

TREK

CCSDS FILE DELIVERY PROTOCOL (CFDP)

USER GUIDE



January 2025

Approved for Public Release; Distribution is Unlimited.

TABLE OF CONTENTS

<u>PARAGRAPH</u>	<u>PAGE</u>
1 Welcome.....	1
1.1 Getting Started.....	1
2 Technical Support.....	1
3 Introduction.....	1
4 Overview of the User Interface.....	6
4.1 Main Window.....	6
4.2 Toolbar	8
4.3 Menus.....	8
5 Quick Start Guides	9
5.1 How to Configure the Application for Native CFDP	9
5.2 How to Configure the Application for ION CFDP	9
5.3 How to Configure Application Defaults.....	10
5.4 Drag and Drop Features.....	10
5.5 How to Save a CFDP Command List	10
5.6 How to Start and Stop the CFDP Service	11
5.7 How to Put (Send) a File	11
5.8 How to Get (Retrieve) a File	12
5.9 How to Monitor File Transfers.....	12
5.10 How to Configure the Transactions Area	12
5.11 How to Turn on Message Logging	13
5.12 How to Turn on Statistics Snapshot Recording	13
5.13 How to Turn on Metrics Logging.....	14
5.14 How to Use the CFDP Command Line in Native CFDP Mode	14
5.15 How to Use the CFDP Command Line in ION CFDP Mode	15
6 Details.....	17
6.1 Configuration	18
6.1.1 Native CFDP Tab	18
6.1.2 ION CFDP Tab.....	23
6.1.3 Options Tab	25
6.1.4 Cryptography Tab.....	29
6.1.5 Summary Tab.....	33
6.2 Transactions	33
6.2.1 Configure Transactions Area Dialog	35
6.3 Statistics	36
6.4 Metrics.....	38
6.5 Configure Message Logging	40
6.6 Configure Statistics Snapshot Recording	40
6.7 Manage E-Mail and Text Settings Dialog	41
6.8 Application Messages.....	54
6.9 Application Configuration File.....	57
6.10 Application Settings	57
6.11 Application Command Line Arguments.....	57
7 FAQ and Troubleshooting	58

7.1	Is There an Easy Way to Transfer the Contents of a Directory?	58
7.2	What is class1 and class2?.....	58
7.3	What is “///”?	59
7.4	Source and Destination Constraints.....	59
7.5	I Dropped My File into the List and it Turned Red	59
7.6	My File Starts to Transfer and Then Stops	60
7.7	Transfer Results When Item Exists At Destination.....	60
7.8	Important Things To Know When Using The Get Primitive	60
7.9	How Does Pause Transactions Work?.....	60
7.10	CFDP Transactions in an AOS/LOS Environment.....	61

FIGURES

<u>FIGURE</u>	<u>PAGE</u>
Figure 1 CFDP Sender and Receiver	2
Figure 2 Main Window	6
Figure 3 Configure Dialog (Native CFDP Tab)	19
Figure 4 Configure Dialog (ION CFDP Tab)	23
Figure 5 Configure Dialog (Options Tab)	25
Figure 6 Configure Dialog (Cryptography Tab)	29
Figure 7 Configure Packet Encryption and Time Authentication Dialog	30
Figure 8 Encrypt Dropbox	32
Figure 9 Encrypt Dropbox	33
Figure 10 CFDP Dropbox	33
Figure 11 Decrypt Dropbox	33
Figure 12 Summary Tab	33
Figure 13 Configure Transactions Area Dialog	35
Figure 14 Configure Message Logging Dialog	40
Figure 15 Configure Statistics Snapshot Recording Dialog	41
Figure 16 Manage E-Mail and Text Settings Dialog (Global Settings Account Tab)	42
Figure 17 Manage E-Mail and Text Settings (Export Dialog)	43
Figure 18 Manage E-Mail and Text Settings Dialog (Global Settings E-Mail List Tab)	44
Figure 19 Manage E-Mail and Text Settings Dialog (Global Settings Cell List Tab)	45
Figure 20 Manage E-Mail and Text Settings (Set Carrier Dialog)	46
Figure 21 Manage E-Mail and Text Settings Dialog (Global Settings Group List Tab)	47
Figure 22 Manage E-Mail and Text Settings (Add Group Dialog)	47
Figure 23 Manage E-Mail and Text Settings Dialog (Application Alerts Tab)	48
Figure 24 Manage E-Mail and Text Settings (Add Alert Dialog)	49
Figure 25 Manage E-Mail and Text Settings Dialog (E-Mail and Text Dropboxes Tab)	51
Figure 26 Manage E-Mail and Text Settings (Add Dropbox Dialog)	52
Figure 27 Manage E-Mail and Text Settings Dialog (Send E-Mail Tab)	53
Figure 28 Manage E-Mail and Text Settings Dialog (Send Text Tab)	54
Figure 29 Messages Dialog	55
Figure 30 Configure Messages Dialog	56
Figure 31 Clear Messages Dialog	56

TABLES

<u>TABLE</u>	<u>PAGE</u>
Table 1 ION CFDP Transmission Properties	3
Table 2 CFDP Directives.....	4
Table 3 CFDP Directives Source/Destination Requirements	5
Table 4 CFDP Directives (ION Mode).....	16
Table 5 CFDP Directives Source/Destination Requirements (ION Mode)	17

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 CFDP application provides the capability to transfer files using the Consultative Committee for Space Data Systems (CCSDS) File Delivery Protocol (CFDP).

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:

E-Mail: trek.help@nasa.gov

Messages sent to this address are automatically forwarded to the TReK team.

The HOSC Help Desk (256-544-5066) can provide assistance as needed and is available 24x7.

3 Introduction

The TReK CFDP application provides the capability to transfer files using the Consultative Committee for Space Data Systems (CCSDS) File Delivery Protocol (CFDP).

The CCSDS File Delivery Protocol (CFDP) was developed by the Consultative Committee for Space Data Systems (CCSDS). Official specifications are contained in a CCSDS document called the CFDP Blue Book (available at www.ccsds.org). The CFDP protocol provides reliable transfer of files from one computer to another and has been designed to work well over space links. It can be used to perform space to ground, ground to space, space to space, and ground to ground file transfers.

CFDP requires a sender and a receiver. The sender and receiver must be configured and running at the same time to perform a file transfer. Each party is referred to as an “Entity”. The sender is an entity and the receiver is an entity. Each “Entity” must have a unique Entity ID. For example:



Figure 1 CFDP Sender and Receiver

To move a file from one computer to another, you will enter one or more CFDP Commands (primitives) to indicate the action to be taken.

The TReK CFDP application provides support for CFDP using the following modes:

- Native CFDP or CFDP over User Datagram Protocol (UDP) using a Goddard Space Flight Center (GSFC) CFDP library that performs the CFDP work.
- ION CFDP or CFDP over Bundle Protocol (BP) using the Jet Propulsion Lab (JPL) Interplanetary Overlay Network (ION) Delay Tolerant Networking software. In the ION CFDP configuration, the TReK CFDP application communicates with the ION software which performs the CFDP work.

There are differences in capabilities and syntax between the CFDP Native mode and the ION CFDP mode. These differences are summarized below.

Native CFDP Configuration

The syntax of a primitive is as follows:

[CFDP Directive] [Transmission] [source-path] [remote-EID] [destination-path]

Native CFDP Example: `put class2 "D:\file1.txt" 2 "/home/username/file1.txt"`

The TReK CFDP application currently supports multiple CFDP Directives defined below.

Valid Transmission values are class1 or class2. Class1 does not guarantee reliable delivery of the file to the destination. Class2 does ensure reliable delivery.

The file you want to transfer is considered the "Source" and the location it should be transferred to is considered the "Destination".

When entering a Source or Destination in a CFDP command line, it must be encapsulated in double quotes.

ION CFDP Configuration

The syntax of a primitive is as follows:

[CFDP Directive] [Transmission] [source-path] [remote-EID] [destination-path]

ION CFDP Example: `put //// "D:\file1.txt" 2 "/home/username/file1.txt"`

The TReK CFDP application currently supports multiple CFDP Directives for both Native and ION CFDP modes. These are defined in the CFDP Directives section below.

The Transmission entry for ION CFDP is composed of five properties. Once these properties are configured, a “////” string is used to indicate that the pre-configured values should be used. The “////” nomenclature is shorthand notation for the following combination of values:

Lifespan/Bundle Protocol Class of Service/Expedited Priority Ordinal/Transmission Mode/Criticality

When the values are empty it indicates that pre-configured values should be used for these properties.

A summary of the ION CFDP Transmission properties is provided below in Table 1. For details, please reference section 6.1.2.

Property	Description
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.
Bundle Protocol Class of Service	The Bundle Protocol Class of Service defines the transmission priority of outbound bundles from three ION priority queues corresponding to bulk, standard, and expedited priorities. 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.
Expedited Priority Ordinal	The expedited priority ordinal is only associated with the expedited priority class of service.
Transmission Mode	The transmission mode defines the reliability of bundle delivery to a destination. The three transmission modes supported are best effort, assured, and assured with custody transfer.
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.

Table 1 ION CFDP Transmission Properties

CFDP Directives

The TReK CFDP application currently supports multiple CFDP Directives for all CFDP modes. This includes get and put, multiple filestore directives, and the message directive. These are defined in Table 2 below:

Directive	Description
append_file ²	Append a file at the remote entity to another file at the remote entity.
bit_rate ³	Changes the aggregate file transfer bit rate, in real time, for local or remote entities hosting a TReK implementation of Native CFDP. The “affected EID” may be the local entity ID or a remote entity ID. The "bit_rate" primitive is delivered to a remote entity in the form of a TReK CFDP message.
close_rec_file ³⁴	Send a directive to a TReK Record library to close one or all open record files. If the record file name is not included in the primitive, all open record files associated with the TReK Record library are closed. The TReK Record library automatically opens a new record file after it closes a current record file. The “affected EID” may be the local entity ID or a remote entity ID. The "close_rec_file" directive is delivered to a remote entity in the form of a TReK CFDP message.
create_dir ²	Create a directory at the remote entity.
create_file ²	Create an empty file at the remote entity.
delete_file ²	Delete a file at the remote entity. Will fail if file does not exist.
deny_dir ²	Delete a directory at the remote entity. (like <i>remove_dir</i> , but does not fail if the directory does not exist. Directory must be empty.)
deny_file ²	Delete a file at the remote entity. (like <i>delete_file</i> , but does not fail if the file does not exist)
get ¹	Copy one file from the remote entity to the local entity. (File cannot be empty.)
message ²	Send a text string to the remote entity.
put	Copy a file from the local entity to the remote entity. (File cannot be empty.)
remove_dir ²	Delete a directory at the remote entity (directory must be empty).
rename_file ²	Rename a file at the remote entity.
replace_file ²	Replace a file (contents) at the remote entity with another file (contents) at the remote entity.

Table 2 CFDP Directives

¹ – Not supported in all CFDP implementations. Requires TReK on send and receive side.

² – Not supported in modes using the GSFC library unless it has TReK enhancements.

³ – Not a CCSDS standard. Implemented outside of standard.

⁴ – Requires the TReK Record Library.

Some directives only require a Source. The following table describes what is required for Source and Destination for each directive. Name of file, filename, and name of directory refer to an absolute path.

Directive	Source (first file)	Destination (second file)
append_file ²	Name of file whose contents form first part of new file and name of the new file	Name of file whose contents will form second part of new file
bit_rate	Aggregate file transfer bit rate	
close_rec_file ³⁴	Name of the TReK record library device	Name of the TReK record file to close (if not included all record files associated with the record device are closed)
create_dir ²	Name of directory to be created	
create_file ²	Filename to be created	
delete_file ²	Filename to be deleted	
deny_dir ²	Name of directory to be deleted	
deny_file ²	Filename to be deleted	
get ¹	File or directory name of file(s) to retrieve	File or directory name for file(s) retrieved
message ²	Message	
put	File or directory name of file(s) to send	File or directory name for file(s) sent
remove_dir ²	Name of directory to be deleted	
rename_file ²	Old filename	New filename
replace_file ²	Filename whose contents are to be replaced	Filename whose contents will replace the contents of the first filename

Table 3 CFDP Directives Source/Destination Requirements

TReK also provides the capability to create several different types of dropboxes. These include CFDP dropboxes, Fragmentation dropboxes, and Cryptography dropboxes. These dropboxes are available in all CFDP modes. Dropbox configuration parameters include where the dropbox is located and the destination of each file placed in the dropbox. CFDP dropboxes can be used to push files to a remote destination. Fragmentation dropboxes can be used to split a file into smaller fragments and reassemble it, and Cryptography dropboxes can be used to encrypt and decrypt files. Dropboxes can be used together. For example, the CFDP and Fragmentation dropboxes can be used to transfer a very large multi-Gigabyte file in fragments, and the CFDP and Cryptography dropboxes can be used to encrypt a file prior to transferring it using CFDP.

In addition to this application, TReK also includes a CFDP console application and a CFDP library. If you need CFDP functionality onboard a spacecraft consider the TReK CFDP console application. If you need to include CFDP functionality in your own

application, consider the TReK CFDP library. The TReK CFDP library can be used to include CFDP functionality in a ground or flight application.

4 Overview of the User Interface

4.1 Main Window

The main window contains several areas as shown in Figure 2. Each area is a dock window 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.

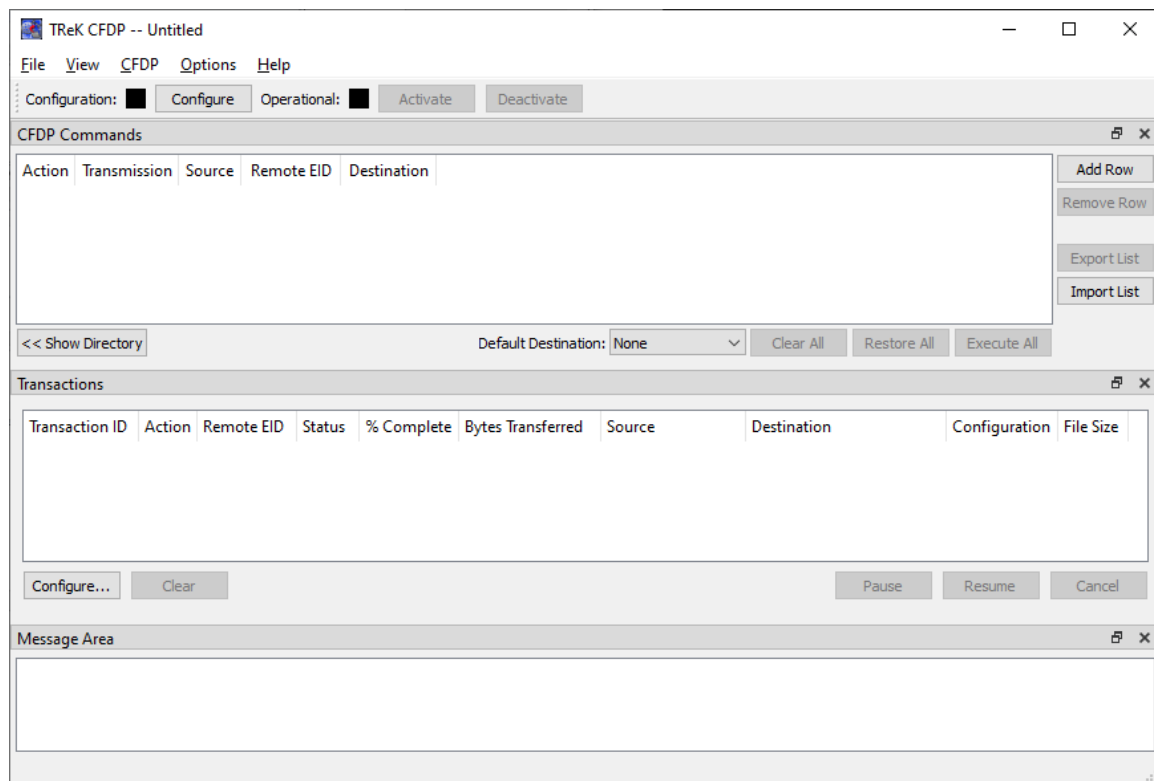


Figure 2 Main Window

Toolbar

The toolbar at the top of the window provides quick access to configure the application and start and stop the CFDP service.

