maximum Time Directory Is Open Checkbox is used to indicate whether recording files should be placed in sub-directories within the parent base directory. The directories will be open/closed based on Day, Calendar Week, Calendar Month, or Year. A new record file is opened immediately after the current record file is closed.

Record Buffer

A Record Buffer may be used to buffer multiple packets up to the record buffer size in bytes prior to making a write call to the record file. Zero implies every packet has an associated write call to the record file. A record buffer may be used to improve the performance of the record library.

Record Order

There are three options for Record Order. Each is described below:

*Record as Receive*d

Record as Received will record packets in the order they are received.

Reorder Before Recording

Reorder Before Recording will reorder packets in time order using the embedded time stamp in the individual packets. The reorder queue must be sized to hold the maximum sequence of out of order packets or the packets will not be recorded correctly. For example, packets arriving in the order A,B,C,D,M,N,O,E,F,G,H,I,J,K,L,P,Q,R would require a reorder queue size of four to record the proper packet sequence of A,B,C,D,E,F,G,H,I,J,L,K,M,N,O,P,Q,R.

Reorder and Remove Duplicates Before Recording

Reorder and Remove Duplicates Before Recording will reorder packets in time order using the embedded time stamp in the individual packets. Duplicate packets will not be recorded. Duplicate packets are identified using the packet's embedded time and sequence count. The reorder queue must be sized to hold the maximum sequence of out of order packets or duplicate packets or the packets will not be recorded correctly. For example, packets arriving in the order A,B,C,D,M,E,F,G,H,I,J,K,L,M,N,O,P,Q,R would require a reorder queue size of two to record the proper packet sequence of A,B,C,D,E,F,G,H,I,J,L,K,M,N,O,P,Q,R.

Reorder Queue Size
The Reorder Queue Size is the queue size used to reorder the packets. It should be set to a value greater than or equal to the expected maximum sequence error of the received packets. If the queue size is smaller than the maximum sequence error, packets may not be reordered in the proper sequence. If the reorder queue size is set to zero, the record library will set the reorder queue size to twice or double the recorded packet's maximum sequence error assuming a sequence count field is defined in the packet's header.

6.1.5   Service Dialog (Forward Tab)

The Service Dialog Forward tab is shown in Figure 23. The Forward tab is used to configure the service to forward incoming data. The Filter Type will determine which packets will be forwarded. If the Filter is set to Packet List, the Packet List will further determine whether a packet is forwarded.
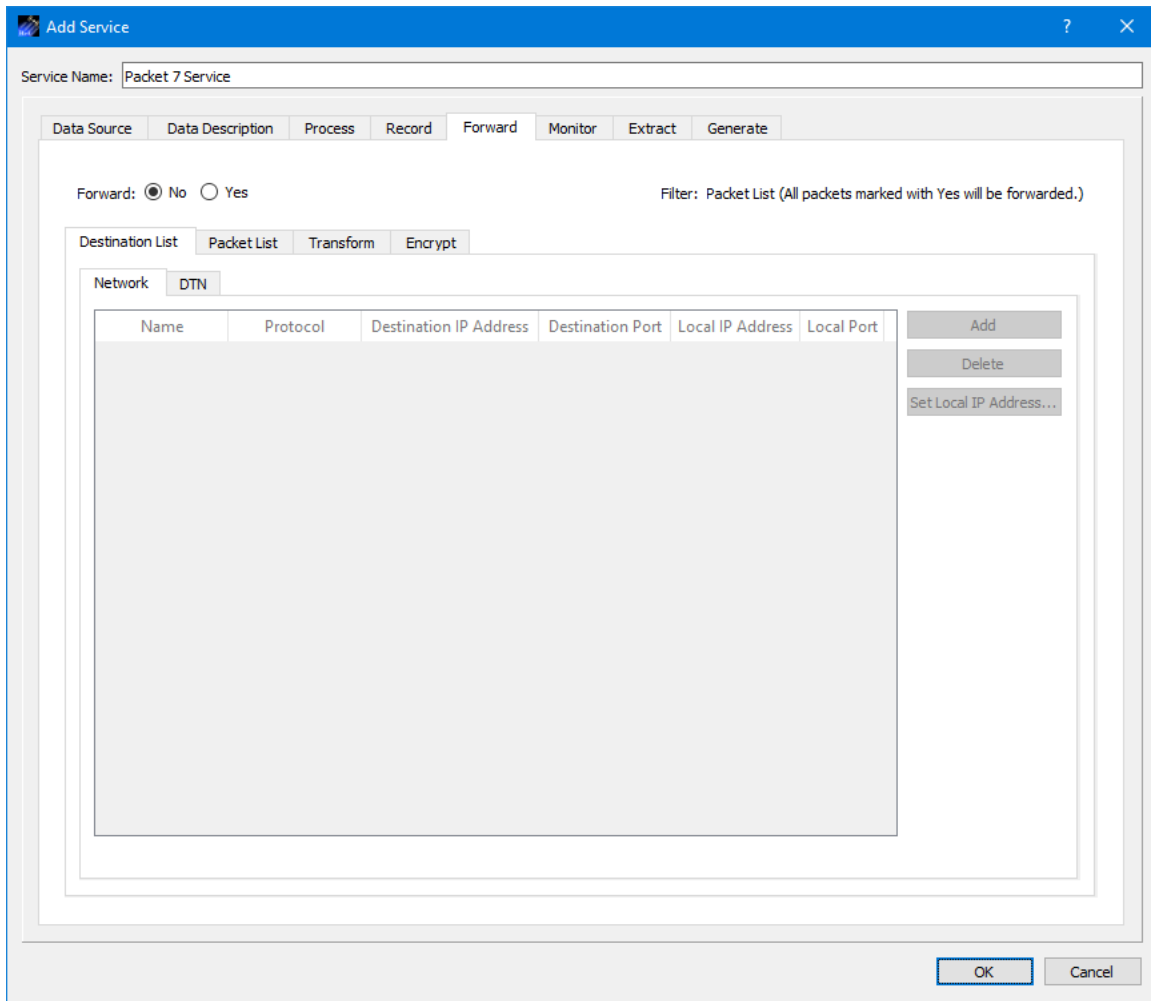
Figure 23 Service Dialog (Forward Tab)

Each field is described below.

Forward
The No and Yes radio buttons disable or enable data forwarding of incoming packets described in the service. The Filter Type setting determines which packets are forwarded.

Destination List
The destination list is used to identify the list of destinations to which the data should be forwarded. Data can be forwarded to a network destination or a Delay Tolerant Network (DTN) destination.

A network destination example is shown in Figure 24. For a network destination, each destination must include a user defined name that is unique in this destination list, a Protocol, and the applicable settings required for the protocol selected. The Protocols supported are UDP and TCP. The Protocol menu provides the capability to select the type of socket to use when forwarding the data: UDP, TCP Client, or TCP Listener socket. Figure 24 shows three different destinations in the Destination List.   When using a TCP Listener socket it is not necessary to define a Destination IP Address or a Destination Port. When the Local Port is set to 0, the operating system will automatically select a port to use for the socket that is created to send data to the destination. This is the default as it saves you the trouble of keeping up with ports. However, you can enter a specific port if you would like. This is advisable if you are using a TCP Listener socket since another party will be connecting to the socket. The Add and Delete buttons are used to add a row to the list and delete a row from the list respectively. The Set Local IP Address button can be used to browse for a local IP address and set the value in selected Local IP Address cells.

A DTN destination example is shown in Figure 25. For a DTN destination, each destination must include a destination node number, and a destination service number. General properties that must be input for all DTN destinations include Source Service Number, Lifespan, Bundle Protocol Class of Service, Expedited Priority Ordinal, Transmission Mode, and Criticality. Descriptions of these properties can be found in the Data Source General Tab section above.

Note: Regardless of whether the Forward selection is set to Yes or No, only valid destination information will be saved in the service. If Forward is set to No, any invalid destination information will be removed when you click OK.
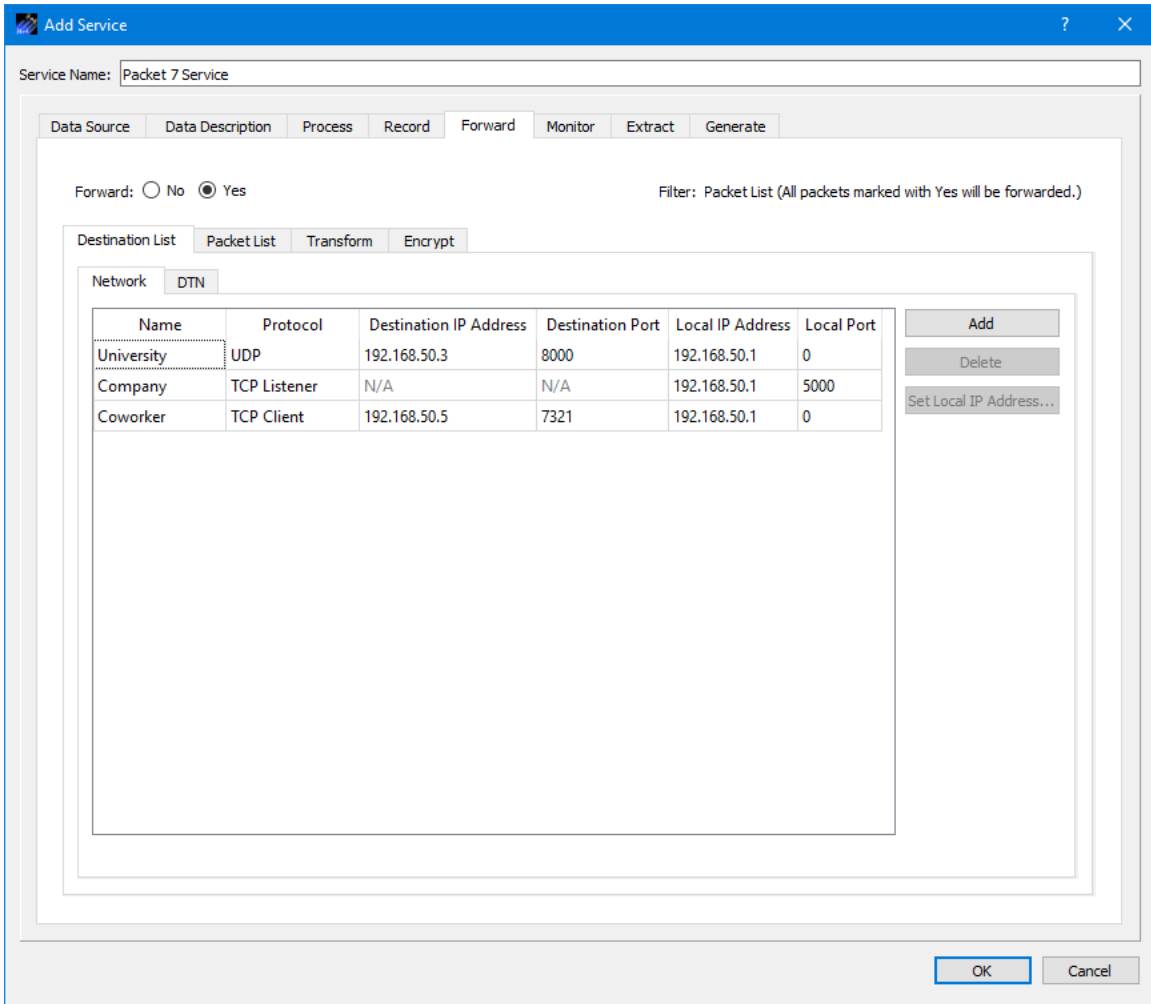
Figure 24 Forward Network Destination List
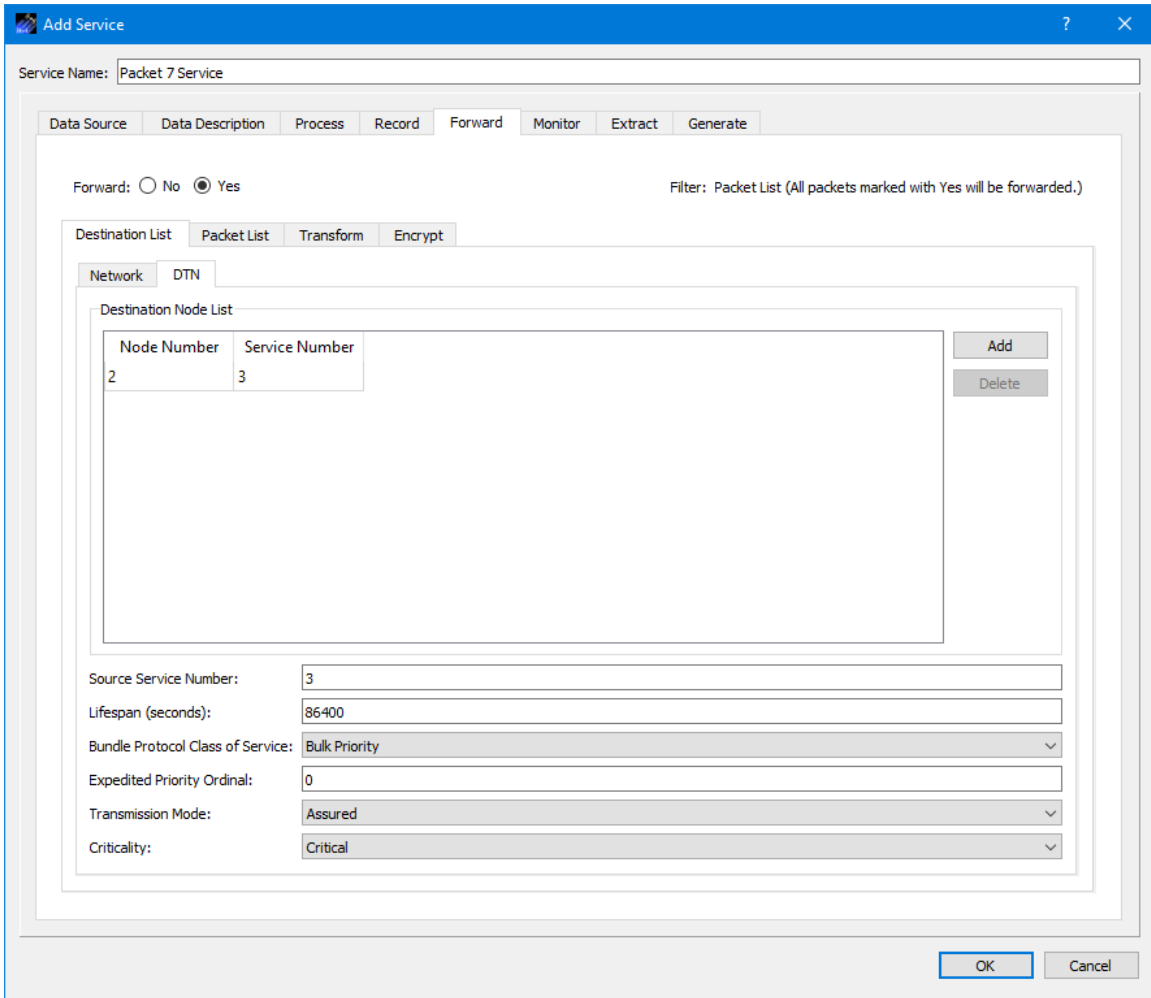
Figure 25 Forward DTN Destination List

The Packet List tab is shown in Figure 26.
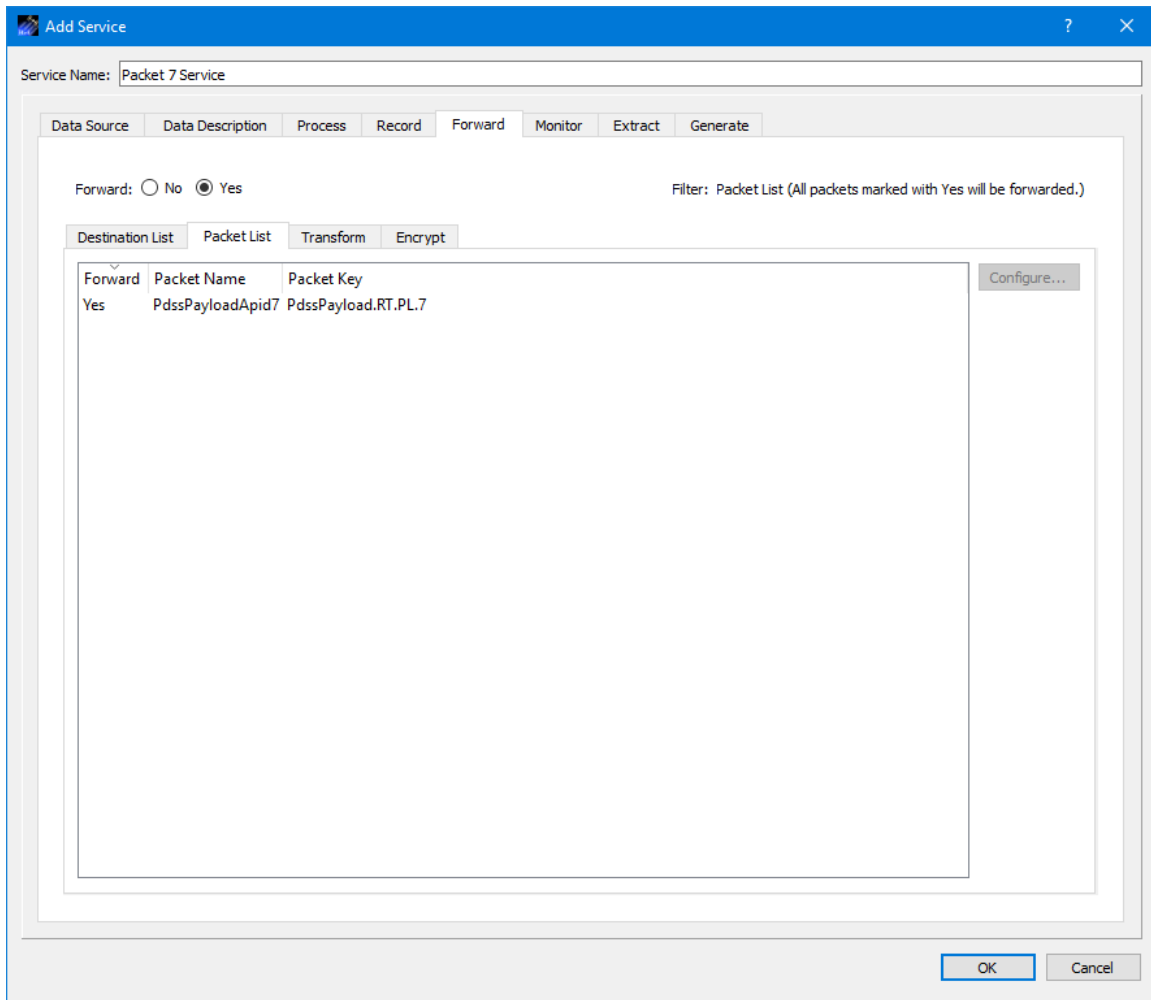
Figure 26 Service Dialog Forward Tab Packet List

The packets displayed in the Packet List are the ones that were entered on the Data Description tab. You may configure the service to receive multiple packets and use this list to limit the packets that are forwarded. The Forward column Yes or No value indicates whether the packet should be forwarded. The Configure button is used to configure the Yes or No property. Multiple packets can be selected and modified at the same time.

The Transform tab is shown in Figure 27. The Transform tab provides the capability to enable the transform feature which can be used to remove a specific number of bytes from the beginning of each packet before the packet is forwarded.
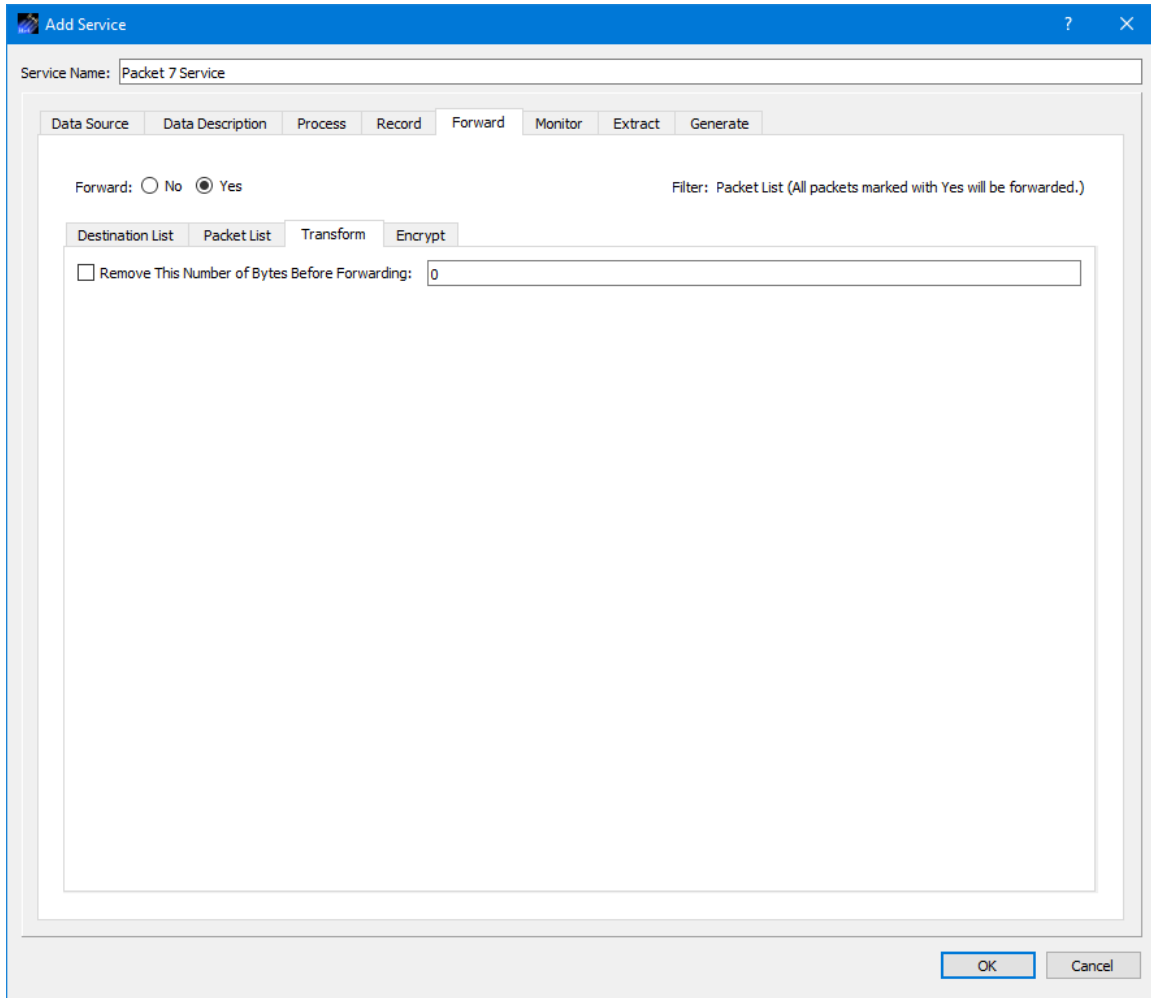
Figure 27 Service Dialog Forward Tab Transform

The Encrypt tab is shown in Figure 28.   The Encrypt tab provides the capability to encrypt data sent to a destination. Encryption is controlled per destination.
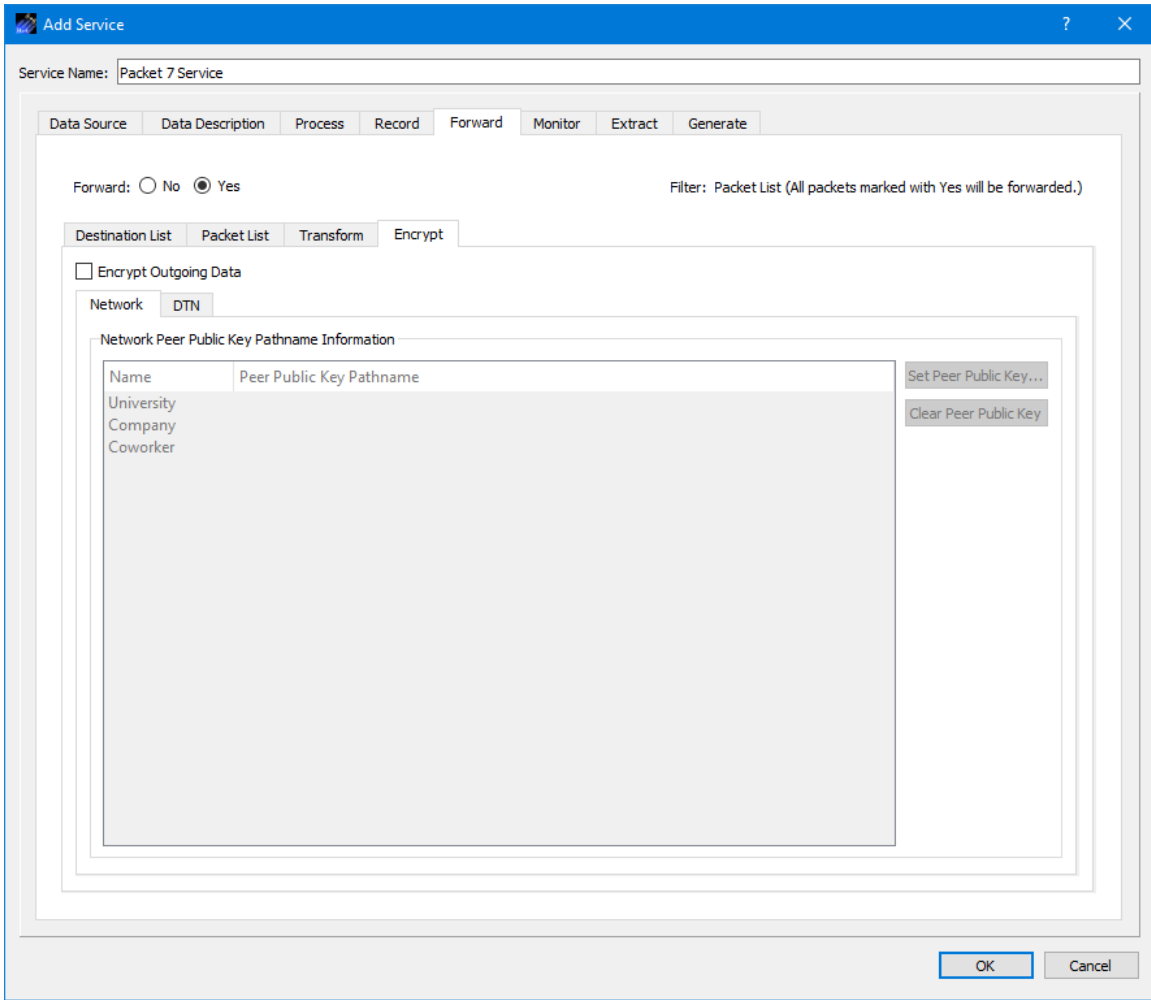
Figure 28 Service Dialog Forward Tab Encrypt Network Destination
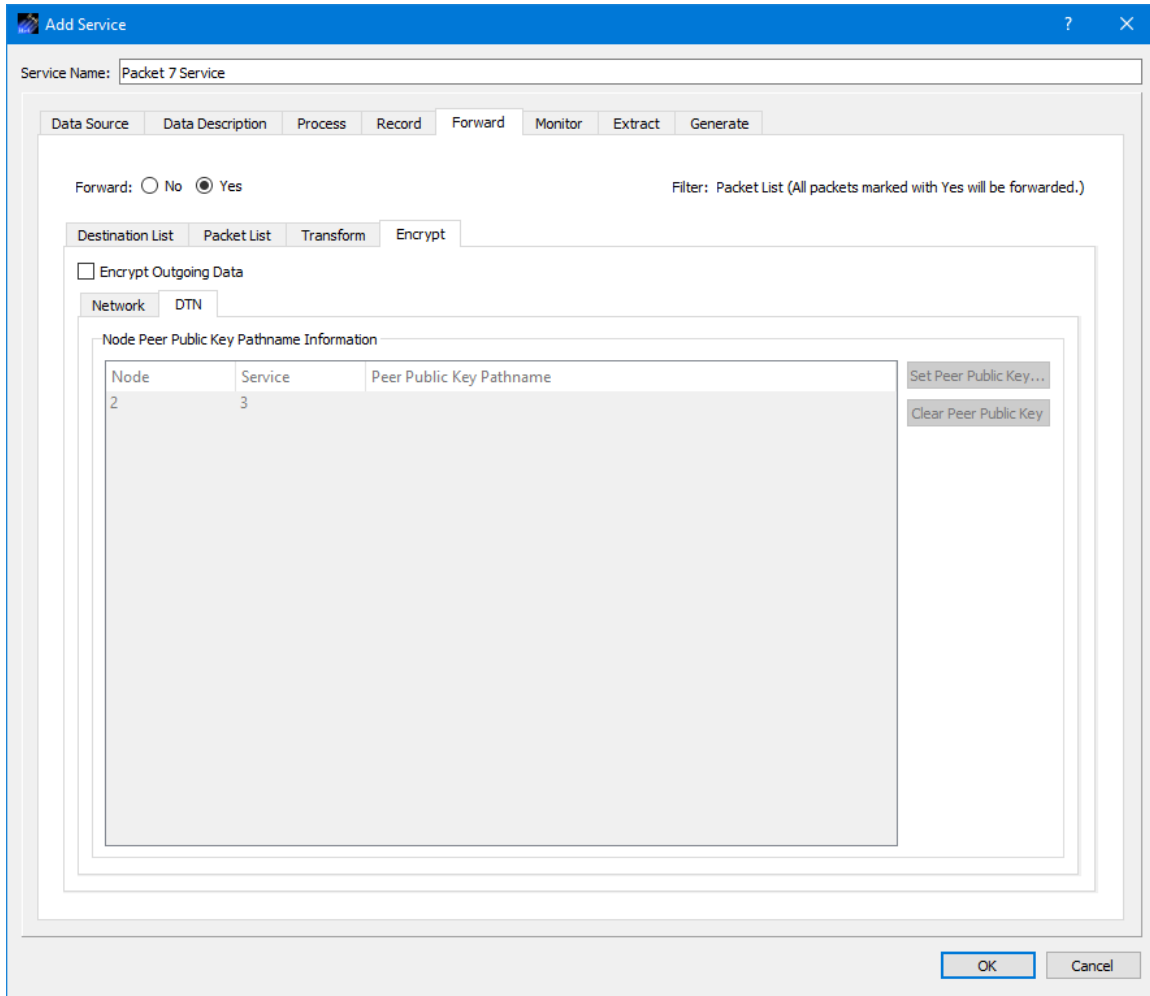
Figure 29 Service Dialog Forward Tab Encrypt DTN Destination

The Peer Public Key Information is populated using the Destination List. To encrypt data going to a specific destination, check the Encrypt Outgoing Data checkbox, and identify the absolute path to the Peer Public Key associated with that destination. The Set Peer Public Key button is used to browse the local disk for a peer public key file. The Clear Peer Public Key button is used to clear a peer public key pathname. One or more rows must be selected to use the Set Peer Public Key and Clear Peer Public Key buttons.