CFDP Commands

The CFDP Commands area provides a way to add and execute one or more CFDP commands (primitives). For example, you can add a “put” command to send a file to a remote entity. The “Show Directory” button provides access to the local file system. Files can be dragged from this view of the local file system or from a file explorer window. Files can also be added by pushing the Add Row button and typing in the file transfer information. To delete a file from the list, put your cursor in the row you would

like to delete and push the Remove Row button. To delete all files in the list, push the Clear All button. The Export List button provides a way to save the list of CFDP Commands in a file. The Import List button provides a way to load a list of CFDP Commands from a file. Each CFDP command entered into the list must include a directive, transmission information, the absolute path of the source file, the Remote Entity ID (Remote EID), and the absolute path of the destination file. To execute all the CFDP commands in the list, push the Execute All button. After you push the Execute All button, the Restore All button can be used to restore the list of commands. The Restore All button will only restore the list of CFDP commands previously sent by pushing the Execute All button. The Default Destination menu can be used to identify a default destination. This can save typing when dragging and dropping files into the list. If the Default Destination is set, the destination selected will automatically be copied into the Destination field when a file is dropped into the list. The Default Destination menu can be populated using the Configure dialog.

Note: When entering Source and Destination information in the CFDP Commands List, do not wrap the Source and Destination information in double quotes as you do on a CFDP Command Line.

Note 2: You can enter the absolute path for a directory in the Source and Destination fields. All the files in the first level of the directory will be transferred. Subdirectories will not be transferred. Each file in the directory will result in the execution of an individual CFDP Command (primitive). Therefore, the transactions area will contain transaction information for each file transferred.

Note 3: There are two types of configuration files for the CFDP application: the CFDP Application Configuration File and the CFDP Commands List file. File/Save/Save As can be used to save an Application Configuration File. The File/Open command provides a way to open an Application Configuration File. The Export List button provides a way to save a CFDP Commands List file. The Import List button provides a way to load a CFDP Commands List file.

Transactions

The Transactions area displays file transfer activity as it is in progress. The Configure button displays the Configure dialog which provides a way to show and hide columns and rearrange the order of the columns. To Clear, Pause, Resume, or Cancel one or more transactions, select the transactions in the list and push the desired button.

Message Area

The Message Area displays important status and error messages. Messages can be cleared using the View menu.

4.2 Toolbar

The toolbar provides visual information about the state of the application and provides access to common application functions.

Configuration Status

When the Configuration status is black, this indicates the application has not been configured. When the Configuration status is green, this indicates the application has been configured and the CFDP service can be activated.

Use the Configure button to access the Configure dialog to configure the application.

Operational Status

When the Operational status is black, this indicates the CFDP service is inactive. When the Operational status is green, this indicates the CFDP service is active and file transfer is supported. The application must be properly configured before the Activate button will be available. The CFDP service must be active before the Deactivate button will be available.

Use the Activate button to activate the CFDP service. This will initiate all internal activities needed to prepare the application to send and receive files. When you activate the CFDP service, you will see activation status messages in the main window message area. If you need to reconfigure the CFDP application, deactivate the CFDP service, and then push the Configure button to reconfigure.

4.3 Menus

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

File Menu

The File menu provides the capability to manage configurations and exit the application.

View Menu

The View menu provides the capability to clear application messages and show and hide different areas in the main window.

CFDP Menu

The CFDP menu provides the capability to configure the application, activate and deactivate the CFDP service, apply Pause, Resume, Cancel, or Clear to all transactions in progress, and Reset Metrics. Reset Metrics can be used to reset all the metrics to 0 in the metrics log file that is currently open. The Metrics log file will only be open when Metrics Logging is on and the CFDP service is active.

Options Menu

The Options menu provides access to the Messages dialog, the Configure Message Logging dialog, the Configure Statistics Snapshot Recording dialog, Reset Statistics, and Manage Email and Text Settings. The Messages dialog displays application messages. The Configure Message Logging dialog provides the capability to configure message logging. The Configure Statistics Snapshot Recording dialog provides the capability to configure statistics snapshot recording. Reset Statistics can be used to reset all the statistics to 0 in the statistics snapshot record file that is currently open. The statistics snapshot record file will only be open when statistics snapshot recording is on. Email and text settings allow control of what messages can be sent when supported events occur.

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 Configure the Application for Native CFDP

The following steps describe the minimum necessary to configure the application. For additional information and details about the Configure dialog, please reference section 6.1.

1. Push the Configure button to display the Configure dialog.
2. Select the Native CFDP radio button.
3. Enter your Entity ID in the Local Entity ID field.
4. Push the + button to create a row to enter Remote Entities information. For each remote entity, enter the Remote Entity ID, the Remote IP Address, and Remote Port. You must enter one or more remote entities.
5. Ensure the CFDP Socket Local IP Address contains a valid local IP address.
6. Push the OK button to save the configuration information and exit the dialog.

If the application is configured correctly, the Configuration status will be green.

5.2 How to Configure the Application for ION CFDP

The following steps describe the minimum necessary to configure the application. For additional information and details about the Configure dialog please reference section 6.1.

1. Push the Configure button to display the Configure dialog.
2. Select the ION CFDP radio button.
3. Modify the ION CFDP properties as needed.
4. Push the OK button to save the configuration information and exit the dialog.

If the application is configured correctly, the Configuration status will be green.

5.3 How to Configure Application Defaults

This section describes how to configure application defaults using the Configure dialog Options tab.

1. Push the Configure button to display the Configure dialog.
2. Go to the Options tab.
3. Enter a Default Remote EID. When you drag and drop files into the “CFDP Commands” list or the CFDP Command field, the default Remote EID entered here will automatically be used as the Remote EID.
4. Enter one or more Default Destination Paths. These paths will be added to the Default Destination menu shown on the main window. The Default Destination menu will also contain a "None" item and a "Same As Source" item. When dragging and dropping files, the item selected in the Default Destination menu will determine what is placed in the Destination field. This will work as follows:
 - If "None" is selected the Destination field will be blank.
 - If "Same As Source" is selected, the Source information will be copied into the Destination field.
 - If a path is selected and you are dragging and dropping a file the path selected on the Default Destination menu will be copied into the Destination field and appended with the Source filename.
 - If a path is selected and you are dragging and dropping a directory the path selected on the Default Destination menu will be copied into the Destination field.
5. Push the OK button to save the configuration information and exit the dialog.

5.4 Drag and Drop Features

Drag and Drop is the fastest way to create a list of CFDP commands to transfer one or more files and/or directories. Simply Drag and Drop one or more files from the Directory area in the CFDP main window (“CFDP Commands” area) or from an Explorer window.

You can optimize your Drag and Drop experience by setting application defaults such as Default Remote EID and Default Destination Paths. To set these defaults see section 5.3.

5.5 How to Save a CFDP Command List

A CFDP Command List can be saved by saving the application configuration using the File menu’s Save/Save As items or by using the Export List button on the Main Window. If the application configuration is saved, the entire application configuration, including the CFDP Command List, will be saved in the configuration file. If the Export List button on the Main Window is used, only the CFDP Command List will be saved in the file.

The File menu's Open menu item can only open a TReK CFDP Application Configuration file.

The Import List button on the Main Window can only be used to read a CFDP Command List file.

5.6 How to Start and Stop the CFDP Service

This section describes how to start and stop the CFDP service.

1. Before the CFDP service can be started, you must configure the application. To learn more about this see section 5.1. The Configure status must be green before you can start the CFDP service.
2. If you are configured for ION CFDP, you must start the ION software before starting the CFDP service.
3. To start the CFDP service, push the Activate button on the toolbar. If this is successful, the Operational status will turn green. When the Operational status is green you can transfer files (send or receive files).
4. To stop the CFDP service, push the Deactivate button.
5. When activating or deactivating, important status and/or error messages will be displayed in the Main Window message area.

5.7 How to Put (Send) a File

This section describes how to put (send) a file. This procedure applies to all CFDP modes.

1. The CFDP application must be configured and the CFDP service must be active.
2. Drag and Drop a file into the "CFDP Commands" area.
3. Ensure the Put, Transmission, Source, Remote EID and Destination information is correct. The Transmission dropdown menu will change based on the CFDP mode selected when configuring. The Source should identify the absolute path of the file to be sent. The Remote EID should identify the target Entity. The Destination should identify where to store the file at the target location.
4. Push the Execute All button.

Note: When entering Source and Destination information in the CFDP Commands List, do not wrap the Source and Destination information in double quotes as you do on a CFDP Command Line.

Note 2: If you want to transfer the contents of a directory, you can enter the absolute path for a directory in the Source and Destination fields. All the files in the first level of the directory will be transferred. Subdirectories will not be transferred. Be sure to include a forward slash '/' at the end of the directory path.

If the text is red, this indicates there is problem with the information provided. Until this is corrected it will not be possible to successfully perform the file transfer.

5.8 How to Get (Retrieve) a File

This section describes how to get (retrieve) a file. This procedure applies to all CFDP modes.

1. The CFDP application must be configured and the CFDP service must be active.
2. Enter information into the “CFDP Commands” area for the file you wish to get. Ensure the Get, Transmission, Source, Remote EID, and Destination information is correct. The Source field should identify the absolute path of the file to be retrieved from the target entity. The Remote EID should identify the target Entity. The Destination field should identify the location (including filename) where you want the file to be stored when retrieved.
3. Push the Execute All button.

Note: When entering Source and Destination information in the CFDP Commands List, do not wrap the Source and Destination information in double quotes as you do on a CFDP Command Line.

Note 2: If you want to transfer the contents of a directory, you can enter the absolute path for a directory in the Source and Destination fields. All the files in the first level of the directory will be transferred. Subdirectories will not be transferred. Be sure to include a forward slash ‘/’ at the end of the directory path.

If the text is red, this indicates there is problem with the information provided. Until this is corrected it will not be possible to successfully perform the file transfer.

5.9 How to Monitor File Transfers

File Transfers can be monitored using the Transactions area in the main window. No transactions will appear until a file transfer is in progress. Transactions will appear when a send or receive is in progress. The details about the file transfer will stay in the Transactions area until they are cleared out.

5.10 How to Configure the Transactions Area

This section describes how to configure the Transactions area.

1. In the Transactions area, push the Configure button to display the Configure Transactions Area dialog.
2. To show or hide columns, select the column(s) you would like to show or hide and push the arrow buttons to move the columns to the Available list or the Columns Showing list as desired.

3. To order the columns, use the Move Up and Move Down buttons to order the list.
The top item will be the left most column.
4. To configure where the most recent transaction appears in the transactions list, use the radio buttons to select whether it goes to the bottom of the list or the top of the list.
5. Push the OK button to save the configuration and exit.

The Transactions list can be safely configured while transactions are in progress. The configuration is saved as part of the application settings.

5.11 How to Turn on Message Logging

This section describes how to turn on message logging. Various types of application messages are generated. As you use the application, messages will be displayed in the main window message area and the Messages dialog. Messages can also be logged to a file by turning on Message Logging. Message Logging will only capture messages generated after Message Logging is turned on. Any messages generated before message logging was turned on will not appear in the message log file.

1. Go to the Options menu and select 'Configure Message Logging'.
2. Check the Log Messages checkbox to turn Message Logging On.
3. Enter a directory for the Log File in the Log File Path field.
4. Enter a name for the Log in the Log File Name field.
5. You can select whether debug messages are written to the Message Log using the Log Debug Messages checkbox.
6. Push OK to save the configuration and exit the Configure Message Logging dialog.

5.12 How to Turn on Statistics Snapshot Recording

This section describes how to turn on statistics snapshot recording. Various types of application statistics are generated. 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 statistic snapshot information is overwritten each time the latest statistics information is written to the file.

1. Go to the Options menu and select 'Configure Statistics Snapshot Recording'.
2. Check the Record Statistics Snapshot checkbox to turn Statistics Snapshot Recording On.
3. Enter a directory for the Statistics Snapshot File in the File Path field.
4. Enter a name for the Statistics Snapshot File in the File Name field.
5. You can select whether packet statistics are written to the Statistics Snapshot file using the Include Packet Statistics checkbox.
6. Push OK to save the configuration and exit the Configure Statistics Snapshot Recording dialog.

5.13 How to Turn on Metrics Logging

This section describes how to turn on metrics logging. Various types of CFDP metrics are generated. Metrics are generated and captured in memory when the CFDP service is active. Metrics can also be logged to a file by turning on Metrics Logging. The Metrics Log file provides a snapshot of the current CFDP metrics starting from the time the CFDP service was activated or the last metrics reset.

1. Go to the CFDP menu and select 'Configure'.
2. In the Configure dialog select the Options tab.
3. Check the Log Metrics checkbox to turn Metrics Logging On.
4. Enter a directory for the Log File in the Log File Path field.
5. Enter a name for the Log in the Log File Name field.
6. Push OK to save the configuration and exit the Configure dialog.

5.14 How to Use the CFDP Command Line in Native CFDP Mode

This section describes how to use the CFDP Command Line when configured for Native CFDP.

1. Go to the View menu and select File Transfer Command Line.
2. Set the Default Destination menu if you would like the application to automatically fill in the default destination when you drop a file.
3. Drag and Drop a file or Type a CFDP Command into the CFDP Command field.

The following syntax must be used:

[CFDP Directive] [Transmission] [source-path] [remote-EID] [destination-path]

You may use one of the directives described below.

You may use class1 or class2 for Class of Service.

All paths must be absolute paths.

Example:

```
put class2 "D:\file1.txt" 2 "C:\myfiles\file1.txt"
```

Note: When entering a Source or Destination in a CFDP command line, it must be encapsulated in double quotes.

The TReK CFDP application currently supports multiple CFDP Directives in the NATIVE CFDP mode. This includes get and put, multiple filestore directives, and the message directive. The CFDP directives are defined in Section 3 in Table 2 and Table 3.

4. Push the Execute button to execute the CFDP command.

The Clear button can be used to clear the CFDP Command field and the Restore button can be used to restore the last command executed.

Note: If you want to transfer the contents of a directory, you can enter the absolute path for a directory in the [source-path] and [destination-path] fields. All the files in the first level of the directory will be transferred. Subdirectories will not be transferred. Be sure to include a forward slash '/' at the end of the directory path.

5.15 How to Use the CFDP Command Line in ION CFDP Mode

This section describes how to use the CFDP Command Line when configured for ION CFDP.

Special Note: ISS Change Request (CR) 13351 Ku-Band Forward Access for Payload Operations only required support for the "Put" directive. Therefore, the Get directive is not supported in all ISS CFDP implementations. It is supported by TReK when both the sender and receiver are TReK CFDP implementations (TReK CFDP application, TReK CFDP console application, or TReK CFDP Library).

1. Go to the View menu and select File Transfer Command Line.
2. Set the Default Destination menu if you would like the application to automatically fill in the default destination when you drop a file.
3. Drag and Drop a file or Type a CFDP Command into the CFDP Command field.

The following syntax must be used:

[CFDP Directive] [Transmission] [source-path] [remote-EID] [destination-path]

ION CFDP Example: put /// "D:\file1.txt" 2 "/home/username/file1.txt"

Note: When entering a Source or Destination in a CFDP command line, it must be encapsulated in double quotes.

The TReK CFDP application currently supports multiple CFDP Directives in the ION CFDP mode. This includes get and put, multiple filestore directives, and the message directive. These are defined Table 4 below.

Directive	Description
append_file	append a file at the remote entity to another file at the remote entity.

Directive	Description
close_rec_file	send a directive to a TReK Record library to close one or all open record files. If the record file name is not included in the primitive, all open record files associated with the TReK Record library are closed. The TReK Record library automatically opens a new record file after it closes a current record file. The “affected EID” may be the local entity ID or a remote entity ID. The "close_rec_file" directive is delivered to a remote entity in the form of a TReK CFDP message.
create_dir	create a directory at the remote entity.
create_file	create an empty file at the remote entity.
delete_file	delete a file at the remote entity.
deny_dir	delete a directory at the remote entity. (like <i>remove_dir</i> , but does not fail if the directory does not exist. Directory must be empty.)
deny_file	delete a file at the remote entity. (like <i>delete_file</i> , but does not fail if the file does not exist)
get	copy one file from the remote entity to the local entity. (File cannot be empty.)
message	send a text string to the remote entity.
put	copy one file from the local entity to the remote entity. (File cannot be empty.)
remove_dir	delete a directory at the remote entity (directory must be empty).
rename_file	rename a file at the remote entity.
replace_file	replace a file (contents) at the remote entity with another file (contents) at the remote entity.

Table 4 CFDP Directives (ION Mode)

Some directives only require a Source. Table 5 describes what is required for Source and Destination for each directive. Name of file, filename, and name of directory refer to an absolute path.

Directive	Source (first file)	Destination (second file)
append_file	name of file whose contents form first part of new file and name of the new file	name of file whose contents will form second part of new file
close_rec_file	name of the TReK record library device	name of the TReK record file to close (if not included all record files associated with the record device are closed)
create_dir	name of directory to be created	
create_file	filename to be created	
delete_file	filename to be deleted	
deny_dir	name of directory to be deleted	
deny_file	filename to be deleted	

Directive	Source (first file)	Destination (second file)
get	file or directory name of file(s) to retrieve	file or directory name for file(s) retrieved
message	message	
put	file or directory name of file(s) to send	file or directory name for file(s) sent
remove_dir	Name of directory to be deleted	
rename_file	old filename	new filename
replace_file	filename whose contents are to be replaced	filename whose contents will replace the contents of the first filename

Table 5 CFDP Directives Source/Destination Requirements (ION Mode)

The Transmission entry for ION CFDP is composed of five properties. Once these properties are configured, a “////” string is used to indicate that the pre-configured values should be used. The “////” nomenclature is shorthand notation for the following combination of values:

Lifespan/Bundle Protocol Class of Service/Expedited Priority Ordinal/Transmission Mode/Criticality

When the values are empty it indicates that pre-configured values should be used for these properties.

The Transmission properties for ION are defined in Section 3 in Table 1.

Example:

```
put //// "D:\file1.txt" 2 "/home/username/file1.txt"
```

Note: When entering a Source or Destination in a CFDP command line, it must be encapsulated in double quotes.

4. Push the Execute button to execute the CFDP command.

The Clear button can be used to clear the CFDP Command field and the Restore button can be used to restore the last command executed.

Note: If you want to transfer the contents of a directory, you can enter the absolute path for a directory in the [source-path] and [destination-path] fields. All the files in the first level of the directory will be transferred. Subdirectories will not be transferred. Be sure to include a forward slash ‘/’ at the end of the directory path.

6 Details

This section covers various application details.

6.1 Configuration

The Configure dialog provides the capability to configure for different CFDP modes:

- Native CFDP – Uses UDP to communicate with another CFDP entity or node.
- ION CFDP – Uses bundle protocol through an ION node to communicate with another CFDP instance.

Each of the above modes will have a tab that provides configuration items unique to the mode. Options and Cryptography tabs are used to configure parameters that are optional and apply to any CFDP mode. The Summary tab provides a summary of all configuration parameters.

6.1.1 Native CFDP Tab

The Native CFDP tab is shown in Figure 3. Each field is described below.

Configure [?] [X]

Configuration: ☒ Native CFDP ☐ ION CFDP

Native CFDP Options Cryptography Summary

Local Entity ID:

Remote Entities

Remote EID	Remote IP Address	Remote Port

[Add] [Delete]

CFDP Socket Local IP Address: [Browse...]

CFDP Socket Local Port:

CFDP Socket Queue Size:

Ack Timeout (seconds):

Ack Limit:

Nak Timeout (seconds):

Nak Limit:

Nak Maximum PDU Packet Size (bytes):

Inactivity Timeout (seconds):

Outgoing File Chunk Size (bytes):

Aggregate File Transfer Rate (bits/sec):

Transaction Cycle Time Interval (milliseconds):

Steps Per Transaction Cycle:

☐ Auto Suspend and Resume

Mode:

Port:

Connection Timeout (seconds):

☒ Automatically Resize Nak Maximum PDU Packet Size if the Nak Packet Times Out

[OK] [Cancel]

Figure 3 Configure Dialog (Native CFDP Tab)

Local Entity ID

This field should contain your Entity ID.

Remote Entities List

The CFDP application provides the capability to communicate with one or more entities when transferring files. The Remote Entities List identifies the Remote Entity ID, the Remote IP Address, and the Remote Port for each remote entity.

CFDP Socket Local IP Address

A UDP socket is created to send and receive CFDP packets. This is the local IP address used for the UDP socket.

CFDP Socket Local Port

A UDP socket is created to send and receive CFDP packets. This is the local port used for the UDP socket.

CFDP Socket Queue Size

The UDP socket that is created to receive CFDP packets may store CFDP packets in a queue prior to the packets being processed by the CFDP library. This queue minimizes the chances of a CFDP packet being dropped due to packet transmission bursts or a temporary CPU spike on the receiving platform. In general, a larger queue size is needed for higher transmission rates. If an unacceptable number of CFDP packet retransmissions is occurring, increasing the queue size or decreasing the file transfer rate may help decrease or eliminate the CFDP packet retransmissions. Minimum value is 0, maximum value is 1,000,000 and the default value is 1000.

Ack Timeout

The CFDP library sends positive acknowledgment on reception of the end-of-file packet and finished packet. This timeout defines the number of seconds the CFDP library will wait for the ACK packet to arrive prior to retransmitting the end-of-file or finished packet. Minimum value is 1, maximum value is 2,147,483,647 and the default value is 15 seconds.

Ack Limit

The ACK limit is the number of ack timeouts that may occur prior to cancelling the CFDP transaction. Minimum value is 1, maximum value is 2,147,483,647 and the default value is 25.

Nak Timeout

The CFDP library sends a NAK packet identifying the CFDP packets that were not received by the CFDP library. This timeout defines the number of seconds the CFDP library will wait for the retransmission of the requested CFDP packets. Minimum value is 1, maximum value is 2,147,483,647 and the default value is 15 seconds.

Nak Limit

The NAK limit is the number of Nak timeouts that may occur prior to cancelling the CFDP transaction. Minimum value is 1, maximum value is 2,147,483,647 and the default value is 100.

Nak Maximum PDU Packet Size

The NAK maximum PDU size is the maximum size of a NAK PDU packet in bytes. If the CFDP transaction identifies multiple gaps in the data transmission, and the gap information cannot fit in a single NAK PDU, the CFDP library will generate multiple NAK PDUs until all the data gaps are filled or the number of NAK PDUs surpasses the NAK limit. Providing a limit on the maximum size of the NAK PDU ensures the PDU will not be dropped because its size exceeds the limits of its transport medium. Minimum value is 50, maximum value is 64042 and the default value is 16000.

Inactivity Timeout

The inactivity timeout is the length of time in seconds that the CFDP library is required to wait between CFDP packet receptions prior to cancelling the CFDP transaction.

Minimum value is 1, maximum value is 2,147,483,647 and the default value is 300 seconds.

Outgoing File Chunk Size

The outgoing file chunk size is the maximum size in bytes of the data zone of the CFDP packets created by the CFDP library. Minimum value is 1, maximum value is 65,200 and the default value is 1300 bytes.

Aggregate File Transfer Rate

The aggregate file transfer rate represents the maximum transmission rate in bits per second of the CFDP packets created by the CFDP library. Minimum value is 1, maximum value is 2,147,483,647 and the default value is 10,000,000 bits/second.

Transaction Cycle Time Interval

The transaction cycle time interval in milliseconds controls the processing rate of CFDP library transactions. Minimizing the cycle time increases the transaction speed or processing rate. The default value is 1 millisecond. The minimum value is 0 milliseconds and the maximum value is 2,147,483,647 milliseconds. This value should only be incremented if CPU usage on the host platform is unexpectedly high while idling or while processing a transaction.

Steps Per Transaction Cycle

The steps per transaction cycle defines how many steps or transaction cycles are performed prior to delaying the prescribed transaction cycle time. Increasing the steps per transaction cycle increases the transaction speed or processing rate. The default value is 10. The minimum value is 1 and the maximum value is 2,147,483,647 milliseconds. This value should be incremented if the CFDP library is not able to achieve the aggregate file transfer rate. This value should be decremented if CPU usage on the host platform is unexpectedly high while idling or while processing a transaction.

Auto Suspend and Resume

The auto suspend and resume checkbox enables the automatic suspension or resumption of all CFDP transactions associated with a remote entity ID when a network connection to that remote entity ID has been lost or found. The TReK CFDP library creates a UDP socket that sends and receives four byte packets to confirm network connectivity. This capability may be used to detect Acquisition Of Signal (AOS) and Loss Of Signal (LOS) events enabling native CFDP to successfully transfer files across multiple AOS/LOS windows without manual intervention. Auto suspend and resume is only supported by the TReK CFDP library. Therefore, the TReK CFDP library software must be running on both the local and remote nodes. The default value is false.

Auto Suspend and Resume Mode

The auto suspend and resume mode identifies the auto suspend and resume relationship between the local node and the remote nodes. The three auto suspend and resume mode parameter values are *Peer to Peer Mode*, *Client or Ground Mode*, and *Server or Flight Mode*. A peer to peer configuration allows all peer to peer nodes to perform CFDP transactions with each other. A client server configuration restricts CFDP transactions. A client may only perform CFDP transactions with a server and a server may only perform CFDP transactions with a client. A client may perform CFDP transactions with multiple server nodes and a server may perform CFDP transactions with multiple client nodes. The four byte connectivity packet is always being transmitted by all nodes in a peer to peer configuration regardless of network connectivity or AOS/LOS periods. In a client/ground and server/flight configuration, the connectivity packet is always being transmitted by the client/ground node, but the server/flight node only transmits the connectivity packet over a confirmed network connection during AOS periods. The default value is *Peer to Peer Mode*.

Auto Suspend and Resume Port

The auto suspend and resume port is used to create the UDP socket that sends and receives the four byte connectivity packet. The default port value is 45600 (minimum value 0 and maximum value 65535).

Auto Suspend and Resume Connection Timeout

The auto suspend and resume connection timeout value is the length of time, in seconds, that must pass between the receipt of connectivity packets before a connection between two entity IDs or nodes is declared lost. Connectivity packets are sent once every half second. Minimum value is 1, maximum value is 2,147,483,647 and the default value is 5.

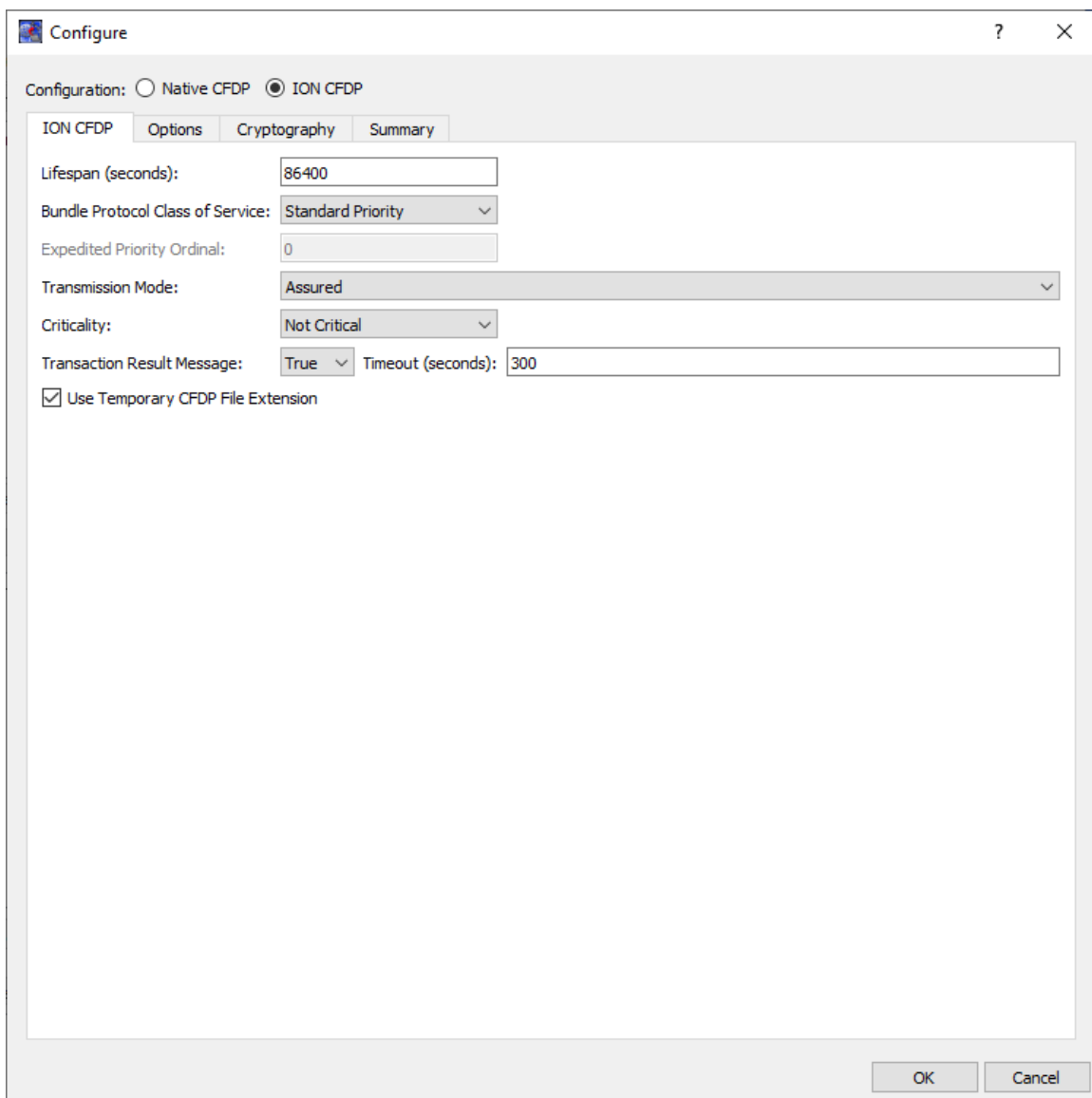
Automatically Resize Nak Maximum PDU Packet Size if the Nak Packet Times Out

The `auto_resize_nak_max_pdu_size` boolean enables the automatic detection of dropped NAK PDUs and the resizing of the NAK maximum PDU packet size. The auto resize capability is advantageous when a CFDP transaction experiences a very large number of dropped packets or data gaps, and the size of the associated NAK PDU packet that is identifying the gaps exceeds the capability of the transport medium (i.e., the NAK PDU packet is heavily fragmented and cannot successfully reach its destination). Under these conditions, CFDP's best option is to reduce the size of the NAK PDU by splitting it up across multiple NAK PDUs. The CFDP auto resize code attempts to determine an acceptable value for the NAK maximum PDU size given the limitations of the transport medium. Also, the understanding that the CFDP library's best performance is achieved by setting the NAK maximum PDU size to the largest value supported by the transport medium. If auto resize of the NAK maximum PDU size has been enabled, and a CFDP transaction determines no NAK PDU packet has been successfully transmitted to its destination, the auto resize code automatically halves the NAK maximum PDU size and retransmits the PDU. The auto resize code continues to halve the NAK maximum PDU size and retransmit a smaller NAK PDU until the NAK PDU reaches its destination, or the NAK maximum PDU size drops below 1280 bytes. Once a NAK PDU packet is successfully transmitted to its destination, the auto resize code is no longer exercised for

that transaction and subsequent dropped NAK PDUs are not resized. Each new CFDP transaction initiates a new instance of the auto resize code. Therefore, the value for the maximum NAK PDU size may be different with different CFDP transactions. The auto resize code initializes the maximum NAK PDU size to the value provided by the `nak_max_pdu_size` CFDP parameter. By resetting the `nak_max_pdu_size` CFDP parameter in the CFDP configuration file or CFDP GUI to the value determined by the auto resize code, the CFDP application may avoid dropping NAK PDU packets that are too large to be supported by the transport medium. The default value is true.

6.1.2 ION CFDP Tab

The ION CFDP tab is shown in Figure 4. Each field is described below.