6.1.6 Service Dialog (Monitor Tab)

The Service Dialog Monitor tab is shown in Figure 30. The Monitor tab is used to configure the service to monitor incoming data for out of limit or expected state conditions. A parameter can be monitored if it is in one of the packets identified on the Data Description tab, the packet is configured to be processed on the Process tab, and an Alarm has been assigned to the parameter. An alarm can be assigned to a parameter by modifying the packet definition using the Metadata application. The Metadata application can be used to create, assign or modify an Alarm. If a parameter value

triggers an out of limit or expected state condition, a monitoring message will be generated. A message is also generated for parameter values that return to the normal state (e.g., no longer out of limit). Monitoring messages are displayed in the Manage Monitoring dialog. You can also choose to generate an e-mail, e-mail and text, or text alert. The frequency setting applies to monitoring messages and alerts. The frequency monitoring messages and alerts are generated can be controlled using the tolerance setting.
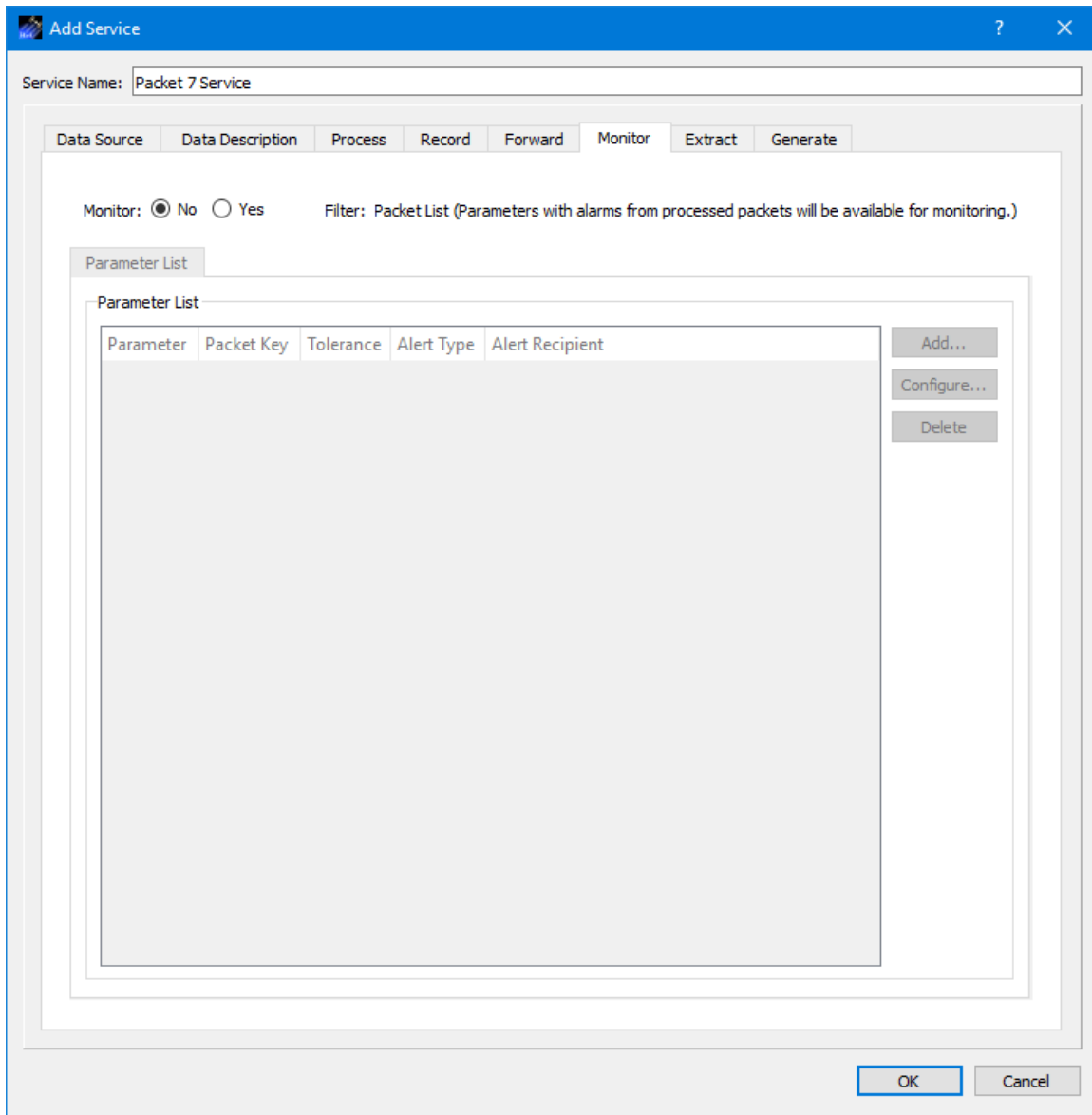
Figure 30 Service Dialog Monitor Tab

Each field is described below.

<u>Monitor</u>
The No and Yes radio buttons disable or enable monitoring of parameters.

Parameter List Tab
The Parameter list provides a way to identify the parameters to be monitored.

Add
The Add button provides a way to add parameters to the list. Once you add metadata information for a packet on the Data Description tab, you can configure monitoring. However, remember that monitoring requires processing, so be sure the parameter's packet will be processed. Parameters that appear in the Add Parameter dialog list come from packets identified on the Data Description tab that have an alarm assigned. If none of the packets on the Data Description tab contain any parameters with an assigned Alarm, the list in the Add Parameter dialog will be empty. When you add a parameter it will be added with default values for each of the columns. You can use the Configure dialog to change a parameter's monitoring configuration.

Configure
The Configure button is available when you select a parameter. Pushing the Configure button will display the Configure Monitor Parameter dialog shown in Figure 31. This dialog provides the capability to set monitoring properties associated with the parameter selected. Tolerance provides the capability to control how often monitoring messages and alerts are generated. The tolerance number indicates how many times the parameter value can go out of limits or expected state contiguously before it triggers a message or alert. When the parameter goes back into a nominal state the tolerance count starts over. The Alert checkbox provides the capability to add an e-mail, e-mail and text, or text alert. To use the E-Mail and Text options, you must enter E-Mail and Text information using the Manage E-Mail and Text Settings dialog available from the Options menu. The Recipient list will be populated based on the Type selected and the information entered in the Manage E-Mail and Text Settings dialog. The recipient identifies who should be notified when the alarm is triggered. If you select E-Mail in the Type menu, the Recipient list will be populated with e-mails from the E-Mail List tab and groups that contain at least one e-mail address from the Group List tab. If you select E-Mail and Text in the Type menu, the Recipient list will be populated with groups from the Group List tab that contain at least one e-mail address and one cell phone number. If you select Text in the Type menu, the Recipient list will be populated with cell phone numbers from the Cell List tab and groups that contain at least one cell phone number from the Group List tab. For additional information, please reference the Manage E-Mail and Text Settings dialog.
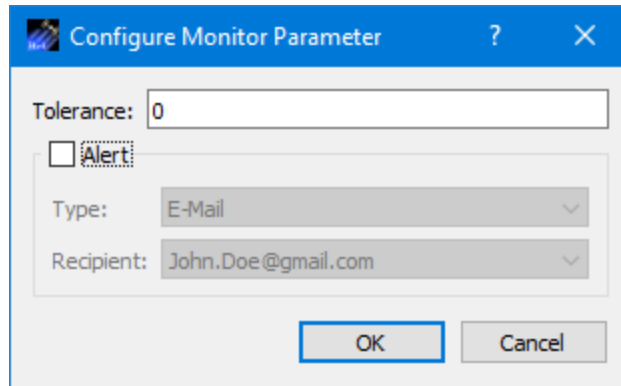
Figure 31 Configure Monitor Parameter

<u>Delete</u>
The Delete button is available when one or more parameters are selected. Pushing this button will delete the selected parameters.

6.1.7   Service Dialog (Extract Tab)

The Service Dialog Extract tab is shown in Figure 32. The Extract tab is used to configure the service to extract parameter values from incoming data and write them to a file. A parameter can be extracted if it is in one of the packets identified on the Data Description tab and the packet is configured to be processed on the Process tab. When the service is activated parameter values will be extracted as data arrives. The extraction function will stop when the service is deactivated.
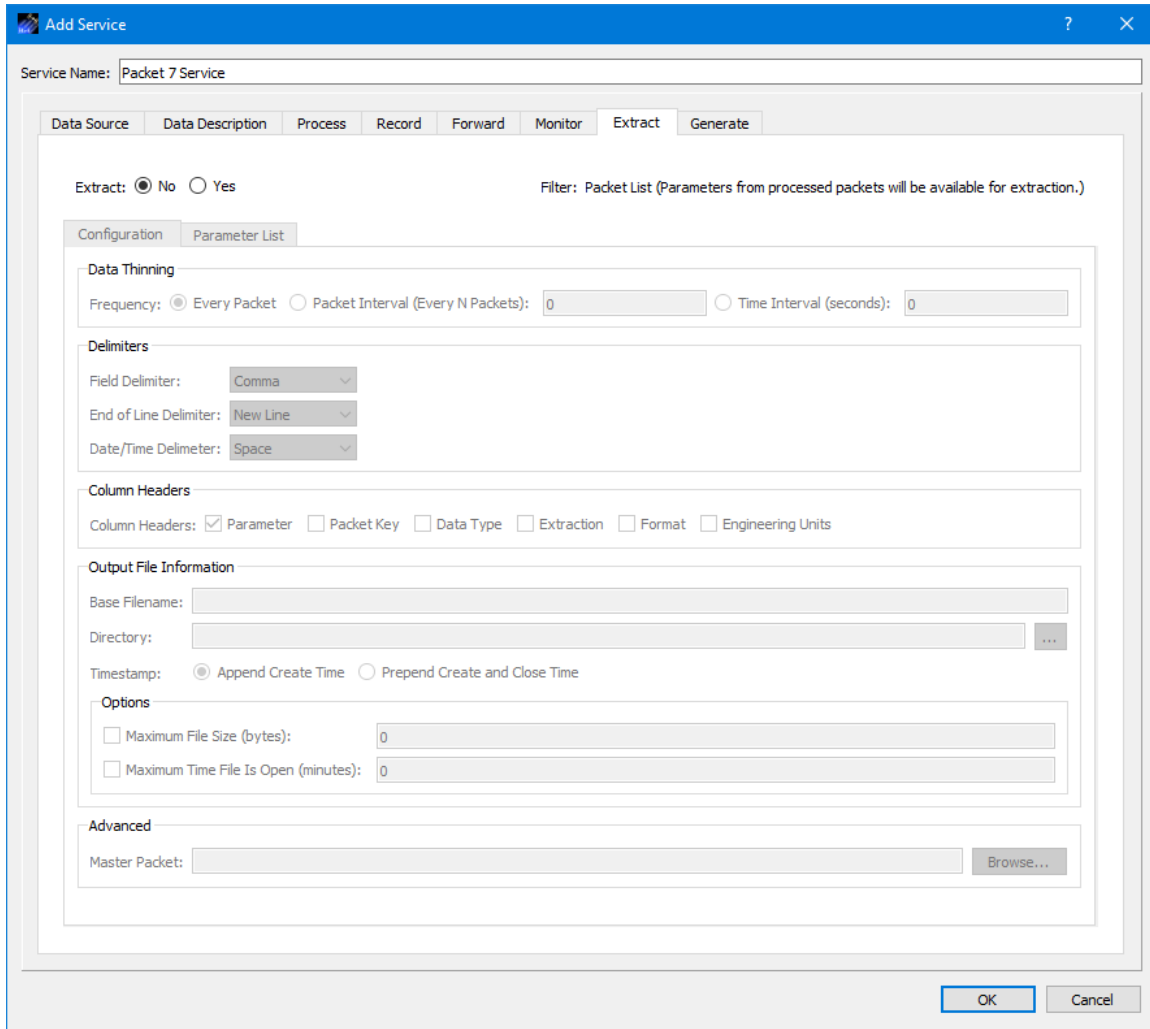
Figure 32 Service Dialog Extract Tab

Each field is described below.

Extract
The No and Yes radio buttons disable or enable data extraction.

Configuration Tab
The Configuration tab, shown in Figure 32, provides the capability to configure the extraction.

Data Thinning
Data Thinning determines how often an extraction is performed (line written to file). The three options are Every Packet, Packet Interval, and Time Interval.

Every Packet
Each new packet will cause a line to be written to the file. If multiple packets are used in the extraction, a line will be written to the file when any one arrives.

44

Packet Interval (Every N Packets)
After the arrival of the first packet, data is written only after the specified number of packets arrives. If no master packet is defined each packet that is extracted from is counted. If a master packet is defined, then only the master packet is counted for determining the interval.

Time Interval (Every N Seconds)
Data is extracted based on the time specified.

Delimiters
The Delimiters area provides a way to set the field delimiter, end of line delimiter, and date/time delimiter used in the output file.

Column Headers
This area provides a way to identify the column headers written at the beginning of the output file.

Output File Information

Base Filename
When data is extracted, the values are stored in one or more files in a local directory. A base filename (provided by you) is used for part of the filename and the rest of the filename is generated by the TReK software. TReK adds timestamp information indicating either the time the file was created or the time the file was created and closed.

Directory
The Directory information is used to identify which directory should be used for the extracted data files. This field requires a complete directory path. An example of this is C:\Users\<username>\trek_workspace\extracted_data\. If you don't like to type or you need help defining the complete path, you can push the … (dot dot dot) button located to the right of the Directory field. This will bring up a Browse dialog you can use to select the local directory where you want to store the extracted data files.

Timestamp
Timestamp options include the time the file was created or the time the file was created and closed. If a master packet is in use, and there is an embedded time field in the master packet definition, the embedded time will be used for the time.

Base Filename: test.txt
Create Timestamp: test2022-06-17-13-39-22.txt
Create and Close Timestamp: 2022-06-21 20-04-33 2022-06-21 20-04-42 test.txt

Maximum File Size
The Maximum File Size information is used to determine when to close a recorded data file. A new record file is opened immediately after the current record file is closed.

Maximum Time File Is Open
The Maximum Time File Is Open Checkbox is used to indicate whether the file should be closed based on a maximum time. The Maximum Time File Is Open property is used in addition to the Maximum File Size property. If the maximum file size is reached before the maximum time, the file will be closed based on maximum file size. However, if the maximum time is reached before the maximum size is reached, the file will be closed based on the maximum time. The file open timer starts when the record file is created. A new record file is opened immediately after the current record file is closed. A record file will not be closed based on maximum time if no packets have been recorded in the file.

Advanced

Master Packet
The master packet can be used to control data thinning with the packet interval option. Additionally, if a master packet is specified then the embedded time stamp of that packet is used to create unique file names. If an embedded time is not available, the system time will be used. Master Packet is optional.

Parameter List Tab
The Parameter List tab is shown in Figure 33. The Parameter list provides a way to identify the parameters to be extracted.
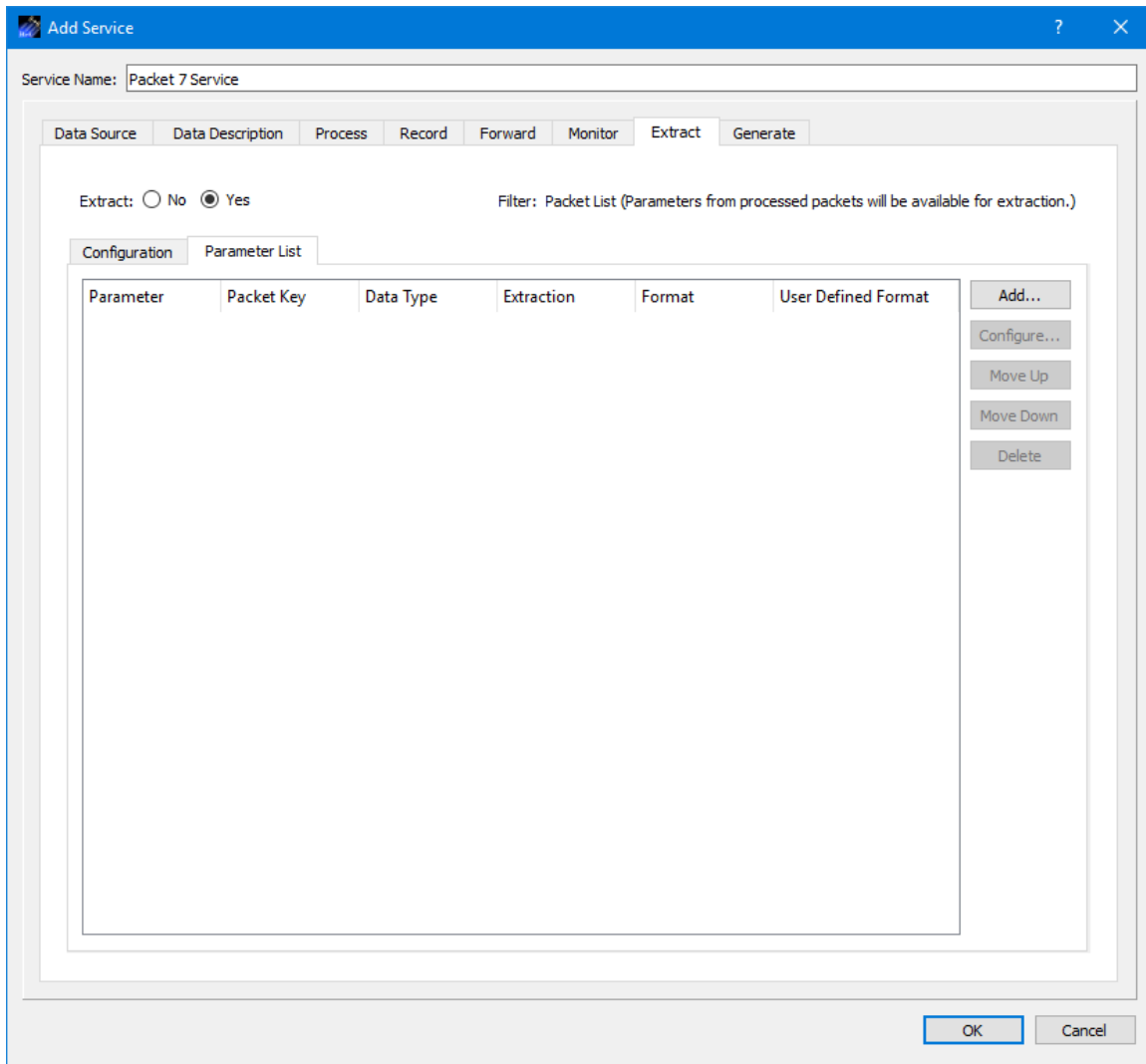
Figure 33 Service Dialog Extract Tab Parameter List Tab

Add
The Add button provides a way to add parameters to the list. You can select from a list of parameters in the packets identified on the Data Description tab. A parameter can be extracted if it is in one of the packets identified on the Data Description tab and the packet is configured to be processed on the Process tab. When you add a parameter to the list, it will be added with default values for each of the columns. You can use the Configure dialog to change a parameter's extraction configuration.

Configure
The Configure button is available when you select a parameter. Pushing the Configure button will display the Configure Extraction Parameter dialog shown in Figure 34. This dialog provides a way to select settings used when the parameter value is extracted and written to the file. The Extraction menu is used to select the level of extraction for the selected parameter. Depending on the parameter selected, options you may see are Raw, Converted, Calibrated, or Enumerated. The Format menu is used to select the format for

the value extracted when it is written to the file. The options available depend on the data type of the parameter selected. Options you may see include Integer, Double, and User Defined Format. If you select User Defined Format, you can enter the user defined format in the User Defined Format field.
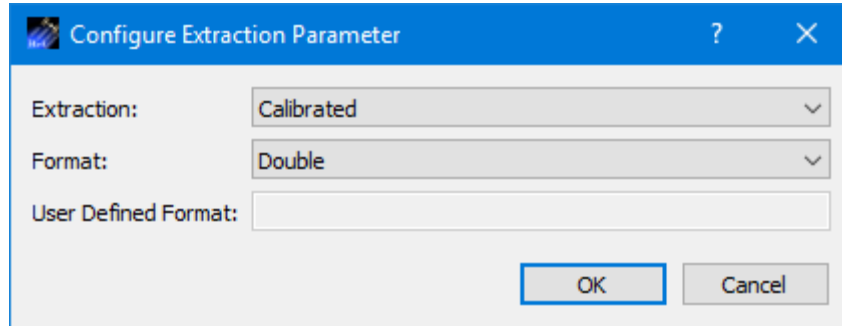
Figure 34 Configure Extraction Parameter Dialog.

Move Up
The Move Up button is available when a parameter is selected. Pushing this button will move the selected parameter up in the list.

Move Down
The Move Down button is available when a parameter is selected. Pushing this button will move the selected parameter down in the list.

Delete
The Delete button is available when one or more parameters are selected. Pushing this button will delete the selected parameters.

6.1.8   Service Dialog (Generate Tab)

The Service Dialog Generate tab is shown in Figure 35. The Generate tab is used to configure the service to generate a custom packet formatted as a Ground Support Equipment (GSE) packet. A parameter can be added to a GSE packet if it is in one of the packets identified on the Data Description tab and the packet is configured to be processed on the Process tab.
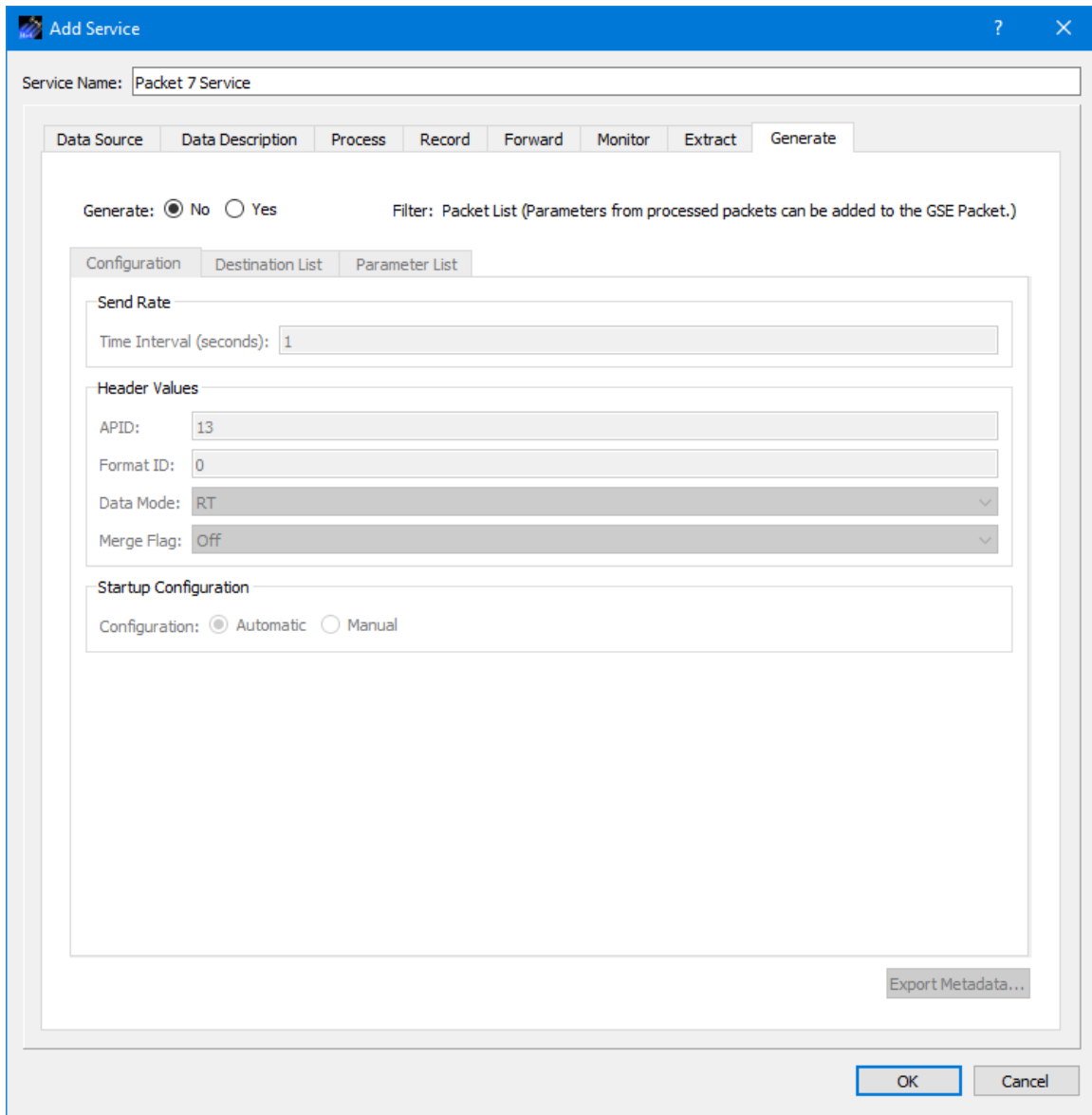
Figure 35 Service Dialog Generate Tab

Each field is described below.

Generate
The No and Yes radio buttons disable or enable generation of GSE packets.

Configuration Tab
The Configuration tab, shown in Figure 35, provides the capability to configure the GSE packet generation.

Send Rate
The send rate defines the rate to use when sending the GSE packets.

Header Values
The Header Values section provides a way to enter values for the APID, Format ID, Data Mode, and Merge Flag header fields in the GSE packet.

Startup Configuration
The Startup Configuration provides a way to select when the GSE packet generation should start. If you select Automatic, the GSE packet data flow will start as soon as the service is activated. If you select Manual, the GSE packet data flow will start when you select "Start GSE Packets" from the Service menu.

Destination List Tab
The GSE packets generated will be sent to the destinations identified on the Destination List tab. The Destination List tab provides the same capabilities as those shown on the Service dialog Forward Tab. Please reference the Forward tab for details.

Parameter List Tab
The Parameter List tab is shown in Figure 36. The Parameter list provides a way to define and order the parameters in the GSE packet.
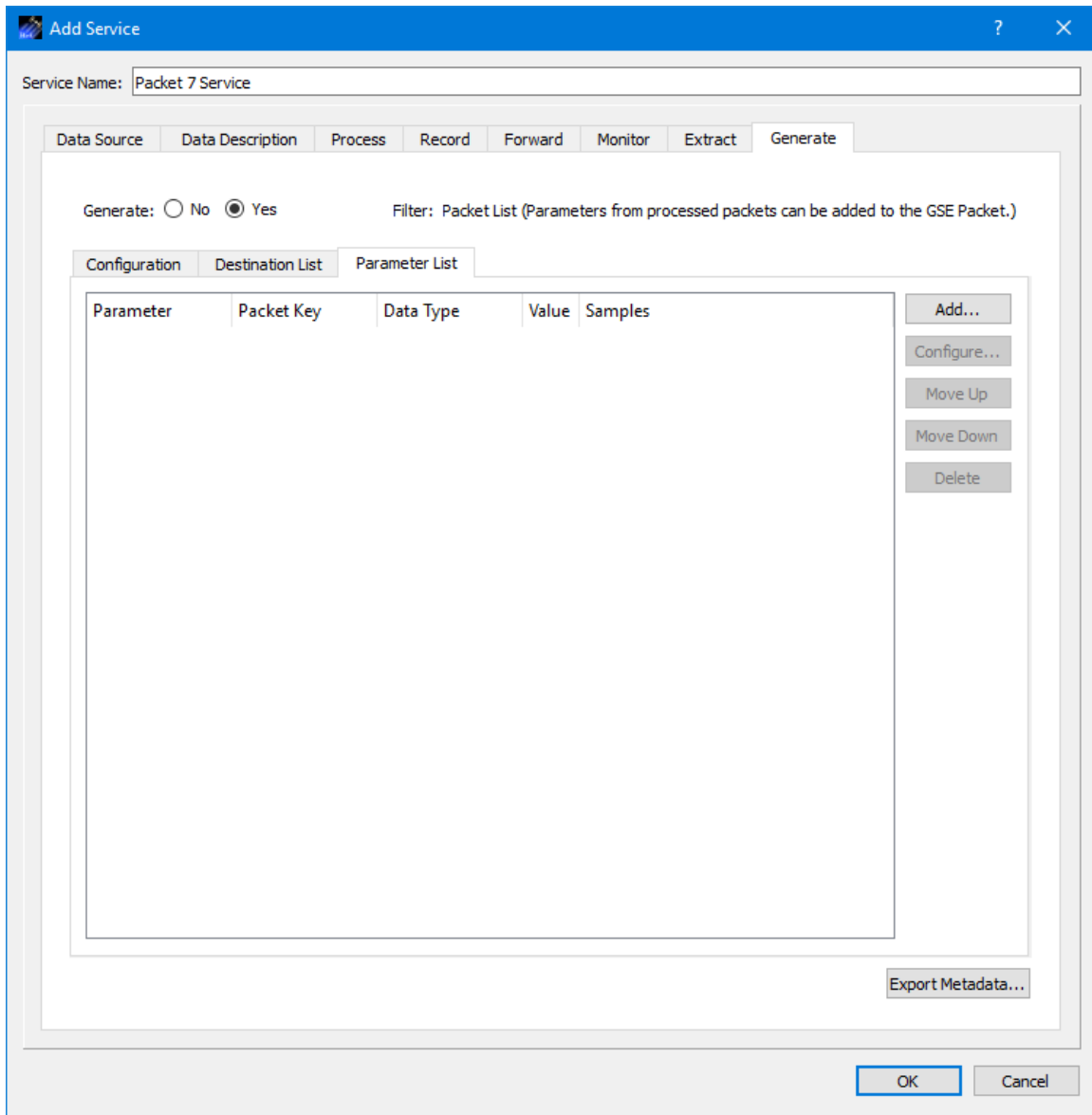
**Figure 36 Service Dialog Generate Tab Parameter List Tab**

Add

The Add button provides a way to add parameters to the list. You can select from a list of parameters in the packets identified on the Data Description tab. Each parameter in the GSE packet must be in one of the packets identified on the Data Description tab and configured to be processed on the Process tab. When you add a parameter to the list, it will be added with default values for each of the columns. You can use the Configure dialog to change a parameter's properties.

Configure

The Configure button is available when you select a parameter. Pushing the Configure button will display the Modify Properties dialog shown in Figure 37. This dialog

provides a way to modify properties like the number of samples or the type of value to be placed in the GSE packet for the selected parameter.
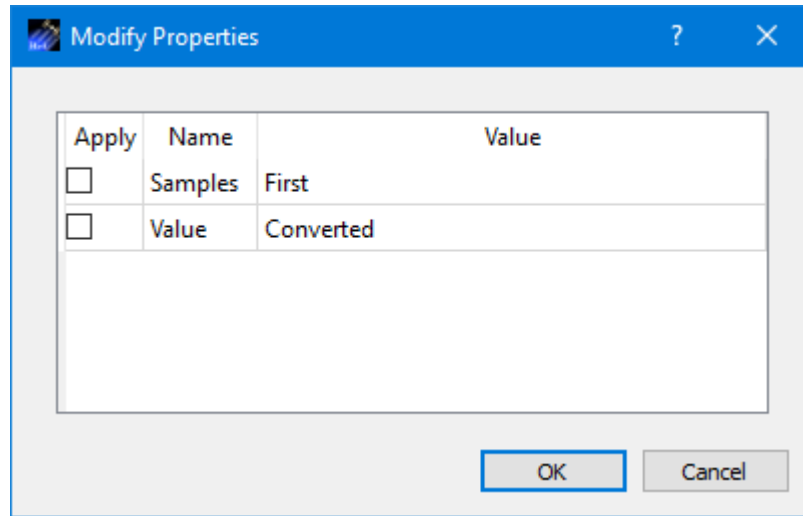
Figure 37 Modify Properties Dialog.

Move Up
The Move Up button is available when a parameter is selected. Pushing this button will move the selected parameter up in the list.

Move Down
The Move Down button is available when a parameter is selected. Pushing this button will move the selected parameter down in the list.

Delete
The Delete button is available when one or more parameters are selected. Pushing this button will delete the selected parameters.

6.2   Parameters

The Parameters dialog is shown in Figure 38. You can access this dialog from the Parameter menu. When one or more services are configured with processing turned on, the Parameters dialog will list all the parameters from all the packets that are configured to be processed. If a parameter is selected, the Details button can be used to access detailed information about the parameter as shown in Figure 39.
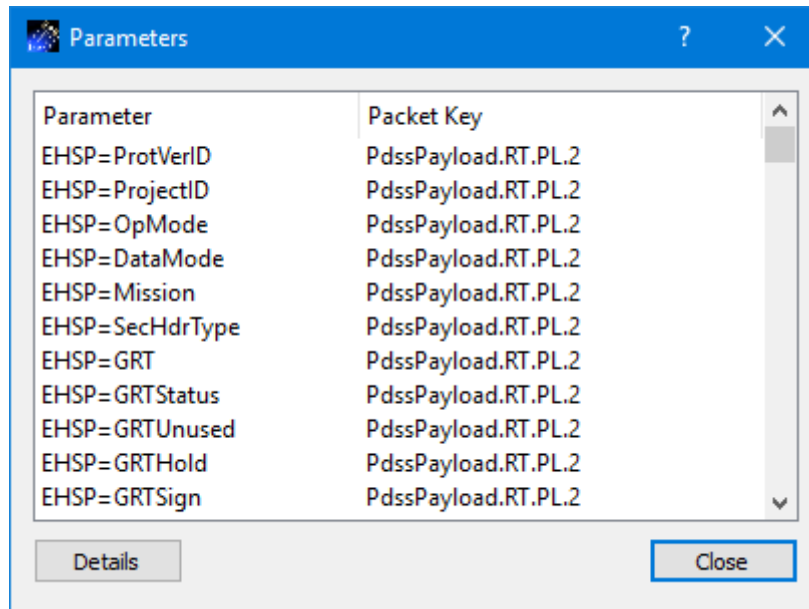
Figure 38 Parameters Dialog

Figure 39 Parameter Details Dialog

6.3   Manage Displays

The Manage Displays dialog is shown in Figure 40. This dialog is used to manage auto-generated displays and custom displays. You can access this dialog from the Parameters menu.
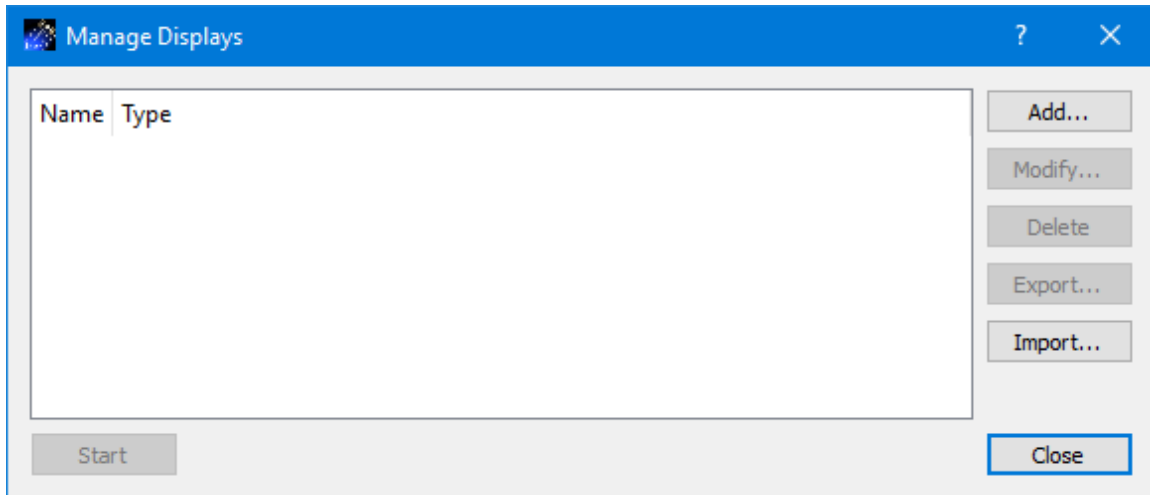
Figure 40 Manage Displays Dialog

The main area of the dialog is used to display a list of available displays. There are two types of displays: Predefined Displays and Custom Displays.

Predefined Displays
When a service is configured with processing turned on, the Data application will auto-generate predefined displays to view the processed data. A predefined display is configured to show all the parameters in a packet, and there is one display per unique packet. Predefined Displays are only available when one or more services are active and configured with processing on for one or more packets. The Manage Displays dialog shown in Figure 41 shows a Predefined Display in the list.
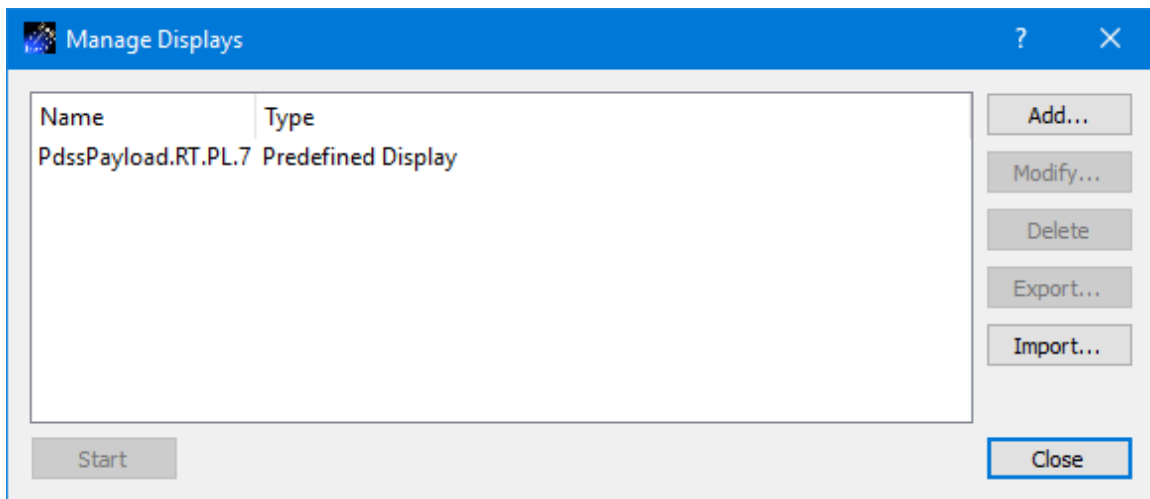
Figure 41 Manage Displays Dialog with Predefined Display

Custom Displays
The Manage Displays dialog also provides the capability to create, modify, delete, export, and import custom displays. Custom Displays are user defined displays. If any custom

displays exist they will be listed in the Manage Displays dialog. Custom Displays only exist in the current application configuration. If you save the configuration, the displays will be saved in the configuration file. If you would like to use a display in a different configuration, you can export it and then import it into the other configuration. The default location for custom displays is the trek_workspace/display directory. However, you can export and import a custom display from outside the trek_workspace.

Starting a Display

The Manage Displays dialog shown in Figure 42 shows both a Predefined Display and a Custom Display. To start a display, select the display in the list and push the Start button or double click on the display in the list. The Manage Displays dialog can be closed after the display is started.
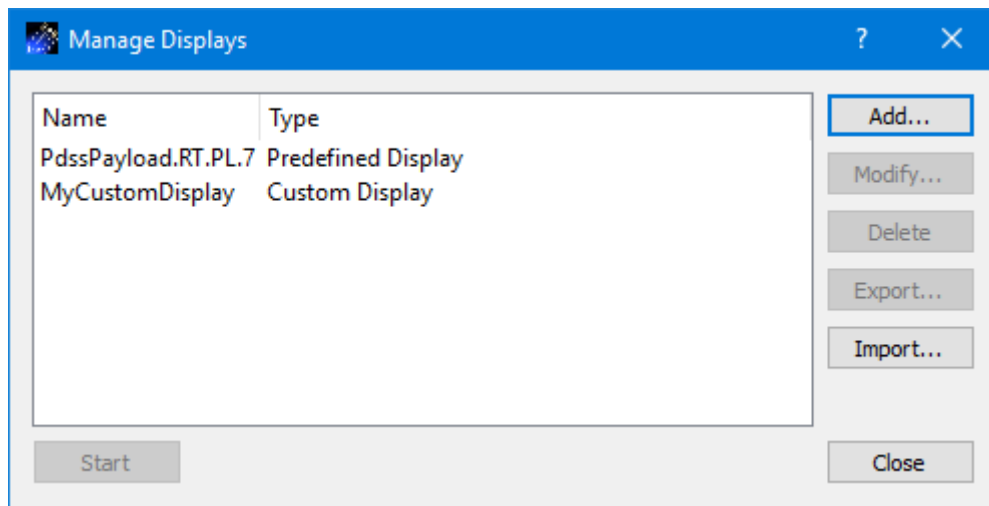
Figure 42 Manage Displays Dialog

Each field is described below.

Display List
The main area of the dialog is used to display a list of available displays.

Add
The Add button provides access to the Add Custom Display dialog. This dialog is used to create a new custom display.

Modify
The Modify button provides access to the Modify Custom Display dialog. This dialog is used to modify an existing custom display.

Delete
The Delete button provides the capability to delete a custom display.

<u>Export</u>
The Export button provides access to the Export Display dialog. It is available when a custom display in the list is selected.

<u>Import</u>
The Import button provides the capability to import a display.

<u>Start</u>
The Start button is used to start a display. It is available when a display in the list is selected.

<u>Close</u>
The Close button closes the dialog.

6.3.1   Display Dialog

Figure 43 shows a predefined display running. The Name column displays the name of the parameter. The Value column displays the value of the parameter. The Status column displays a status character indicating the status of the parameter value. The lines in the display with the yellow and red highlights indicate that limits or expected states associated with those parameters were exceeded. The Status Characters Dialog provides information about what each status character means.

Figure 43 Predefined Display

6.3.2   Status Characters Dialog

If you double click anywhere in the display, the Status Characters Dialog shown in Figure 44 will be displayed.   This dialog provides information about the status shown in the Status column. If you are receiving processed data arriving via a Ground Support Equipment (GSE) packet, you may see a TReK status and a Source status. The Source status will appear after the TReK status and will always be in parentheses. The Source status provides processing status information from the Source that processed the data. Source status characters are source specific. For details regarding Source status characters, please reference documentation provided by the Source (HOSC or TReK).

Status Characters

TReK | Source (HOSC) | Source (TReK)

Status Character	Definition
#	Level 2 delta limit error detected
$	Level 5 low limit error detected
&	Level 1 high limit error detected
*	Level 5 high limit error detected
+	Level 2 high limit error detected
-	Level 2 low limit error detected
0	Level 1 low limit error detected
?	Possible data loss detected
@	Level 1 delta limit error detected
C	Conversion error detected
D	Level 4 delta alarm detected
E	Level 1 expected state error detected
H	Level 4 high alarm detected
K	Calibration switch error detected
L	Level 4 low alarm detected
Q	Level 5 delta alarm detected
R	High range error detected
S	Data is stale; value already retrieved
X	Alarm switch error detected
c	General calibration error detected
d	Level 3 delta limit detected
k	Checksum error detected
l	Bad length error detected
p	Processing error detected
r	Low range error detected
t	Illegal data type for calibration detected
v	Level 3 low limit detected
z	Packet length error detected
^	Level 3 high limit detected

Close

Figure 44 Status Characters (TReK) Dialog
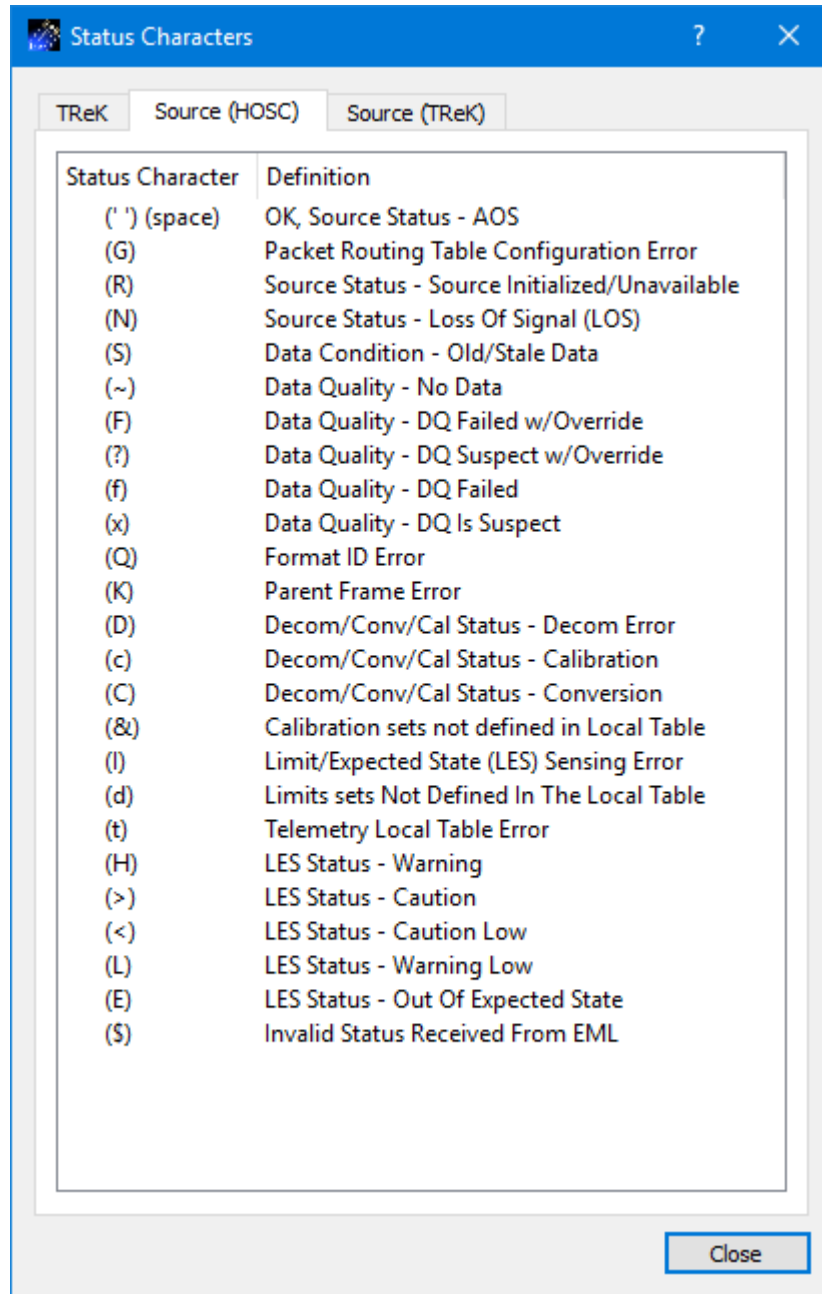
Figure 45 Status Characters (Source HOSC) Dialog
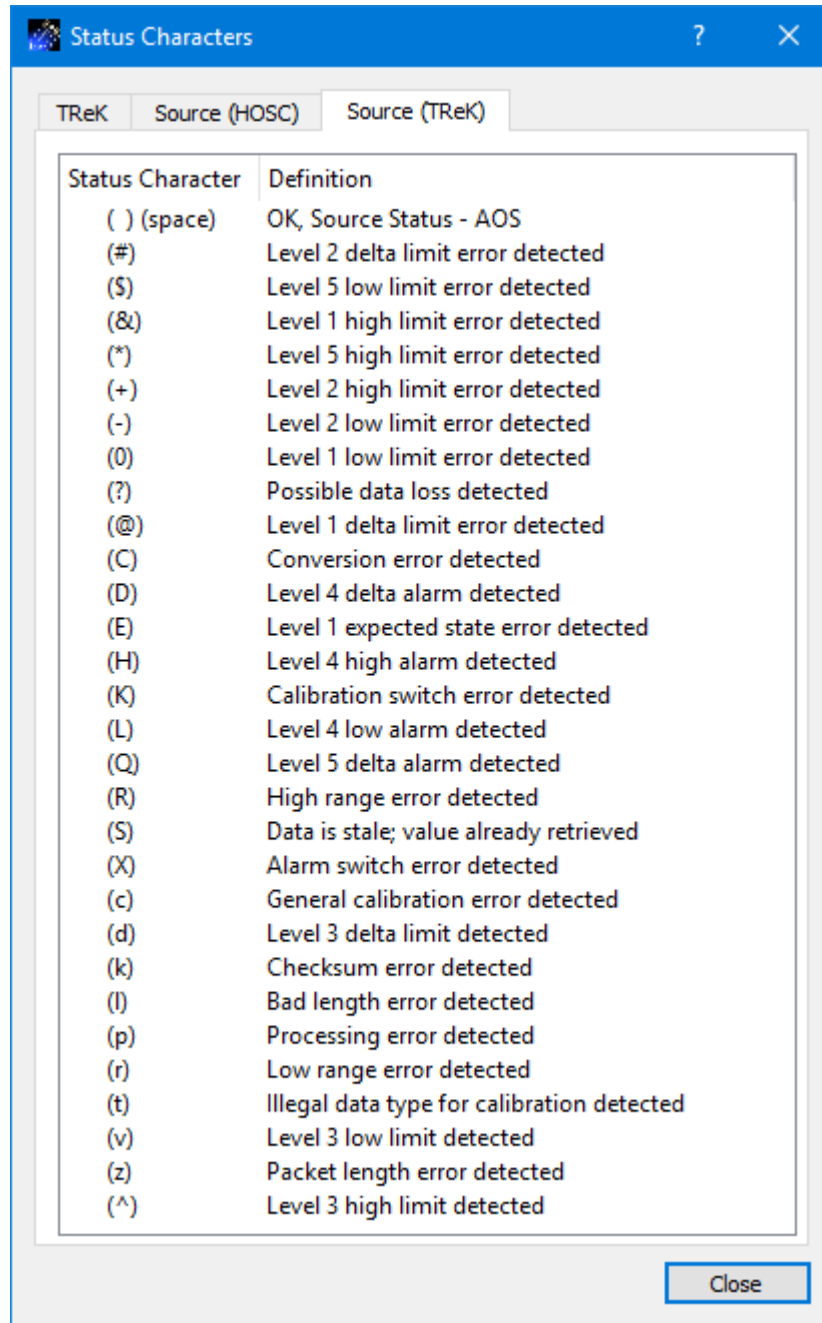
Figure 46 Status Characters (Source TReK) Dialog

6.3.3 Add Custom Display Dialog

The Add Custom Display dialog is used to create a new custom display. It is shown in Figure 47.

61
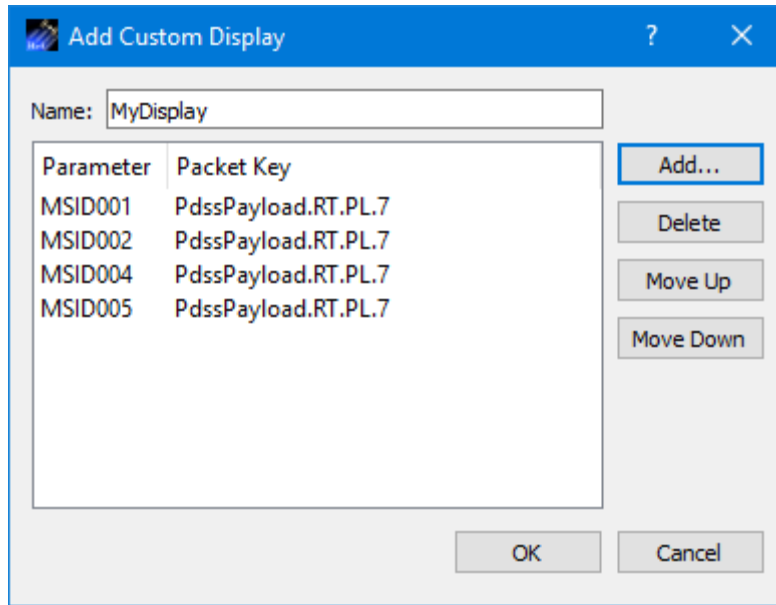
Figure 47 Add Custom Display Dialog

Each item is described below.

Name
The Name field is used to provide a unique name for the custom display.

Parameter List
The Parameter List identifies the parameters that will be on the display. They will be displayed in the order shown in the Parameter List.

Add
The Add button provides access to the Parameters dialog where you can select one or more parameters to add to the display.

Delete
The Delete button can be used to delete a parameter from the Parameter List.

Move Up
When a parameter in the Parameter List is selected, the Move Up button can be used to move the parameter up one row in the list.

Move Down
When a parameter in the Parameter List is selected, the Move Down button can be used to move the parameter down one row in the list.

6.3.4   Modify Custom Display Dialog

The Modify Custom Display dialog is used to modify an existing custom display. It provides the same capabilities that are available in the Add Custom Display dialog.