The screenshot shows a 'Configure' dialog box with a title bar containing a question mark and a close button. Inside the dialog, there are two radio buttons for 'Configuration': 'Native CFDP' and 'ION CFDP'. The 'ION CFDP' radio button is selected. Below the radio buttons are four tabs: 'ION CFDP', 'Options', 'Cryptography', and 'Summary'. The 'ION CFDP' tab is active. The 'ION CFDP' tab contains the following fields:

- 'Lifespan (seconds):' with a text input field containing '86400'.
- 'Bundle Protocol Class of Service:' with a dropdown menu showing 'Standard Priority'.
- 'Expedited Priority Ordinal:' with a text input field containing '0'.
- 'Transmission Mode:' with a dropdown menu showing 'Assured'.
- 'Criticality:' with a dropdown menu showing 'Not Critical'.
- 'Transaction Result Message:' with a dropdown menu showing 'True'.
- 'Timeout (seconds):' with a text input field containing '300'.
- A checkbox labeled 'Use Temporary CFDP File Extension' which is checked.

At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

Figure 4 Configure Dialog (ION CFDP Tab)

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.

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, standard and expedited priorities. The three BP class of service parameter values are *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*.

Transaction Result Message

The support transaction result boolean enables the generation and transmission of a CFDP transaction result message to the source node. If the source node receives the transaction result message within a designated time window, it will update its transaction status with the transaction result (e.g., success or fail). If the support transaction result boolean is set to "true" and the result message is not received within a designated time window, the source node's transaction status is set to "unknown". If this boolean is set to

"false", and the source node did not experience any problems while transmitting the CFDP transaction request, the final transaction status is set to "finished". This capability is only supported by the TReK CFDP library. Therefore, the TReK CFDP library software must be running on both the source and destination nodes. The default value is true.

Transaction Result Message Timeout

The transaction result message timeout is the length of time in seconds that the TReK CFDP library will wait for a transaction result message prior to setting the final status of the transaction to "unknown". Minimum value is 1, maximum value is 2,147,483,647 and the default value is 300.

Use Temporary CFDP File Extension

The Use Temporary CFDP File Extension checkbox corresponds to the "tmp_cfdp" file name extension boolean variable in the TReK CFDP software. If the checkbox is checked, the "tmp_cfdp" file name extension variable will be set to "true". If the checkbox is not checked, the "tmp_cfdp" file name extension variable will be set to "false". The checkbox should be checked if ION is transferring one or more files to a TReK dropbox directory. The most common scenario is if an encryption dropbox has been created and configured to place an encrypted file in an ION CFDP dropbox. If the ION CFDP dropbox is configured to transfer the encrypted file to a decryption dropbox on the destination platform, the "tmp_cfdp" file name extension variable must be "true" on the source or sending platform to properly decrypt the file on the destination platform. If this variable is set to "true", a temporary file name is created for all file transfers by adding a ".tmp_cfdp" file name extension to the original file name on the destination platform. Upon successful completion of the file transfer, the ".tmp_cfdp" extension is removed from the file name on the destination platform. If the destination is a dropbox, the dropbox will use the file name to determine both when the file has completed its transfer and when the file may safely be decrypted by the dropbox. If this variable is set to "false", no temporary file name is used during the file transfer and ION "put" transfers to a TReK dropbox directory are not supported. Native CFDP uses a temporary "tmp_cfdp" file name for all file transfers and does not require this boolean variable when transferring files to a dropbox directory. Setting the "tmp_cfdp" file name extension variable to "true" even if a file transfer destination is not a TReK dropbox directory is supported and does not impact performance. However, the destination platform must be hosting TReK version 5.2.0 or higher to properly remove the ".tmp_cfdp" file name extension. The default value is true.

6.1.3 Options Tab

The Options tab is shown in Figure 5. The Options tab items are applicable regardless of the CFDP mode selected. Each field is described below.

Figure 5 Configure Dialog (Options Tab)

Default Remote EID

The Default Remote EID is used during Drag and Drop. If this field contains a value, this value will be entered as the Remote EID when you drag and drop a file into the “CFDP Commands” list or the “CFDP Command” field.

Default Destination Paths

The Default Destination is used during Drag and Drop. All destinations listed in the Default Destination Paths list will appear in the “Default Destination” menu on the CFDP main window. When you drag and drop a file into the “CFDP Commands” list or the “CFDP Command” field, the destination selected from the Default Destination menu will automatically be entered into the Destination field.

CFDP Dropbox List

The CFDP Dropbox List is used to define one or more CFDP dropboxes to push files to a remote destination.

Dropbox configuration parameters include where the dropbox is located and the destination of each file placed in the dropbox. When the CFDP service is active, a dropbox file is transferred to the dropbox destination immediately after the file is copied to the dropbox. If files exist in the dropbox prior to CFDP service activation, the pre-existing dropbox files are immediately transferred when the CFDP service is activated.

For each CFDP dropbox, you can define the Transmission, the Dropbox path, the Remote entity ID, the Destination Path, the Retry Limit, and the Successful Transaction Path. If the Dropbox path or the Destination Path are part of a dropbox chain, the cell text will be green. The Retry Limit defines the number of additional attempts at transferring a file before declaring the transaction unsuccessful. The successful transaction path is the path to a directory on the dropbox source platform where successfully transferred files are stored upon completion of a transaction. If the successful transaction path is empty, the dropbox will delete the file on the source platform if the file is successfully transferred to its destination. For CFDP class 1 service, files are simply moved or deleted from the dropbox directory when the transaction has completed the number of retry attempts.

The dropbox for ION CFDP is identical to Native CFDP except "class1" or "class2" is replaced by “////” indicating the ION CFDP parameter values defined on the ION CFDP configuration tab will be used. Another important distinction between an ION and Native CFDP dropbox is associated with the Retry Limit. An ION CFDP dropbox ignores the Retry Limit value and resets the value to zero in the TReK CFDP library. There are two important reasons why the ION CFDP dropbox does not attempt to retransmit failed CFDP transactions:

1. ION CFDP uses the original filename when populating the destination file. Any attempt to retransmit a file must also include a "delete" filestore directive to ensure no file with the original filename exists at the destination.

2. If transaction result messages are being processed and an incorrect "transaction_result_message_timeout" is chosen, a successfully transferred file will be incorrectly deleted.

Dropbox files are renamed with a ".dropbox" extension while they are being processed by the dropbox. If a dropbox fails to successfully transfer a file to the destination directory, a class 2 CFDP dropbox will initiate additional transfer attempts up to the "Retry Limit" designated by the dropbox configuration. A class 1 CFDP dropbox will blindly repeat the file transfer up to the "Retry Limit". If the final status message of a file transaction identifies an unsuccessful file transfer, the file is renamed with an ".unsuccessful" extension. If the CFDP library fails to receive the final status of a file transaction, the file is renamed with an ".unknown" extension. If an error occurred during the file transfer, the file is renamed with a ".droperror" extension. Only successfully transferred files are moved or deleted from the dropbox directory.

Fragmentation Dropbox List

The Fragmentation Dropbox List is used to define one or more Fragmentation dropboxes. There are three types of Fragmentation dropboxes: frag dropbox, frag_cfdp dropbox, and a defrag dropbox. A frag dropbox is used to fragment a file. A frag_cfdp dropbox is used to fragment a file that will be transferred using CFDP, and a defrag dropbox is used to reassemble a file from file fragments. A Fragmentation Dropbox is often used in conjunction with a CFDP Dropbox in order to split apart a very large file, transfer the individual file pieces using CFDP, and then reassemble the file from the individual file pieces.

Dropbox configuration parameters include the type of fragmentation dropbox, where the dropbox is located, the destination directory, the size of the file fragments, and the successful transaction directory. If the Dropbox path or the Destination Path are part of a dropbox chain, the cell text will be green.

When the CFDP service is activated, any pre-existing dropbox files are immediately fragmented. If the local destination directory of a frag dropbox is a CFDP dropbox, the file fragment will automatically be transferred to the CFDP dropbox's remote destination directory. If the CFDP dropbox's remote destination directory is a defrag dropbox, the fragmented file will automatically be put back together and moved to the defrag dropbox's destination directory when all the file fragments have been received by the defrag dropbox. By chaining together frag and defrag dropboxes with a CFDP dropbox, a completely automated file fragmentation, CFDP file transfer, and file defragmentation chain may be created and set in motion by placing a file in the local frag dropbox. In addition, encrypt and decrypt dropboxes may be chained to the frag and defrag dropboxes producing an automated sequence of file encryption, file fragmentation, CFDP file transfer, file defragmentation and file decryption. The fragmentation dropbox comes in two flavors: "frag" or "frag_cfdp". A "frag" dropbox creates a series of file fragments and immediately places the fragments in the dropbox's destination directory which may or may not be a CFDP dropbox directory. If the "frag" dropbox destination directory is a

CFDP dropbox, the file fragments are downlinked simultaneously in a series of independent CFDP transactions. A "frag_cfdp" dropbox creates a series of fragments, but only after the successful CFDP transfer of the previous file fragment to the remote destination of CFDP dropbox. In other words, a "frag_cfdp" dropbox's destination directory must be a CFDP dropbox directory and the "frag_cfdp" dropbox will only create the next file fragment after the previous file fragment has been successfully transferred by the CFDP dropbox. For this reason, a "frag_cfdp" dropbox's destination directory must be CFDP dropbox directory. If multiple files are added to a "frag_cfdp" dropbox simultaneously, the "frag_cfdp" dropbox will process the files one at a time, fragmenting and transferring all the fragments from one file prior to fragmenting and transferring all the fragments from the next file in the "frag_cfdp" dropbox. A "frag_cfdp" dropbox will require more time to transfer a very large file but has the advantage of an orderly and immediate cancellation of file fragmentation if there are problems transferring a file fragment using CFDP.

The frag or frag_cfdp dropbox breaks up a file into fragments sized to match the desired file fragmentation size in bytes and creates a new file fragment name by adding the current file fragment count and total fragment count to the fragmented file's dropbox extension. The defrag dropbox parses the file fragment name to identify the file's current and total fragment count prior to reconstructing the original file. The frag and defrag dropboxes also include a destination path to the local directory where the file fragments or reconstructed files are stored. If the successful path is defined, the dropbox will move the original file or file fragments placed in the dropbox to the successful directory if and only if new file fragments or reconstructed files are successfully created and stored in the dropbox's destination directory. If the successful path is empty, the dropbox will delete the original file or file fragments placed in the dropbox if and only if new file fragments or reconstructed files are successfully created and stored in the dropbox's destination directory. If the frag or defrag dropbox fails to fragment or reconstruct the file, the file will be renamed with a time tagged ".droperror" extension and remain in the dropbox. The frag or defrag dropbox will not attempt to fragment or defragment/reconstruct a file with a ".droperror" extension in its filename.

Log Metrics

The CFDP application provides the capability to write metrics to a file. If you check Log Metrics, metrics will be written to the log file specified. Metrics Logging will start when CFDP is activated and stop if you uncheck the box or CFDP is deactivated. See Section 6.4 for details on what metrics are logged.

Log File Path

The Log File Path should contain the absolute path to the directory where the log file should be written.

Log File Name

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

6.1.4 Cryptography Tab

The Cryptography tab is shown in Figure 6. Each field is described below.

Figure 6 Configure Dialog (Cryptography Tab)

Cryptography Checkbox

The Cryptography checkbox is used to identify that Cryptography services are in use.

Public Key Pathname

The Public Key Pathname field is used to enter the absolute path to a public key. The Browse button can be used to browse the local disk for the file.

Private Key Pathname

The Private Key Pathname field is used to enter the absolute path to a private key. The Browse button can be used to browse the local disk for the file.

Use Passphrase

The Use Passphrase checkbox is used to specify that the private key requires a passphrase to unwrap/decrypt the private key in the private key file. 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.

Show Text

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

Cipher Class

The Cipher class identifies what cipher class should be used when performing the cryptography functions.

Packet Encryption and Time Authentication

The Packet Encryption and Time Authentication area provides the capability to identify that cryptography services (encryption and decryption) should be used when communicating with a specific remote entity. All CFDP packets will be encrypted before being sent and decrypted upon reaching the destination when this feature is enabled. This capability can only be used with Native CFDP. Please note that if you turn this feature on for a remote entity, and you also define an encryption dropbox that will communicate with the remote entity, this will result in double encryption. The list will contain all remote entities that were entered into the Remote Entities list on the General tab. If you do nothing, all CFDP communication with the remote entities listed will be unencrypted. If you would like to use cryptography services when communicating with the remote entity, you should provide a peer public key for the remote entity. The public key from another computer is a peer public key. TReK will use peer public key terminology when referring to another computer's public key. To encrypt the packets for a specific remote entity, you assign a peer public key for that remote entity. Doing this will identify that you wish to use cryptography services when communicating with that remote entity. In addition to encrypting the stream, you can also choose to use the time authentication

feature to provide protection against inadvertent or malicious replay of the packets. The time authentication feature uses an encrypted timestamp, sequence count, and time to live value to provide replay resistance time authentication. The time authentication software compares the packet's decrypted time stamp with the operating system time (plus or minus the decrypted TTL) to determine if the packet's decrypted time falls within the authentication time window. In addition, the time authentication software does not allow a packet to be processed if the decrypted time and sequence count stay the same or decreases when compared to the previous decrypted packet time and sequence count. These features can be configured for each Remote Entity by selecting the Remote Entity in the list and pushing the Configure button. The Configure Packet Encryption and Time Authentication dialog shown in Figure 7 will be displayed.

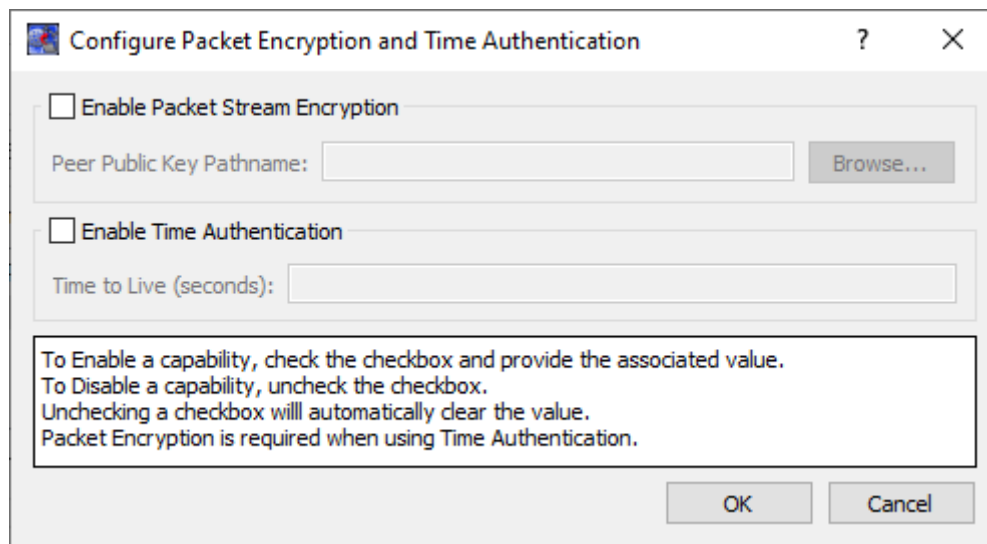


Figure 7 Configure Packet Encryption and Time Authentication Dialog

Enable Packet Stream Encryption

To enable packet stream encryption, check the checkbox and provide a Peer Public Key Pathname value. To disable packet stream encryption uncheck the checkbox. When the checkbox is unchecked the Peer Public Key Pathname field will be cleared.

Peer Public Key Pathname

A Peer Public Key must be identified if Packet Stream Encryption is enabled. You can use the browse button to select the Peer Public Key file or enter the complete path for the peer public key file.

Enable Time Authentication

To enable time authentication, check the checkbox and provide a Time to Live value. To disable time authentication, uncheck the checkbox. When the checkbox is unchecked, the Time to Live field will be cleared.

Time to Live

A Time to Live (TTL) must be defined if Time Authentication is enabled. The encrypted TTL value is in seconds and must be between 0-65535.

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 stream.

Cryptography Dropbox List

The Cryptography Dropbox List is used to define one or more Cryptography dropboxes. There are two types of Cryptography dropboxes: encrypt and decrypt. An encrypt dropbox is used to encrypt a file. A decrypt dropbox is used to decrypt a file.