6.3.5   Export Display Dialog

The Export Display dialog is used to save a custom display outside the current Data application configuration. The default location is the trek_workspace/display directory. However, it can be exported to another location. The Export Display dialog is shown in Figure 48.
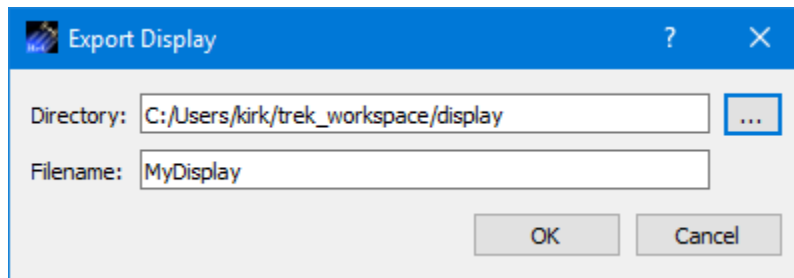
Figure 48 Export Display Dialog

6.4   Manage Monitoring Dialog

Monitoring provides the capability to monitor data values for limit/expected state conditions and issue alerts. Monitoring is available at the service level and globally (across services). If you want to monitor parameters from packets in a single service you can configure monitoring as part of the service. If you want to monitor parameters from packets across services or from different types of packets, you can define a global monitor set using the Manage Monitoring dialog. Parameters are only available for monitoring if they are in a packet that is being processed, the packet is active, and the parameter has an alarm assigned. The Manage Monitoring dialog is shown in Figure 49. It is used to view monitoring messages, manage monitor sets, and manage monitor logging. A monitor set identifies one or more parameters to monitor for alarm conditions (limit or expected state alarms). The Manage Monitoring dialog is available from the Parameters menu.
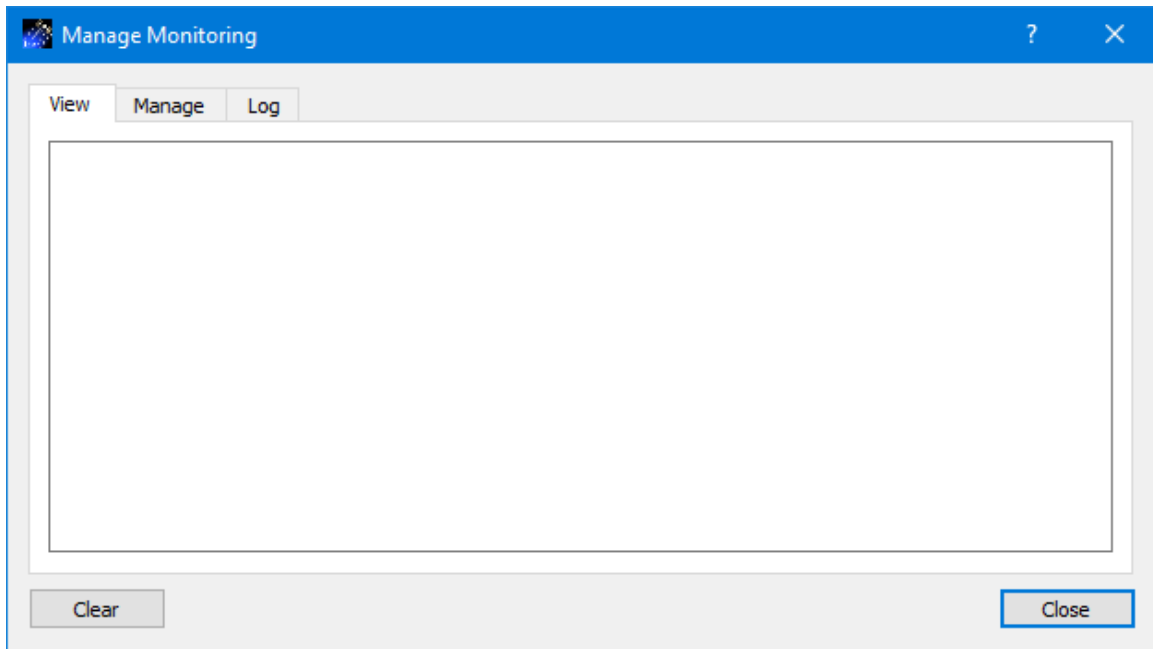
Figure 49 Manage Monitoring Dialog

6.4.1   Manage Monitoring Dialog (View Tab)

The View Tab is shown in Figure 50. This tab is used to view monitoring messages generated by monitoring defined in services and globally. The Clear button can be used to clear the messages.
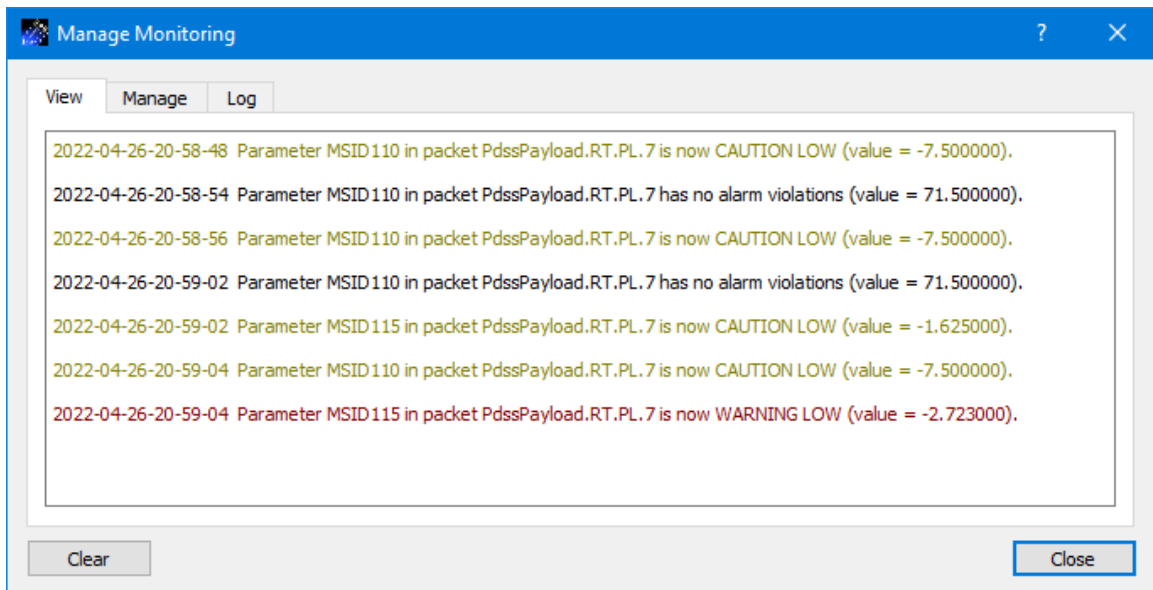
Figure 50 Manage Monitoring Dialog (View Tab)

6.4.2   Manage Monitoring Dialog (Manage Tab)

The Manage Tab is shown in Figure 51. This tab is used to manage monitor sets.
Monitor Sets listed in this dialog only exist in the current application configuration. If
you save the configuration, the monitor sets will be saved in the configuration file. If you
would like to use a monitor set in a different configuration, you can export it and then
import it into the other configuration. The default location for monitor sets is the
trek_workspace/monitor_set directory. However, you can export and import a monitor
set from outside the trek_workspace.
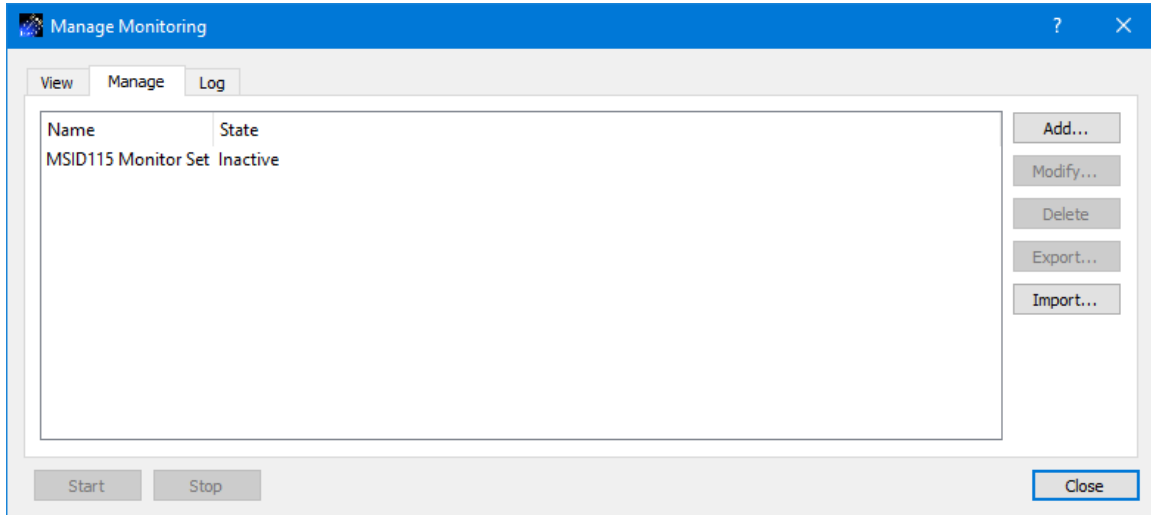
Figure 51 Manage Monitoring Dialog (Manage Tab)

Each button is described below.

Add
The Add button provides access to the Add Monitor Set dialog shown in Figure 52. This
dialog is used to create a new monitor set. For details please reference section 6.4.2.1.
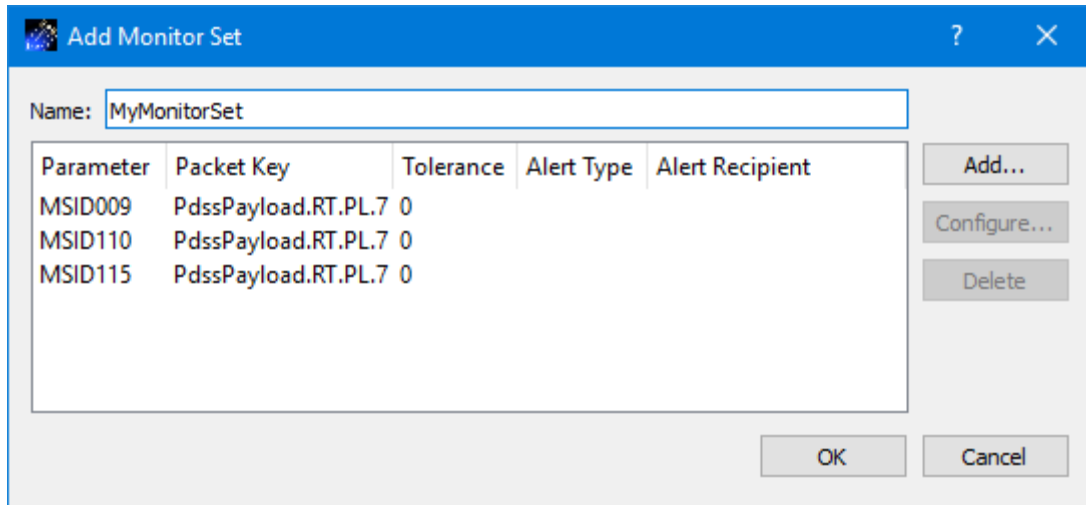
Figure 52 Add Monitor Set Dialog

Modify

The Modify button provides access to the Modify Monitor Set dialog. This dialog is used to modify an existing monitor set. It provides the same capabilities that are available in the Add Monitor Set dialog.

Delete

The Delete button provides the capability to delete a monitor set.

Export

The Export button provides access to the Export Monitor Set dialog. The Export Monitor Set dialog is used to save a monitor set outside the current Data application configuration. The default location is the trek_workspace/monitor_set directory. However, it can be exported to another location. The Export Monitor Set dialog is shown in Figure 53.
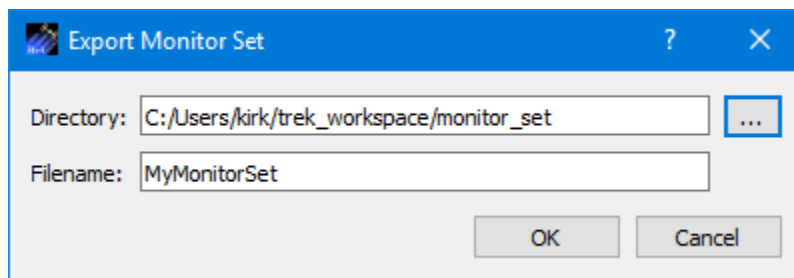
Figure 53 Export Monitor Set Dialog

Import

The Import button provides the capability to import a monitor set.

Start

The Start button is used to start monitoring for a selected set. It is available when you select a set that is Inactive.

Stop
The Stop button is used to stop monitoring for a selected set. It is available when you select a set that is Active.

6.4.2.1   Add Monitor Set Dialog
Add Monitor Set dialog is shown in Figure 54.
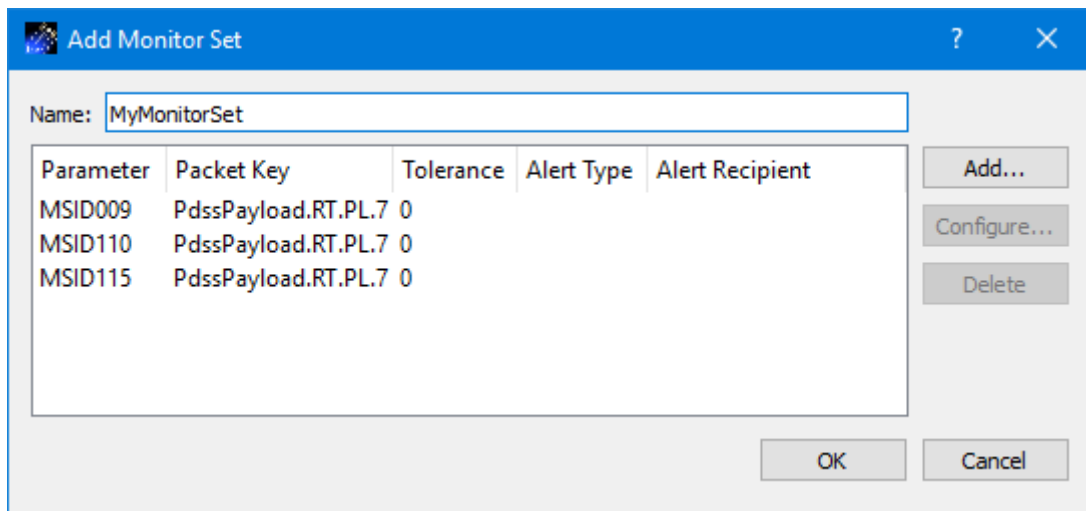
Figure 54 Add Monitor Set Dialog

Each item is described below.

Name
The Name field is used to provide a unique name for the monitor set.

Parameter List
The Parameter List identifies the parameters to be monitored.

Add
The Add button provides access to the Parameters dialog where you can select one or more parameters to add to the parameter list. The Parameters dialog will only list parameters that are in a packet that is actively being processed and the parameter has an alarm assigned. When you add a parameter it will be added with default values for each of the columns. You can use the Configure dialog to change a parameter's monitoring configuration.

Configure

The Configure button provides access to the Configure Monitor Parameter dialog shown in Figure 55.   The Configure button is available when you select a parameter. This dialog provides the capability to set monitoring properties associated with the parameter selected. Tolerance provides the capability to control how often a monitoring message or monitoring alert is generated. The tolerance number indicates how many times the parameter value can go out of limits or expected state contiguously before it triggers an alert. When the parameter goes back into a nominal state the tolerance count starts over. The Alert checkbox provides the capability to add an e-mail, e-mail and text, or text alert when a monitoring state changes. To use the Alert options, you must enter E-Mail and Text information using the Manage E-Mail and Text Settings dialog available from the Options menu. For additional information, please reference the Manage E-Mail and Text Settings dialog. In the Configure Monitor Parameter dialog, the Recipient list will be populated based on the Type selected and the information entered in the Manage E-Mail and Text Settings dialog. The recipient identifies who should be notified when the monitor state change is triggered.
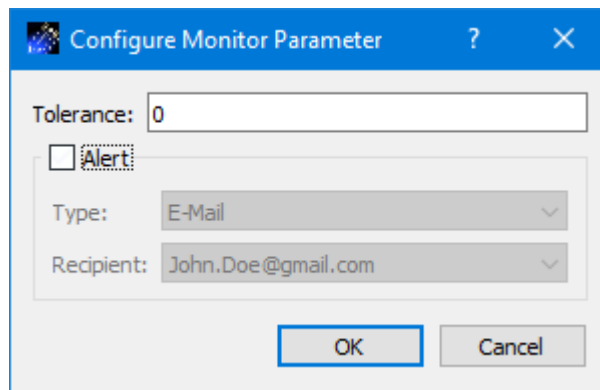
Figure 55 Configure Monitor Parameter Dialog

Delete
The Delete button can be used to delete a parameter from the Parameter List.

6.4.3   Manage Monitoring Dialog (Log Tab)

The Log Tab is shown in Figure 56. This tab provides the capability to configure monitor message logging. If you turn on monitor message logging, monitor messages generated after logging is turned on will be written to the specified log file. Pushing the Configure button will display the Configure Monitor Message Logging dialog shown in Figure 57.
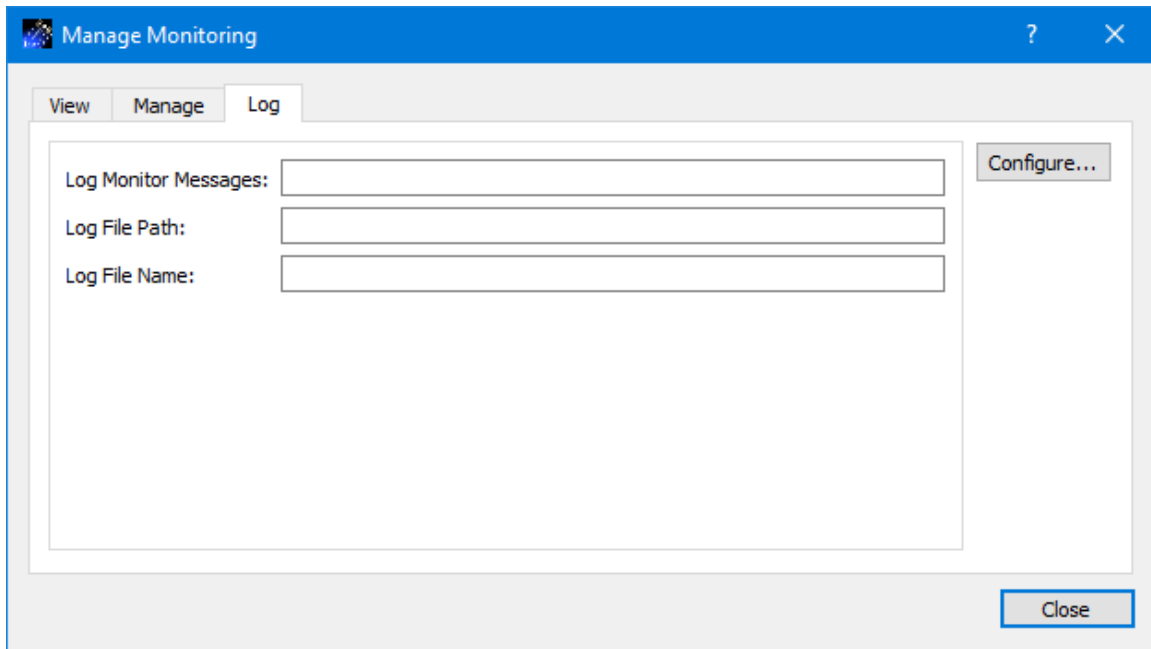
Figure 56 Manage Monitoring Dialog (Log Tab)
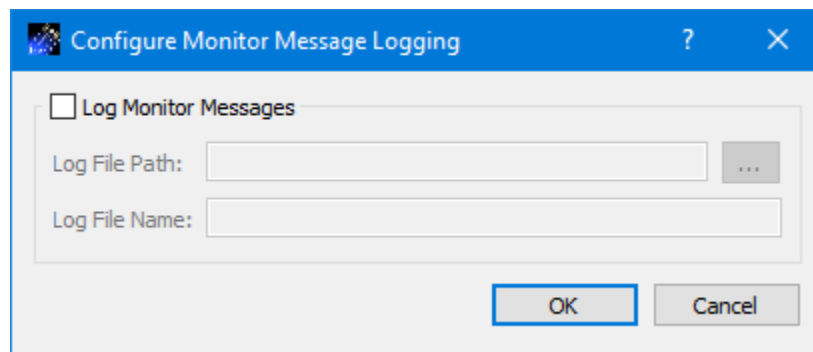
Figure 57 Configure Monitor Message Logging Dialog

Each item is described below.

Log Monitor Messages
The Log Monitor Messages checkbox provides the capability to turn logging on or off. If the Log Monitor Messages checkbox is not checked, logging will be off. If the Log Monitor Messages checkbox is checked, logging will be on.

Log File Path
The Log File Path should contain the absolute path to the directory where the log file should be written. If you don't like to type or you need help defining the complete path, you can push the … (dot dot dot) button located to the right of the Log File Path field. This will bring up a Browse dialog you can use to select the local directory where you want to store the log files.

Log File Name
The Log File Name field should contain the name to use for the log file.

The log file generated will use the log file name you enter followed by a timestamp. It will look similar to the following:

Example Log File: monitor_2017-06-06-12-06-41.log

6.5   Manage Extraction Dialog

Extraction provides the capability to extract data values from incoming data streams and write the values to a file. Extraction is available at the service level and globally (across services). If you want to extract parameters from packets in a single service you can configure extraction as part of the service. If you want to extract parameters from packets across services or from different types of packets, you can define a global extraction using the Manage Extraction dialog. Parameters are only available to add to a global extraction if they are in a packet that is actively being processed. Extraction for a selected global extraction is started when you push the Start button and stopped when you push the Stop button. The Manage Extraction dialog is available from the Parameters menu.
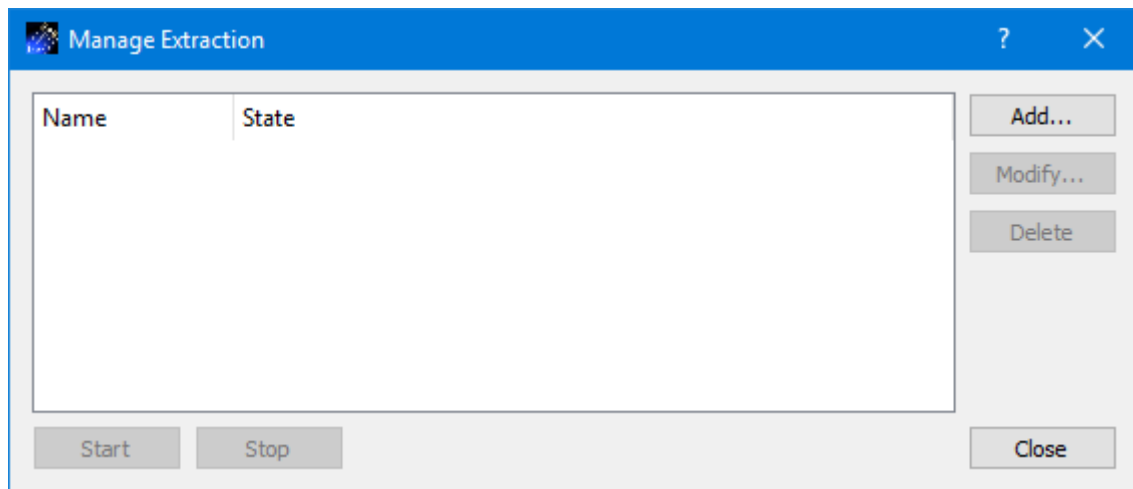
Figure 58 Manage Extraction Dialog

Each field is described below.

Extraction List
The main area of the dialog is used to display a list of global extraction definitions. An extraction handled by a service is not displayed in this dialog.

70

<u>Add</u>
The Add button provides access to the Add Parameter Extraction dialog. It is used to create a new global extraction definition.

<u>Modify</u>
The Modify button provides access to the Modify Parameter Extraction dialog. It is used to modify an existing global extraction definition.

<u>Delete</u>
The Delete button provides the capability to delete a global extraction definition.

<u>Start</u>
The Start button provides the capability to start a global extraction.

<u>Stop</u>
The Stop button provides the capability to stop a global extraction.

<u>Close</u>
The Close button closes the dialog.

6.5.1   Add Parameter Extraction Dialog

The Add Parameter Extraction dialog is used to create a new global extraction definition. It is shown in Figure 59.

Figure 59 Add Parameter Extraction Dialog

Each field is described below.

Name
Each extraction definition must have a unique name.

Configuration Tab
The Configuration tab, shown in Figure 59, provides the capability to configure the extraction.

Data Thinning
Data Thinning determines how often an extraction is performed (line written to file). The three options are Every Packet, Packet Interval, and Time Interval.

Every Packet

Each new packet will cause a line to be written to the file. If multiple packets are used in the extraction, a line will be written to the file when any one arrives.

Packet Interval (Every N Packets)
After the arrival of the first packet, data is written only after the specified number of packets arrives. If no master packet is defined each packet that is extracted from is counted. If a master packet is defined, then only the master packet is counted for determining the interval.

Time Interval (Every N Seconds)
Data is extracted based on the time specified.

Delimiters
The Delimiters area provides a way to set the field delimiter, end of line delimiter, and date/time delimiter used in the output file.

Column Headers
This area provides a way to identify the column headers written at the beginning of the output file.

Output File Information

Base Filename
When data is extracted, the values are stored in one or more files in a local directory. A base filename (provided by you) is used for part of the filename and the rest of the filename is generated by the TReK software. TReK adds timestamp information indicating either the time the file was created or the time the file was created and closed.

Directory
The Directory information is used to identify which directory should be used for the extracted data files. This field requires a complete directory path. An example of this is C:\Users\<username>\trek_workspace\extracted_data\. If you don't like to type or you need help defining the complete path, you can push the … (dot dot dot) button located to the right of the Directory field. This will bring up a Browse dialog you can use to select the local directory where you want to store the extracted data files.

Timestamp
Timestamp options include the time the file was created or the time the file was created and closed. If a master packet is in use, and there is an embedded time field in the master packet definition, the embedded time will be used for the time.

Base Filename: test.txt
Create Timestamp: test2022-06-17-13-39-22.txt
Create and Close Timestamp: 2022-06-21 20-04-33 2022-06-21 20-04-42 test.txt

Maximum File Size
The Maximum File Size information is used to determine when to close a recorded data file. A new record file is opened immediately after the current record file is closed.

Maximum Time File Is Open
The Maximum Time File Is Open Checkbox is used to indicate whether the file should be closed based on a maximum time. The Maximum Time File Is Open property is used in addition to the Maximum File Size property. If the maximum file size is reached before the maximum time, the file will be closed based on maximum file size. However, if the maximum time is reached before the maximum size is reached, the file will be closed based on the maximum time. The file open timer starts when the record file is created. A new record file is opened immediately after the current record file is closed. A record file will not be closed based on maximum time if no packets have been recorded in the file.

Advanced

Master Packet
The master packet can be used to control data thinning with the packet interval option. Additionally, if a master packet is specified then the embedded time stamp of that packet is used to create unique file names. If an embedded time is not available, the system time will be used. Master Packet is optional.

Parameter List Tab
The Parameter List tab is shown in Figure 60. The Parameter list provides a way to identify the parameters to be extracted.
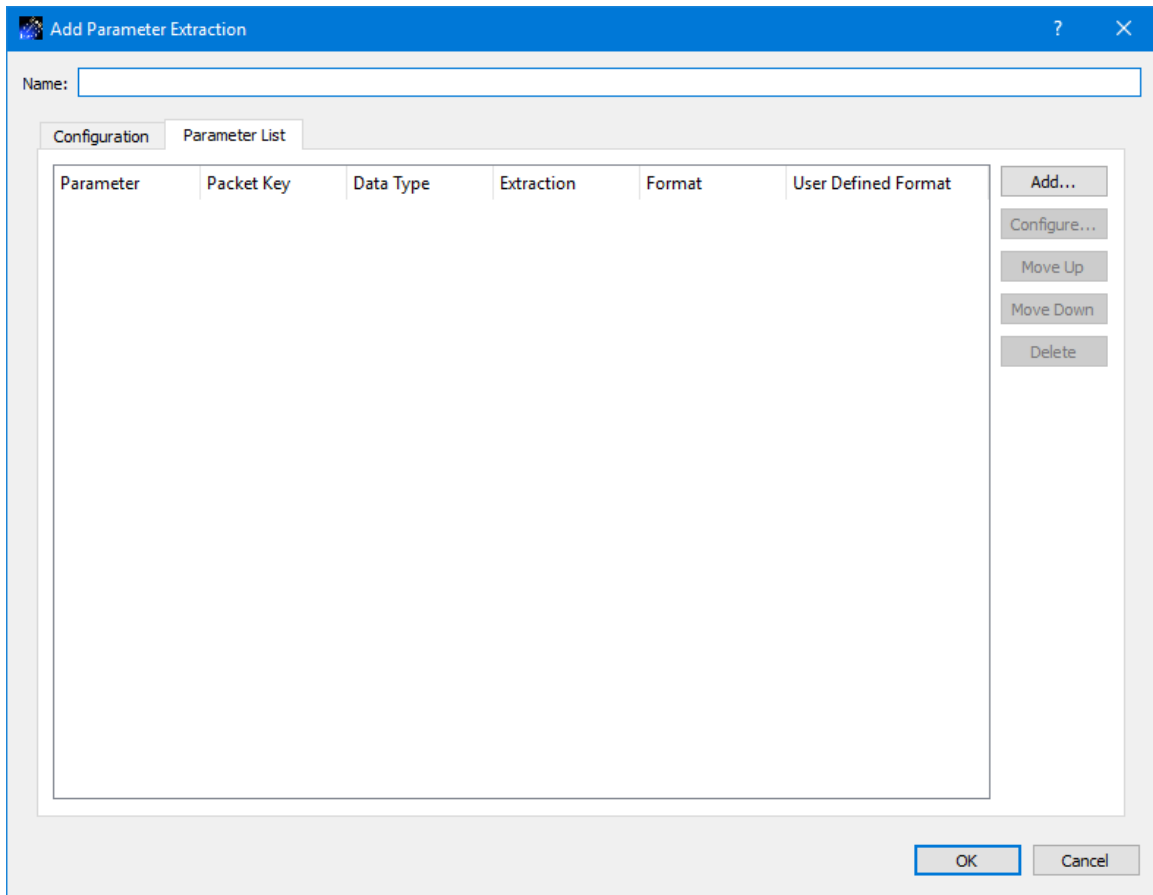
Figure 60 Add Parameter Extraction Dialog Parameter List Tab

Add

The Add button provides a way to add parameters to the list. You can select parameters from packets that are actively being processed. When you add a parameter to the list, it will be added with default values for each of the columns. You can use the Configure dialog to change a parameter's extraction configuration.

Figure 61 Add Parameter Extraction Add Parameters Dialog

Configure

The Configure button is available when you select a parameter. Pushing the Configure button will display the Configure Extraction Parameter dialog shown in Figure 62. This dialog provides a way to select settings used when the parameter value is ex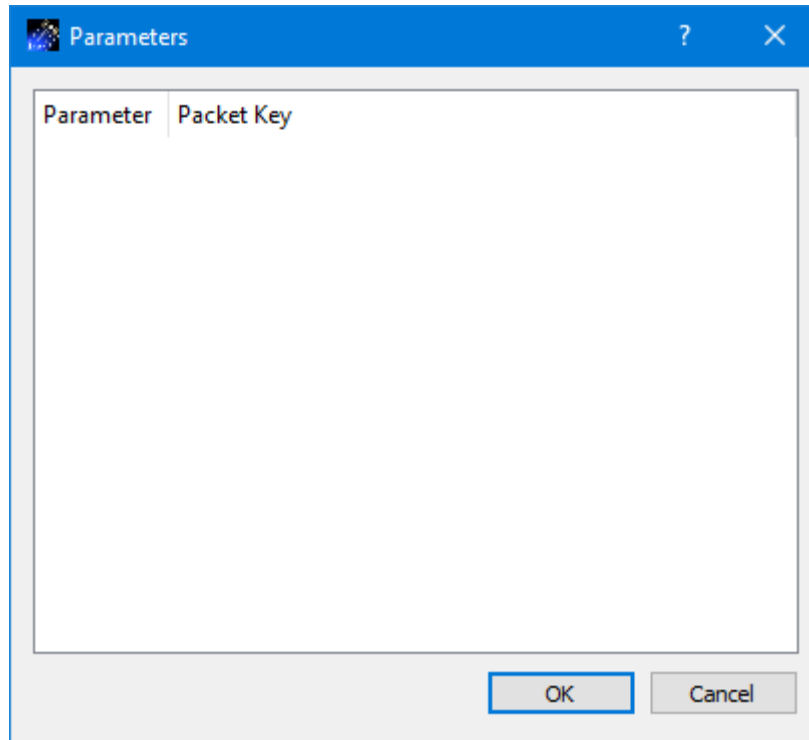tracted and written to the file. The Extraction menu is used to select the level of extraction for the selected parameter. Depending on the parameter selected, options you may see are Raw, Converted, or Calibrated. The Format menu is used to select the format for the value extracted when it is written to the file. The options available depend on the data type of the parameter selected. Options you may see include Integer, Double, and User Defined Format. If you select User Defined Format, you can enter the user defined format in the User Defined Format field.
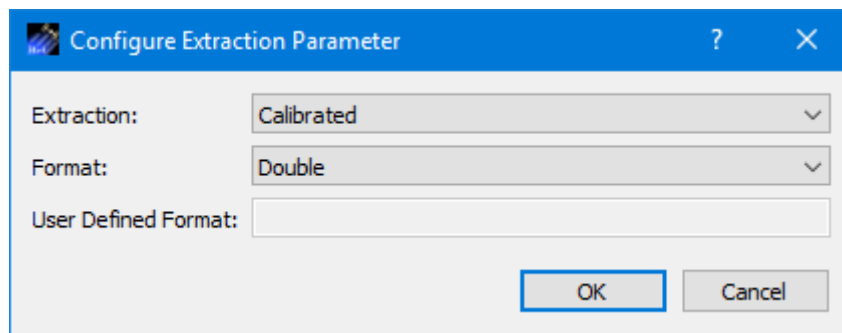
Figure 62 Configure Extraction Parameter Dialog.

Move Up
The Move Up button is available when a parameter is selected. Pushing this button will move the selected parameter up in the list.

Move Down
The Move Down button is available when a parameter is selected. Pushing this button will move the selected parameter down in the list.

Delete
The Delete button is available when one or more parameters are selected. Pushing this button will delete the selected parameters.

6.5.2   Modify Parameter Extraction Dialog

The Modify Parameter Extraction dialog is used to modify an existing extraction definition. It provides the same capabilities that are available in the Add Parameter Extraction dialog.

6.6   Manage Ground Support Equipment (GSE) Packet Generation Dialog

The GSE Packet Generation capability can be used to extract data values from incoming data streams and place the values in a custom packet for distribution. The packets will be formatted in the Ground Support Equipment (GSE) packet defined in the Payload to Generic User Interface Definition Document (PGUIDD) SSP-50305 Volume 1. The GSE Packet Generation capability is available at the service level and globally (across services). If you want to generate a custom packet with parameters from packets in a single service you can configure GSE packet generation as part of the service. If you want to generate a custom packet from parameters in packets across services or from different types of packets, you can define a global GSE packet generation definition using the Manage GSE Packet Generation dialog. Parameters are only available to add to a global GSE packet generation definition if they are in a packet that is actively being processed. The Manage GSE Packet Generation dialog is available from the Parameters menu.
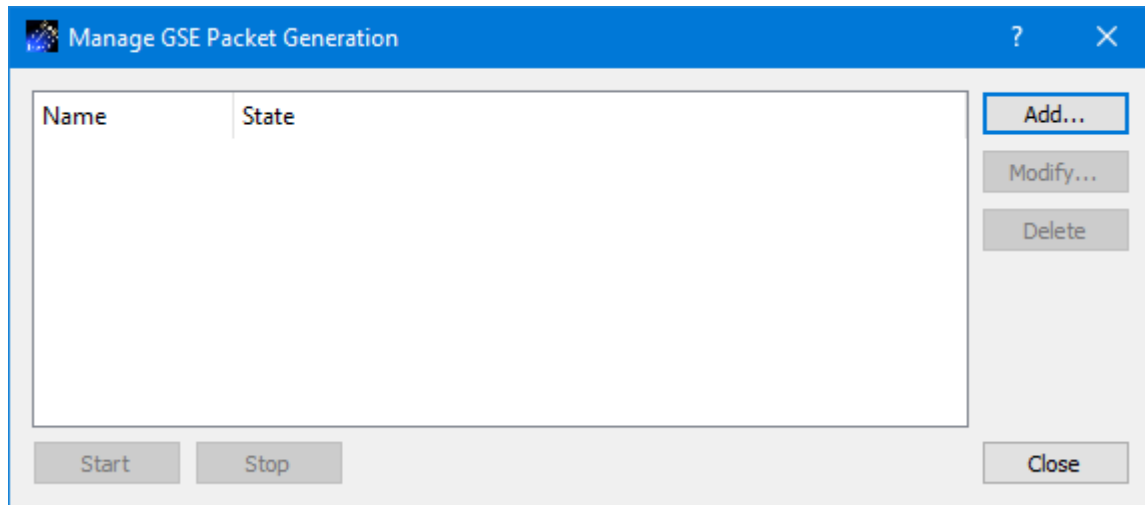
Figure 63 Manage GSE Packet Generation Dialog

Each field is described below.

GSE Packet Generation List
The main area of the dialog is used to display a list of global GSE Packet Generation definitions. GSE packet generation handled by a service is not displayed in this dialog.

Add
The Add button provides access to the Add GSE Packet Generation Definition dialog. It is used to create a new global GSE Packet Generation definition.

Modify
The Modify button provides access to the Modify GSE Packet Generation Definition dialog. It is used to modify an existing global GSE Packet Generation definition.

Delete
The Delete button provides the capability to delete a global GSE Packet Generation definition.

Start
The Start button provides the capability to start the global GSE packet generation.

Stop
The Stop button provides the capability to stop the global GSE packet generation.

Close
The Close button closes the dialog.

6.6.1 Add GSE Packet Generation Definition Dialog

The Add GSE Packet Generation Definition dialog is used to create a new "global" GSE Packet Generation definition. It is shown in Figure 64. For global GSE Packet Generation, the GSE packet data flow will start when you select "Start" on the Manage GSE Packet Generation dialog.

Figure 64 Add GSE Packet Generation Definition Dialog

Each field is described below.

Name
Each GSE Packet Generation definition must have a unique name.

Configuration Tab
The Configuration tab, shown in Figure 64, provides the capability to configure the GSE packet generation definition.

Send Rate

The send rate defines the rate to use when sending the GSE packets.

Header Values

The Header Values section provides a way to enter values for the APID, Format ID, Data Mode, and Merge Flag header fields in the GSE packet.

Destination List Tab

The GSE packets generated will be sent to the destinations identified on the Destination List tab. The Destination List tab provides the same capabilities as those shown on the Service dialog Forward Tab. Please reference the Forward tab for details.

Parameter List Tab

The Parameter List tab is shown in Figure 65. The Parameter list provides a way to define the parameters in the GSE packet.
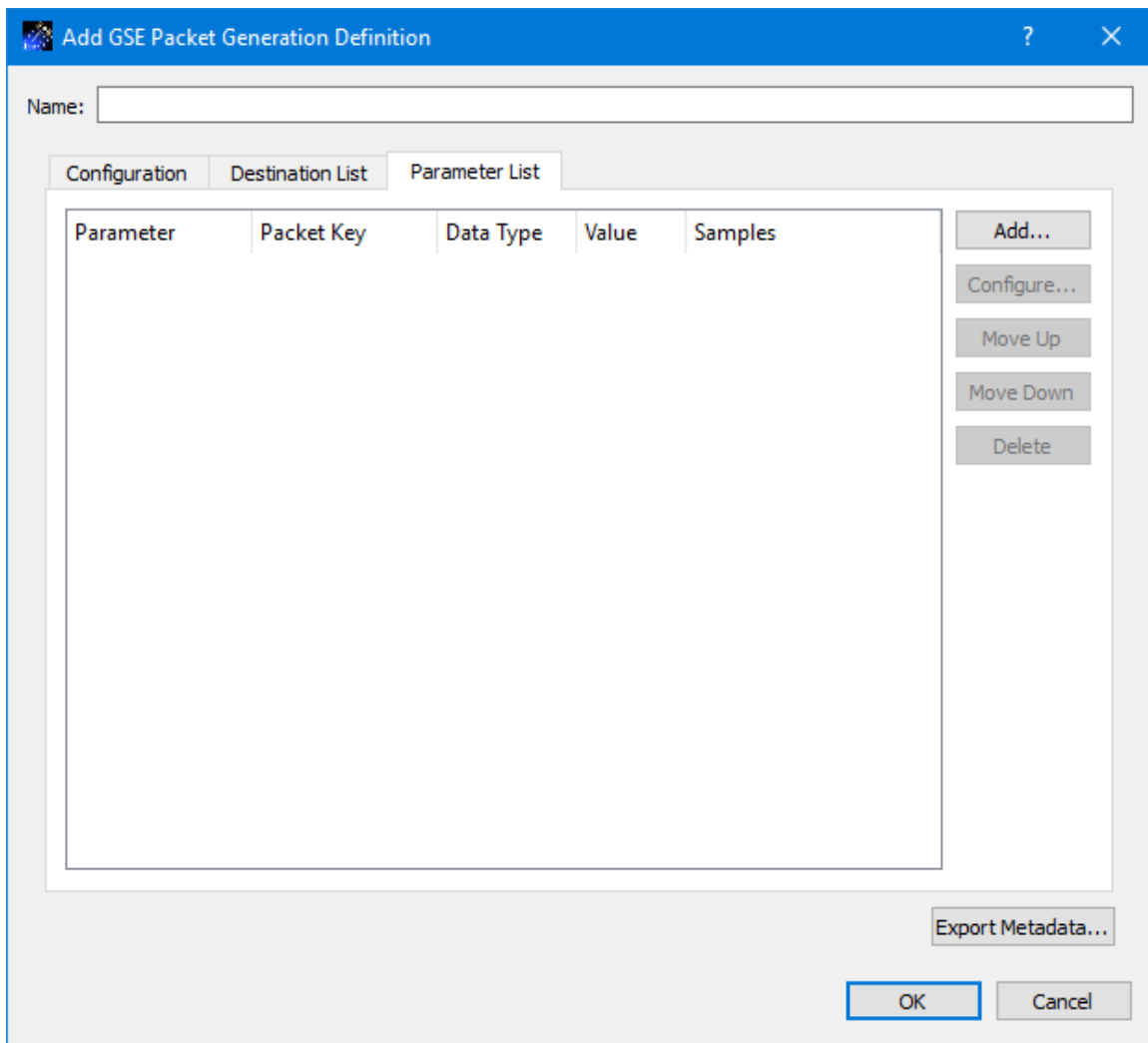
Figure 65 Add GSE Packet Generation Definition Dialog Parameter List Tab

Add

The Add button provides a way to add parameters to the list. You can select parameters from packets that are actively being processed. When you add a parameter to the list, it will be added with default values for each of the columns. You can use the Configure dialog to change a parameter's properties.
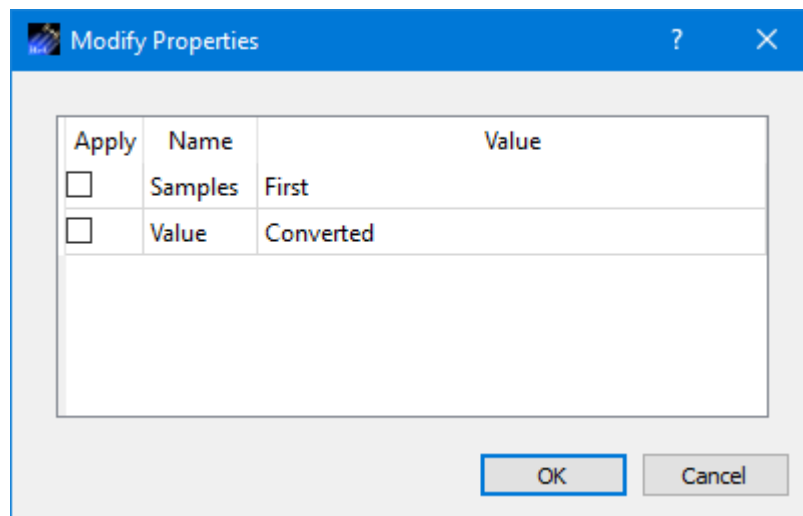
Configure

The Configure button is available when you select a parameter. Pushing the Configure button will display the Modify Properties dialog shown in Figure 66. This dialog provides a way to modify properties like the number of samples or the type of value to be placed in the GSE packet for the selected parameter.

Figure 66 Modify Properties Dialog.

Move Up

The Move Up button is available when a parameter is selected. Pushing this button will move the selected parameter up in the list.

Move Down

The Move Down button is available when a parameter is selected. Pushing this button will move the selected parameter down in the list.

Delete

The Delete button is available when one or more parameters are selected. Pushing this button will delete the selected parameters.

6.7   Statistics

Statistics displays information about incoming data and services such as processing, recording, and forwarding. Statistics information is displayed in a dock window in the Main Window and in the Statistics dialog available from the Options menu. Figure 67 shows the Statistics dock window in the Main Window. Figure 68 shows the Statistics dialog.
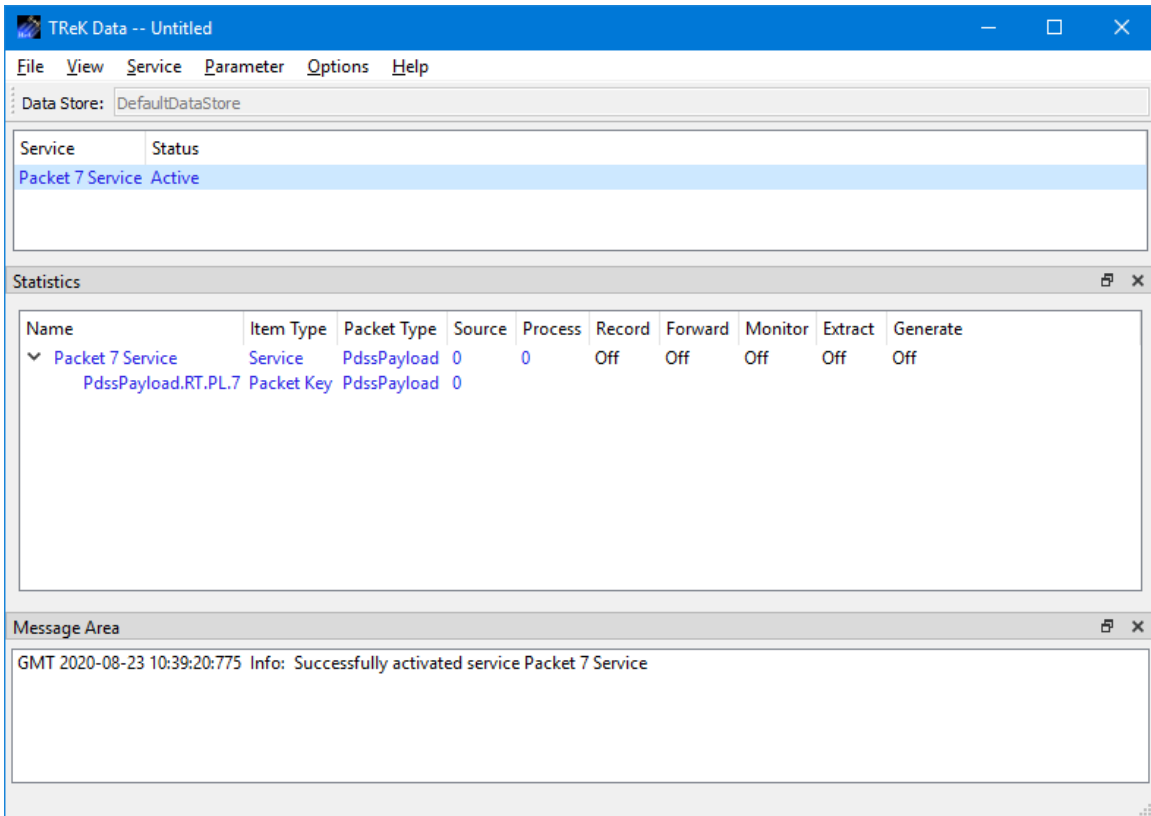

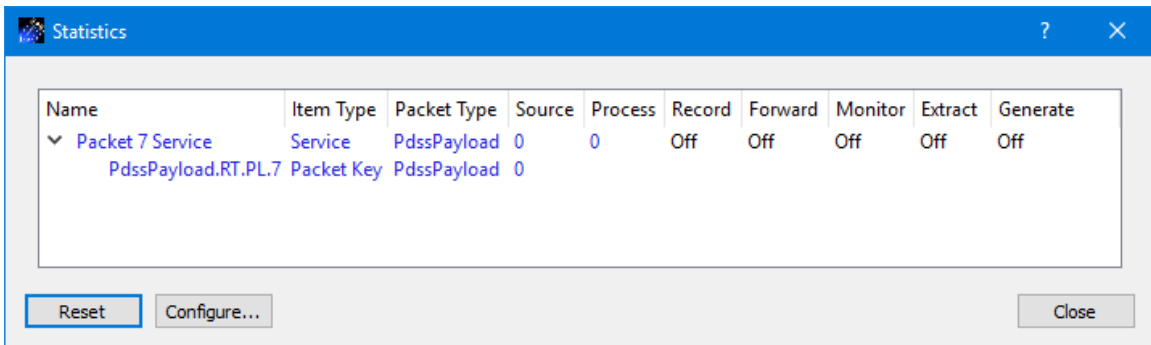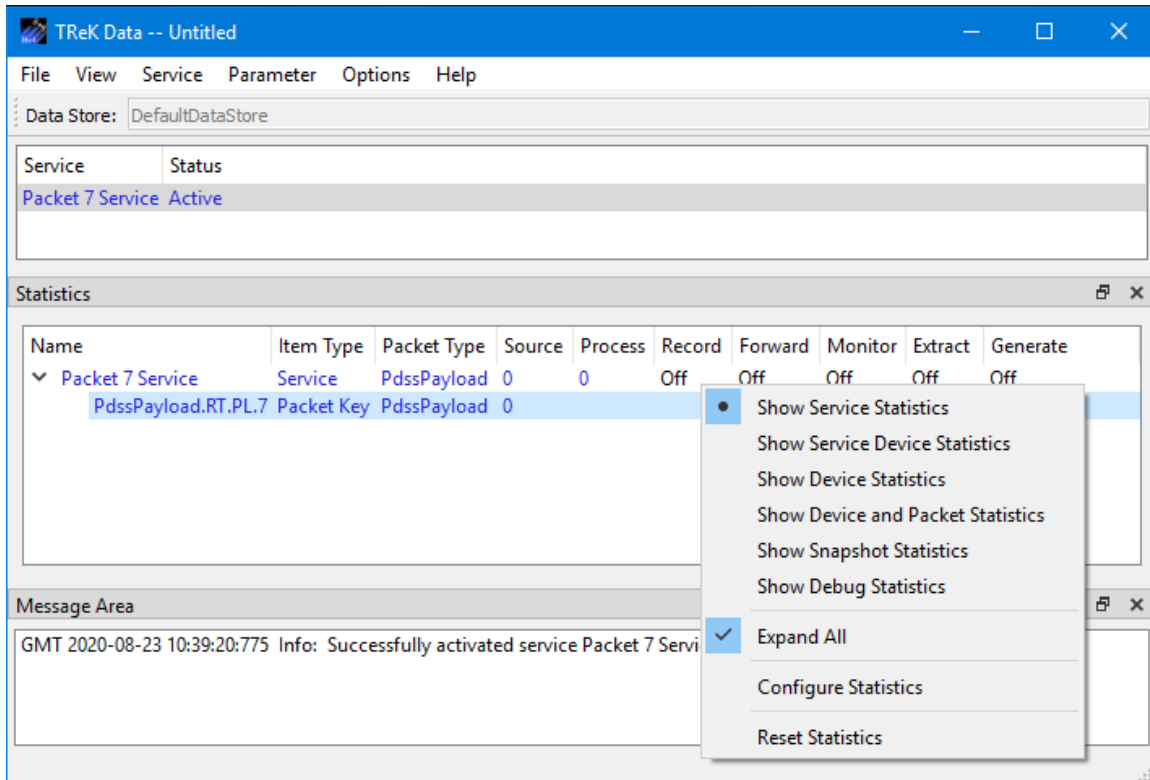**Figure 67 Statistics in the Main Window**

Figure 68 Statistics Dialog

Statistics can be configured to display different views of the statistics information. The view options can be accessed using the Statistics area pop-up menu. The pop-up menu is shown in Figure 69 and can be accessed by clicking the right mouse button in the statistics area.

Figure 69 Statistics Pop-Up Menu

The Statistics pop-up menu has several options. Each is described below:

Show Service Statistics
Service Statistics is the default view. It is shown in Figure 67. This view shows statistics associated with each service in the service list. If the service is configured with the "Packet List" or "Pattern Match Using Packet Type" filter, you will be able to expand the service item to see information about arriving packets.

Show Service Device Statistics
Service Device Statistics shows the same information as Service Statistics with the addition of devices that are used by the service. Figure 70 shows an example of a service configured to receive data, process data, and record data. In this view you can see the service is configured to receive two packets (Packet 7 and Packet 24) on a unicast socket, process the data, and record the data. Figure 71 shows the view after some data has arrived. Each row is described below:

Packet 7 Service: Indicates that two packets arrived on the source socket. One packet was processed and one packet was recorded.

PdssPayload.RT.PL.24: Indicates that no packets arrived that matched this packet key.

PdssPaload.RT.PL.7: Indicates that one packet arrived that matched this packet key.

PdssPayload.RT.UDSM.7: Indicates that you received a UDSM packet for packet 7. While this is not a packet you are configured to receive and identify, this view will list additional packets received on the source socket and attempt to identify the packet. Since the Packet 7 Service was configured to receive packets that matched the packet key "PdssPayload.RT.PL.7" the "PdssPayload.RT.UDSM.7" packet was identied since it uses a similar identification scheme but it was not processed or recorded per the service's configuration.

1.1.127.0.0.1.6100.1: Indicates that you received two packets on this unicast socket.

4.Packet 7 ServiceProcessLibrary: This item is a process library device was created behind the scenes to process incoming data. This shows that one packet was processed by the process library device per the service's configuration. Only packets that match the service filter will be passed to library devices created to support service functions.