Dropbox configuration parameters include the type of cryptography dropbox, where the dropbox is located, the destination directory, the absolute path to the peer public key, the crypt block size, and the successful directory. Each parameter is described below:

Cryptography

Cryptography values are encrypt and decrypt. This identifies whether the dropbox is encrypting or decrypting files.

Dropbox Path

The Dropbox Path identifies the local directory to be used for the encrypt or decrypt dropbox. If the Dropbox path is part of a dropbox chain, the cell text will be green.

Destination Path

The Destination Path identifies a local directory where the new encrypted or decrypted file is created and stored. If the Destination Path is part of a dropbox chain, the cell text will be green.

Peer Public Key Pathname

The Peer Public Key Pathname identifies the absolute path to the peer public key file. The peer public key is the public key of the destination platform.

Crypt Block Size

The Crypt Block Size is an unsigned 32 bit value identifying the number of bytes that are read and encrypted or decrypted with every file read. A large crypt block size improves encryption and decryption performance but may also tax a CPU.

Successful Path

If the Successful Path is defined, the dropbox will move the original file placed in the dropbox to the successful directory if and only if a new encrypted or decrypted file is successfully created and stored in the dropbox's destination directory. If the successful path is empty, the dropbox will delete the original file placed in the dropbox if and only if a new encrypted/decrypted file is successfully created and stored in the dropbox's

destination directory. If the encrypt or decrypt dropbox fails to encrypt or decrypt a file, the file will be renamed with a time tagged ".droperror" extension and remain in the dropbox. The encrypt or decrypt dropbox will not attempt to encrypt or decrypt a file with a ".droperror" extension in its filename.

An encrypt or decrypt dropbox file is encrypted or decrypted prior to being transferred to a local destination directory on the dropbox platform. Pre-existing dropbox files are immediately encrypted or decrypted as soon as the CFDP service is activated. If the local destination directory of an encrypt dropbox is a CFDP dropbox, the encrypted file will automatically be transferred to the CFDP dropbox's remote destination directory. If the CFDP dropbox's remote destination directory is a decrypt dropbox, the encrypted file will automatically be decrypted and placed in the decrypt dropbox's destination directory. By chaining together encrypt and decrypt dropboxes with a CFDP dropbox, a completely automated encrypt, CFDP file transfer, decrypt chain may be created and set in motion by placing a file in the local encrypt dropbox.

The encrypt, decrypt, and CFDP dropbox chain is currently the only method TReK provides to automate file encryption/decryption using ION CFDP.

Figure 8 shows an example of an encrypt dropbox definition. A file placed in the Dropbox Path (C:\encrypt_dropbox) will be encrypted using the peer public key identified and a 1,000,000 crypt block size. Since a Successful Path has been provided, the original file will be moved from the Dropbox Path directory to the Successful Path directory upon successful encryption.

Cryptography Dropbox List

Cryptography	Dropbox Path	Destination Path	Peer Public Key Pathname	Crypt Block Size	Successful Path	
encrypt	C:\encrypt_dropbox	C:\cfdp_dropbox	C:\peer_public_key	1000000	C:\encrypt_dropbox_success	Add Delete Set Dropbox Path... Set Peer Public key... Set Successful Path...

Figure 8 Encrypt Dropbox

Figure 9 and Figure 10 show how an encrypt dropbox and a CFDP dropbox can be used together to encrypt a file and then transfer it using CFDP. In Figure 9, the encrypt dropbox Destination Path points to the CFDP Dropbox Path. This “chains” the two dropboxes together. When a file is placed in the C:\encrypt_dropbox directory and successfully encrypted, it will be placed in the C:\cfdp_dropbox folder and transferred to the CFDP dropbox Destination Path.

Cryptography Dropbox List

Cryptography	Dropbox Path	Destination Path	Peer Public Key Pathname	Crypt Block Size	Successful Path	
encrypt	C:\encrypt_dropbox	C:\cfdp_dropbox	C:\peer_public_key	1000000	C:\encrypt_dropbox_success	

Add
Delete
Set Dropbox Path...
Set Peer Public key...
Set Successful Path...

Figure 9 Encrypt Dropbox

CFDP Dropbox List

Transmission	Dropbox Path	Remote EID	Destination Path	Retry Limit	Successful Path	
class2	C:\cfdp_dropbox	2	C:\downlinked_files	0	C:\cfdp_dropbox_success	

Add
Delete
Set Dropbox Path...
Set Successful Path...

Figure 10 CFDP Dropbox

Once the encrypted file reaches its destination, you can leave it encrypted or decrypt it using a decrypt dropbox as shown in Figure 11.

Cryptography Dropbox List

Cryptography	Dropbox Path	Destination Path	Peer Public Key Pathname	Crypt Block Size	Successful Path	
decrypt	C:\downlinked_files	C:\decrypted_files	C:\peer_public_key_kirk	1000000		

Add
Delete
Set Dropbox Path...
Set Peer Public key...
Set Successful Path...

Figure 11 Decrypt Dropbox

When the encrypted file arrives in the C:\downlinked_files directory on the remote computer, decryption will be applied and if successful, the decrypted file will be placed in the C:\decrypted files directory. There is no need to define a decrypt dropbox if you wish to leave the file encrypted when it reaches its destination. If a decrypt dropbox is not defined, the C:\downlinked_files directory would be the final destination for the encrypted file.

6.1.5 Summary Tab

The Summary tab is shown in Figure 12. This tab displays a summary of all the configuration parameters specified on the other tabs. If a Dropbox path or Destination Path is green, this means it is part of a dropbox chain.

Figure 12 Summary Tab

6.2 Transactions

This section describes the columns in the main window Transactions area.

Transaction ID

The transaction ID. A unique ID used to identify a transaction.

Action

The action (put, get, etc.) executed by the transaction.

Remote EID

The Entity ID of the other party involved in the transfer.

Status

The status of the transaction: Sending, Receiving, Finished, Success, Fail, Unknown, etc. The Status field updates as the transaction progresses.

The final status of a transaction using ION CFDP is “Finished” if the TReK CFDP application is not configured to receive a final transaction message from the remote site. If the TReK CFDP application is configured to receive a final transaction message, and the message does not arrive in the user defined timeout period, the final status is “Unknown”.

% Complete

The % complete of the file transfer. The % Complete field updates as the transaction progresses.

This field is not relevant for ION CFDP filestore directives and message directives.

Bytes Transferred

The number of bytes transferred. The Bytes Transferred field updates as the transaction progresses.

This field is not relevant for ION CFDP filestore directives and message directives.

Source

The source identified in the CFDP command.

Destination

The destination identified in the CFDP command.

This field is not relevant for ION CFDP message directives and some filestore directives.

Configuration

The configuration field indicates the direction of the file transfer: “Sending” or “Receiving”.

File Size

The File Size field displays the size of the file being transferred in bytes.

This field is not relevant for ION CFDP filestore directives and message directives.

6.2.1 Configure Transactions Area Dialog

The Configure Transactions Area dialog is shown in Figure 13. This dialog provides the capability to configure the columns shown in the Transactions area and the position where the most recent transaction is displayed in the list. Under Column Preferences, the Columns Showing list identifies the columns that will be displayed. The arrow buttons provide the capability to move items between the Available Columns list and the Columns Showing list. To hide a column, move it from the Columns Showing list to the Available Columns list. The Move Up and Move Down buttons provide the capability to specify the order of the columns showing. The item listed at the top of the list will appear in the left most location in the Transactions area. The Order Preferences area provides the capability to specify whether the most recent transaction is displayed at the bottom of the transaction list or the top of the transaction list. When you change this setting it will be applied to the next incoming transaction. The position of existing items will not be changed.

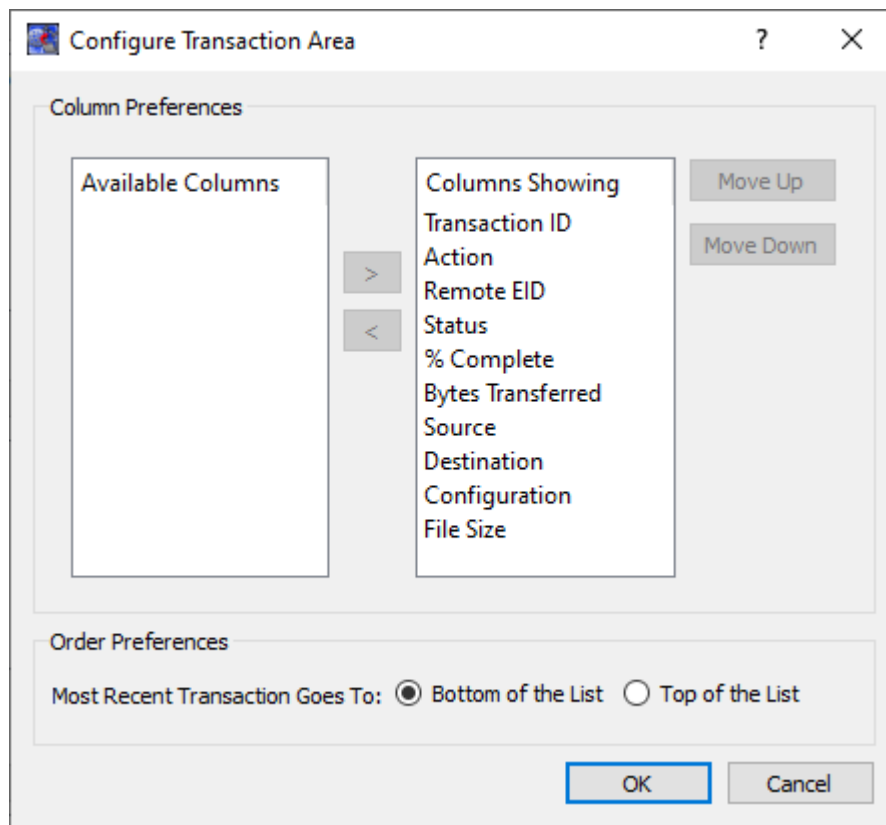


Figure 13 Configure Transactions Area Dialog

6.3 Statistics

This section describes the statistics that can be logged by the application to a user specified file. Statistics include device statistics and packet statistics. The snapshot of device and packet statistics is updated once a second with current statistics information at both the device and packet level. Device statistics provide information on all packets that are being received or sent by the device. Packet statistics provide information on the individual packet groups that are being received or sent by the device. The TReK CFDP library that performs this work for the application does not divide packets into groups, so packet statistics mirror device statistics.

When configured for ION CFDP, the TReK CFDP library relies upon the bundle protocol to assure delivery of file segments. So in ION CFDP mode, device and packet statistics are not relevant.

Device Statistics

Device Key

A character string that uniquely identifies each device.

IP Address

The IP address of the device if it is a socket.

Port (C/L/S)

The port number of the device if it is a socket. If the socket is a client socket, then the port number will be followed by two '/'. If the client socket is connected to a listener socket, the listener's port number is also listed. 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. If the socket is a listener socket, the listener's port number is listed between two '/'.

Protocol

The IP transportation protocol, either TCP or UDP, if the device is a socket.

Segments Rcvd

The number of segments received by the device if the device is a TCP socket.

Pkts Rcvd

The total number of packets received by the device.

Pkts Sent

The total number of packets sent by the device.

Pkt Rcv Rate

The number of packets received by the device in the last second.

Max Pkt Rcv Rate

The maximum packet receive rate experienced by the device.

Kbit Rcv Rate

The number of kilobits received by the device in the last second.

Max Kbit Rcv Rate

The maximum kilobit receive rate experienced by the device.

Pkt Send Rate

The number of packets sent by the device in the last second.

Max Pkt Send Rate

The maximum packet send rate experienced by the device.

Kbit Send Rate

The number of kilobits sent by the device in the last second.

Max Kbit Send Rate

The maximum kilobit send rate experienced by the device.

Pkts Dropped

The total number of packets that were dropped because they could not be temporarily stored in a queue or buffer. The most likely cause of dropped packets is packets arriving at very high packet rates and/or a queue size that is too small.

Packet Statistics

Packet Key

A character string that uniquely identifies each packet type.

Pkts Rcvd

The total number of packets that are received and identified as this packet type.

Pkts Sent

The total number of packets that are sent and identified as this packet type.

Pkt Rcv Rate

The number of packets received and identified as this packet type in the last second.

Max Pkt Rcv Rate

The maximum packet receive rate experienced by this packet type.

Kbit Rcv Rate

The number of kilobits received and identified as this packet type in the last second.

Max Kbit Rcv Rate

The maximum kilobit receive rate experienced by this packet type.

Pkt Send Rate

The number of packets of this packet type sent in the last second.

Max Pkt Send Rate

The maximum packet send rate experienced by this packet type.

Kbit Send Rate

The number of kilobits of this packet type sent in the last second.

Max Kbit Send Rate

The maximum kilobit send rate experienced by this packet type.

Pkts Dropped

The total number of packets of this type that were dropped because they could not be processed by another device. The most likely cause of dropped packets is packets arriving at very high packet rates.

Pkt Seq Errors

The total number of packet sequence errors identified for this packet type. For example, the primary header of the CCSDS packet contains a 14-bit number that is used as a sequence count. For each packet that arrives, the sequence count is compared to the sequence count of the previous packet. If the count is not the next in the sequence, the packet sequence error value is incremented.

Max Pkt Seq Error

The maximum packet sequence error experienced by this packet type.

6.4 Metrics

This section describes the CFDP metrics that can be logged by the application. The snapshot of CFDP metrics is updated once a second with the completion status of each CFDP transaction. The CFDP metrics are divided into sending and receiving categories and grouped by file size ranging from less than a one megabyte to over a gigabyte. The metrics include calculations on the number and percent of files sent or received, the minimum, maximum, and average file transfer time, and the number and percent of files that required packet retransmission.

The following Metrics are provided for Sending and Receiving.

File Size (MB)

The minimum and maximum file size in megabytes for the group.

Success Count

The number of successful file transfers for the group.

Success %

The percentage of successful file transfers for the group.

Cancel Count

The number of canceled file transfers for the group.

Abandon Count

The number of abandoned file transfers for the group.

Fail Count

The number of failed file transfers for the group.

Unknown Count

The number of unknown file transfers for the group.

Min Trans Time (sec)

The minimum successful file transfer time in seconds.

Max Trans Time (sec)

The maximum successful file transfer time in seconds.

Avg Trans Time (sec)

The average successful file transfer time in seconds.

Success W/NAK Cnt

The number of successful file transfers that required one or more NAK packets.

Success W/ NAK %

The percentage of successful file transfers that required one or more NAK packets.

Min NAK Cnt/Trans

The minimum number of NAK packets that had to be transferred for a successful file transfer requiring NAK packets.

Max NAK Cnt/Trans

The maximum number of NAK packets that had to be transferred for a successful file transfer requiring NAK packets.

Avg NAK Cnt/Trans

The average number of NAK packets that had to be transferred for a successful file transfer requiring NAK packets.

6.5 Configure Message Logging

This section describes how to configure message logging. The Configure Message Logging dialog is shown in Figure 14. This dialog can be displayed using the Options menu Configure Message Logging menu item.

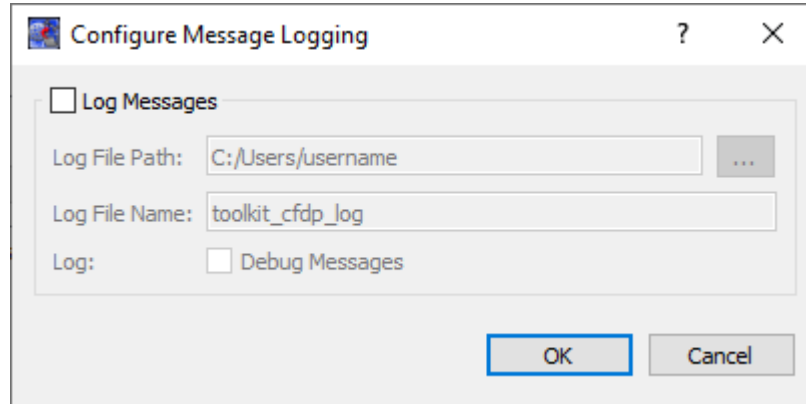


Figure 14 Configure Message Logging Dialog

Each field is described below.