4.Packet 7 ServiceRecordLibrary: This item is a record library device that was created behind the scenes to record incoming data. This shows that one packet was recorded by the record library device per the service's configuration. Only packets that match the service filter will be passed to library devices created to support service functions.
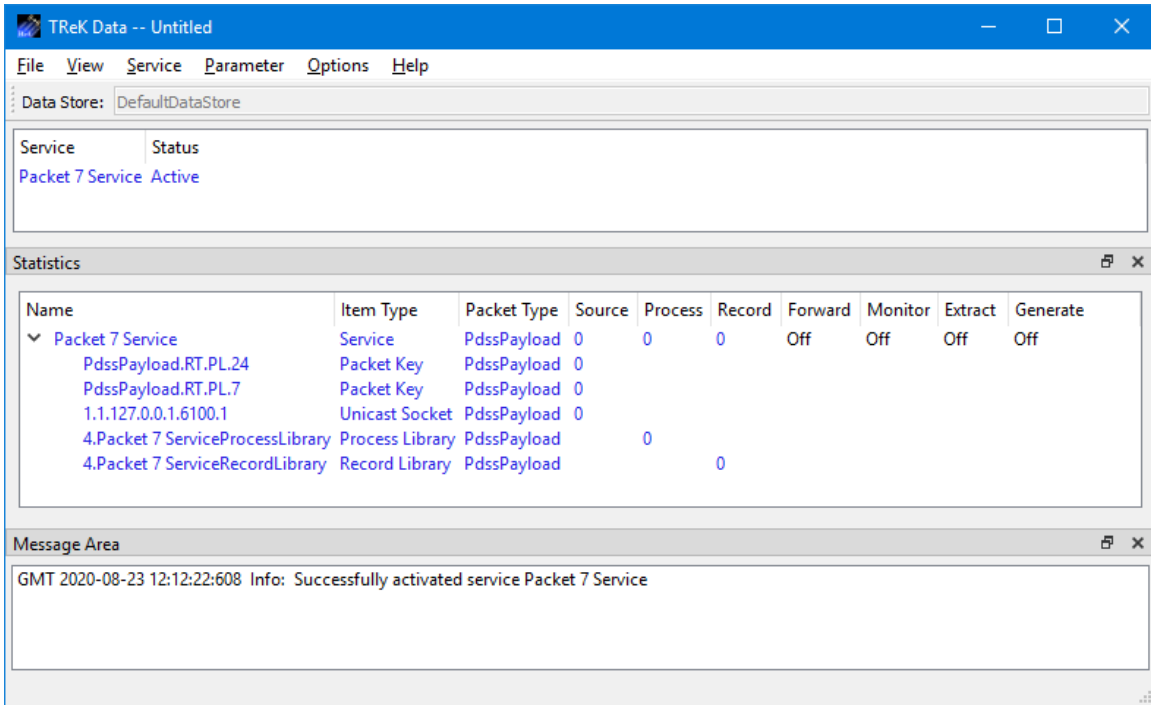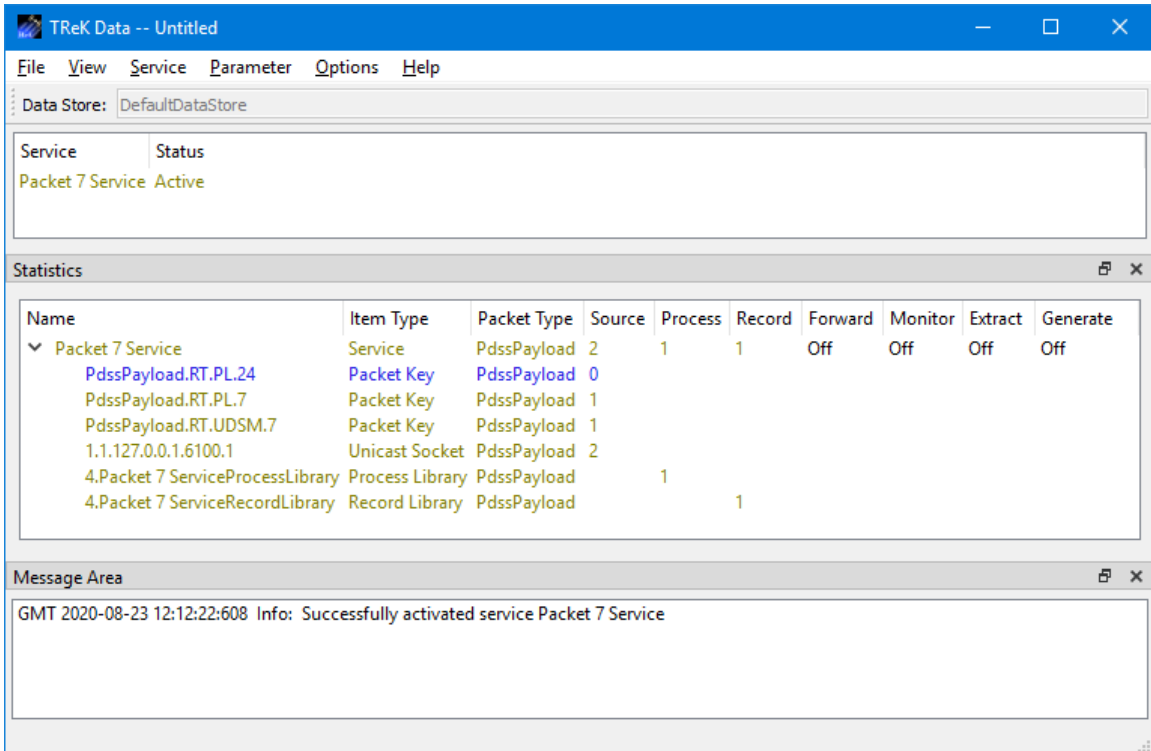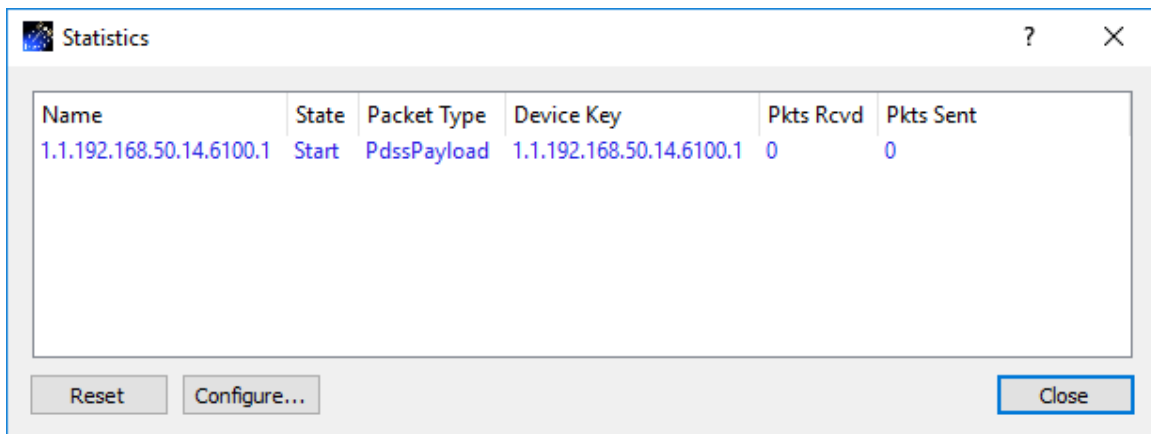
Figure 70 Service Device Statistics

Figure 71 Service Device Statistics After Receiving Data

TREK-USER-0013

Show Device Statistics

Device Statistics displays all the network sockets or devices in use by all active services being used to receive or forward data. When the device is a network socket it will include the IP address and Port. When the device is a library device that performs a specific function such as handling bundle protocol data, the name will reflect the device's function. Figure 72 shows the device statistics view. In this example, there is one network socket displayed. When data is received on this socket the Pkts Rcvd column will update reflecting the number of packets received. If a socket is being used to forward data, the Pkts Sent column will reflect the number of packets sent.

Figure 72 Device Statistics View

Show Device and Packet Statistics

The Device and Packet Statistics option will display both device statistics and packet statistics. Figure 73 shows the device and packet statistics view. In this example, there is one network socket displayed and this device can be expanded to display additional packet statistics. In this view you can see that this device was configured to accept packets with the packet key "PdssPayload.RT.PL.7". When any data is received on this socket the Pkts Rcvd column will update reflecting the number of packets received. The line showing packet statistics will reflect the number of packets received that match the packet key "PdssPayload.RT.PL.7".

86

Figure 73 Device and Packet Statistics

Figure 74 shows a network socket that has received 87 packets and packet statistics for "PdssPayload.RT.PL.7" that has received 76 packets. This indicates that some packets were received on the network socket that did not match the "PdssPayload.RT.PL.7" packet key. This can be helpful in understanding what incoming data you are receiving.

Figure 74 Device Receiving Unexpected Packets

Show Snapshot Statistics

Figure 75 shows the Snapshot view. This view provides a snapshot of the current state of incoming packets. In Figure 75 you can see that two packets are blue and one is green. Blue indicates the software is configured to receive the packets but no packets have been received. Green indicates packets are arriving.
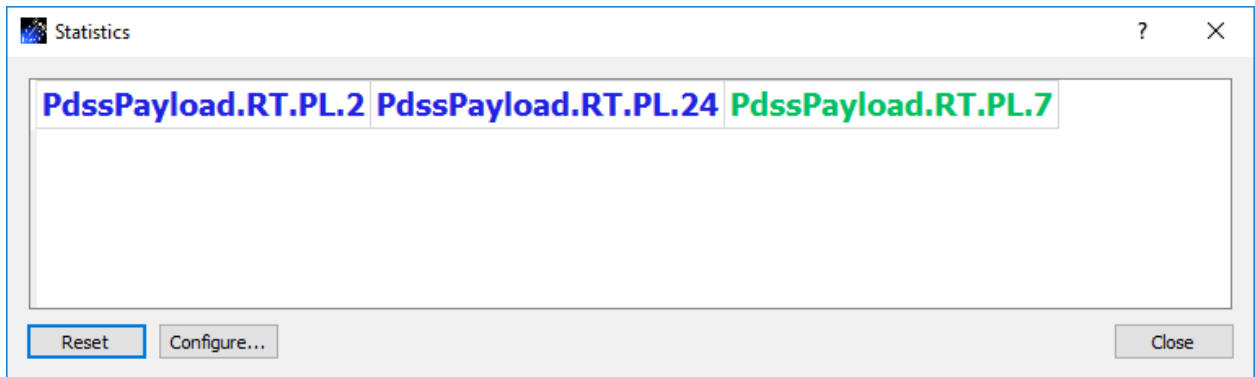
Figure 75 Snapshot Statistics

Show Debug Statistics

The Debug Statistics view shows the most detailed information of all the various views. It shows device statistics and packet statistics associated with each type of function requested (processing, recording, and forwarding) for each active service. In Figure 76 there is one service in the service list. It is named "Packet 7 Service". The statistics dock window has been configured to show the Debug Statistics View. The Packet 7 Service is configured to receive data on IP Address 192.168.50.14 port 6100. The Data Description tab Filter Type was set to 'Packet List' and one packet was listed with packet key "PdssPayload.RT.PL.7" . The Packet 7 Service is configured to process the data received, record the data received, and forward the data received using the UDP protocol. In the statistics area, the line with the name "1.1.192.168.50.14.6100.1" is a network socket that the Packet 7 Service created to receive data using IP Address 192.168.50.14 and port 6100. The line with the name "1.1.192.168.50.14.55551.1" is a network socket that the Packet 7 Service created to forward data using IP Address 192.168.50.14 and port 55551. The line with the name "Packet 7 ServiceProcessLibrary" identifies the processing statistics for the Packet 7 Service. The line with the name "Packet 7 ServiceRecordLibrary" identifies the recording statistics for the Packet 7 Service. The Pkts Rcvd and Pkts Sent columns reflect the associated statistics for each line item. 101 packets were received. 100 packets were sent (forwarded). 100 packets were processed. 100 packets were recorded. You may be wondering why 101 packets were received but only 100 packets were processed, recorded, and forwarded. The answer to this question can be found by expanding the view. The view can be expanded by selecting "Expand All" on the Statistics pop-up menu.
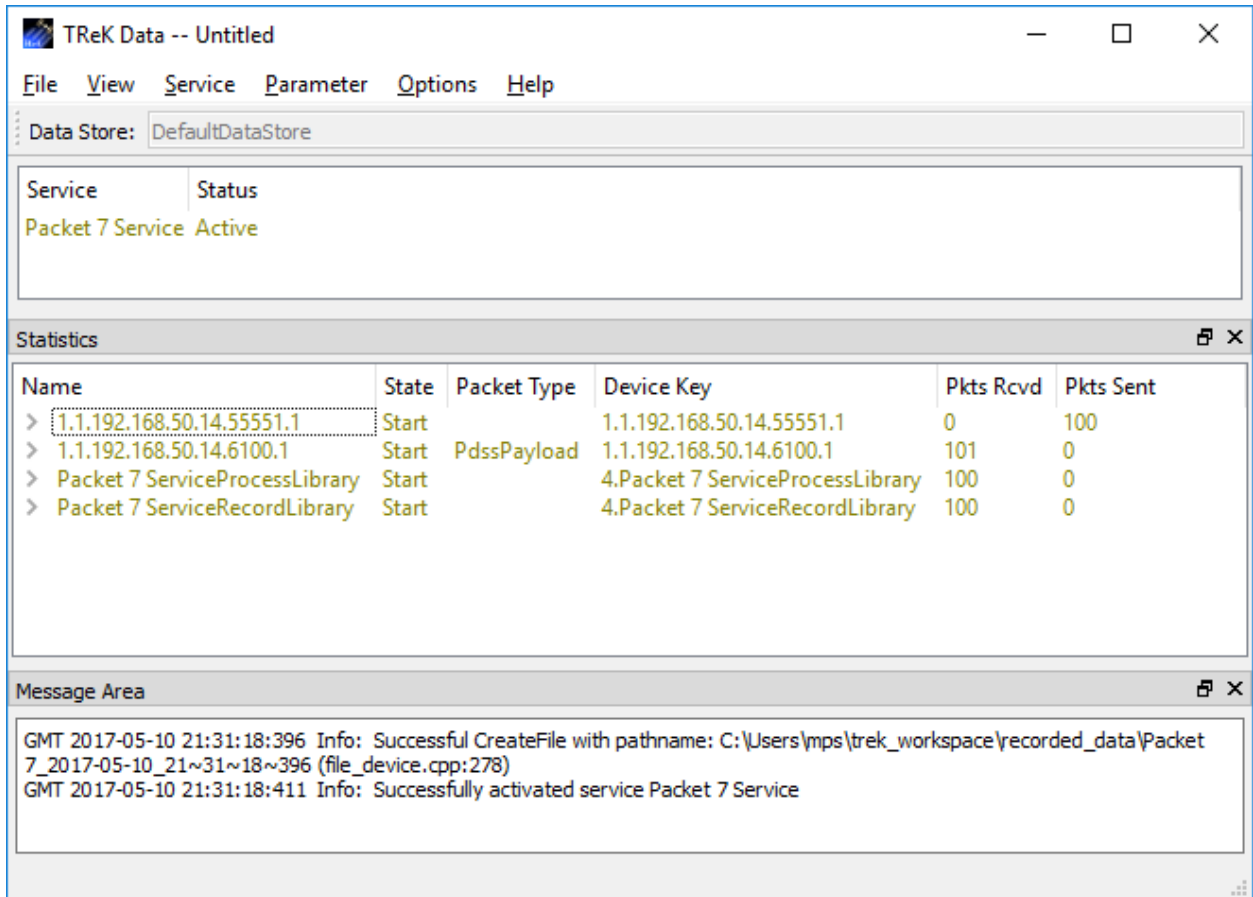
Figure 76 Debug Statistics View for Packet 7 Service

Figure 77 shows the Debug Statistics Expanded View for the Packet 7 Service. Now you can see the packet keys for the packets that were received on the network socket at 192.168.50.14 port 6100. You can see that 100 packets with the packet key "PdssPayload.RT.PL.7" were received and 1 packet with the packet key "PdssPayload.RT.UDSM.7" was received. This solves the mystery of the extra packet. Since the Packet 7 Service was configured to receive packets that matched the packet key "PdssPayload.RT.PL.7" the "PdssPayload.RT.UDSM.7" packet was identified but it was not processed, recorded, or forwarded per the service's configuration.

Figure 77 Debug Statistics Expanded View for Packet 7 Service

Expand All
The Expand All option will expand the Statistics tree to show all items. The Statistics tree will only appear for views that show packet statistics such as the 'Device and Packet Statistics' view and the "Debug Statistics' view.

Configure Statistics
The statistics information displayed can be configured using the Configure Statistics dialog. This dialog can be accessed using the statistics pop-up menu or the Configure button in the Statistics dialog. Detailed information is covered in section 6.7.1.

Reset Statistics
Reset Statistics will reset all statistics in all views to zero.

6.7.1   Configure Statistics Dialog

The Configure Statistics Dialog is context dependent based on the current statistics configuration. It provides the capability to show and hide columns. Each configuration is described below.

Service and Service Device Statistics Configuration
The Configure Statistics Dialog shown in Figure 78 is displayed when the statistics configuration is set to Service Statistics or Service Device Statistics.
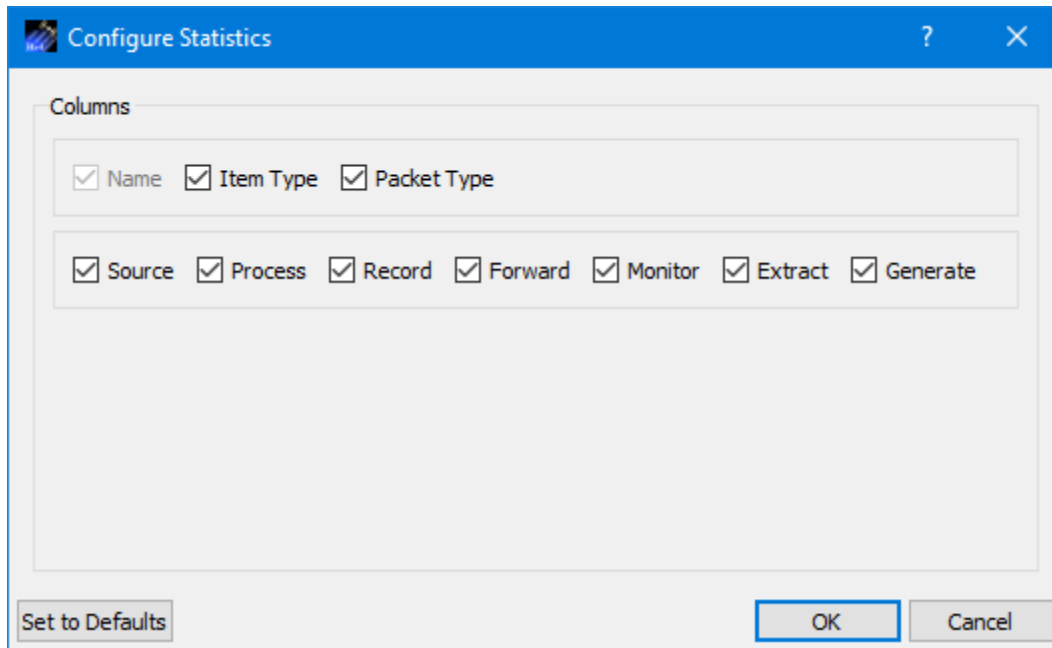
Figure 78 Configure Statistics Dialog (Service and Service Device)

Each field is described below.

Name
Name corresponds to the service in the main window service list.

Item Type
Item Type identifies the type of item for which statistics are being provided. In the Service Statistics view types include Service and Packet Key. In the Service Device Statistics view you will see additional devices such as socket devices and library devices.

Packet Type
Packet Type corresponds to the Packet Type identified on the service's Data Description tab.

Service Function Columns
The Source, Process, Record, Forward, Monitor, Extract, and Generate columns provide statistics associated with specific functions. For example, the Source column indicates

how many packets have been received on the source device (e.g. receive socket) while the Process column indicates how many incoming packets have been processed.

Configure Statistics (Device Statistics, Device and Packet Statistics, Debug Statistics)
The Configure Statistics Dialog shown in Figure 79 is displayed when the statistics configuration is set to Device Statistics, Device and Packet Statistics, or Debug Statistics.
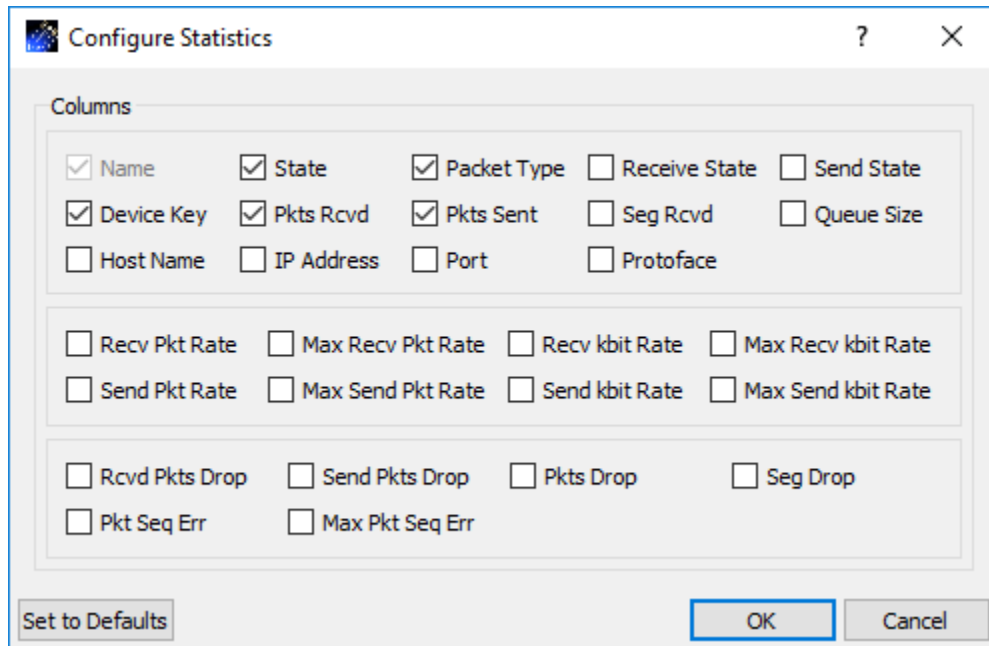
Figure 79 Configure Statistics Dialog (Device, Device and Packet, Debug)

Each field is described below.

Name
Name is a character string that uniquely identifies each device and packet type. The device name is the device key if no device name is provided when the device is created. The packet name is the packet key associated with the packet.

State
State is the current state or condition of a device. Valid states include Start, Stop, Pause, Pulse, Ready and Undefined. If you check the State checkbox, the State column will be displayed.

Packet Type
Packet Type is a character string identifying the configuration of a device's packet header processor. If a device does not have to have an associated packet header processor, the Packet Type column is blank. Packet header processors process individual fields in the packet header producing packet keys. If you check the Packet Type checkbox, the Packet Type column will be displayed.

Receive State
Receive State is the current receive state of an object. Valid receive states include Ready To Receive, Receiving and Not Receiving. If you check the Receive State checkbox, the Receive State column will be displayed.

Send State
Send State is the current receive state of an object. Valid receive states include Ready To Send, Sending and Not Sending. If you check the Send State checkbox, the Send State column will be displayed.

Device Key
Device Key is a character string that uniquely identifies each device. If you check the Device Key checkbox, the Device Key column will be displayed.

Pkts Rcvd
Packets received represents the number of packets received. If you check the Pkts Rcvd checkbox, the Pkts Rcvd column will be displayed.

Pkts Sent
The number of packets sent to a destination. If you check the Pkts Sent checkbox, the Pkts Sent column will be displayed. Pkts Sent is not the same as packets forwarded. Pkts Sent is used to represent the number of packets sent across a socket that is configured to receive and send packets. Pkts Sent never indicates packets forwarded. To see the number of packets forwarded, look at the Pkts Fwd column.

Seg Rcvd
Segments Received represents the number of segments received. This column is only applicable for TCP. If you check the Seg Rcvd checkbox, the Seg Rcvd column will be displayed.

Queue Size
Queue Size is the size of the queue that temporarily buffers packets that are being processed by a device. A device does not have to be associated with a queue. The device's queue size is defined when the device is created. If you check the Queue Size checkbox, the Queue Size column will be displayed.

Host Name
Host Name is a unique identifier that serves as the name of the computer. If you check the Host Name checkbox, the Host Name column will be displayed.

IP Address
IP Address is the IP address of a device if the device is a socket. If you check the IP Address checkbox, the IP Address column will be displayed.

Port
Port is the port number of the device if it is a socket. The port number is a string identifying the type of socket (e.g., client, listener or server) formatted as "c/l/s". If the socket is a client socket then the port number will be followed by two "/" (e.g., 6100//). If the client socket is connected to a listener socket, the listener's port number is also listed (e.g., 6100/5432/). If the socket is a server socket then the client port number that is connected to the server is listed first, followed by two "/" and the server's listener port number (e.g., 6100//7890). If the socket is a listener socket the listener's port number is listed between two "/" (e.g., /5555/). If you check the Port checkbox, the Port column will be displayed.

Protoface
Protoface is the IP transportation protocol, either TCP or UDP, of a socket device. If you check the Protoface checkbox, the Protoface column will be displayed.

Recv Pkt Rate
Receive Packet Rate represents the number of packets received in the last second. If you check the Recv Pkt Rate checkbox, the Recv Pkt Rate column will be displayed.

Max Recv Pkt Rate
Maximum Receive Packet Rate represents the maximum packet rate seen thus far. If you check the Max Recv Pkt Rate checkbox, the Max Recv Pkt Rate column will be displayed.

Recv kbit Rate
Receive kilobit Rate represents the current number of kilobits per second that are being received. If you check the Recv kbit Rate checkbox, the Recv kbit Rate column will be displayed.

Max Recv kbit Rate
Maximum Receive kilobit Rate represents the maximum kilobit rate seen thus far. If you check the Max Recv kbit Rate checkbox, the Max Recv kbit Rate column will be displayed.

Send Pkt Rate
Send Packet Rate represents the number of packets sent in the last second. If you check the Send Pkt Rate checkbox, the Send Pkt Rate column will be displayed.

Max Send Pkt Rate
Maximum Send Packet Rate represents the maximum packet rate sent thus far. If you check the Max Send Pkt Rate checkbox, the Max Send Pkt Rate column will be displayed.

Send kbit Rate
Send kilobit Rate represents the current number of kilobits per second that are being sent. If you check the Send kbit Rate checkbox, the Send kbit Rate column will be displayed.

Max Send kbit Rate
Maximum Send kilobit Rate represents the maximum kilobit rate sent thus far. If you check the Max Send kbit Rate checkbox, the Max Send kbit Rate column will be displayed.

Rcvd Pkts Drop
Received Packets Dropped represents the number of packets that TReK received and then dropped. If you check the Rcvd Pkts Drop checkbox, the Rcvd Pkts Drop column will be displayed.

Send Pkts Drop
Send Packets Dropped represents the number of packets that TReK attempted to send but dropped. If you check the Send Pkts Drop checkbox, the Send Pkts Drop column will be displayed.

Pkts Drop
Packets Dropped represents the number of packets that were dropped because they could not be processed by another device. If you check the Pkts Drop checkbox, the Pkts Drop column will be displayed.

Seg Drop
Segments Dropped represents the number of segments that TReK received and then dropped. This column is only applicable for TCP. If you check the Seg Drop checkbox, the Seg Drop column will be displayed

Pkt Seq Err
Packet Sequence Error represents the number of packet sequence errors that occurred for a packet that is being received. A packet sequence error occurs when a packet arrives out of order (i.e. a packet with a sequence count of six was expected but instead a packet with a sequence count of seven was received). This calculation assumes a zero sequence count implies a sequence count reset and is not considered a packet sequence error. If you check the Pkt Seq Err checkbox, the Pkt Seq Err column will be displayed.

Max Pkt Seq Err
Maximum Packet Sequence Error represents the maximum packet sequence error that occurred for a packet that is being received. TReK determines the maximum packet sequence error by calculating the delta or difference between the expected packet

TREK-USER-0013

sequence count and the actual packet sequence count. This calculation assumes a zero sequence count implies a sequence count reset and is not considered a packet sequence error. If you check the Max Pkt Seq Err checkbox, the Max Pkt Seq Err column will be displayed.

Set To Defaults
Set To Defaults will set all the fields to their default values.

Configure Statistics (Snapshot Statistics)
The Configure Statistics Dialog shown in Figure 80 is displayed when the statistics configuration is set to Snapshot Statistics.
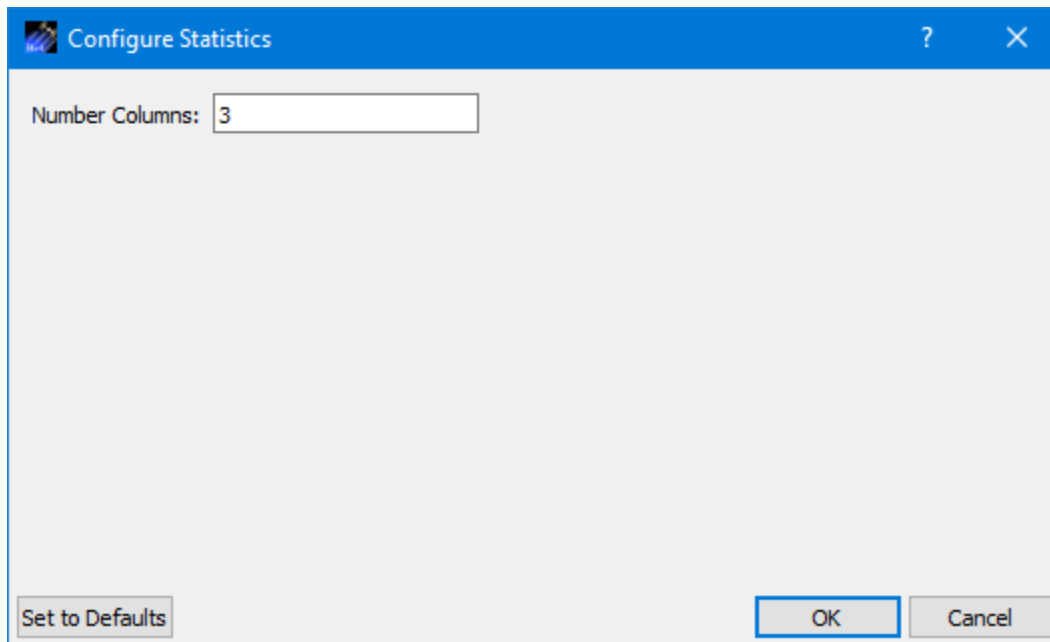
Figure 80 Configure Statistics Dialog (Snapshot)

Each field is described below.

Number Columns
Identifies the number of columns to display in a row.

6.8   Configure Statistics Snapshot Recording Dialog

The Configure Statistics Snapshot Recording dialog is shown in Figure 81. Statistics are generated and captured in memory as you use the application. A snapshot of the statistics can also be recorded to a file by turning on Statistics Snapshot Recording.   When Statistics Snapshot Recording is on, the snapshot is updated once a second with the latest statistics and written to a file. Previous statistics snapshot information is overwritten each time the latest statistics information is written to the file. Statistics are only

available when there are services that are active. If you deactivate all services before turning off Statistics Snapshot Recording, the statistics snapshot file will be empty.
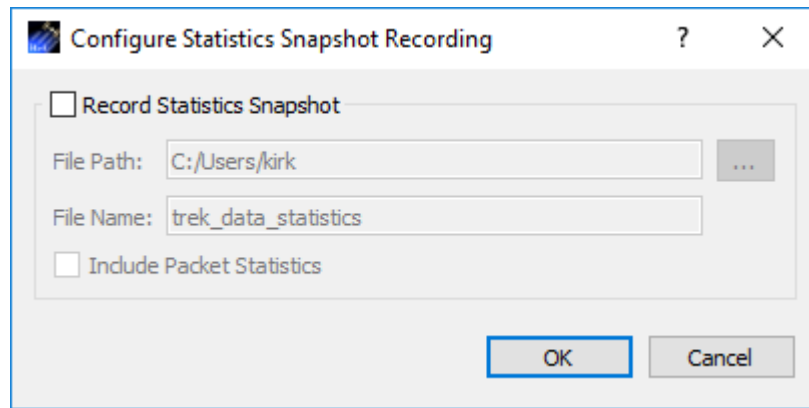
Figure 81 Configure Statistics Snapshot Recording Dialog

Each field is described below:

Record Statistics Snapshot
The Data application provides the capability to write a snapshot of application statistics to a file. If you check Record Statistics Snapshot, a snapshot of the application statistics will be written to the file specified.

File Path
The File Path should contain the absolute path to the directory where the statistics snapshot file should be written.

File Name
The File Name field should contain the name to use for the statistics snapshot file.

Include Packet Statistics
The Include Packet Statistics checkbox specifies whether packet statistics should be written to the file.

6.9   View Packet Dialog

The View Packet Dialog is shown in Figure 82. It is used to view the packet content of any active packet or active device.   The packet content will be displayed in a text/hexadecimal format if packet header information is available. It will be displayed in hexadecimal format if no packet header information is available.
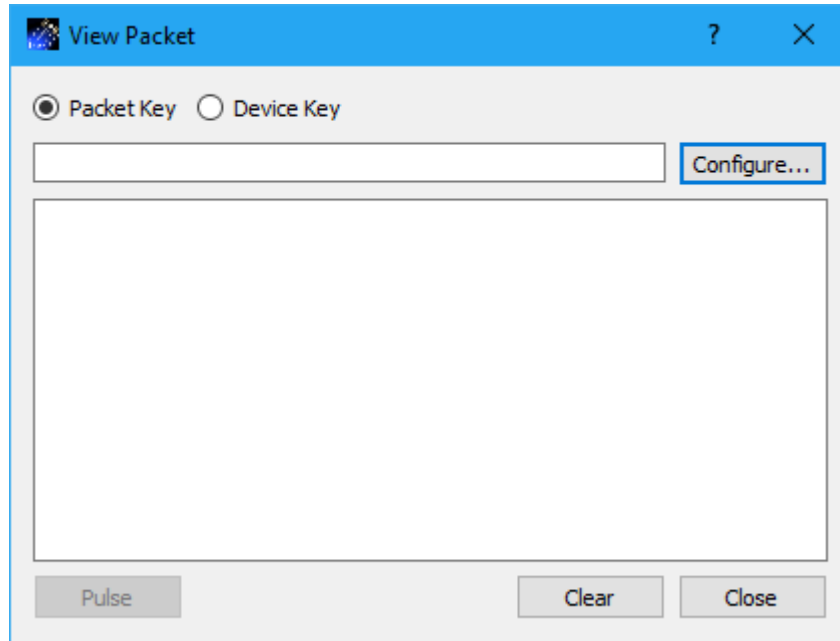
Figure 82 View Packet Dialog

Each field is described below.

Packet Key
The Packet Key radio button indicates you want to identify a packet key to select the packet content you want to view. When the Configure button is pushed the dialog displayed will list available packet keys.

Device Key
The Device Key radio button indicates you want to identify a device key to select the packet content you want to view. When the Configure button is pushed the dialog displayed will list available device keys.

Configure
The Configure button displays the Configure dialog shown in Figure 83. It is used to select a packet key or device key.
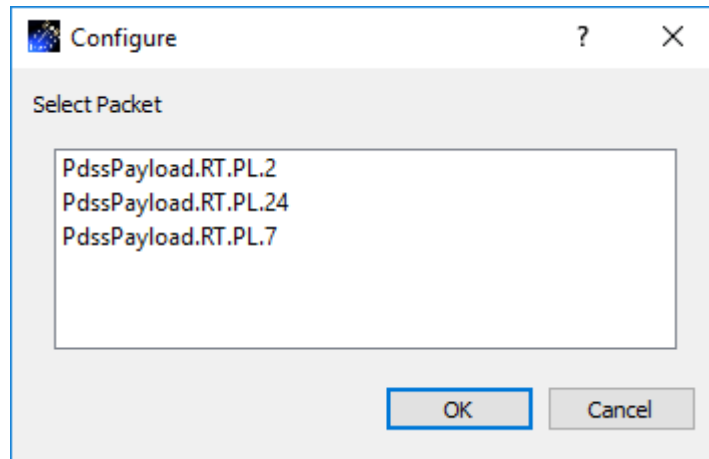
Figure 83 View Configure Dialog

Pulse

The Pulse button is used to request to the content of the latest packet that has arrived. If you push the Pulse button and no data has arrived, nothing will be displayed since there is no data to display. When you push the Pulse button after data has arrived, the packet content will be displayed as shown in Figure 84.
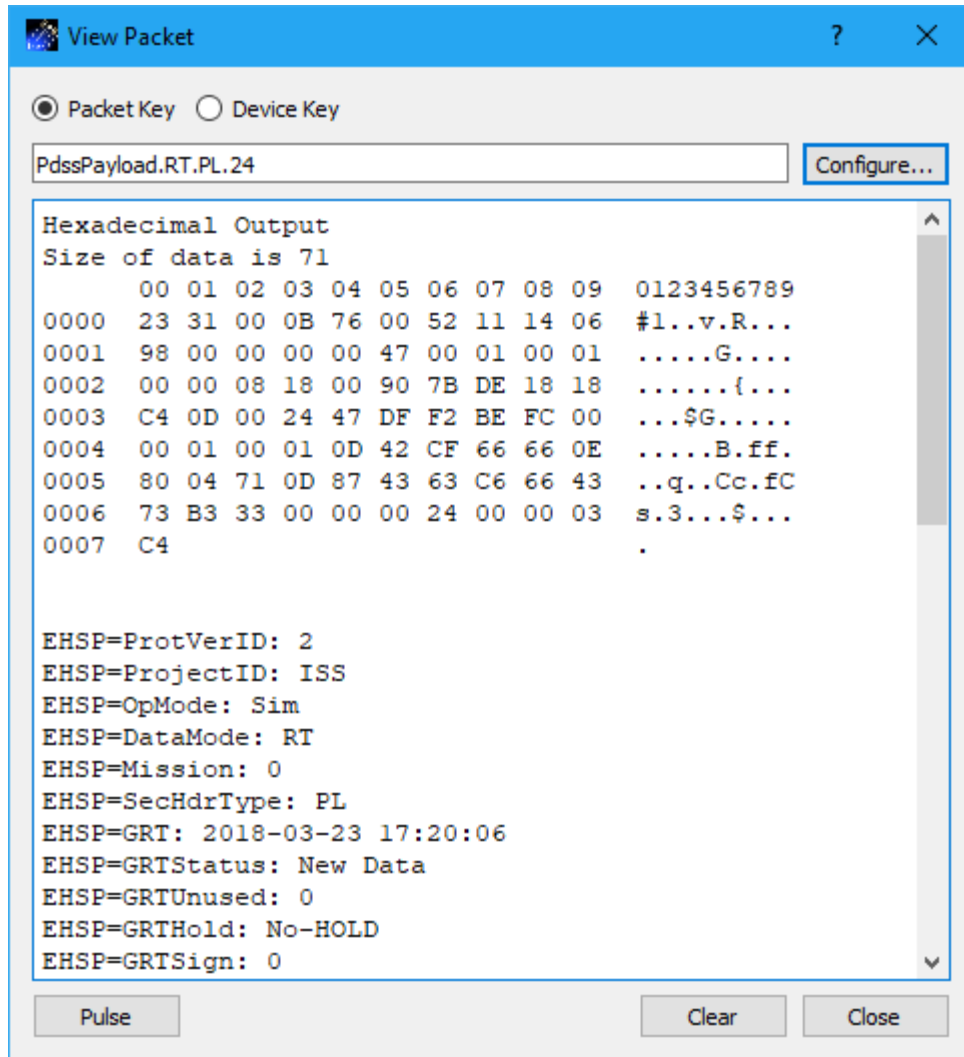
Figure 84 View Packet Example

Clear
The Clear button will clear the packet content area.

Close
The Close button will close the dialog.

6.10 Change Data Store Dialog

The Change Data Store dialog is shown in Figure 85. It is used to change the data store name. None of the services can be active when changing the data store name.

TREK-USER-0013
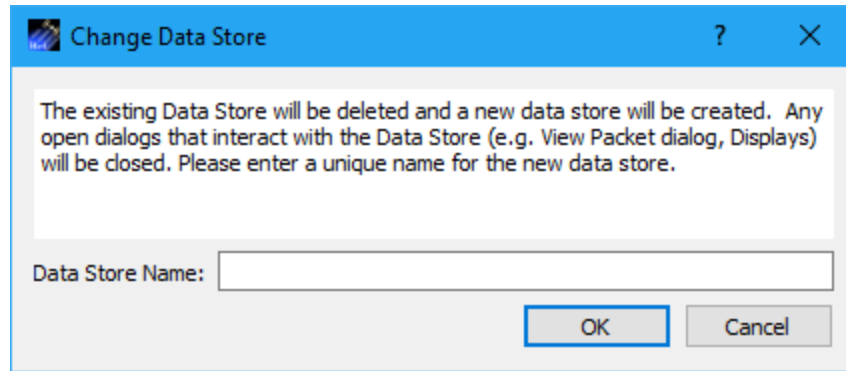
Figure 85 Change Data Store Dialog

Each field is described below.

Data Store Name

This field should contain the name of the data store. This name is important since it is one of the arguments you will pass to TReK API calls when accessing this data store to retrieve data.

6.11 Configure Data Preferences Dialog

The Configure Data Preferences dialog is shown in Figure 86. This dialog is used to configure data preferences.   The Set to Defaults button can be used to reset the properties in this dialog to application defaults.
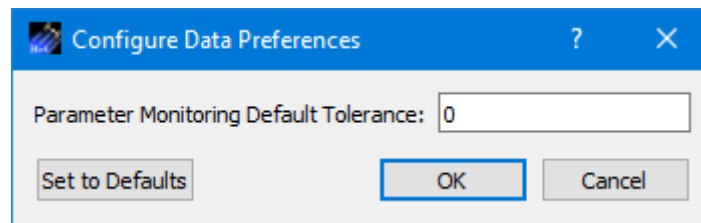
Figure 86 Data Preferences Dialog

Each field is described below.

Parameter Monitoring Default Tolerance
Parameter Monitoring Tolerance provides the capability to control how often a parameter monitor message/alert is generated. The tolerance number indicates how many times the parameter value can go out of limits or expected state contiguously before it triggers a message/alert. When the parameter goes back into a nominal state the tolerance count starts over. The Parameter Monitoring Default Tolerance value will be used when you add a parameter to be monitored.

101

6.12 Manage E-Mail and Text Settings Dialog

The Manage E-Mail and Text Settings Dialog is shown in Figure 87. This dialog provides the capability to manage global e-mail and text settings, application alert settings, e-mail and text dropboxes, and the capability to send an e-mail or text.
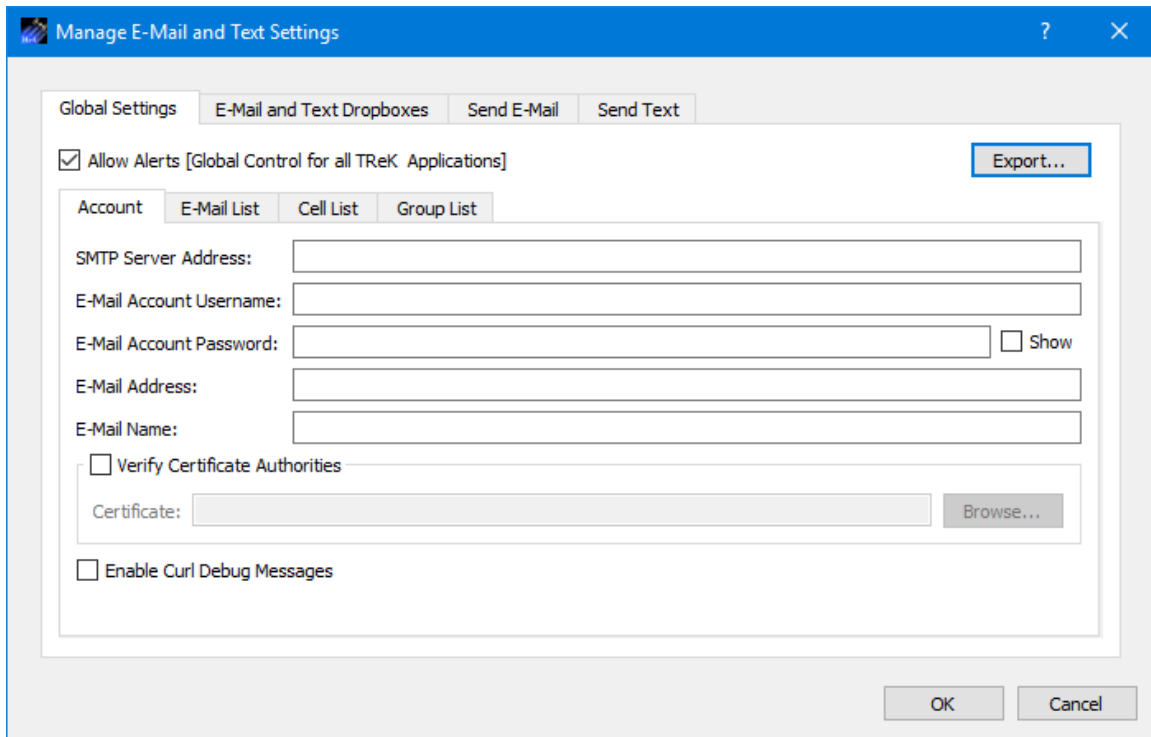
Figure 87 Manage E-Mail and Text Settings Dialog (Global Settings Account Tab)

The TReK software's e-mail and text capability is dependent on libcurl, an open source client-side URL transfer library developed by the cURL project. The libcurl library provides C API functions that configure the library to programmatically establish a secure connection with an email server using a Transport Layer Security (TLS) version 1.3 socket prior to logging into an email account using an email account name and password.

The TReK email and text capability has been successfully tested with the Google Gmail server. It is recommended that users create a new Gmail account and use it to send emails and texts to designated recipients. The TReK software does not support retrieving emails from the user's Gmail account. When creating the Gmail account to send emails and texts you will need to configure your Gmail account to enable two-step verification and you need to generate a Gmail App Password for TReK. Please reference Gmail Help for instructions. The Gmail App Password is used in place of your e-mail account password on the Global Settings Account tab in the "Manage E-Mail and Text Settings"

dialog. TReK recommends only using the Gmail account to send emails and texts using the TReK software. TReK does not recommend using the account to receive emails.

The maximum size of a text message is approximately 900 characters. However, if you send more than 900 characters your message may be broken up during transmission and then concatenated on the recipient's phone. The maximum length of a TReK email message is 65,000 characters or bytes. The maximum length of an email with a file attachment is generally considered to be 10MB (email message size plus file attachment size). Note, file attachments may become much larger than their original file sizes. This is due to the encoding employed by email servers when sending non text-based information.

Global Settings
Global Settings are e-mail and text settings used in all TReK applications. They can be changed in any TReK application with a Manage E-Mail and Text Settings dialog. When you change a setting on the Global Settings tab, it will be changed for all TReK applications. Each Tab is described below.

Allow Alerts
The Allow Alerts Checkbox is a global setting to turn on and off all alerts in all TReK applications. If you turn this checkbox off, no alerts will be generated in any applications.

Export
The Export button provides access to the Export dialog shown Figure 88. This dialog provides the capability to save the settings on the Global Settings tab in a TReK email configuration file that can be used with the TReK E-Mail and Text API. You also have the option to include the dropboxes defined on the E-Mail and Text Dropboxes tab.
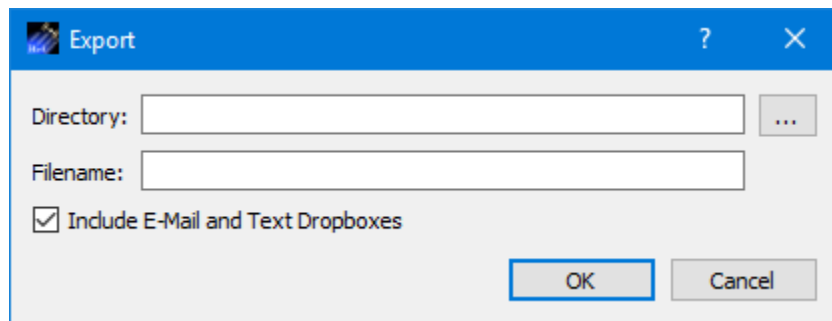
Figure 88 Manage E-Mail and Text Settings (Export Dialog)

Account
In order to use the Alerts capability, you must have a Gmail account. The Gmail account must be configured with two-step verification enabled and you must have a Gmail App Password for TReK. Please reference Gmail Help for instructions. The Account tab is used to enter your Gmail account information. The TReK software only stores account information locally. The account password will be hidden by default and will always be

encrypted when it is stored. Please enter the Gmail App Password you generated for TReK in the E-Mail Account Password field (not your Gmail account password). This password will only be decrypted when it is used communicate with the Gmail server to execute a requested function. An example of account information is shown below.

smtp_server_address: smtp.gmail.com
email_account_username: jane.doe@gmail.com
email_account_password: Gmail App Password for TReK [Hidden unless show
                           checkbox is checked]
email_address: jane.doe@gmail.com
email_name: Jane Doe

The Verify Certificate Authorities checkbox is used to turn on the certificate authority check. If you turn on the certificate authority check, you must provide the complete path to a Certificate file.

The Enable Curl Debug Messages checkbox is used to turn on additional debug messages generated by the curl software library.

E-Mail List
The E-Mail List tab is used to enter e-mail addresses that will be used to populate the e-mail address list that is available when configuring alert functions or sending an e-mail. The E-Mail List tab is shown in Figure 89. The Add button is used to add a row to enter e-mail address information. The Delete button is used to delete a row.
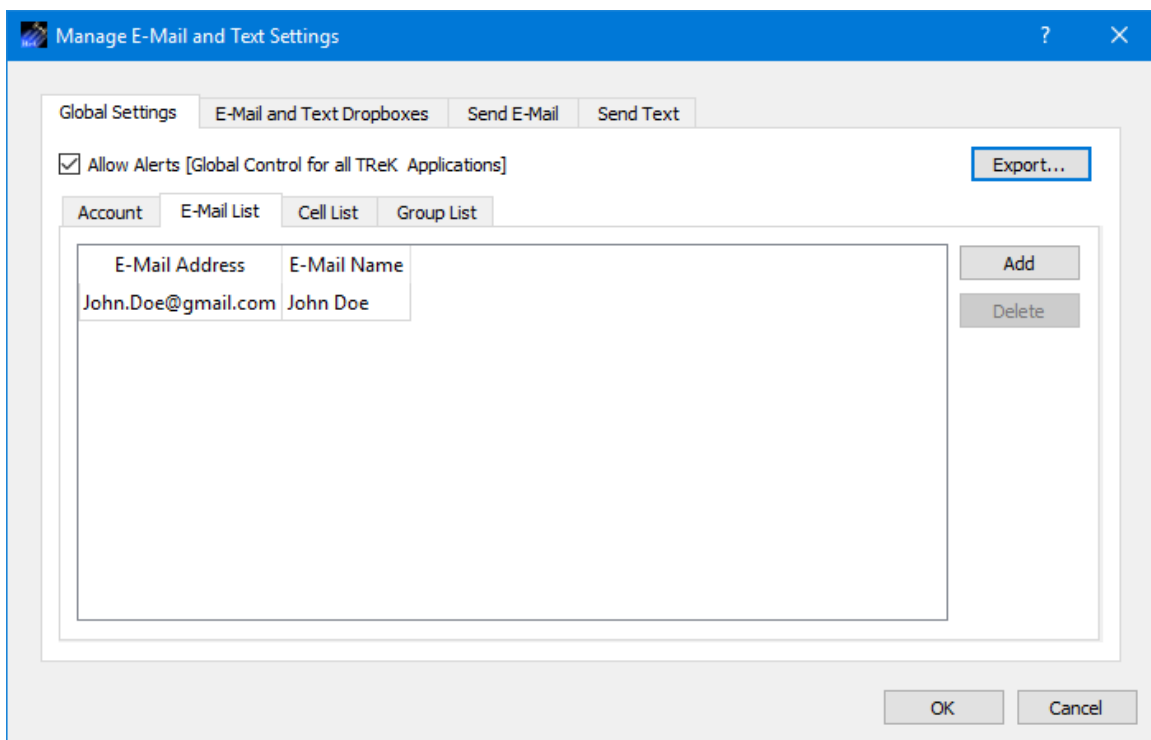
Figure 89 Manage E-Mail and Text Settings Dialog (Global Settings E-Mail List Tab)

Cell List

The Cell List tab is used to enter mobile cell phone numbers that will be used to populate the Cell list that is available when configuring alert functions or sending a text. The Cell List tab is shown in Figure 90. The Add button is used to add a row to enter cell number information. The Delete button is used to delete a row. Cell numbers can be entered with or without dashes. The Set Carrier button is available when a Cell Carrier cell is selected. It is shown in Figure 91 and can be used to select a carrier address. If the carrier address you need is not in the list, you can enter it directly into the cell.

Note: The cell carrier list is populated from a file in the TReK install (config/cell.txt). If you wish to edit the file and make a custom list of carriers to be displayed in the dialog, copy the cell.txt file to the root directory of the TReK workspace and make your changes. If a cell.txt file exists in the root directory of the TReK workspace, it will be used instead of the one available in the install.
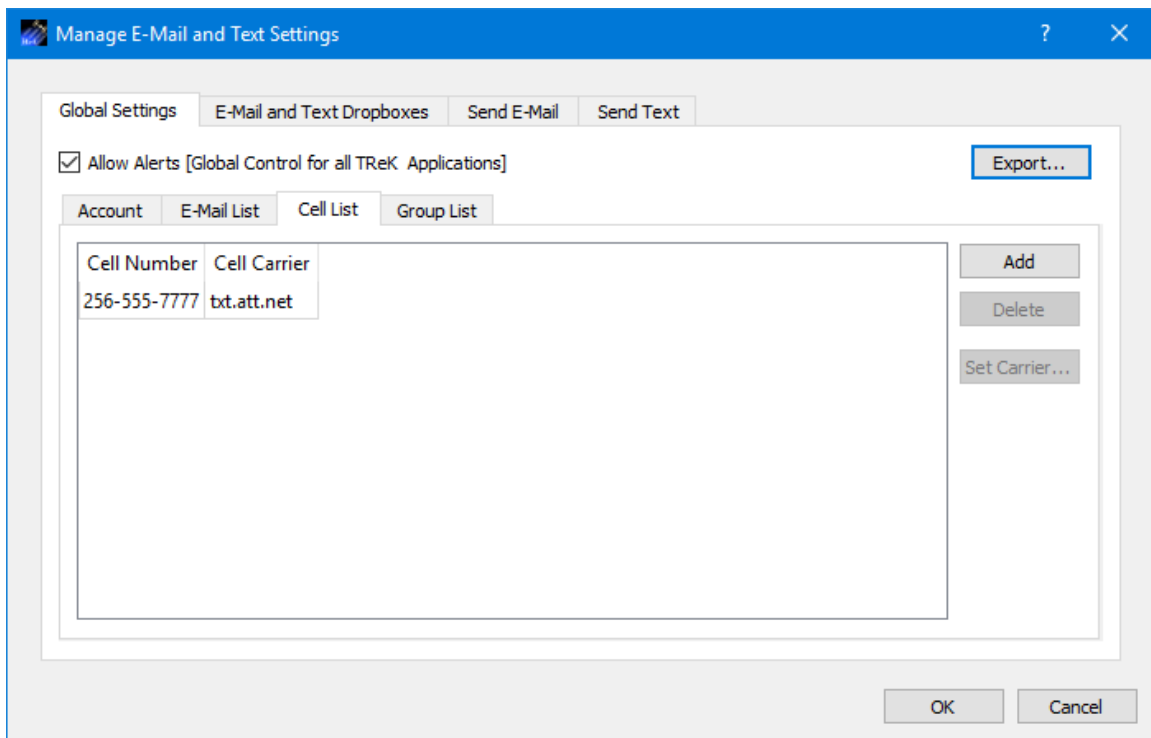
Figure 90 Manage E-Mail and Text Settings Dialog (Global Settings Cell List Tab)
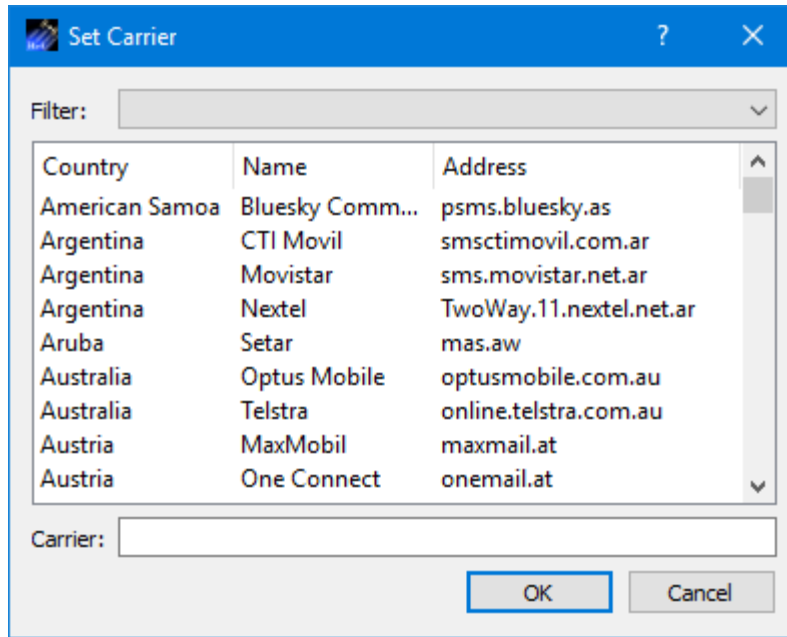
Figure 91 Manage E-Mail and Text Settings (Set Carrier Dialog)

Group List
When configuring an application alert or sending an e-mail or text, you will have the option to identify an e-mail address, a cell phone number, or a group as a recipient. The Group List is shown in Figure 92. You can define zero or more groups. A group can contain e-mail addresses and cell numbers. If you have a group with both e-mail addresses and cell numbers and you send an e-mail to that group, the e-mail generated will only be sent to the e-mail addresses in the group. You can add, modify, and delete a group using the buttons on the right.
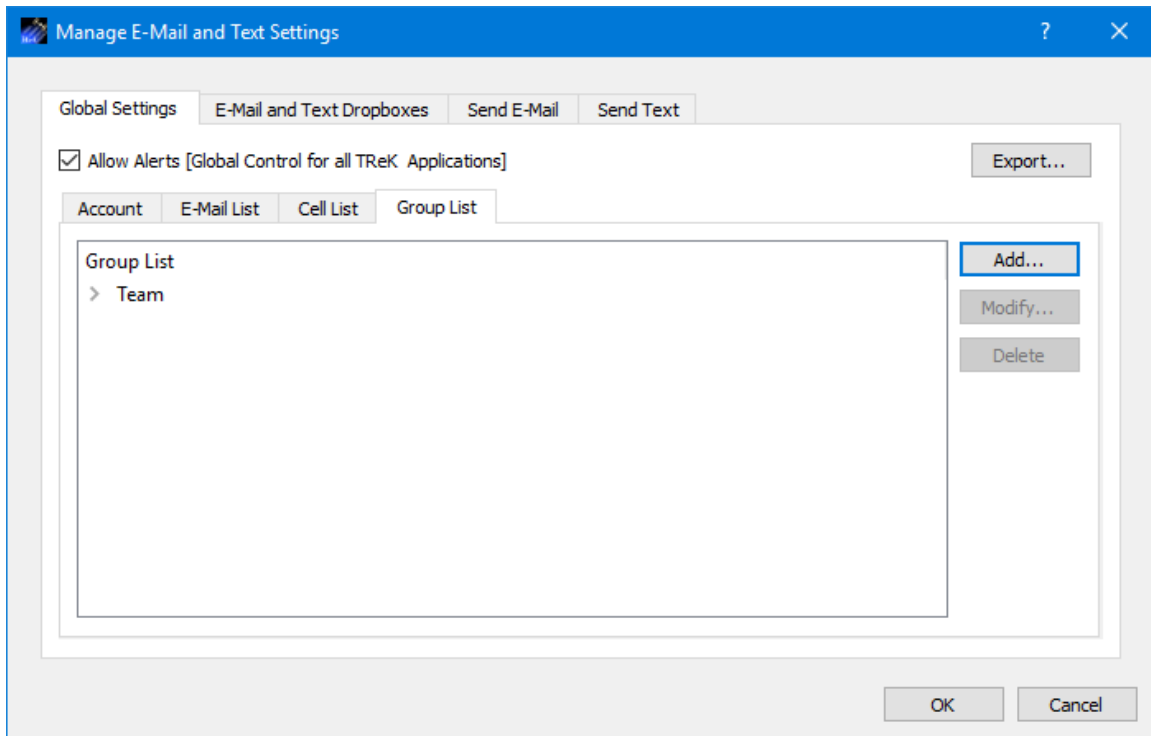
Figure 92 Manage E-Mail and Text Settings Dialog (Global Settings Group List Tab)