Log Messages

The CFDP application provides the capability to write application messages to a file. If you check Log Messages, application messages will be written to the log file specified. Logging will start once it is turned on, so any messages generated before logging was turned on will not appear in the file.

Log File Path

The Log File Path should contain the absolute path to the directory where the log file should be written.

Log File Name

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

Log Debug Messages

The Log Debug Messages checkbox specifies whether debug messages should be written to the log. For example, if Debug is checked, Debug messages will be written to the log.

6.6 Configure Statistics Snapshot Recording

This section describes how to configure statistics snapshot recording. The Configure Statistics Snapshot Recording dialog is shown in Figure 15. This dialog can be displayed using the Options menu Configure Statistics Snapshot Recording menu item. 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. See Section 6.3 for details about the statistics that are logged. When the CFDP service is inactive, there are no application statistics. If you deactivate the CFDP service before turning off statistics snapshot recording, the statistics snapshot file will be empty.

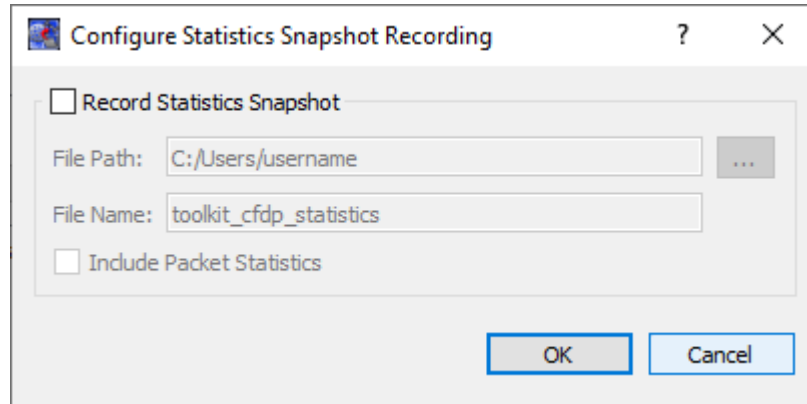


Figure 15 Configure Statistics Snapshot Recording Dialog

Each field is described below.

Record Statistics Snapshot

The CFDP 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.

6.7 Manage E-Mail and Text Settings Dialog

The Manage E-Mail and Text Settings Dialog is shown in Figure 16. 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.

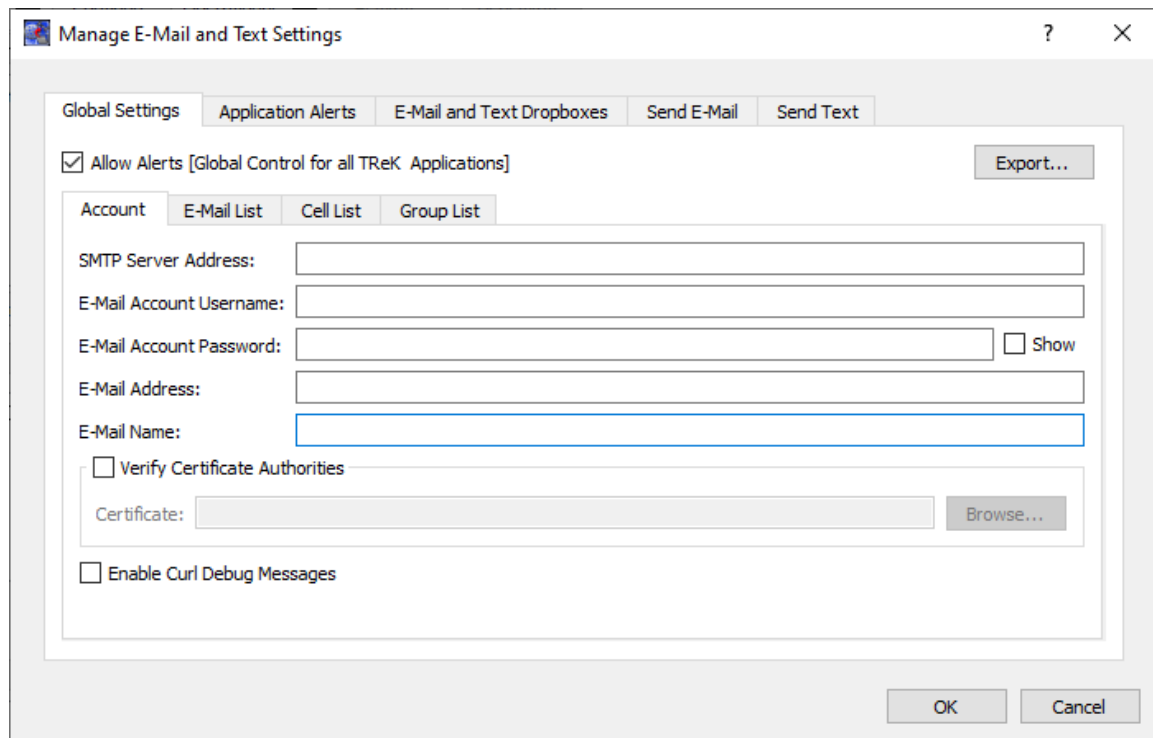


Figure 16 Manage E-Mail and Text Settings Dialog (Global Settings Account Tab)

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 17. 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.

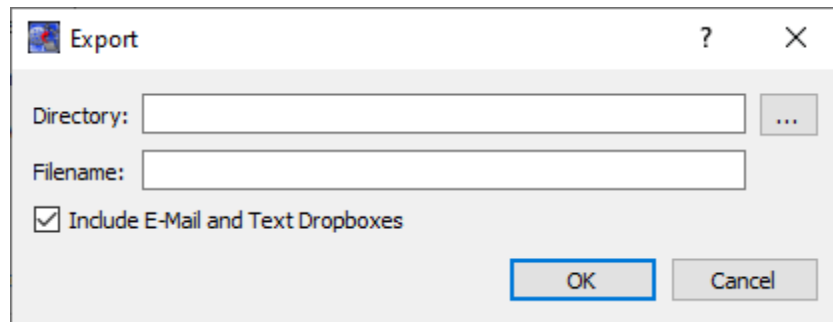


Figure 17 Manage E-Mail and Text Settings (Export Dialog)

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 to 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 18. The Add button is used to add a row to enter e-mail address information. The Delete button is used to delete a row.

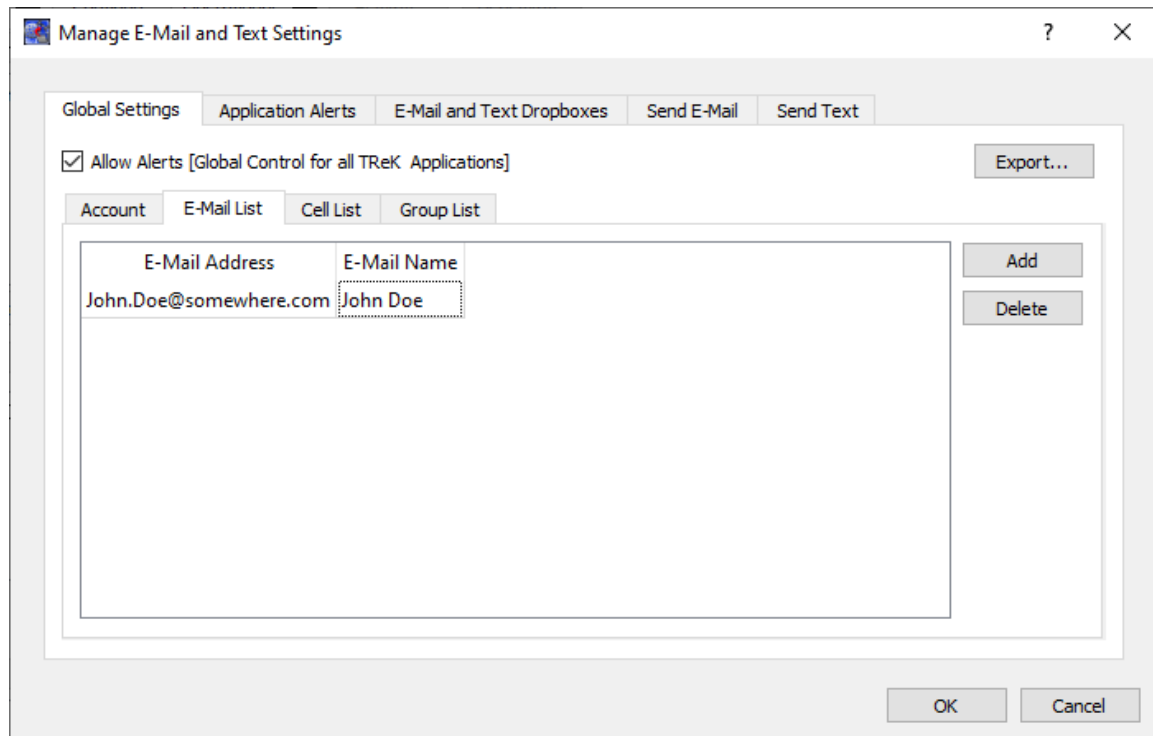


Figure 18 Manage E-Mail and Text Settings Dialog (Global Settings E-Mail List Tab)

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 19. 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 20 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.

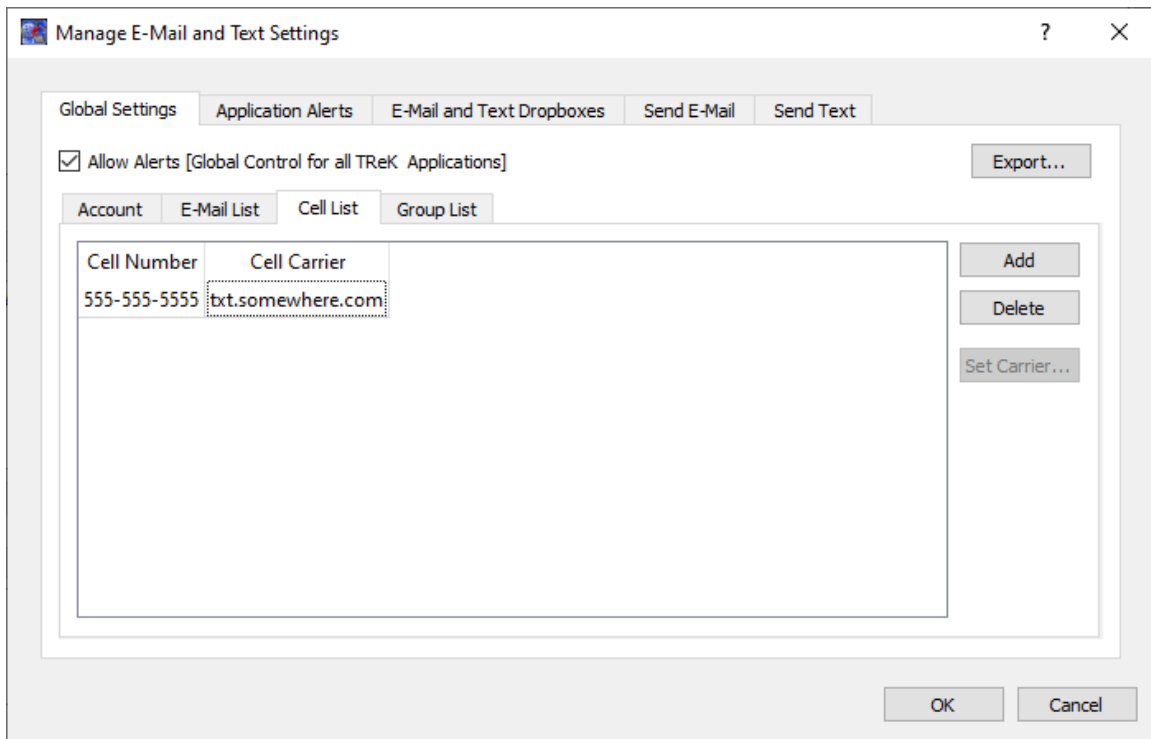


Figure 19 Manage E-Mail and Text Settings Dialog (Global Settings Cell List Tab)

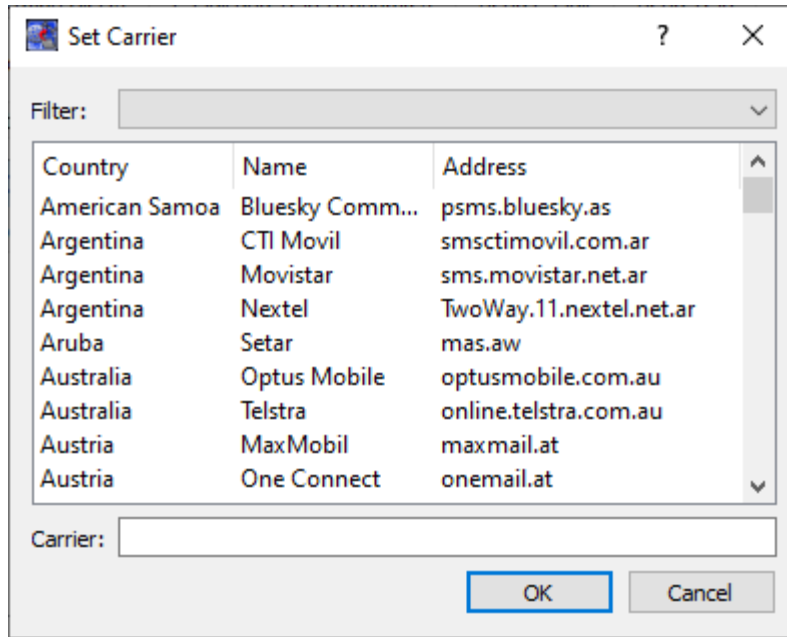


Figure 20 Manage E-Mail and Text Settings (Set Carrier Dialog)

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 21. 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.

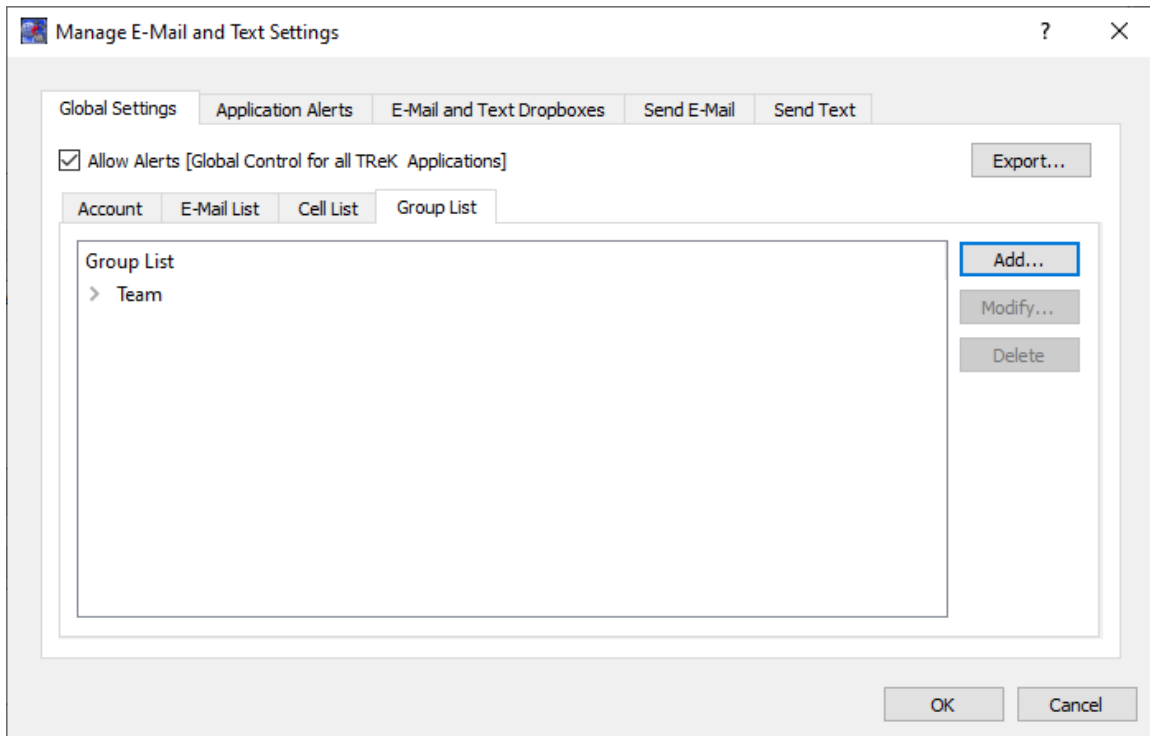


Figure 21 Manage E-Mail and Text Settings Dialog (Global Settings Group List Tab)

The Add button will display the Add Group dialog shown in Figure 22. 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.