The Add button will display the Add Group dialog shown in Figure 93. At the top you can enter a name for the group. On the left you will see all the e-mail addresses and cell numbers you entered on the Global Settings main E-Mail List and Cell List tabs. You can add zero or more e-mail addresses and zero or more cell numbers to a group. To add an e-mail or cell to the group, select the e-mail or cell number on the left and push the Add button to add it to the group. You can use the Delete button to delete a recipient from the group.
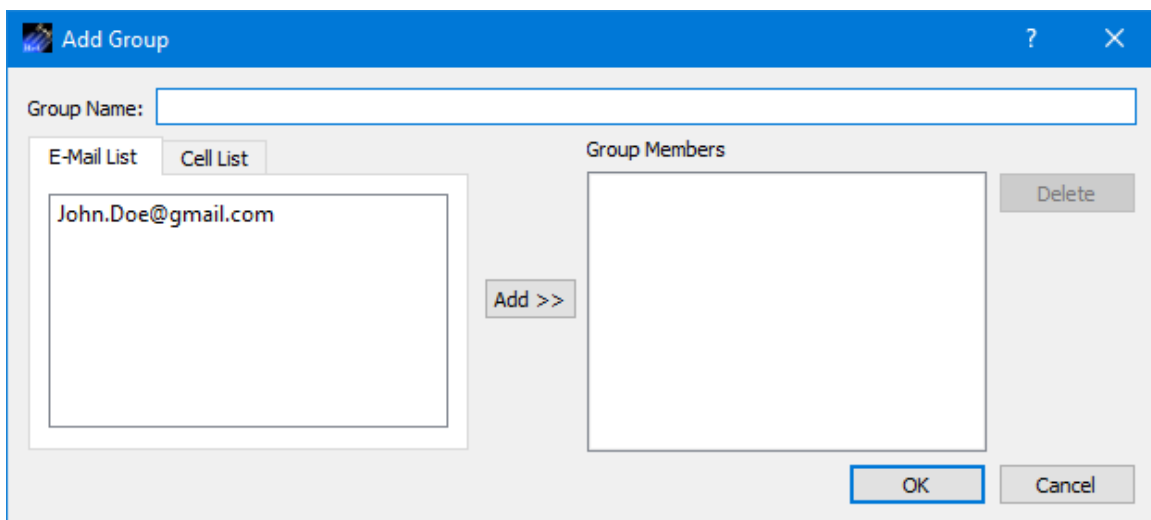
Figure 93 Manage E-Mail and Text Settings (Add Group Dialog)

E-Mail and Text Dropboxes

The E-Mail and Text Dropboxes tab is shown in Figure 94. This tab can be used to define E-Mail and Text Dropboxes. It is important to remember that each E-Mail and Text Dropbox will correspond to a directory on the file system and must be unique. Using a directory for more than one dropbox will result in unexpected behavior. When you define a dropbox using the Manage E-Mail and Text Settings dialog, the dropbox information is automatically saved with that specific application's settings.
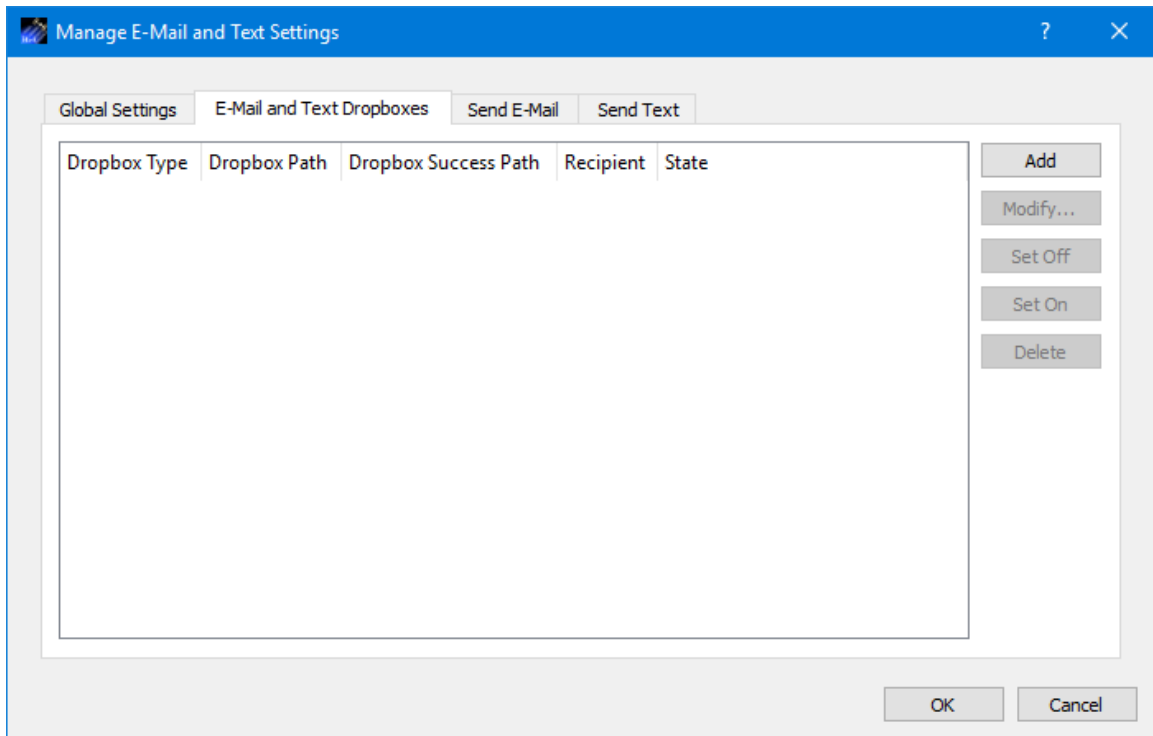
Figure 94 Manage E-Mail and Text Settings Dialog (E-Mail and Text Dropboxes Tab)

Dropbox List

The Dropbox List is used to define zero or more dropboxes. For each dropbox you can define the Dropbox Type, the Dropbox Path, the Dropbox Success Path, a Recipient, and a State. The buttons on the right can be used to add, modify, delete, or change the state of a dropbox. The Add Dropbox dialog is shown in Figure 95.
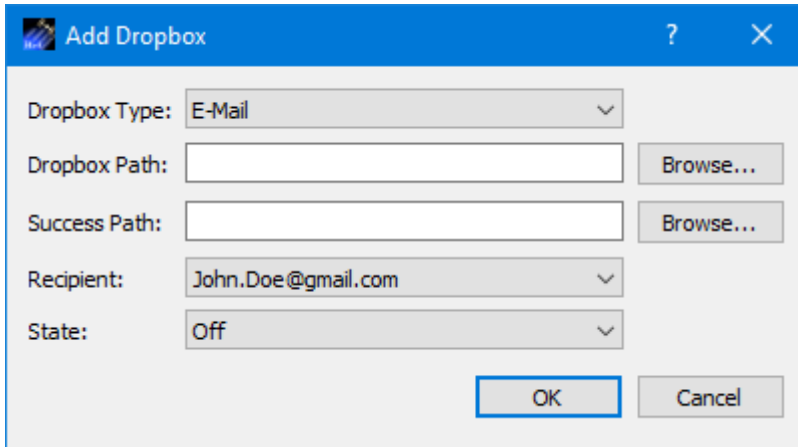
Figure 95 Manage E-Mail and Text Settings (Add Dropbox Dialog)

Dropbox Type
There are three types of dropboxes: E-Mail, E-Mail File, and Text. An E-Mail dropbox will e-mail the contents of a text file placed in the dropbox. An E-Mail File dropbox will e-mail the file placed in the dropbox. A Text dropbox will text the contents of a text file placed in the dropbox. E-Mail and Text dropboxes only support text files. Dropping other file types into these dropboxes will have unexpected results (e.g. send garbage). The E-Mail File dropbox supports many common file types including but not limited to text files, Portable Document Format (PDF) files, and Microsoft Office files. It does not support executable files. The E-Mail File dropbox will generate an error or fail to send file types that are not supported.

Dropbox Path
The Dropbox Path identifies the local directory to be used for the dropbox. The Browse button can be used to select a directory.

Dropbox Success Path
The Dropbox Success Path is optional. If the Dropbox Success Path is defined, the dropbox will move the original file placed in the dropbox to the success directory if and only if the corresponding e-mail or text is successfully delivered to the e-mail server. If the success path is empty, the dropbox will delete the original file placed in the dropbox if and only if the corresponding e-mail or text is successfully delivered to the e-mail server. If the dropbox fails to generate the e-mail or text, the file will be renamed with a time tagged ".droperror" extension and remain in the dropbox. The dropbox will not attempt to generate an e-mail or text for a file with a ".droperror" extension in its filename.

Recipient
The Recipient identifies the designated recipient(s) for the e-mail or text. The Recipient list will be populated with applicable recipients based on the Dropbox Type. For example, if you select E-Mail or E-Mail File in the Type menu, the Recipient list will be populated with e-mails from the E-Mail List Tab and groups with at least one e-mail

address from the Group List Tab. If you select Text in the Type menu, the Recipient list will be populated with cell phone numbers from the Cell List Tab and groups with at least one cell number from the Group List Tab.

State
The state controls whether the dropbox is activated. It can be set to Off or On. If the state is set to Off, the dropbox will not be activated. If the state is set to On, the dropbox will be activated when you push the OK button. If the state is set to On when you exit the application, it will automatically be activated the next time you run the application. If you do not want the dropbox to be activated on application initialization, set the state to Off before exiting the application.

Send E-Mail
The Send E-Mail tab is shown in Figure 96. This tab can be used to send an e-mail if valid information has been entered on the Global Settings tab. Once the To, Subject, optional File (Browse can be used to browse the local disk for a file), and Message information has been entered, press the Send button to send the e-mail. This will initiate a request to send the e-mail. Look at the main window message area for information about whether the e-mail request was successful or encountered any errors.
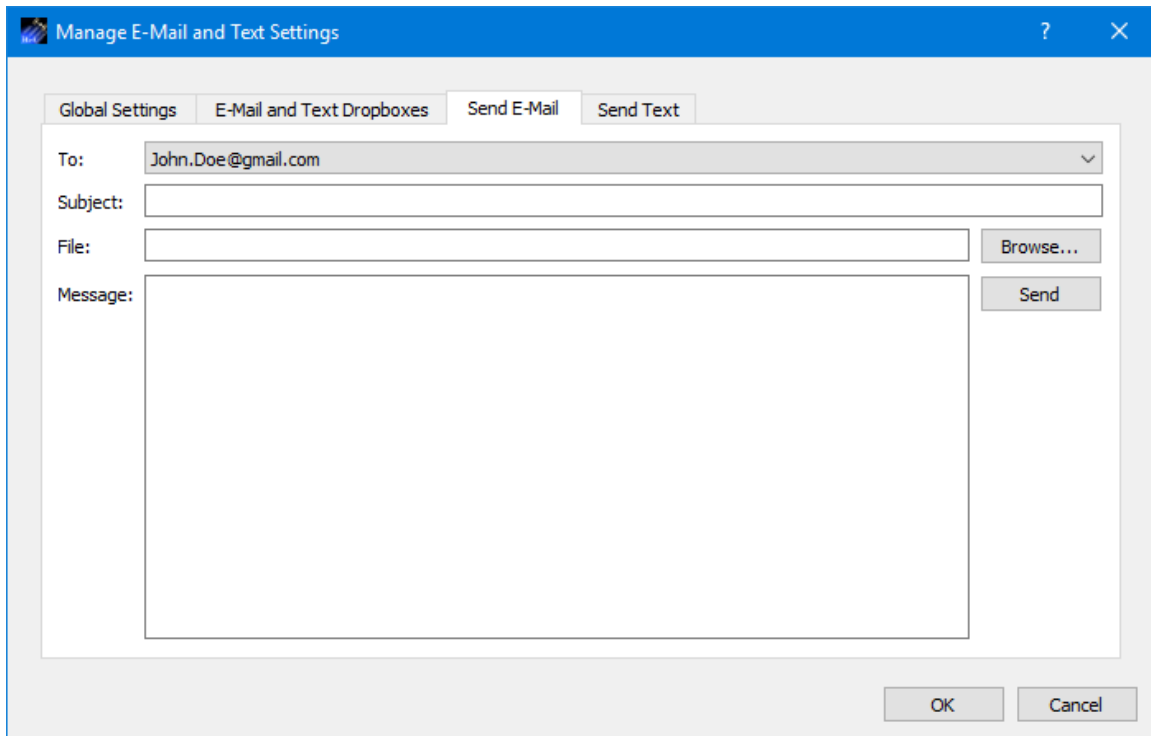
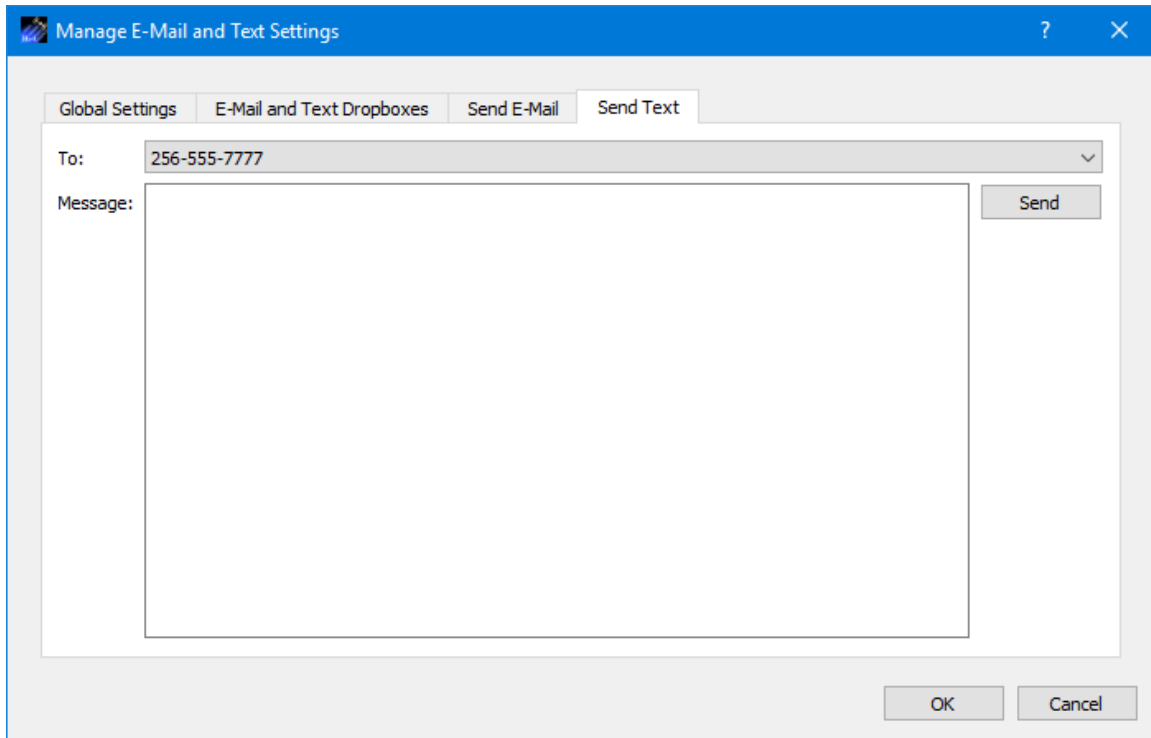**Figure 96 Manage E-Mail and Text Settings Dialog (Send E-Mail Tab)**

Send Text

The Send Text tab is shown in Figure 97. This tab can be used to send a text if valid information has been entered on the Global Settings tab. Once the To and Message information has been entered, press the Send button to send the text. This will initiate a request to send the text. Look at the main window message area for information about whether the text request was successful or encountered any errors.

Figure 97 Manage E-Mail and Text Settings Dialog (Send Text Tab)

6.13 Manage Cryptography Settings Dialog

The Manage Cryptography Settings dialog is shown in Figure 98. It is used to enter cryptography settings. The Cryptography checkbox must be checked and all required cryptography settings must be populated with valid information in order to successfully activate a service that uses cryptography capabilities.
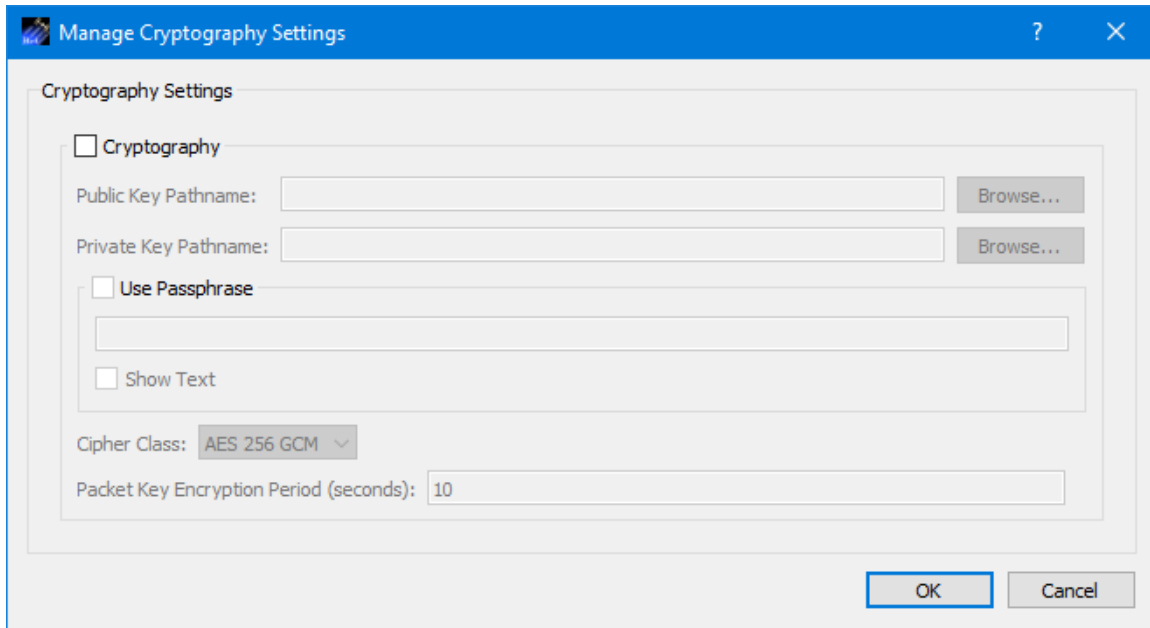
Figure 98 Manage Cryptography Settings Dialog

Each field is described below.

Cryptography Checkbox
The Cryptography checkbox is used to specify you want to use cryptography services.

Public Key Pathname
This is the absolute path for the public key file.

Private Key Pathname
This is the absolute path for the private key file.

Use Passphrase
The Use Passphrase checkbox is used to specify that the private key requires a passphrase. If this box is checked, the passphrase must be entered into the text field. The passphrase text will not be displayed in the clear. If you want to see the text entered in the clear, check the Show Text checkbox. This information is not stored when you save a configuration. You will have to enter it each time you restart the application when using cryptography services.

Show Text
The Show Text checkbox is used to display the passphrase text in the clear.

Cipher Class
This option menu is used to select the cipher class.

Packet Key Encryption Period
The Packet Key Encryption Period is only used when using the Packet encryption feature. As mentioned in the TReK Cryptography Services Tutorial, cryptography keys are used

to generate other keys behind the scenes. One of these keys is called a Cipher Encryption Key (CEK). The Packet Key Encryption period defines how often to generate a new Cipher Encryption Key (CEK) when streaming encrypted data. It can be configured to generate a new CEK for a packet stream once every "x" seconds to support encryption of high rate packet streams. The time period is measured in seconds. If the packet key encryption period is set to zero, the TReK encryption library will generate a new packet encryption key for every packet in the stream. The TReK encryption library can support the encryption of high rate packet streams by setting the packet key encryption period to a non-zero value. The default value is 10 seconds.

6.14 Application Messages

Various types of application messages are generated including information, progress, warning, error, and debug messages. Application messages are stored in memory and written to a temporary log file. The temporary log file is created on application initialization and exists as long as the application is running. It is deleted when you exit the application. The log file is located in the temporary directory provided by the operating system. Only a subset of messages are stored in memory while all messages are written to the temporary log file. The maximum number of application messages stored in memory is controlled by the message storage setting in the Configure Messages dialog. Once the maximum is reached, older messages are deleted to make room for new messages. Setting the maximum value to a large number can impact application performance since it will increase the amount of memory used by the application. Setting this number too low can cause you to miss important messages. The application default was selected to protect against both of these scenarios. Messages stored in memory are displayed in the Main Window Message Area and the Messages dialog. The Messages dialog is shown in Figure 99. The Main Window message area only displays Info, Warning, and Error messages. The Messages dialog displays messages based on the display preferences defined in the Configure Messages dialog. By default, the Messages dialog will display information, progress, warning, and error messages. Columns in the Messages dialog can be sorted by clicking on the column header. The Messages dialog is available from the Options menu.
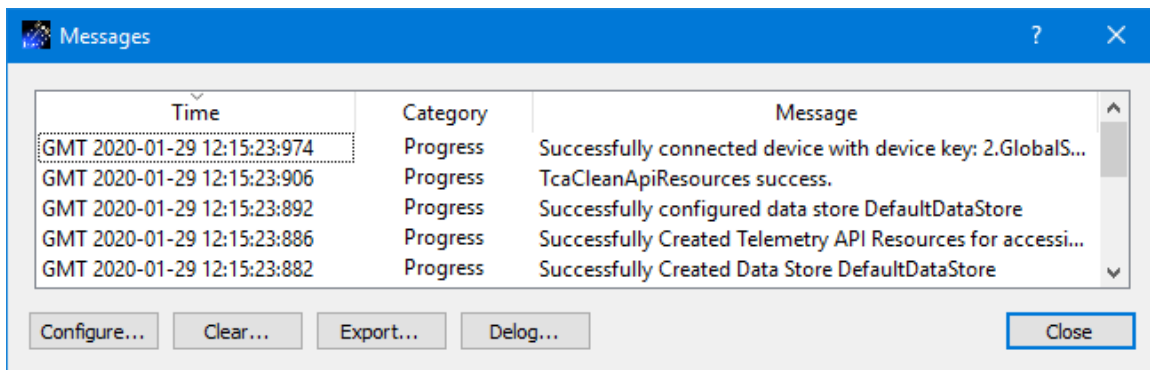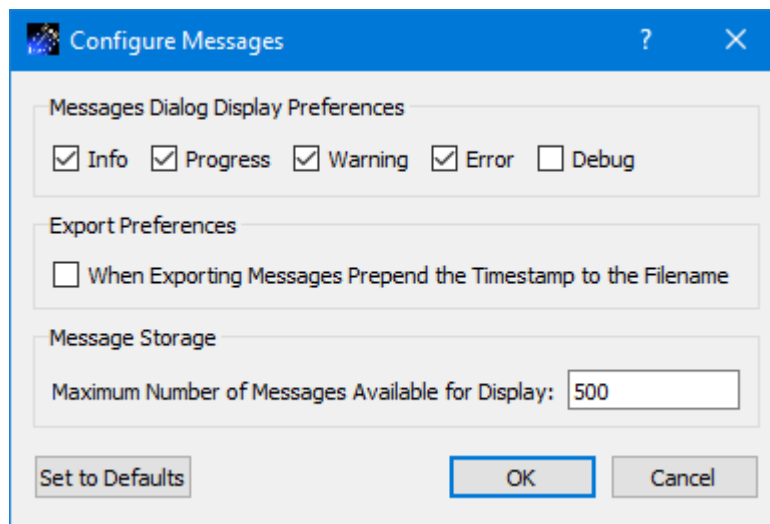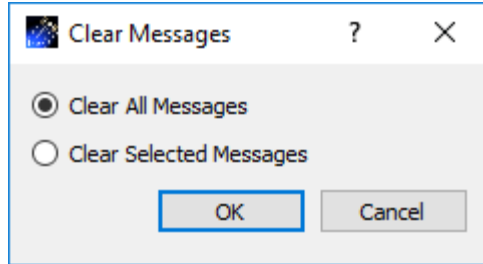

Figure 99 Messages Dialog

Configure

The Configure button provides access to the Configure Messages dialog shown in Figure 100. This dialog provides access to preferences associated with messages. Display preferences can be set to filter the types of messages (category) displayed in the Messages dialog. Export Preferences control how the time tag is added to the filename that is created when messages are exported. See the Export section for details. Message storage defines the maximum number of messages that will be stored in memory while the application is running. Once the maximum is reached, older messages are deleted to make room for new messages. The Set to Defaults button can be used to reset these properties to application defaults.

Figure 100 Configure Messages Dialog

Clear

The Clear button provides access to the Clear Messages dialog shown in Figure 101. This dialog provides two ways to clear application messages stored in memory. You can clear all the messages or clear selected messages. Once you clear messages, the messages are permanently deleted in all views (Main Window Message Area and the Messages dialog).
.

Figure 101 Clear Messages Dialog

Export

The Export button provides the capability to save all the application messages currently in memory to a file. When you push the Export button you will be prompted for a directory and filename. Export will save all messages in memory, not just the messages currently displayed in the Messages dialog (i.e. the Display Preferences are not applied). The name you provide for the file will be modified with a time tag that is added to the filename. The time tag indicates the time the file was closed. The default is to append the time tag to the filename. For example:

Filename Input: messages.txt
Filename Output: messages_2017-05-07_13~03~28.txt

If you would like to prepend the time tag to the filename you can set this preference in the Configure Messages dialog. This would result in the following:

Filename Input: messages.txt
Filename Output: 2017-05-07_13~03~28_messages.txt

Delog

The Delog button provides the capability to save all application messages generated since the application was started. Delog will retrieve the messages from the temporary log file. When you push the Delog button you will be prompted for a directory and filename. A timetag is not applied to the filename.

Filename Input: messages.txt
Filename Output: messages.txt

6.15 Application Configuration File

The Data application saves the following information when you save a configuration:

➢ Contents of the Service List.
➢ Data Store Name.

6.16 Application Settings

The Data application saves application settings each time you exit the application. The next time you run the application, the application will initialize with the previous settings. The following settings are saved:

- ➢ Application Window Size
- ➢ Configure Messages Selections
- ➢ Statistics Configuration
- ➢ E-Mail and Text Settings

6.17 Application Command Line Arguments

The Data application accepts the following command line arguments:

- ➢ trek_data.exe <filename> <passphrase>

filename   to open a configuration file (full path to file)

passphrase   to set the cryptography settings passphrase

A value must be wrapped in double quotes if it contains spaces.

Examples:

- ➢ trek_data.exe "D:/data config.xml"

- ➢ trek_data.exe D:/data_config.xml topsecret

If the configuration is valid, the application will automatically activate all the services in the service list.

7   FAQ and Troubleshooting

This section addresses Frequently Asked Questions and provides tips for troubleshooting common gotchas.

No FAQs Yet.