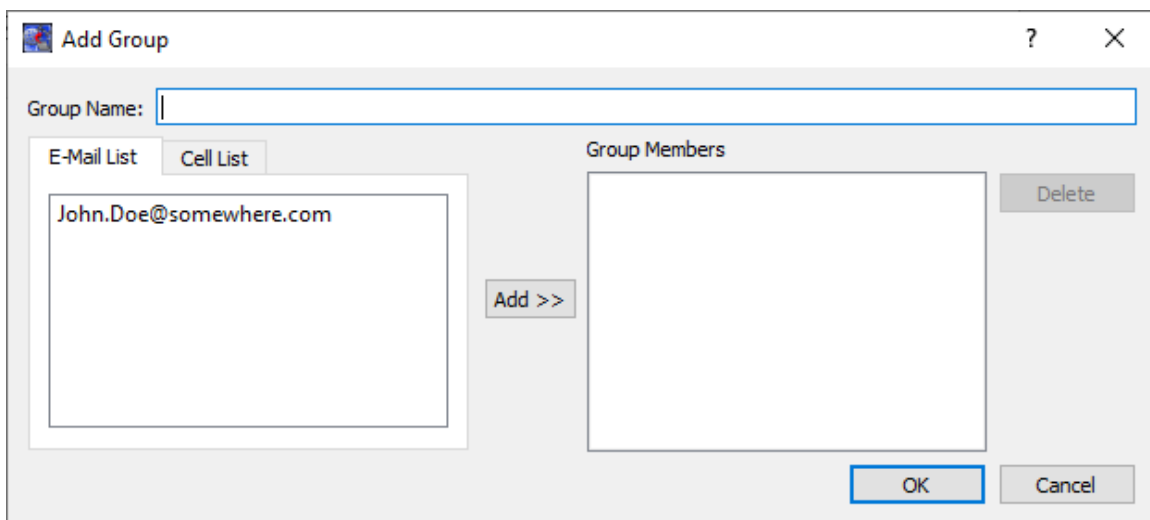


Figure 22 Manage E-Mail and Text Settings (Add Group Dialog)

Application Alerts

The Application Alerts tab is shown in Figure 23. It is used to configure application specific alerts.

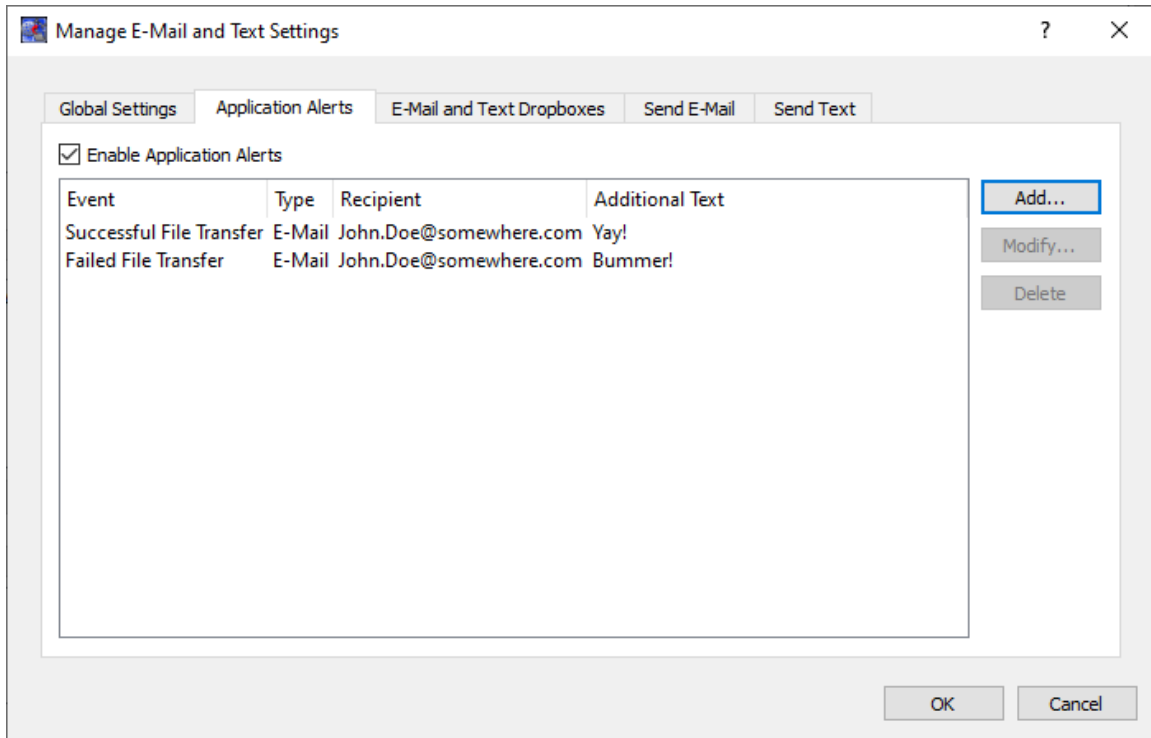


Figure 23 Manage E-Mail and Text Settings Dialog (Application Alerts Tab)

Enable Application Alerts

The Enable Application Alerts Checkbox is used to turn all alerts on or off in the current application. If you uncheck Enable Application Alerts, no alerts will be generated in the CFDP application.

Event List

The Event area provides the capability to identify one or more alerts to send when a specific application event occurs. You can add, modify, and delete alerts using the buttons on the right. The Add button will display the Add Alert dialog shown in Figure 24.

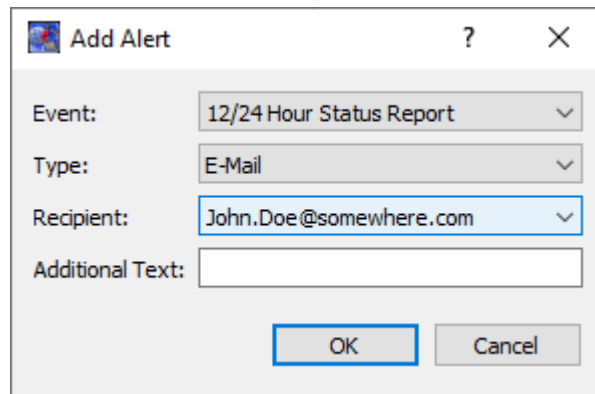


Figure 24 Manage E-Mail and Text Settings (Add Alert Dialog)

Event

The Event is what triggers the alert. There may be one or more events in an application that can trigger an alert. The CFDP application can generate an alert for the following types of events:

Successful File Transfer

This event is triggered when a file is successfully transferred.

Failed File Transfer

This event is triggered when a file transfer fails.

12/24 and 24 Hour Status Reports

There are two status report events that can be triggered: a 12/24 hour status report and a 24 hour status report. The status report events deliver the CFDP status report by sending a text and/or email to a list of designated recipients. The CFDP status report text alert identifies the number of file transfers that were a success, were a failure, were cancelled, were abandoned or were unknown over a twelve and twenty four hour period. The CFDP status report text alert also includes information on the number of TReK error messages that were generated and the number of Native CFDP AOS windows exceeding sixty seconds (assuming TReK Native CFDP is configured to automatically suspend and resume CFDP transactions) that were encountered over the twelve and twenty four hour period. The CFDP status report email alert includes all the information found in the CFDP status report text alert, but also provides an email file attachment detailing each individual file transaction, error message and Native CFDP AOS window. The twelve hour CFDP status report is sent as a text and/or email at 6:00 p.m. local time and the twenty four hour CFDP status report is sent as a text and/or email at 6:00 a.m. local time. After the twenty four CFDP status report alert is sent, all transaction counts, error counts and Native CFDP AOS window counts are reset to zero. The CFDP status report email file attachment includes the last fifty TReK error messages for the twelve and twenty four hour periods. It also includes the details about the Native CFDP AOS windows that exceed sixty seconds in duration for the twelve and twenty four hour periods.

The following is an example of a TReK CFDP status report and includes the messages only found in the CFDP status report email file attachment:

GMT 2020-11-12 11:00:00 to 2020-11-12 23:00:00

CFDP EID 1 status report duration 12:00:00

Status Report

- 2 Successful transactions
- 0 Failed transactions
- 2 Cancelled transactions
- 0 Abandoned transactions
- 0 Unknown transactions
- 2 CFDP AOS windows
- 3 TReK error messages

Success Messages: 2

1. GMT 2020-11-12 13:54:24:575 Transaction 2_1 (/home/name/xfer0030 -> D:/xfer0030) decrypted: successful. File size 300000 bytes.
2. GMT 2020-11-12 13:55:18:581 Transaction 1_2 (D:/1000_scp/xfer0040 -> /home/name/xfer0040a) encrypted: successful. File size 400000 bytes.

Cancel Messages: 2

1. GMT 2020-11-12 13:54:41:576 Transaction 2_2 (/home/name/xfer0030 -> D:/xfer0030) decrypted: cancelled (Filestore rejection). File size 300000 bytes.
2. GMT 2020-11-12 13:54:59:599 Transaction 1_1 (D:/1000_scp/xfer0040 -> /home/name/xfer0040) encrypted: cancelled (Filestore rejection). File size 400000 bytes.

CFDP AOS Windows (greater than 60 seconds): 2

1. GMT 2020-11-12 13:54:18 to 2020-11-12 13:55:30 CFDP AOS window duration of 0:01:12
2. GMT 2020-11-12 13:55:36 Current CFDP AOS window duration of 9:04:24

TReK Error Messages: 3

1. GMT 2020-11-12 13:54:41:522 cfdp_engine: unable to rename 'D:/tmp_cfdp0002488' to 'D:/xfer0030'. (cfdp_transceiver.cpp:319)
2. GMT 2020-11-12 13:54:41:522 cfdp_engine: are they on separate filesystems? (cfdp_transceiver.cpp:319)
3. GMT 2020-11-12 13:54:41:523 :::Fault trans 2_2, fault='Filestore rejection'. (cfdp_transceiver.cpp:319)

Type

The type of alert to send. Options are E-Mail, E-Mail and Text, or Text.

Recipient

The recipient identifies who should be notified when the event is triggered. The Recipient list will be populated with applicable recipients based on Type. 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.

Additional Text

The alert will contain the name of the event that occurred and any text that is provided in the Additional Text field. Additional Text is optional.

E-Mail and Text Dropboxes

The E-Mail and Text Dropboxes tab is shown in Figure 25. 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.

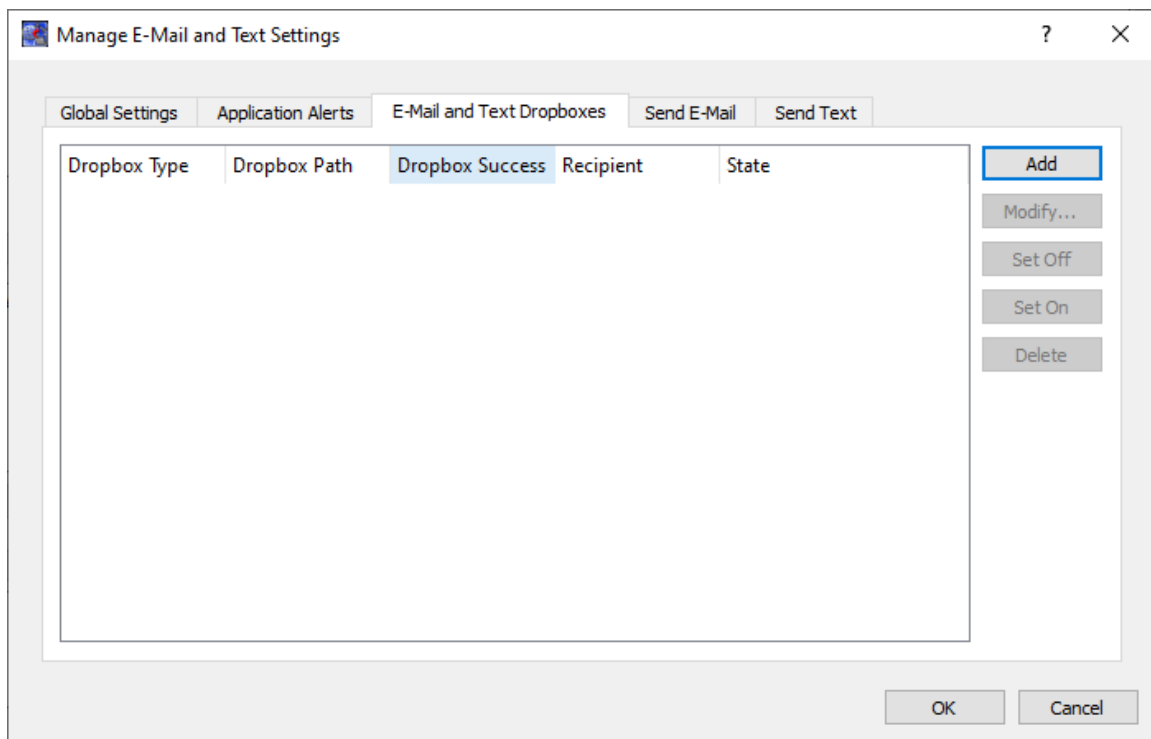
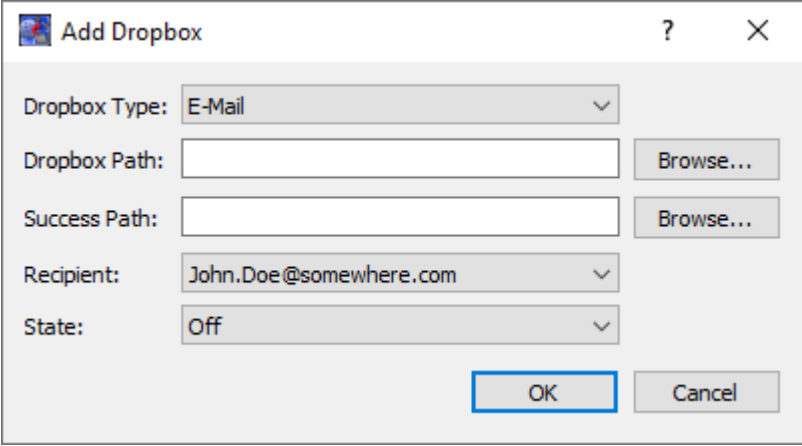


Figure 25 Manage E-Mail and Text Settings Dialog (E-Mail and Text Dropboxes Tab)

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 26.



The image shows a dialog box titled "Add Dropbox" with a standard Windows-style title bar (minimize, maximize, close buttons). The dialog contains the following fields and controls:

- Dropbox Type:** A dropdown menu currently set to "E-Mail".
- Dropbox Path:** A text input field with a "Browse..." button to its right.
- Success Path:** A text input field with a "Browse..." button to its right.
- Recipient:** A dropdown menu currently set to "John.Doe@somewhere.com".
- State:** A dropdown menu currently set to "Off".
- Buttons:** "OK" and "Cancel" buttons at the bottom right. The "OK" button is highlighted with a blue border.

Figure 26 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 27. 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.

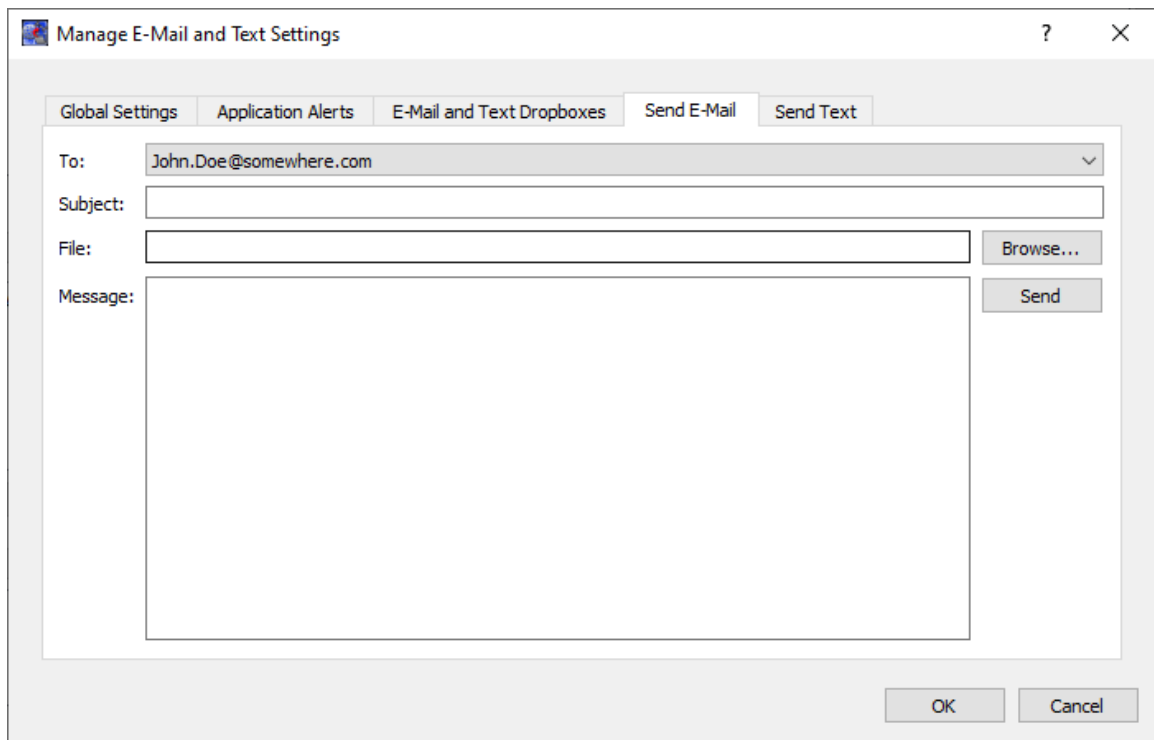


Figure 27 Manage E-Mail and Text Settings Dialog (Send E-Mail Tab)

Send Text

The Send Text tab is shown in Figure 28. 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.

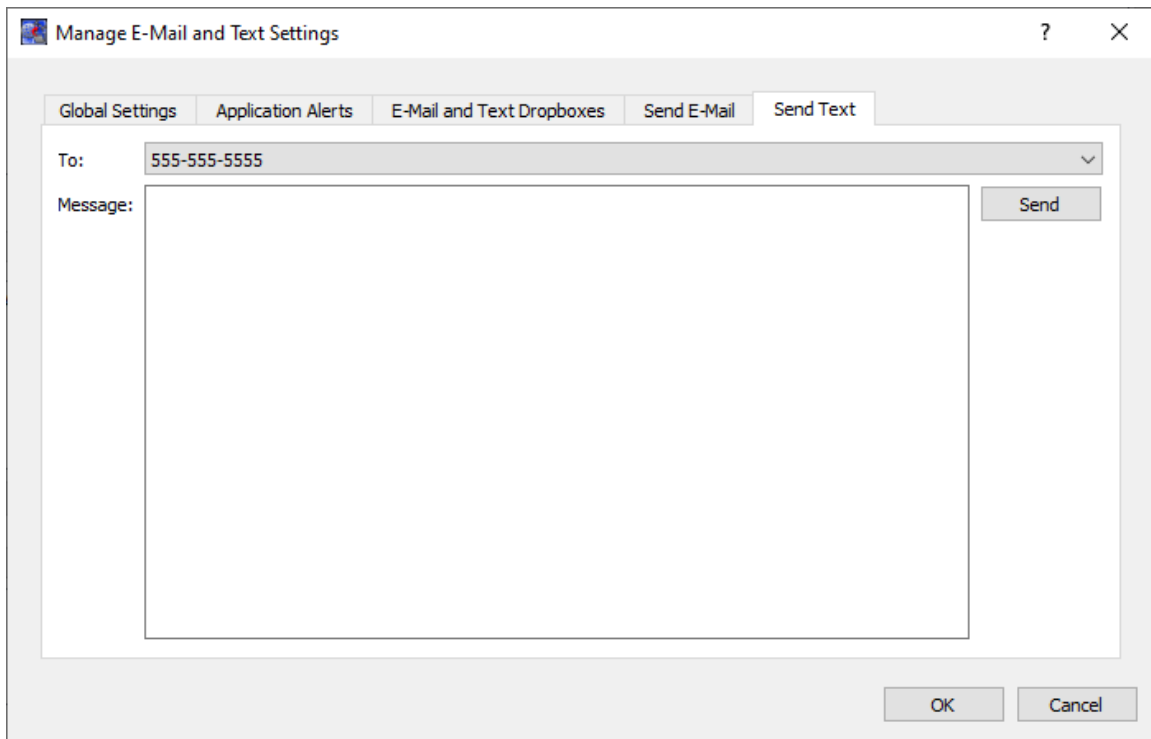


Figure 28 Manage E-Mail and Text Settings Dialog (Send Text Tab)

6.8 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 is 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 29. 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.

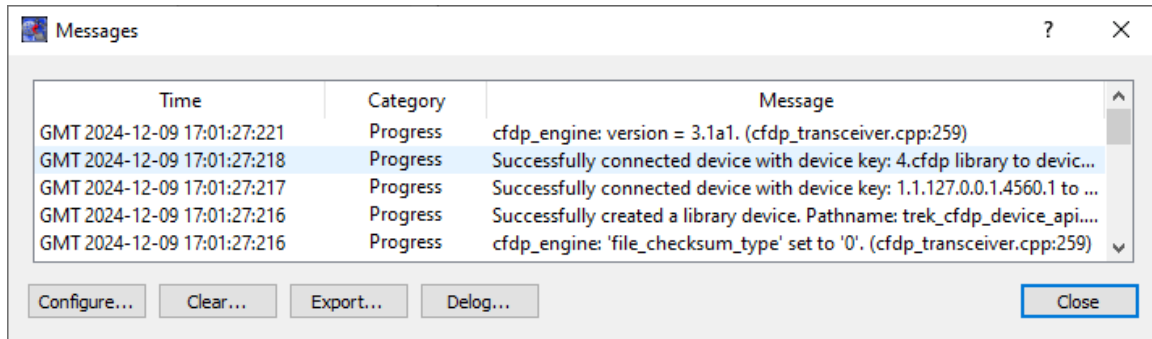


Figure 29 Messages Dialog

Configure

The Configure button provides access to the Configure Messages dialog shown in Figure 30. 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.

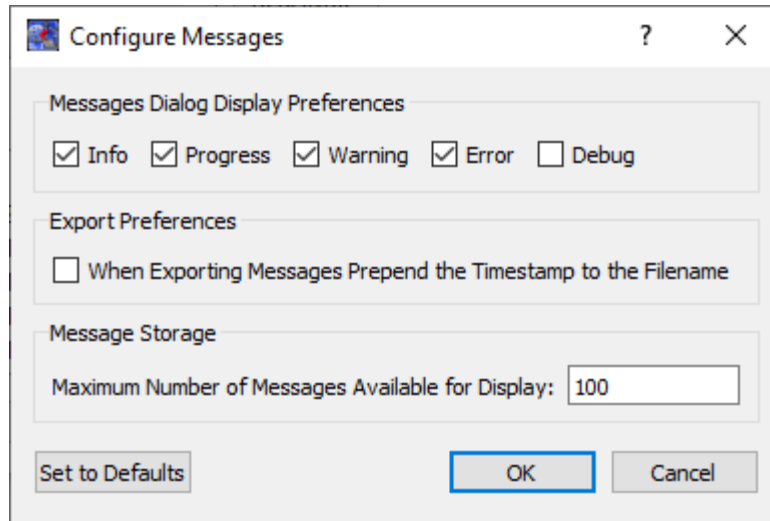


Figure 30 Configure Messages Dialog

Clear

The Clear button provides access to the Clear Messages dialog shown in Figure 31. 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).

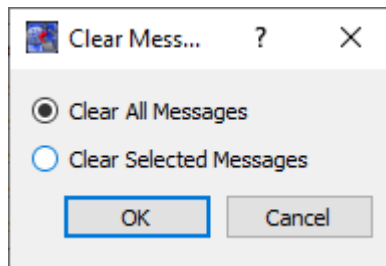


Figure 31 Clear Messages Dialog

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

6.9 Application Configuration File

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

- Configuration information in the Configure Dialog.
- CFDP Commands list displayed in the Main Window CFDP Commands area.
- CFDP Command displayed in the Main Window File Transfer Command Line.
- Default Destination menu selection in the CFDP Commands area.
- Default Destination menu selection in the File Transfer Command Line area.
- Log Messages Configuration
- Record Statistics Snapshot Configuration
- Configure Messages Display Preferences

The configuration of the Transactions area (columns showing/column order) is not saved.

6.10 Application Settings

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

- Application Window Size
- CFDP Transaction List configuration.
- Configure Messages Export Preferences
- Configure Messages Message Storage
- E-Mail and Text Settings

6.11 Application Command Line Arguments

The CFDP application accepts the following command line arguments:

➤ `trek_cfdp.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_cfdp.exe "D:/cfdp config.txt"`

➤ `trek_cfdp.exe D:/cfdp_config.txt topsecret`

If the configuration is valid, the application will automatically activate the CFDP service.

7 FAQ and Troubleshooting

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

7.1 Is There an Easy Way to Transfer the Contents of a Directory?

Yes. To transfer the contents of a directory, enter the absolute path to the directory. The CFDP application will transfer all the files in the first level of the directory. Subdirectories will not be transferred. Be sure to include a forward slash '/' at the end of the directory path when entering the absolute path into the Source and Destination fields.

7.2 What is class1 and class2?

Class1 and class2 are transmission properties used with Native CFDP. Note: Special thanks to NASA/GSFC for the following user friendly definitions:

“CFDP provides three **Service Classes**. Service **Class 1** simply sends each file; there are no replies from the receiver, nor is there any guarantee of reliable delivery. Service **Class 2** ensures reliable file delivery; any required retransmissions are requested and performed by CFDP. Service **Class 3** provides **Proxy Operations** (e.g. Entity ‘A’ tells Entity ‘B’ to make a request of Entity ‘C’).”

The TReK CFDP application supports Class 1 and Class 2 when configured for Native CFDP. When typing in one of these choices please use **class1** and **class2**.

7.3 What is “////”?

“////” is a value used to designate the default set of transmission properties defined in the Configure dialog for ION CFDP. “/” can also be used. When configured for ION CFDP, transmission properties are specified using the Configure dialog and will apply to all CFDP transactions. For more information about transmission properties please reference section 6.1.2.

7.4 Source and Destination Constraints

Source and Destinations must be identified using an absolute path. The absolute path name consists of the full path and the file name. The absolute path must meet the following criteria:

- The ION CFDP library works with a source absolute path limited to 255 bytes and a destination absolute path limited to 246 bytes.
- The Native CFDP library works with primitive strings. The “put” primitive string format is as follows:

put –class2 “source absolute path” eid “destination absolute path”

All Native CFDP library primitives are limited to 255 bytes.

The file size must meet the following criteria:

- The size of the file to be transferred must be greater than 0 Bytes.
- The size of the file to be transferred cannot exceed 4.2 Giga Bytes for Native CFDP.
- The size of the file to be transferred cannot exceed 2.1 Giga Bytes for ION CFDP when transferring from a device hosting the Windows Operating System (OS) to a device hosting the Windows OS.
- The size of the file to be transferred cannot exceed 2.1 Giga Bytes for ION CFDP when transferring from a device hosting the Windows OS to a device hosting the Linux OS.

Consider using the fragmentation and defragmentation dropboxes when transferring files that exceed CFDP’s file size limitations.

7.5 I Dropped My File into the List and it Turned Red

Red indicates the file or directory contains an illegal character. File and directory names must meet the File and Directory Name Constraints described in section 7.4.

7.6 My File Starts to Transfer and Then Stops

Chances are the remote entity is unavailable or is not configured as you expected. Check both the Local and Remote entity configurations and ensure the EIDs are correct, the IP address and port information is correct, and both entities are up and running.

7.7 Transfer Results When Item Exists At Destination

Transfer results when an item exists at a destination differ based on configuration.

When configured for Native CFDP

If you attempt to “put” an item to a destination on a Windows computer, and the item already exists at the destination, you will see a “cancelled (Filestore rejection)” error message and the item will not be overwritten. If you attempt to “put” an item to a destination on a Linux computer, and the item already exists at the destination, the item will be overwritten.

When configured for ION CFDP

If you attempt to “put” an item to a destination on a Windows computer, and the item already exists at the destination, the “put” transaction status will show “Fail”. If you attempt to “put” an item to a destination on a Linux computer, and the item already exists at the destination, the “put” transaction status will show “Fail”.

7.8 Important Things To Know When Using The Get Primitive

The TReK CFDP software provides the capability to “get” or retrieve one or more files from a remote destination. It is important to note that the CFDP Blue Book describes implementation of a “get” as a proxy “put”. TReK Native CFDP implements the CFDP Blue Book defined proxy “put” function using proxy request and response messages.

TReK ION CFDP does not implement proxy “put” function using proxy request and response messages. In addition, the “get” directive is not supported in all ISS CFDP Native and ION implementations. Therefore, the “get” request will only succeed if both sides of the file delivery transaction are using TReK software. The TReK ION CFDP “get” function initiates the file transfer process by delivering an equivalent “put” primitive character string to the remote platform's CFDP software using a “get” request message. In addition, a “get” response message is generated providing transaction status information to the initiator. There is an error scenario in which the initiator of the ION CFDP “get” receives no feedback. If an ION CFDP “get” request message or “get” response message never reaches its target platform, the initiator will receive no status describing the result of the “get” request.

7.9 How Does Pause Transactions Work?

When configured for Native CFDP

CFDP pauses transactions by pausing both data transmission and timeout clocks associated with the local platform's file transfer transactions. The remote platform is not

notified of the pause of file transfer transactions on the local platform and may exceed its timeout limits if the local platform does not resume its file transfer transactions for an extended period of time. If the local file transfer pause is for an extended period of time, the remote platforms should receive a separate pause transaction command to avoid exceeding its timeout limits. Both platforms may resume file transfer transactions when they receive separate resume file transfer transaction commands.

When configured for ION CFDP

The ION CFDP application completes its file transfer responsibilities when it hands off to ION's BP application. The handoff may be relatively quick depending on the size of file. The pause transaction request will not pause/suspend a file transfer after the ION CFDP application hands off a transaction to ION's BP application. The pause transaction request does not affect ION CFDP file reception. The lifespan of the packet bundles must also be considered when pausing for an extended period of time.

7.10 CFDP Transactions in an AOS/LOS Environment

Maintaining CFDP transactions across extended LOS periods is problematic. A user must configure timeouts or manually suspend and resume CFDP at both ends of a transaction to maintain the transaction across an LOS period. The TReK CFDP library solves this native CFDP issue by providing an automatic suspend and resume capability during LOS and AOS periods. When the TReK CFDP library senses an LOS event, it automatically suspends all CFDP transactions. When the TReK CFDP library senses an AOS event, it automatically resumes all CFDP transactions. TReK identifies AOS and LOS events by sending and receiving a four-byte connectivity packet over a predefined UDP socket. TReK's automatic suspend and resume design maintains native CFDP transactions across multiple LOS periods without adjusting timeout values or requiring user intervention. If new CFDP transactions are requested during an LOS period, the pending transaction requests are placed in a queue and are submitted to the TReK CFDP library at the beginning of the next AOS period. The automatic suspend and resume parameters in the TReK CFDP configuration file configure and control TReK's automatic suspend and resume feature. For more information about automatic suspend and resume parameters please reference section 6.1.1.

ION CFDP solves this issue by relying on DTN's store and forward infrastructure. A contact plan that predicts AOS/LOS periods may be used to support ION CFDP transactions between a flight node and a ground node if the two nodes are communicating directly with each other. If the ION CFDP transaction communication path includes the Huntsville Operations Support Center DTN2 node, the DTN2 node will store and forward the ION CFDP transaction during AOS/LOS periods.